

Use Cisco APIs in Cisco SD-WAN Cloud

- API keys for Cisco SD-WAN Cloud, on page 1
- Restrictions for using a Cisco API key, on page 1
- Obtain a Cisco API key, on page 2
- Cisco API request examples, on page 3

API keys for Cisco SD-WAN Cloud

API key, or JSON web tokens (JWT), are unique codes that:

- grant client access to an application programming interface (API),
- serve as a password preventing unauthorized access, and
- are required for Cisco SD-WAN Cloud customer access to Cisco APIs.

A Cisco API key is to be used for Cisco API calls by a specified fabric user. It remains valid until the user is deleted or the user role is changed.

This chapter describes how to acquire a Cisco API key and use Cisco APIs on a Cisco SD-WAN Cloud fabric in Cisco SD-WAN Cloud Release 20.15 and higher.

Restrictions for using a Cisco API key

Use the Cisco API key to access all Cisco APIs from Cisco SD-WAN Cloud through your SSO login, subject to certain restrictions. Refer to Cisco DevNet for more information on Cisco APIs.

- Authentication method

  You must specify the Bearer token authentication method in a header field. Use the value you received from your GET request.

- Cross-site request forgery protection (CSRF/XSRF)

  Your API request header must include an X-XSRF-Token header field to protect against cross-site request forgery. Use the value you received from your GET request.

- API body use

  You can include an API body as needed, based on the API call you are making.

- Rate limit

  Real time APIs and bulk APIs are not available. All other APIs can be used, subject to a rate limit of 10 per second. Cisco SD-WAN Manager imposes an API rate limit of 5 per second.

- No continuous monitoring

  Do not use this feature for continuous monitoring. Refer to the Cisco Catalyst SD-WAN Getting Started Guide for more information on API rate limits.

- Supported categories

  API calls are provided for only these categories of operations:

  - Certificate management
  - Configuration
  - Device and device inventory
  - Monitoring
  - Troubleshooting tools

- No NAT configuration

  NAT configuration using REST APIs is not supported.

Obtain a Cisco API key

Cisco SD-WAN Cloud Release 20.15 provides a mechanism to generate an API key directly. Follow these steps to generate an API key and find the gateway URL and Cross-site request forgery protection (CSRF) token values:

Procedure

Step 1 Log in to the fabric.

Step 2 Select **My Profile** from the drop-down menu under your user ID.

Step 3 Obtain the API key (also called the API token).

a) In Cisco SD-WAN Manager click your user name at the top of the page, and choose **My profile**.

b) In the **API token** area, click **Generate**.

SD-WAN Manager generates and displays the API key.

c) Copy or download the API key.

Step 4 Obtain the organization name.

a) Open **Administration** > **Settings** > **Organization name**.

b) Copy the name from the **Organization name** field.

Step 5 Obtain the API gateway URL.

Use the endpoint information provided in the example here. In the payload, use the organization name in "org" and the API key in "apikey". The response provides the API gateway URL.

Example:

Post

```
https://ssp.sdwan.cisco.com/ssp/api/v6/apigw/info/
```

Payload

```
{
"org": "kdk...",
"apikey": "eyJ0eX...",
"is_redirect": false
}
```

Response

```
{
"gateway_url": "apigw1clouduswest2-1024.viptela.info",
"org": "kdk..."
}
```

Note
If the response is not successful, it might be that a new API gateway was provisioned near your location. Repeat this process to connect to the new gateway serving your overlay.

Step 6 Obtain the cross-site request forgery (CSRF) token.

Using the API key and gateway URL hostname values you received, make a GET request to the endpoint "/dataservice/client/token" to obtain the CSRF token. The response provides the CSRF token.

Example:

Based on the gateway URL returned in this example, the full pathname would be https://apigw1clouduswest2-1024.viptela.info/dataservice/client/token.

What to do next

Use the information you've obtained to make API calls. Some PUT and POST calls require the CSRF token.

Cisco API request examples

The examples in this section demonstrate how to use the API key, gateway URL, and CSRF/XSRF token to execute API calls.

GET API request example using Curl

This GET request retrieves the page at the URL specified in the location parameter.

```
curl --location
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE...'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkYW
...
a_fcNoeAlVYvrXzDXA'
```

PUT/POST API request example using Curl

This PUT request sends the data in the data parameter to the page URL specified in the location parameter.

```
curl --location --request PUT
apigw1clouduswest2-1024.viptela.info/dataservice/settings/configuration/banner'
--header 'X-XSRF-Token: AB0E71CAE72C6D...'
--header 'Content-Type: application/json'
--header 'Authorization: Bearer
eyJ0eXAiOiJqd3QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ2bGluZ2FtcEBjaXNjby5jb20iLCJpc3MiOiJiOGVkYW
...
a_fcNoeAlVYvrXzDXA'
--data '{"mode":"on","bannerDetail":"check"}'
```