ExtraHop 9.6
ExtraHop Explore REST API Guide

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

Published: 2024-06-03

Contents

Introduction to the ExtraHop REST API

The ExtraHop REST API enables you to automate administration and configuration tasks on your ExtraHop system. You can send requests to the ExtraHop API through a Representational State Transfer (REST) interface, which is accessed through resource URIs and standard HTTP methods.

When a REST API request is sent over HTTPS to an ExtraHop system, that request is authenticated and then authorized through an API key. After authentication, the request is submitted to the ExtraHop system and the operation completes.

▶ Video: See the related training: Rest API Overview ↗

Each ExtraHop system provides access to the built-in ExtraHop REST API Explorer, which enables you to view all of the available system resources, methods, properties, and parameters. The REST API Explorer also enables you to send API calls directly to your ExtraHop system.

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

ExtraHop API requirements

Before you can begin writing scripts for the ExtraHop REST API or performing operations through the REST API Explorer, you must meet the following requirements:

- Your ExtraHop system must be configured to allow API key generation for the type of user you are (remote or local).
- You must generate a valid API key.
- You must have a user account on the ExtraHop system with appropriate privileges set for the type of tasks you want to perform.

Access and authenticate to the ExtraHop REST API

Setup users and users with system and access administration privileges control whether users can generate API keys. For example, you can prevent remote users from generating keys or you can disable API key generation entirely. When this functionality is enabled, API keys are generated by users and can be viewed only by the user who generated the key.

> **Note:** Administrators set up user accounts and assign privileges, but then users generate their own API keys. Users can delete API keys for their own account, and users with system and access administration privileges can delete API keys for any user. For more information, see Users and user groups ⤢.

After you generate an API key, you must append the key to your request headers. The following example shows a request that retrieves metadata about the firmware running on the ExtraHop system:

```
curl -i -X GET --header "Accept: application/json" \
--header "Authorization: ExtraHop apikey=2bc07e55971d4c9a88d0bb4d29ecbb29" \
"https://<hostname-or-IP-of-your-ExtraHop-system>/api/v1/extrahop"
```

Privilege levels

User privilege levels determine which ExtraHop system and administration tasks the user can perform through the ExtraHop REST API.

You can view the privilege levels for users through the `granted_roles` and `effective_roles` properties. The `granted_roles` property shows you which privilege levels are explicitly granted to the user. The `effective_roles` property shows you all privilege levels for a user, including those received outside of the granted role, such as through a user group.

The `granted_roles` and `effective_roles` properties are returned by the following operations:

- GET /users
- GET /users/{username}

The `granted_roles` and `effective_roles` properties support the following privilege levels. Note that the type of tasks for each ExtraHop system vary by the available resources listed in the REST API Explorer and depend on the modules enabled on the system and user module access privileges.

Privilege level	Actions allowed
"system": "full"	- Enable or disable API key generation for the ExtraHop system. - Generate an API key. - View the last four digits and description for any API key on the system. - Delete API keys for any user. - View and edit cross-origin resource sharing. - Perform any administration task available through the REST API. - Perform any ExtraHop system task available through the REST API.
"write": "full"	- Generate your own API key. - View or delete your own API key. - Change your own password, but you cannot perform any other administration tasks through the REST API.

Privilege level	Actions allowed
	• Perform any ExtraHop system task available through the REST API.
"write": "limited"	• Generate an API key. • View or delete their own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Perform metric and record queries.
"write": "personal"	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform all GET operations through the REST API. • Perform metric and record queries.
"metrics": "full"	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API. • Perform metric and record queries.
"metrics": "restricted"	• Generate an API key. • View or delete your own API key. • Change your own password, but you cannot perform any other administration tasks through the REST API.
"ndr": "full"	• View security detections • View and create investigations This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"
"ndr": "none"	• No access to NDR module content This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"

Privilege level	Actions allowed
"npm": "full"	- View performance detections - View and create dashboards - View and create alerts This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: "write": "full" "write": "limited" "write": "personal" "write": null "metrics": "full" "metrics": "restricted"
"npm": "none"	- No access to NPM module content This is a module access privilege that can be granted to a user in addition to one of the following system access privilege levels: "write": "full" "write": "limited" "write": "personal" "write": null "metrics": "full" "metrics": "restricted"
"packets": "full"	- View and download packets through the `GET /packets/search` and `POST /packets/search` operations. This is an add-on privilege that can be granted to a user with one of the following privilege levels: "write": "full" "write": "limited" "write": "personal" "write": null "metrics": "full" "metrics": "restricted"
"packets": "full_with_keys"	- View and download packets and session keys through the `GET /packets/search` and `POST /packets/search` operations. This is an add-on privilege that can be granted to a user with one of the following privilege levels: "write": "full" "write": "limited" "write": "personal" "write": null "metrics": "full" "metrics": "restricted"
"packets": "slices_only"	View and download the first 64 bytes of packets through the `GET /packets/search` and `POST /packets/search` operations.

Privilege level	Actions allowed
	This is an add-on privilege that can be granted to a user with one of the following privilege levels: • "write": "full" • "write": "limited" • "write": "personal" • "write": null • "metrics": "full" • "metrics": "restricted"

Manage API key access

Users with system and access administration privileges can configure whether users can generate API keys for the ExtraHop system. You can allow only local users to generate keys, or you can also disable API key generation entirely.

Users must generate an API key before they can perform operations through the ExtraHop REST API. Keys can be viewed only by the user who generated the key or system administrators with unlimited privileges. After a user generates an API key, they must append the key to their request headers.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Access Settings section, click **API Access**.
3. In the Manage API Access section, select one of the following options:

    • **Allow all users to generate an API key**: Local and remote users can generate API keys.
    • **Only local users can generate an API key**: Remote users cannot generate API keys.
    • **No users can generate an API key**: No API keys can be generated by any user.
4. Click **Save Settings**.

Generate an API key

You must generate an API key before you can perform operations through the ExtraHop REST API. Keys can be viewed only by the user who generated the key or by users with system and access administration privileges. After you generate an API key, add the key to your request headers or the ExtraHop REST API Explorer.

Before you begin
Make sure the ExtraHop system is configured to allow API key generation.

1. In the Access Settings section, click **API Access**.
2. In the Generate an API Key section, type a description for the new key, and then click **Generate**.
3. Scroll down to the API Keys section, and copy the API key that matches your description.

You can paste the key into the REST API Explorer or append the key to a request header.

Configure cross-origin resource sharing (CORS)

Cross-origin resource sharing (CORS) allows you to access the ExtraHop REST API across domain-boundaries and from specified web pages without requiring the request to travel through a proxy server.

You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin. Only users with system and access administration privileges can view and edit CORS settings.

1. In the **Access Settings** section, click **API Access**.
2. In the CORS Settings section, specify one of the following access configurations.
   - To add a specific URL, type an origin URL in the text box, and then click the plus (+) icon or press ENTER.

     The URL must include a scheme, such as `HTTP` or `HTTPS`, and the exact domain name. You cannot append a path; however, you can provide a port number.
   - To allow access from any URL, select the Allow API requests from any Origin checkbox.

     Note: Allowing REST API access from any origin is less secure than providing a list of explicit origins.
3. Click **Save Settings** and then click **Done**.

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://<extrahop-hostname-or-ip-address>/api/v1/explore/
```

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. From the Access Setting section, click **API Access**.
3. On the API Access page, click **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

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
},
```

ExtraHop API resources

You can perform operations on the following resources through the ExtraHop REST API. You also can view more detailed information about these resources, such as available HTTP methods, query parameters, and object properties in the REST API Explorer.

APIKey

An API key enables a user to perform operations through the ExtraHop REST API.

You can generate the initial API key for the setup user account through the REST API. All other API keys are generated through the API Access page in the Administration settings.

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

Operation	Description
GET /apikeys	Retrieve all API keys.
POST /apikeys	Create the initial API key for the setup user account.
GET /apikeys/{keyid}	Retrieve information about a specific API key.

Appliance

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

You can retrieve information and establish connections for local and remote ExtraHop appliances.

> **Note:** You can only establish a connection between similar ExtraHop appliances, such as Reveal(x) Enterprise or Performance.

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.
POST /appliances	Establish a new connection to a remote ExtraHop appliance.
DELETE /appliances/{id}	Disconnect a specific ExtraHop appliance from this console.
GET /appliances/{id}	Retrieve a specific remote ExtraHop appliance connected to the local appliance (only valid on consoles).
GET /appliances/{id}/cloudservices	Retrieve the status of ExtraHop Cloud Services on this appliance (only valid on consoles).
GET /appliances/{id}/productkey	Retrieve the product key for a specified appliance (only valid on consoles).
GET /appliances/{ids_id}/association	Retrieve the ID of the packet sensor that the IDS sensor is joined to.

Operation	Description
POST /appliances/{ids_id}/association	Join an IDS sensor to a packet sensor.
GET /appliances/firmware/next	Retrieve firmware versions that remote ExtraHop systems can be upgraded to (only valid on consoles).
POST /appliances/firmware/upgrade	Upgrade firmware on remote ExtraHop systems connected to the local system. Firmware images are downloaded from ExtraHop Cloud Services (only valid on consoles).
`GET /appliances/{ids_id}/association`	Retrieve the ID of the packet sensor that the IDS sensor is joined to (only valid on consoles).
`POST /appliances/{ids_id}/association`	Join an IDS sensor to a packet sensor (only valid on consoles).

ExtraHop

This resource provides metadata about the ExtraHop system.

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

Operation	Description
GET /extrahop	Retrieve metadata about the firmware running on the ExtraHop system.
GET /extrahop/cluster	Retrieve Explore cluster configuration settings.
PATCH /extrahop/cluster	Update Explore cluster configuration settings.
GET /extrahop/edition	Retrieve the edition of the ExtraHop system.
POST /extrahop/firmware	Upload a new firmware image to the ExtraHop system. For more information, see Upgrade ExtraHop firmware through the REST API.
POST /extrahop/firmware/download/url	Download a new firmware image onto the ExtraHop system from a URL.
POST /extrahop/firmware/latest/upgrade	Upgrade the ExtraHop system to the most recently uploaded firmware image.
GET /extrahop/idrac	Retrieve the iDRAC IP address of the ExtraHop system.
GET /extrahop/platform	Retrieve the platform name of the ExtraHop system.
GET /extrahop/processes	Retrieve a list of processes running on the ExtraHop system.
POST /extrahop/processes/{process}/restart	Restart a process running on the ExtraHop system.
GET /extrahop/services	Retrieve settings for all services.
PATCH /extrahop/services	Update the settings for services.
POST /extrahop/restart	Restart the ExtraHop system.

Operation	Description
POST /extrahop/sslcert	Regenerate the SSL certificate on the ExtraHop system. For more information, see Create a trusted SSL certificate through the REST API ↗
PUT /extrahop/sslcert	Replace the SSL certificate on the ExtraHop system.
POST /extrahop/sslcert/signingrequest	Create an SSL certificate signing request. For more information, see Create a trusted SSL certificate through the REST API ↗.
GET /extrahop/ticketing	Retrieve the ticketing integration status.
PATCH /extrahop/ticketing	Enable or disable ticketing integration.
GET /extrahop/version	Retrieve the version of the firmware running on the ExtraHop system.

Implementation information and instructions for each operation are documented in the REST API Explorer. You can click on any operation in the REST API Explorer to view implementation information such as parameters, response class and messages, and JSON model and schema.

Jobs

You can monitor the progress of some administration jobs started through the REST API. If a REST request creates a job, the job ID is returned in the `location` header of the response. The following operations create jobs:

- `POST /extrahop/firmware/latest/upgrade`
- `POST /extrahop/sslcert`

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

Operation	Description
GET /jobs	Retrieve the status of all jobs.
GET /jobs/{id}	Retrieve the status of a specific job.

License

This resource enables you to retrieve and set product keys or to retrieve and set a license.

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

Operation	Description
GET /license	Retrieve the license applied to this ExtraHop system.
PUT /license	Apply and register a new license to the ExtraHop system.
GET /license/productkey	Retrieve the product key to this ExtraHop system.
PUT /license/productkey	Apply the specified product key to the ExtraHop system and register the license.

Running config

The running configuration file is a JSON document that contains core system configuration information for the ExtraHop system.

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

Operation	Description
GET /runningconfig	Retrieve the current running configuration file.
PUT /runningconfig	Replace the current running configuration file. Configuration file changes are not automatically saved.
POST /runningconfig/save	Save the current changes to the running configuration file.
GET /runningconfig/saved	Retrieve the saved running configuration file.

ExtraHop REST API examples

The following examples demonstrate common REST API operations.

- Change a dashboard owner through the REST API ⤢
- Extract the device list through the REST API ⤢
- Create and assign a device tag through the REST API ⤢
- Query for metrics about a specific device through the REST API ⤢
- Create, retrieve, and delete an object through the REST API ⤢
- Query the record log ⤢

Upgrade ExtraHop firmware through the REST API

You can automate upgrades to the firmware on your ExtraHop appliances through the ExtraHop REST API. This guide provides instructions to upgrade through the REST API Explorer, a cURL command, and a Python script.

> **Note:** If your appliance is connected to ExtraHop Cloud Services, you can simplify the upgrade process by viewing available firmware versions and downloading firmware directly to the system from ExtraHop Cloud Services. For more information, see Upgrade ExtraHop firmware through the REST API with ExtraHop Cloud Services ⤢.

While the firmware upgrade process is similar across all ExtraHop appliances, some appliances have additional considerations or steps that you must address before you install the firmware in your environment. If you need assistance with your upgrade, contact ExtraHop Support.

All appliances must meet the following requirements:

- The firmware version must be compatible with your appliance model.
- The firmware version on your appliance must be supported by the upgrade version.
- Command appliances must be running firmware that is greater than or equal to their connected appliances.
- Discover appliances must be running firmware that is greater than or equal to connected Explore and Trace appliances.

If your deployment only includes a sensor, proceed to the API Explorer, cURL or Python upgrade instructions.

If your deployment includes additional appliance types, you must address the following dependencies before proceeding with the upgrade instructions.

If your deployment includes...	Pre-upgrade tasks	Upgrade order
Command appliances	Reserve a maintenance window of an hour for Command appliances managing 50,000 devices or more.	• Command appliance • Discover appliances • All Explore appliances (manager nodes, then data nodes) • Trace appliances
Explore appliances	See Upgrading ExtraHop recordstores.	
Trace appliances	None	

Upgrade ExtraHop firmware through the REST API Explorer

Download firmware and upgrade the appliance

1. Click **POST /extrahop/firmware/download/url**.

2. Click **Try it out**.
3. In the body field, specify the following fields:

    - **firmware_url:** The URL that the firmware .tar file can be downloaded from.

    - **upgrade:** Indicates whether to upgrade the appliance after the firmware download completes. Set this field to `true`.

    The body field should look similar to the following example text:

    ```
    {

        "upgrade": true,

        "firmware_url": "https://example.extrahop.com/eda/8.7.1.tar"

    }
    ```

4. Click **Send Request**.

    In the Response headers, note the value after the last forward slash in the `location` header. You will need this value to monitor the progress of the upgrade job. For example, the job ID in the following example is `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`

    ```
    /api/v1/jobs/ebbdbc9e-7113-448c-ab9b-cc0ec2307702
    ```

Monitor the progress of the upgrade job

1. Click **Jobs**.
2. Click **GET /jobs/{id}**.
3. In the id field, type the value you copied from the `location` header in the previous task.
4. Click **Send Request**.
5. In the Response body, view information about the job.

    The `status` field is `DONE` when the job is complete.

Upgrade ExtraHop firmware with cURL

You can upgrade the firmware on an appliance through the cURL command.

Before you begin

- The cURL tool must be installed on your machine.
- The system firmware .tar file must be downloaded on your machine.

1. Open a terminal application.
2. Download firmware and upgrade the appliance.

    Run the following command, where `YOUR_KEY` is the API key for your user account, `HOSTNAME` is the hostname of your ExtraHop appliance, and `FIRMWARE_URL` is the URL that the firmware .tar file can be downloaded from:

    ```
    curl -v -X POST https://HOSTNAME/api/v1/extrahop/firmware/download/url -H
      "Authorization: ExtraHop apikey=YOUR_KEY" -H "Content-Type: application/
    json" -d "{ \"upgrade\": true, \"firmware_url\": \"FIRMWARE_URL\"}"
    ```

    In the command output, note the job ID in the Location header. For example, the job ID in the following example is `ebbdbc9e-7113-448c-ab9b-cc0ec2307702`:

    ```
    < Location: /api/v1/jobs/ebbdbc9e-7113-448c-ab9b-cc0ec2307702
    ```

3. Monitor the progress of the upgrade job.

Run the following command, where `YOUR_KEY` is the API key for your user account `HOSTNAME` is the hostname of your appliance, and `JOB_ID` is the ID you recorded in the previous step:

```
curl -v -X GET https://HOSTNAME/api/v1/jobs/JOB_ID -H "Authorization:
  ExtraHop apikey=API_KEY"
```

The command displays an object that contains information about the upgrade job. The upgrade is complete when the `status` field is `DONE`. If the upgrade is not complete, wait a few minutes and run the command again.

Retrieve and run the example Python script

The ExtraHop GitHub repository contains an example Python script that upgrades multiple appliances by reading URLs, API keys, and firmware file paths from a CSV file.

> **Important:** The example python script authenticates to the sensor or console through an API key, which is not compatible with the Reveal(x) 360 REST API. To run this script with Reveal(x) 360, you must modify the script to authenticate with API tokens. See the py_rx360_auth.py ⤢ script in the ExtraHop GitHub repository for an example of how to authenticate with API tokens.

> **Note:** The script does not automatically disable record ingest for ExtraHop recordstores. You must manually disable record ingest before running the script for an ExtraHop recordstores.

1. Go to the ExtraHop code-examples GitHub repository ⤢ and download the contents of the upgrade_system directory to your local machine.
2. In a text editor, open the `systems.csv` file and replace the example values with the hostnames and API keys of your appliances.
3. Run the `upgrade_system_url.py` script.

   The following arguments are optional:

   --max-threads {int}

   Specifies the maximum number of concurrent threads. The default value is 2.

   --wait {float}

   Specifies the number of minutes to wait before checking the progress of an upgrade job. The default value is 0.5.

   For example, the following command upgrades a maximum of 3 appliances at a time:

   ```
   python3 upgrade_system_url.py --max-threads 3
   ```

   > **Note:** If the script returns an error message that the SSL certificate verification failed, make sure that a trusted certificate has been added to your sensor or console ⤢. Alternatively, you can add the `verify=False` option to bypass certificate verification. However, this method is not secure and not recommended. The following code sends an HTTP GET request without certificate verification:
   >
   > ```
   > requests.get(url, headers=headers, verify=False)
   > ```

Upgrading ExtraHop recordstores

Pre-upgrade tasks

Before upgrading an ExtraHop recordstore, you must halt record ingest. You can halt record ingest for all of the nodes in a cluster from a single node.

> **Note:** The message `Could not determine ingest status on some nodes` and `Error` might appear on the Cluster Data Management page in the Administration settings of the

upgraded nodes until all nodes in the cluster are upgraded. These errors are expected and can be ignored.

1. Open a terminal application.
2. Run the following command, where `YOUR_KEY` is the API for your user account, and `HOSTNAME` is the hostname of your ExtraHop recordstore:

```
curl -X PATCH "https://HOST/api/v1/extrahop/cluster" -H "accept:
 application/json" -H "Authorization: ExtraHop apikey=YOUR_KEY" -H
 "Content-Type: application/json" -d "{ \"ingest_enabled\": false}"
```

Post-upgrade tasks

After you have upgraded all of the nodes in the recordstore cluster, enable record ingest.

1. Open a terminal application.
2. Run the following command, where `YOUR_KEY` is the API for your user account, and `HOSTNAME` is the hostname of your ExtraHop recordstore:

```
curl -X PATCH "https://HOST/api/v1/extrahop/cluster" -H "accept:
 application/json" -H "Authorization: ExtraHop apikey=YOUR_KEY" -H
 "Content-Type: application/json" -d "{ \"ingest_enabled\": true}"
```