Cisco IMC Supervisor REST API Getting Started Guide, Release 2.2

Revised: May 29, 2019

Getting Started with Cisco IMC Supervisor REST API

Overview

Why use the REST API

The Cisco IMC Supervisor REST API allows an application to interact with Cisco IMC Supervisor programmatically. These requests provide access to resources in Cisco IMC Supervisor.

The API accepts and returns HTTP messages that contain Extensible Markup Language (XML) documents. The XML payload contained in an HTTP message describes a method or managed object (MO) in Cisco IMC Supervisor. You can use any programming language to generate the messages and the XML payload.

How the API Works

In RESTful APIs, the HTTP method specifies the action you want to perform and the URI specifies the resource you want to access.

REST API uses the following HTTP methods to perform create, read, update, and delete (CRUD) operations:

HTTP Method	Description
GET	Retrieves the specified resource . GET is a read-only operation that does not change the engine state. • The HTTP GET operation should not have a request body. If information is passed in a GET request, query parameters must be used instead. • Unless specified, the HTTP GET operation returns the configured state. For example, an HTTP GET operation on the Faults table returns the current list of faults for servers being managed in the system.
POST	Submits data to be processed by the specified resource. The data to be processed is included in the request body. A POST operation can create a new resource. • Every POST request must include an XML body containing a definition of the new resource. • For a POST operation to create a new resource, the location header in the HTTP response must contain the complete URL to be used for subsequent PUT, GET, and DELETE commands. • The HTTP POST response to a create request must have a 200 return code and a location header containing the URI of the newly created resource in the HTTP header.

HTTP Method	Description
PUT	Updates the specified resource with new information. The data that is included in the PUT operation replaces the previous data. • The PUT operation cannot be used to create a new resource. • The request body of a PUT operation must contain the complete representation of the mandatory attributes of the resource in XML format.
DELETE	Deletes a resource. • If you delete a resource that has already been deleted, a `404 Not Found` response is returned. • The HTTP DELETE operation should not have a request body. If information is passed in a GET request, query parameters must be used instead.

Note For GET APIs, the **Resource URL** displayed in the editable field may not match the URL value displayed above. You must edit the text field such that the **Resource URL** matches the one displayed above. The API will then execute correctly.

How to use the REST API

To access the REST API browser through Cisco IMC Supervisor, you must have a valid Cisco IMC Supervisor user account and an API access key. The API access key is required for Cisco IMC Supervisor to authenticate API requests. This access key is a unique security access key code that is associated with a specific Cisco IMC Supervisor user account. For more information about how to generate an API access key, see Generating an API Access Key, on page 4.

You must pass the REST API access key as a *name:value* header following standard HTTP syntax and semantic rules. For example, a valid *name:value* header is *X-Cloupia-Request-Key: F90ZZF12345678ZZ90Z12ZZ3456FZ789*. For more information about the API request header, see How to Make a REST API Request, on page 7 and RFC2616 Header Field Definitions.

The REST API call can be made in one of the following ways:

- Cisco IMC Supervisor GUI—Cisco IMC Supervisor provides a developer menu option to offer the report metadata and REST API Browser for developers. To access these features, enable the developer menu. For more information about how to enable the developer menu, see Enabling the Developer Menu Options, on page 5.

  On enabling the developer menu, you gain access to the following features:

  - Report Metadata— Report Metadata enables you to view the REST API URL for every report displayed in Cisco IMC Supervisor. For more information about how to access Report Metadata, see Accessing the Report Metadata, on page 6.
  - REST API Browser—The REST API Browser is accessible from the **Policies** > **API and Orchestration** menu of Cisco IMC Supervisor. The REST API Browser provides API information and API code generation capabilities that make it easy to see and work with all the available APIs, such as the REST APIs. For more information about how to access REST API Browser, see Using the REST API Browser.

- REST Client—The REST Client is a useful widget for parsing and viewing API requests and responses. In this widget, you can enter a REST URL and apply an HTTP method such as POST, PUT, or DELETE to the URL for data manipulation. The REST Client provides a simple user interface for entering an URL to fetch data from the Cisco IMC Supervisor server.

- If you are using Mozilla Firefox, download RESTClient from Add-ons for Firefox.
- If you are using Google Chrome, download Advanced REST Client from the Chrome Web Store.

Note If you are logged into Cisco IMC Supervisor, use any supported web browser to send API requests and get responses.

- CURL—It is a command line utility and can be used to query data from Cisco IMC Supervisor and configure Cisco IMC Supervisor.

Prerequisites

Before you start using the Cisco IMC Supervisor REST APIs, ensure that:

- Cisco IMC Supervisor is installed and running on your system. For more information about how to install Cisco IMC Supervisor, refer the Cisco IMC Supervisor Install and Upgrade Guide.
- You have an API access key. For more information about how to generate an API access key, see Generating an API Access Key, on page 4
- You have a REST client to execute RESTful web services.

Note
- If you are using Mozilla Firefox, download RESTClient from Add-ons for Firefox.
- If you are using Google Chrome, download Advanced REST Client from the Chrome Web Store.

Generating an API Access Key

Procedure

Step 1 In Cisco IMC Supervisor, click your login name in the upper right.

For example, if you log in as admin, Cisco IMC Supervisor displays **admin** in the upper right.

Step 2 In the **User Information** dialog box, click the **Advanced** tab.

Step 3 To copy the value displayed in the **REST API Access Key** area, click **Copy Key Value**.

Step 4 Save the access key in a secure location, and use it in the API request header.

For more information about the API request header, see Request Format.

Step 5 If you want to change the API access key, click **Regenerate Key**.

After you generate a new key, the old key code is retired and you cannot use it.

Setting Up the Environment for Using the REST API Through the GUI

Enable the developer menu option to access the REST API Browser and Report Metadata information in Cisco IMC Supervisor. The REST API Browser and Report Metadata features provide you with site-specific API data.

The HTTP request code provided by the Report Metadata view yields immediate API service results. You can use these options in every situation where you need API information.

The Cisco IMC Supervisor REST API Browser provides API information and API code generation capabilities that make it easy to see and work with all of the available APIs, including the REST APIs.

To use REST API in the GUI, perform the following tasks:

- Enabling the Developer Menu Options, on page 5
- Using the REST API Browser
- Accessing the Report Metadata, on page 6

Enabling the Developer Menu Options

Before you begin

Obtain one or more user accounts that provide the same administrative access to data that your application users will have. Your Cisco UCS Director administrator can explain the data access limitations associated with different administrator and end-user roles. You may want multiple user accounts to test the user experiences associated with different data accesses and security controls.

Procedure

Step 1 In Cisco UCS Director, hover the mouse over the user icon at the top right corner and choose **Edit My Profile** from the drop-down list.

Step 2 On the **Edit My Profile** page, click **Show Advanced Settings**.

Step 3 Check **Enable Developer Menu (requires re-login)**.

The **REST API Browser** is activated in the **Orchestration** page, and the **Report Metadata** option becomes available in the report views.

Tip The **Advanced** area displays the REST API Access Key code for the account.

Step 4 Click **Close**.

Using the REST API Browser

The Cisco IMC Supervisor REST API Browser provides API information and API code generation capabilities that assist and educate developers in the use of all available Cisco IMC Supervisor XML-formatted REST APIs. The primary view lists the Task folders that contain the APIs. The task names supply the categories under which the APIs are listed. For example, all the APIs pertaining to Firmware Management tasks are available inside the folders with these names.

Before you begin

- Obtain one or more user accounts that provide exactly the same administrative access to data that your application users will have. Your Cisco IMC Supervisor administrator can explain the data access limitations associated with different administrator and operator roles. For more information about users and roles, see the Creating Users and User Roles chapter in the *Cisco IMC Supervisor Rack-Mount Servers Management Guide*. You may want multiple user accounts to test the user experiences associated with different data accesses and security controls.
- Enable the developer menu option for the session.

Procedure

Step 1 On the menu bar, choose **Policies** > **API and Orchestration**.

Step 2 Click the **REST API Browser** tab.

Click the right scroll arrow, if necessary, to navigate to the **REST API Browser** tab.

Step 3 Open the task folder that contains the API you want to view.

Tip You can use the **Search** field at the top right corner of the **Rest API Browser** tab to find a specific API if you do not know which task folder it belongs to. Enter a string that occurs in the API Resource, Operation or Description field to narrow your search. You can also use the other options on that menu bar, such as the **Add Advanced Filter**, to help you find a specific API.

Step 4 Double-click a row that contains an API resource and operation that is required.

The REST API browser displays the following:

- **API Examples** tab—Displays the API data for your selection and enables you to generate a sample URL. Depending on the operation and resource that you have selected, this tab might also include data entry boxes that accept parameter values. If available in a data entry box, click **Select** to open data search filters that can help you sort and select the data that you need to enter.
- **Details** tab—Provides additional details about the API, including the API definition, input parameters, and output parameters.
- **Sample Java Code** tab—Provides sample code for the API.

  Note This tab is not applicable for the current release.

Accessing the Report Metadata

Report Metadata enables you to view the API code used by Cisco IMC Supervisor, including the API request code for every report displayed in Cisco IMC Supervisor. This code includes a complete URL that is ready to paste into a browser to send the URL request to Cisco IMC Supervisor. The immediate API responses provide a lot of information for the developer. To see the API request code, navigate to a report and select **Report Metadata**.

Before you begin

- Obtain one or more user accounts that provide exactly the same administrative access to data that your application users will have. Your Cisco IMC Supervisor administrator can explain the data access limitations associated with different administrator

and end-user roles. You may want multiple user accounts in order to test the user experiences associated with different data accesses and security controls.

- Enable the Developer Menu option for the session.

Procedure

Step 1 In Cisco IMC Supervisor, navigate to the page for which you want to see the API code.

For example, choose one of the following:

- **Systems** > **Firmware Management** > **Images - Local**
- **Systems** > **Physical Accounts**

Step 2 Click **Report Metadata**.

Step 3 In the **Information** dialog box, review the REST API URL.

How to Interpret the HTTP Response

The following HTTP status codes are returned by Cisco IMC Supervisor:

- **401 Unauthorized**—The API key is not a valid key.
- **200 OK**—Cisco IMC Supervisor has processed the request. The actual status of the request is in the body of the response.

The Cisco IMC Supervisor response body is in JSON format as determined by the FormatType parameter specified in the API request.

API Response (Service Result) Data Types

The service result (payload) sent in a response to a Cisco IMC Supervisor REST API request is specified for the operation. The service result can be an operation-specific set of name-value pairs, or it can be formatted as a standard data type for this API, that is, as a report or as an XML object.

How to Make a REST API Request

A REST Client parses and labels the API data in a useful & informative way. You can use any supported Web browser to send API requests and get responses. Download a supported REST Client in a Web browser to execute the REST URLs.

- In Mozilla Firefox, download RESTClient from Add-ons for Firefox.
- In Google Chrome, download Advanced REST Client from the Chrome Web Store.

API clients use an HTTP request to interact with Cisco IMC Supervisor. To pass the REST API access key, each request must be associated with an http header called `X-Cloupia-Request-Key` with its value set to the current REST API access key. For information about how to generate the REST API access key, see Generating an API Access Key.

Requests made to the API have the following characteristics:

- Requests are sent over HTTP.

- Request must contain a valid URL as in the following format:

Example API URL:

```
http://serverip/cloupia/api-v2/CreateNetworkImage
```

HTTP method: POST

```
<operationType>NETWORK_IMAGE_CREATE</operationType>
<payload>
<![CDATA[
<CreateNetworkImage>
<profileName></profileName>
<platform></platform>
<networkServerType>NFS</networkServerType>
<!-- Set this value only when networkServerType equals to HTTP -->
<locationLink></locationLink>
<!-- Set this value only when networkServerType not equals to HTTP -->
<networkPath></networkPath>
<!-- Set this value only when networkServerType not equals to HTTP -->
<sharePath></sharePath>
<!-- Set this value only when networkServerType not equals to HTTP -->
<remoteFileName></remoteFileName>
<nwPathUserName></nwPathUserName>
<nwPathPassword></nwPathPassword>
<!-- Set this value only when networkServerType equals to CIFS -->
<mountOptions></mountOptions>
</CreateNetworkImage>
]]>
</payload>
</cuicOperationRequest>
```

The HTTP response for creating network image is:

```
<?xml version="1.0" encoding="UTF-8"
standalone="yes"?><cuicOperationResponse><operationStatus>0</operationStatus><response><CreateNetworkImageResponse><Success>Network
 Image Profile test saved
successfully.</Success></CreateNetworkImageResponse></response><responseMap><entry><key>Success</key><value>Network
 Image Profile test saved successfully.</value></entry></responseMap></cuicOperationResponse>"
```

For REST API examples, see the *Cisco IMC Supervisor REST API Cookbook, Release 2.0*.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.