



ExtraHop 7.4

ExtraHop Trace REST API Guide

© 2020 ExtraHop Networks, Inc. All rights reserved.

This manual in whole or in part, may not be reproduced, translated, or reduced to any machine-readable form without prior written approval from ExtraHop Networks, Inc.

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

Published: 2020-02-22

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

Contents

Introduction to the ExtraHop REST API	4
ExtraHop API requirements	4
Access and authenticate to the ExtraHop REST API	5
Privilege levels	5
Manage API key access	7
Generate an API key	7
Configure cross-origin resource sharing (CORS)	7
Learn about the REST API Explorer	9
Open the REST API Explorer	9
View resource information	9
View operation information	10
Identify objects on the ExtraHop system	10
Learn about the ExtraHop REST API	12
ExtraHop API resources	12
Appliance	12
APIKey	12
ExtraHop	13
License	13
Running config	14

Introduction to the ExtraHop REST API

The ExtraHop REST API enables you to automate administration and configuration tasks on your ExtraHop appliances. 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 appliance, 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.

Each ExtraHop appliance 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 appliance.



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 appliance 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 appliance with appropriate [privileges](#) set for the type of tasks you want to perform.

Access and authenticate to the ExtraHop REST API

Administrators, or users with unlimited 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 unlimited 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 appliance:

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

Privilege levels

User privilege levels determine which ExtraHop Web UI and ExtraHop Admin UI 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:

Privilege level	Actions allowed
"system": "full"	<ul style="list-style-type: none"> • Enable or disable API key generation for the ExtraHop appliance. • 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. • Transfer ownership of any non-system dashboard to another user. • Perform any Admin UI task available through the REST API. • Perform any Web UI task available through the REST API.
"write": "full"	<ul style="list-style-type: none"> • Generate your own API key. • View or delete your own API key. • Change your own password, but you cannot perform any other Admin UI tasks through the REST API. • Perform any Web UI task available through the REST API.
"write": "limited"	<ul style="list-style-type: none"> • Generate an API key.

Privilege level	Actions allowed
	<ul style="list-style-type: none"> View or delete their own API key. Change your own password, but you cannot perform any other Admin UI tasks through the REST API. Perform all GET operations through the REST API. Modify the sharing status of dashboards that you are allowed to edit. Delete dashboards and activity maps that you own. Perform metric and record queries.
"write": "personal"	<ul style="list-style-type: none"> Generate an API key. View or delete your own API key. Change your own password, but you cannot perform any other Admin UI tasks through the REST API. Perform all GET operations through the REST API. Delete dashboards and activity maps that you own. Perform metric and record queries.
"metrics": "full"	<ul style="list-style-type: none"> Generate an API key. View or delete your own API key. Change your own password, but you cannot perform any other Admin UI tasks through the REST API. View dashboards and activity maps shared with you. Perform metric and record queries.
"metrics": "restricted"	<ul style="list-style-type: none"> Generate an API key. View or delete your own API key. Change your own password, but you cannot perform any other Admin UI tasks through the REST API. View dashboards and activity maps shared with you.
"packets": "full"	<ul style="list-style-type: none"> View and download packets from an ExtraHop Discover appliance through the GET/packetcaptures/{id} operation. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> "write": "full" "write": "limited" "write": "personal" "write": null "metrics": "full" "metrics": "restricted"
"packets": "full_with_keys"	<ul style="list-style-type: none"> View and download packets from an ExtraHop Discover appliance through the GET/packetcaptures/{id} operation. <p>This is an add-on privilege that can be granted to a user with one of the following privilege levels:</p> <ul style="list-style-type: none"> "write": "full" "write": "limited" "write": "personal" "write": null

Privilege level	Actions allowed
	<ul style="list-style-type: none"> "metrics": "full" "metrics": "restricted"
	 Note: Although this privilege level enables a user to view and download session keys through the Web UI, you cannot access session keys through the REST API.

Manage API key access

Users with unlimited privileges can manage which users are able to generate API keys on the ExtraHop appliance.

1. Log into the ExtraHop Admin UI through the following URL:

```
https://<hostname-or-IP-of-your-ExtraHop-appliance>/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

After you log into the Admin UI on the ExtraHop appliance, if API key generation is enabled, you can generate an API key.

Before you begin

Make sure the ExtraHop appliance 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 administrative users with unlimited 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.

Important: Clicking the **Try it out!** button causes the specified operation to be performed on your ExtraHop appliance.

Open the REST API Explorer

You can open the REST API Explorer from the ExtraHop Admin UI or through the following URL:

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

1. Log into the Admin UI on the ExtraHop appliance.
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.

Enter your API key here

ExtraHop REST API Explorer

The REST API Explorer is a web-based tool that enables you to view and manipulate operation information and examples for the ExtraHop REST API. You can test API operations such as methods, schemas, parameters, and response messages directly through the API Explorer. In addition, you can copy and paste sample code for cURL, Python 2.7, and Ruby from the API Explorer into your development environment.

Both the REST API and the API Explorer authenticate through an API Key and allow you to communicate with the ExtraHop system over HTTPS.

Resource	Method	Description	Show/Hide	List Operations	Expand Operations
Activity Group	GET	/activitygroups	Retrieve all activity groups from the ExtraHop appliance.		
Activity Group	GET	/activitygroups/[id]/dashboards	Retrieve all dashboards related to a specific activity group.		
Activity Map					
Alert					
Analysis Priority					
APIKey					
Appliance					
Application					
Audit Log					

Click to expand the resource and see available options

Click to expand the operation to see available parameters

View resource information

Click on any resource group in the REST API Explorer to view the available operations and the expected URL syntax for the resource.

The following options enable you to manage the information displayed on the main page.

- **Show/Hide:** Expands and collapses information about the resource.

- **List Operations:** Expands information about the resource operations.
- **Expand Operations:** Expands information about all of the resource operations. Clicking the method or path of the expanded operation will collapse the additional information.

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
Implementation Notes	Provides all of the fields for the request body and supported values for each field.
Response Class	Provides the response code and type for successful requests.
Parameters	Provides information about the available query parameters.
Response Messages	Provides information about the possible HTTP status codes for the resource.
Model	Provides the JSON body objects and descriptions.
Model Schema	Provides the JSON body schema. Red text indicates strings. Green text indicates Boolean and number values.

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. To perform API operations on a specific object, you must locate the object ID.

You can locate an object ID through the following methods:

- 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, such as:

```
{
  "date": "Wed, 25 Nov 2015 17:39:06 GMT",
  "via": "1.1 localhost",
  "server": "Apache",
  "content-type": "text/plain; charset=utf-8",
  "location": "/api/v1/pages/221",
  "cache-control": "private, max-age=0",
  "connection": "Keep-Alive",
  "keep-alive": "timeout=45, max=89",
  "content-length": "0"
}
```

The location for the newly created page is `/api/v1/pages/221` and the ID for the page is 221.

- 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
},

```

To perform further requests on a specific device, add the ID in the request for that device.

- The object ID is provided in the URL for most objects. For example, in the ExtraHop Web UI, click on Metrics, and then Devices. Select any device. The URL for that device page displays an OIDD=<number>, such as:

```

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

```

To perform further 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:

```

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

```

You can also find the short_code in Dashboard Properties in the command menu  from any dashboard.

Learn about the ExtraHop REST API

The ExtraHop REST API enables you to automate tasks for the ExtraHop Admin UI. In addition, you can view and try all of the available resources through the REST API Explorer and perform operations directly on your ExtraHop appliance.


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.

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.
POST /appliances	Establish a new connection to a remote ExtraHop appliance.
GET /appliances/{id}	Retrieve a specific remote ExtraHop appliance connected to the local appliance.
GET /appliances/{id}/productkey	Retrieve the product key of the specified appliance.

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.

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 ExtraHop Admin UI.

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

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

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.

ExtraHop

This resource provides metadata about the ExtraHop appliance, such as the firmware version or if the appliance is a Command appliance.

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 appliance.
GET /extrahop/idrac	Retrieve the iDRAC IP address of the ExtraHop appliance.
GET /extrahop/platform	Retrieve the platform name of the ExtraHop appliance.
GET /extrahop/processes	Retrieve a list of processes running on the ExtraHop appliance.
POST/extrahop/processes/{process}/restart	Restart a process running on the ExtraHop appliance.
POST /extrahop/sslcert	Regenerate the SSL certificate on the ExtraHop appliance.
PUT /extrahop/sslcert	Replace the SSL certificate on the ExtraHop appliance.
POST /extrahop/sslcert/signingrequest	Create an SSL certificate signing request
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 appliance.

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.

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 appliance.
PUT /license	Apply and register a new license to the ExtraHop appliance.
GET /license/productkey	Retrieve the product key to this ExtraHop appliance.
PUT /license/productkey	Apply the specified product key to the ExtraHop appliance and register the license.

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.

Running config

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

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.

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.