API

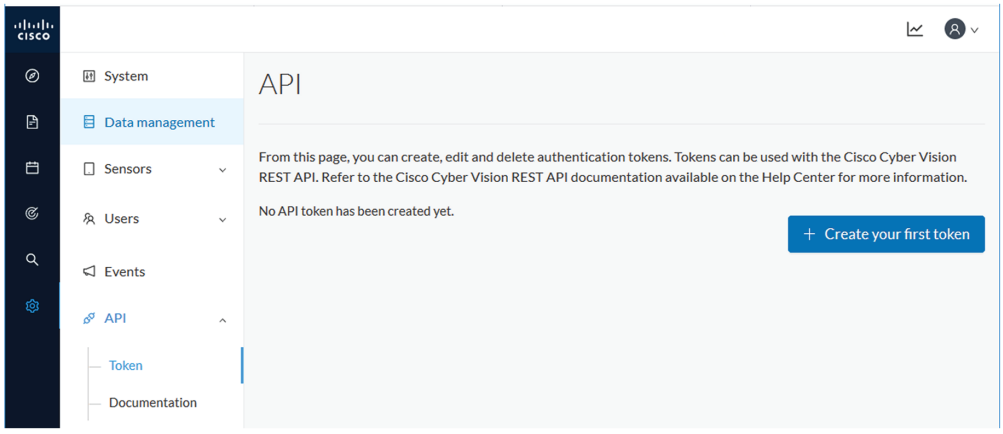
- Token, on page 1
- Documentation, on page 2

Token

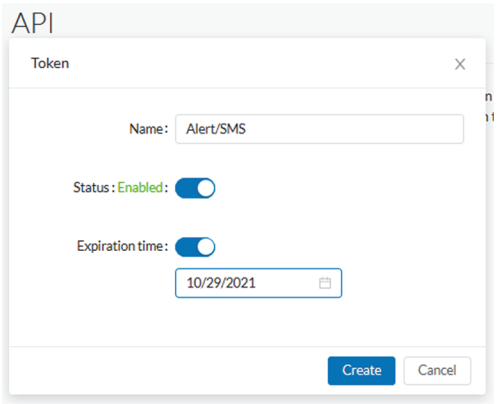
Cisco provides a REST API. To use it you first need to create a token through the API administration page.

A token is a random password which authenticates a request to Cisco Cyber Vision to access or even modify the data in the Center through the REST API. For instance, you can request the latest 10 components detected on Cisco Cyber Vision or create new references. Requests can be used by external applications like a SOC solution.

Note Best practice: create one token per application so you can remove or expire accesses separately.



Create your first token and enter a name that will help you identifying the token. For security reasons you can also use the status toggle button to disable authorization to use the token (for example, if the token created is to be used later and you want to prevent access until then) and set an expiration time.



Once the token is created click show to see and copy the token to the clipboard.

For more information about the REST API refer to the REST API user documentation available on cisco.com.

Documentation

This page is a simplified API development feature. It contains an advanced API documentation with a list of all possible routes that can be used and, as you scroll down the page to Models, a list of possible data responses (data type, code values and meaning).

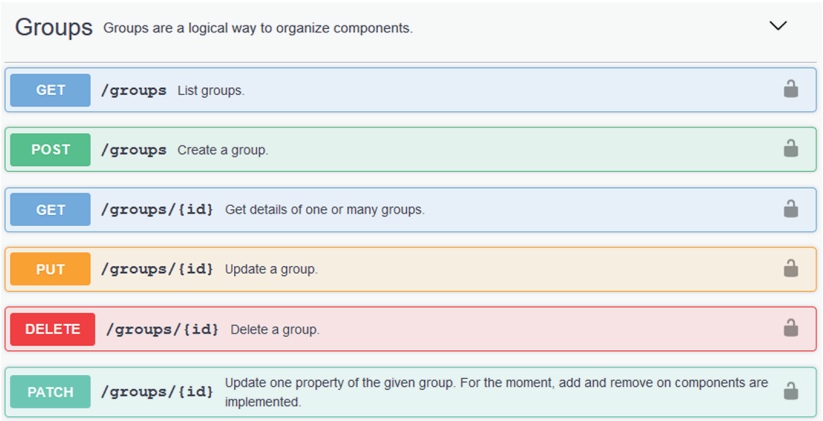
In addition to information research, this page allows you to perform basic tests and call the API by sending requests such as GET, DELETE and POST. You will get real results from the Center dataset. Specifications about routes are available such as the route's structure, and parameters and arguments that can be set. An URL is generated and curl can be used in a terminal as it is.

However, for an advanced use, you must create an application that will send requests to the API (refer to the REST API documentation).

Important All routes other than GET will modify data on the Center. As some actions cannot be reversed, use DELETE, PATCH, POST, PUT with caution.

Routes are classified by Cisco Cyber Vision's elements type (activities, baselines, components, flows, groups, etc.).

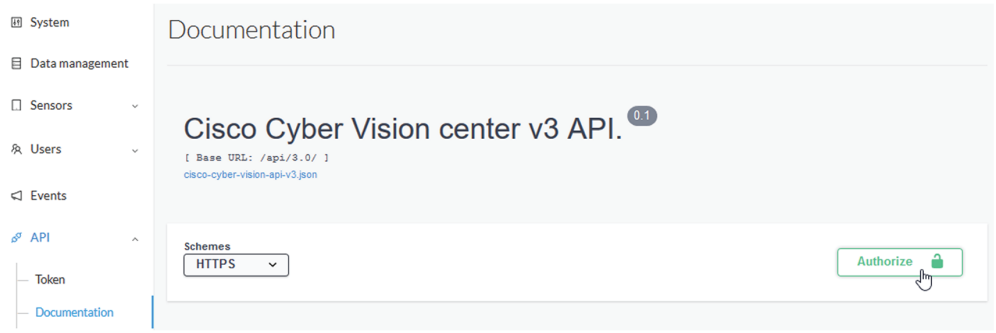
The category "Groups" containing all possible group routes:



To authorize API communications:

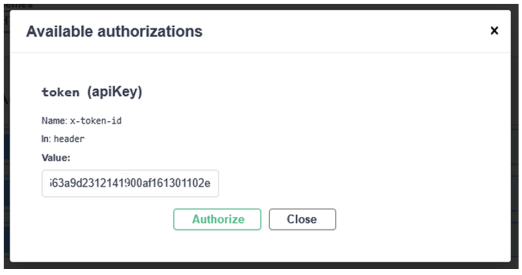
Step 1 Access the API Token menu to create and/or copy a Token.

Access the API Documentation page and click the Authorize button.

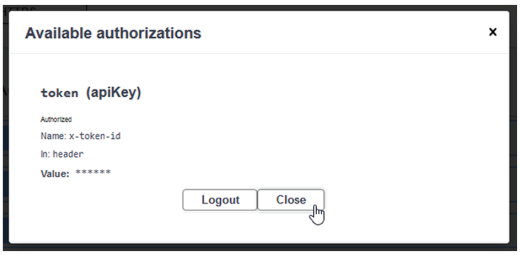


Step 2 Paste the token.

Step 3 Click Authorize.



Step 4 Click Close.

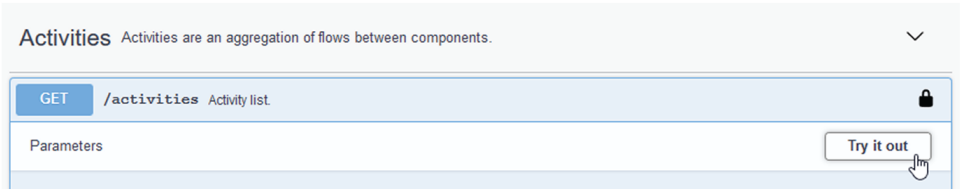


Closed lockers displays. They indicate that routes are secured and authorization to use them is up.

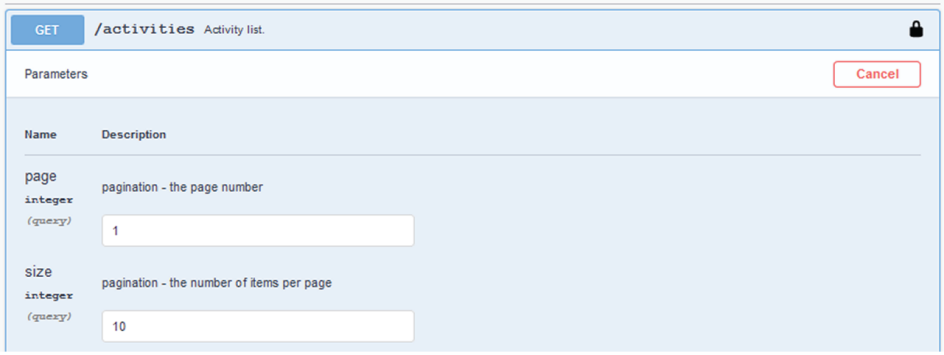
To use a route:

Step 5 Click a route to deploy it. In the example, we choose Get activity list.

Step 6 Click Try it out.



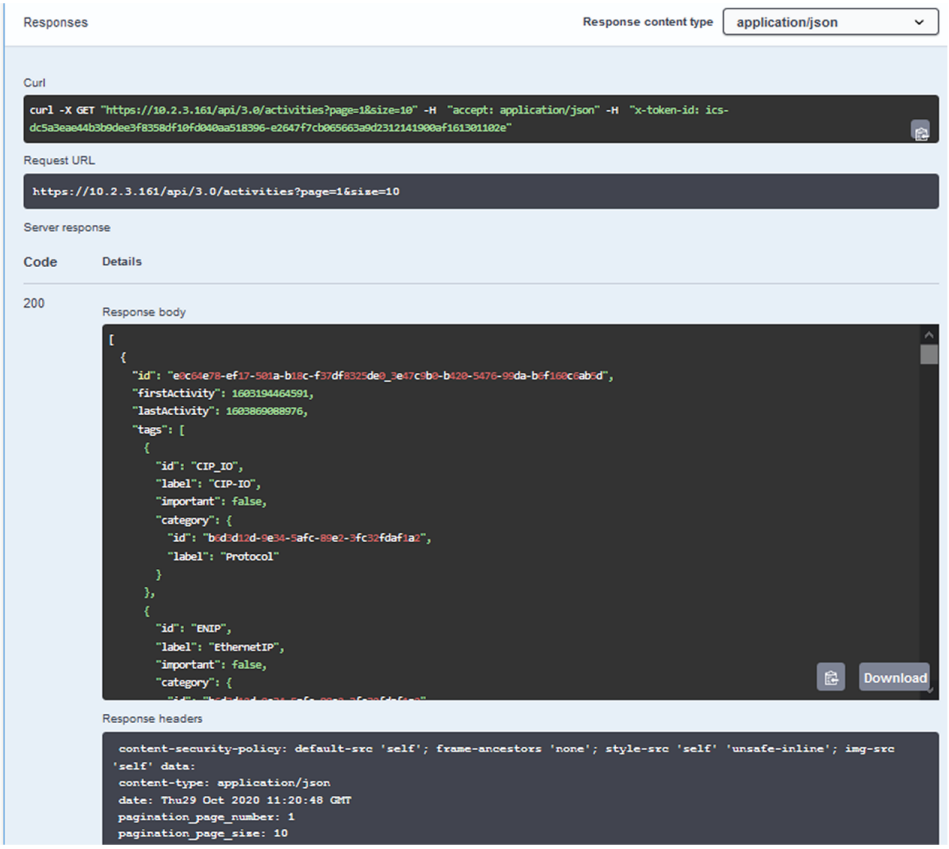
Step 7 You can set some parameters. In the example, we set page to 1 and size to 10.



Step 8 Click Execute.

Note You can only execute one route at a time.

A loading icon appears for a few moments. Responses display with curl, Request URL and the server response that you can copy or even download.



Step 9 When you're finished, click the Authorize button.

Step 10 Logout to clean the token variable, and click Close.