# ExtraHop 7.3
# ExtraHop Explore REST API Guide

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

Published: 2018-07-07

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

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.

## Get started

If you have a user account for your ExtraHop appliance, you can connect to the REST API Explorer and begin browsing through the available resources.

1. From the Access Setting section, click **API Access**.
2. On the API Access page, click **REST API Explorer**.
3. Locate a resource you want and click **List Operations** to view all operations that you can perform on that resource.
4. Click an operation name to view implementation information such as parameters, response class and messages, and JSON model and schema that are applicable to the operation.

**Next steps**

Access and authenticate to the ExtraHop REST API

Enable CORS for the ExtraHop REST API

Learn about the REST API Explorer

Learn about the ExtraHop REST API

# 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.

After you generate an API key, you must append the key to your request headers. The following example shows a request that would retrieve 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" | • Enable or disable API key generation for the ExtraHop appliance.<br>• Generate an API key.<br>• View the last four digits and description for any API key on the system.<br>• Delete API keys for any user.<br>• View and edit cross-origin resource sharing.<br>• Transfer ownership of any non-system dashboard to another user.<br>• Perform any Admin UI task available through the REST API.<br>• Perform any Web UI task available through the REST API. |
| "write": "full" | • Generate your own API key.<br>• View or delete your own API key.<br>• Change your own password, but you cannot perform any other Admin UI tasks through the REST API.<br>• Perform any Web UI task available through the REST API. |
| "write": "limited" | • Generate an API key.<br>• View or delete their own API key.<br>• Change your own password, but you cannot perform any other Admin UI tasks through the REST API. |

| Privilege level | Actions allowed |
| --- | --- |
| | • Perform all GET operations through the REST API.<br>• Modify the sharing status of dashboards that you are allowed to edit.<br>• Delete dashboards and activity maps that you own.<br>• Perform metric and record queries. |
| "write": "personal" | • Generate an API key.<br>• View or delete your own API key.<br>• Change your own password, but you cannot perform any other Admin UI tasks through the REST API.<br>• Perform all GET operations through the REST API.<br>• Delete dashboards and activity maps that you own.<br>• Perform metric and record queries. |
| "metrics": "full" | • Generate an API key.<br>• View or delete your own API key.<br>• Change your own password, but you cannot perform any other Admin UI tasks through the REST API.<br>• View dashboards and activity maps shared with you.<br>• Perform metric and record queries. |
| "metrics": "restricted" | • Generate an API key.<br>• View or delete your own API key.<br>• Change your own password, but you cannot perform any other Admin UI tasks through the REST API.<br>• View dashboards and activity maps shared with you. |
| "packets": "full" | • View and download packets from an ExtraHop Discover appliance through the `GET/packetcaptures/{id}` operation.<br><br>This is an add-on privilege that can be granted to a user with one of the following privilege levels:<br><br>• "write": "full"<br>• "write": "limited"<br>• "write": "personal"<br>• "write": null<br>• "metrics": "full"<br>• "metrics": "restricted" |
| "packets": "full_with_keys" | • View and download packets from an ExtraHop Discover appliance through the `GET/packetcaptures/{id}` operation.<br><br>This is an add-on privilege that can be granted to a user with one of the following privilege levels:<br><br>• "write": "full"<br>• "write": "limited"<br>• "write": "personal"<br>• "write": null<br>• "metrics": "full"<br>• "metrics": "restricted" |

| Privilege level | Actions allowed |
| --- | --- |
| | **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.

## Delete an API Key

You can delete an API key from the ExtraHop appliance.

1. In the Access Settings section, click **API Access**.
2. In the Keys section, click the delete (X) icon next to the API key you want to delete.
3. Click **OK**.

# Enable CORS for the ExtraHop REST API

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.

## View CORS settings

In the Access Settings section, click **API Access**.
The CORS Settings section displays the following settings:

- The list of URLs that can access the REST API.
- The status of the **Allow API requests from any Origin** option.

## Add an allowed origin

You can configure one or more allowed origins or you can allow access to the ExtraHop REST API from any origin.

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**.

## Delete an allowed origin

You can delete a URL from the list of allowed origins or disable access from all origins.

1. In the Access Settings section, click **API Access**.
2. In the CORS Settings section, modify one of the following access configurations.
   - To delete a specific URL, click the delete (X) icon next to the origin you want to delete.
   - To disable access from any URL, clear the **Allow API requests from any Origin** checkbox.
3. Click **Save Settings**.

# 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.

## 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. |

### GET requests

GET requests retrieve information about the objects in the associated resource. You can request information about all of the objects in a resource or you can specify an object ID to retrieve detailed information about only that object.

### POST requests

POST requests create objects and queries for the associated resource.

### PATCH requests

PATCH requests update existing objects with modified or missing information.

### DELETE requests

DELETE requests remove objects from the system. You must have an object ID to perform a DELETE operation.

### PUT requests

For limited operations, you can erase and replace the content in a resource with a PUT request.

# 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 /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. |

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/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.