# Manage Destination Lists via Curl with Secure Access API

## Contents

## Introduction

This document describes how to manage destination lists via curl with Secure Access API.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Secure Access
- Secure Access API
- curl
- Json

### Components Used

The information in this document is based on these software and hardware versions:

- Secure Access
- Secure Access APIs
- curl
- Json

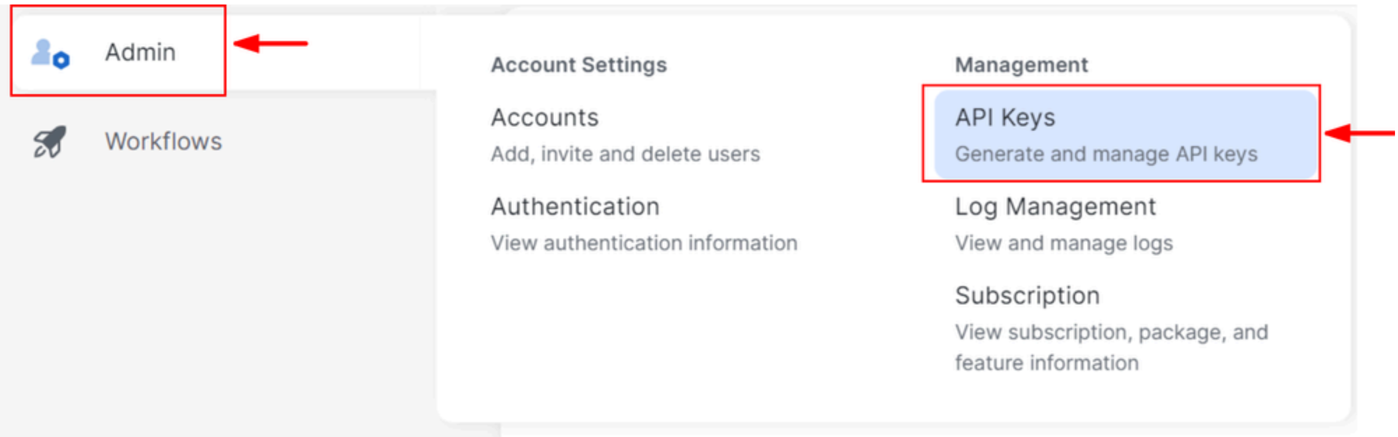
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

# Configure

## 1.Create your API key

Navigate to [Secure Access Dashboard.]()

- Click on Admin > Api Keys > Add



Admin

Workflows

Account Settings

Accounts

Add, invite and delete users

Authentication

View authentication information

Management

API Keys

Generate and manage API keys

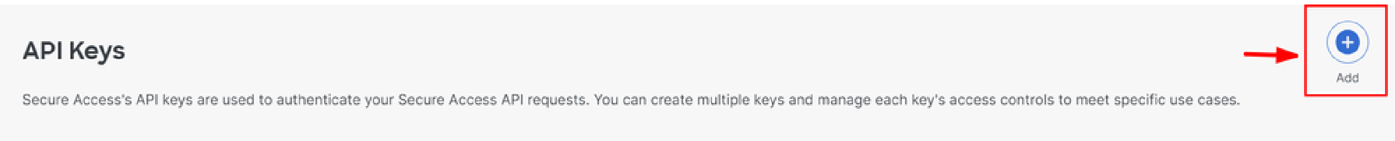
Log Management

View and manage logs

Subscription

View subscription, package, and feature information

*Create your API Key 1*



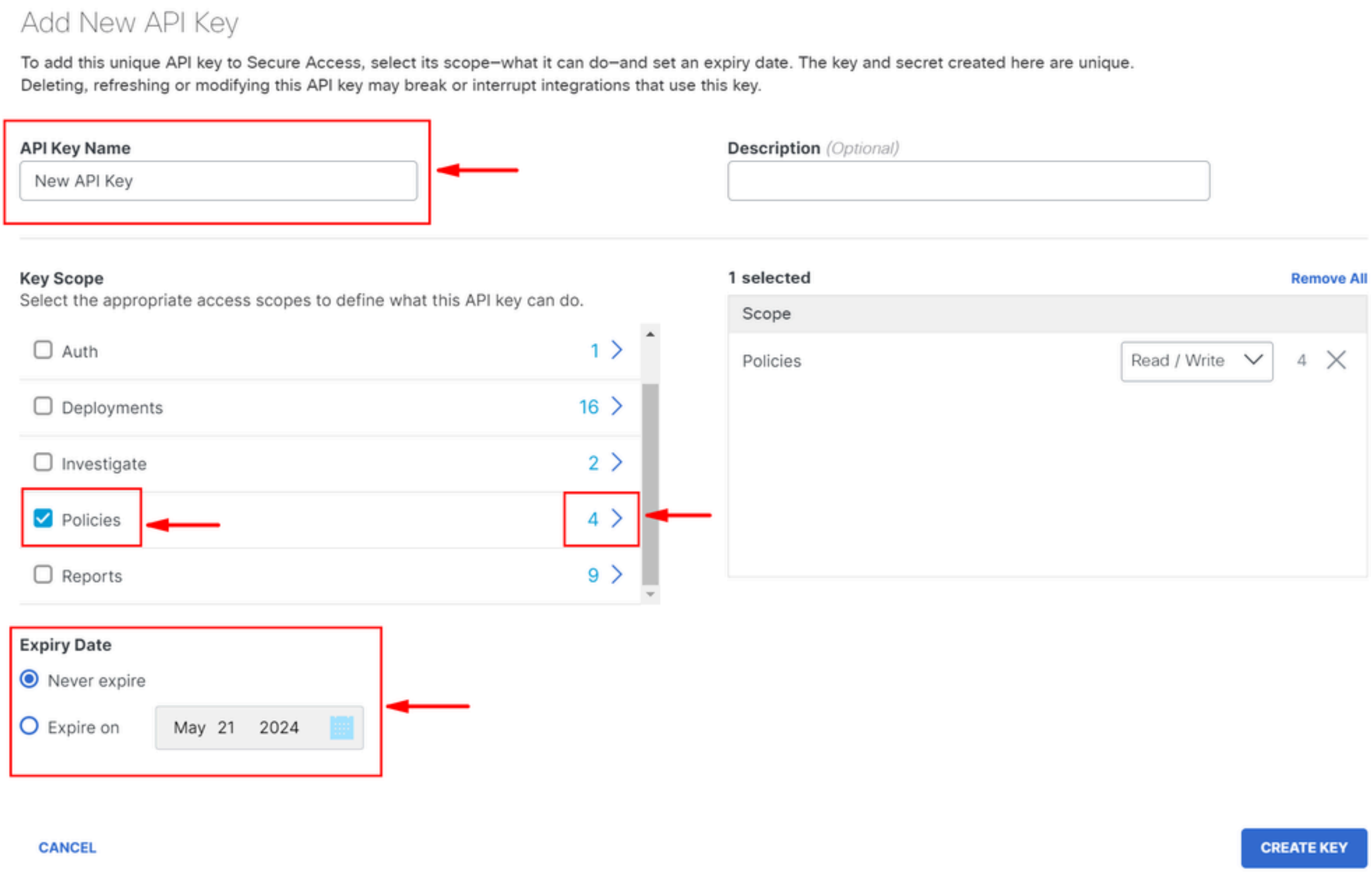
API Keys

Secure Access's API keys are used to authenticate your Secure Access API requests. You can create multiple keys and manage each key's access controls to meet specific use cases.

Add

*Create your API Key 2*

- Add desired API Key Name , Description (Optional) , Expiry Date as required



Add New API Key

To add this unique API key to Secure Access, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key.

API Key Name: New API Key

Description (Optional):

Key Scope
Select the appropriate access scopes to define what this API key can do.

- ☐ Auth 1
- ☐ Deployments 16
- ☐ Investigate 2
- ☑ Policies 4
- ☐ Reports 9

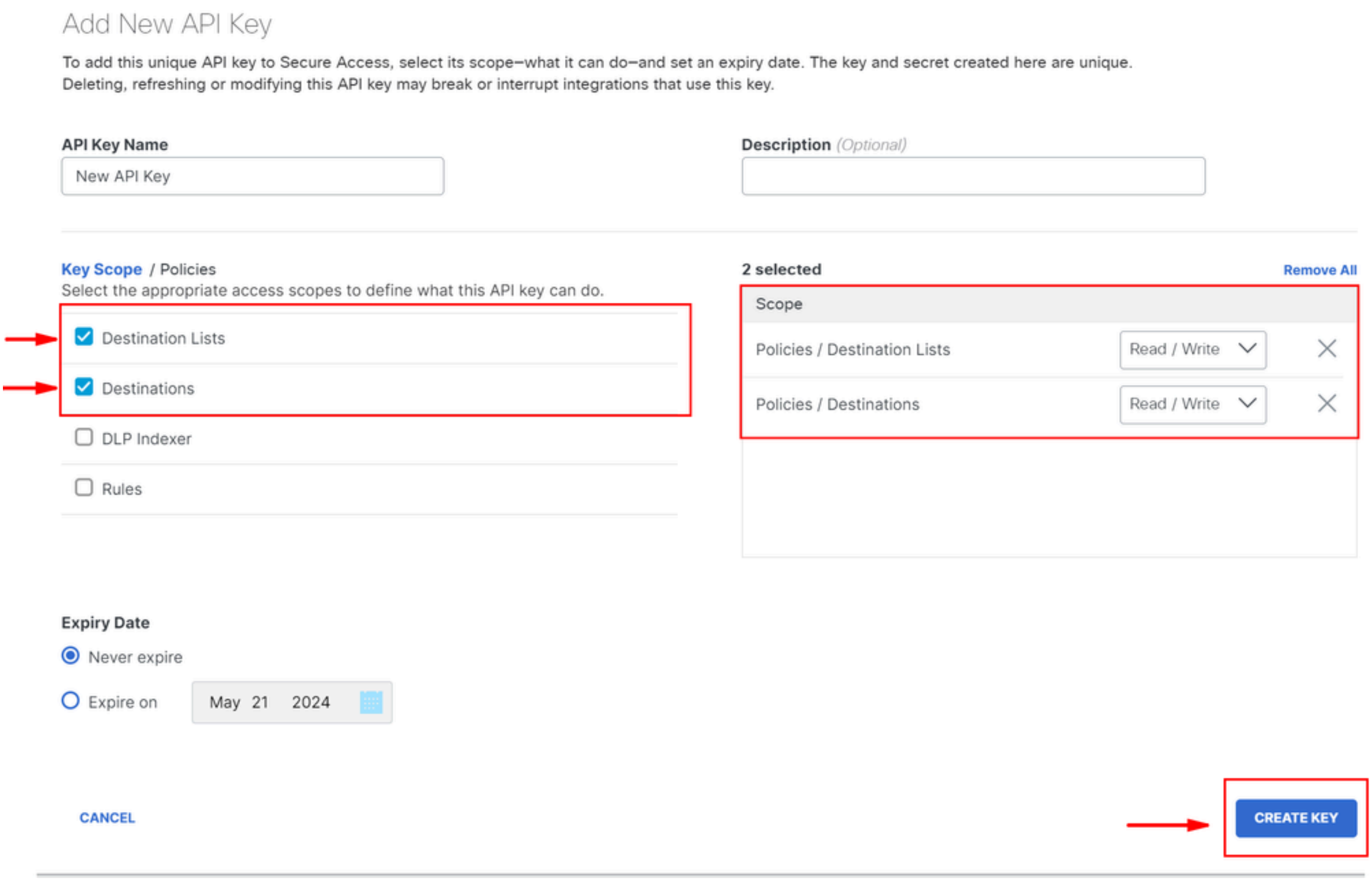
1 selected

| Scope | | | |
|---|---|---|---|
| Policies | Read / Write | 4 | ✕ |

Expiry Date
- ● Never expire
- ○ Expire on May 21 2024

*Create your API Key 3*

- Under Key Scope, chose Policies then Expand policies
- Chose Destination Lists and Destinations
- Change Scope if required, otherwise keep as Read/Write
- Click on CREATE KEY



Add New API Key

To add this unique API key to Secure Access, select its scope—what it can do—and set an expiry date. The key and secret created here are unique. Deleting, refreshing or modifying this API key may break or interrupt integrations that use this key.

API Key Name: New API Key

Description (Optional):

Key Scope / Policies
Select the appropriate access scopes to define what this API key can do.

- ☑ Destination Lists
- ☑ Destinations
- □ DLP Indexer
- □ Rules

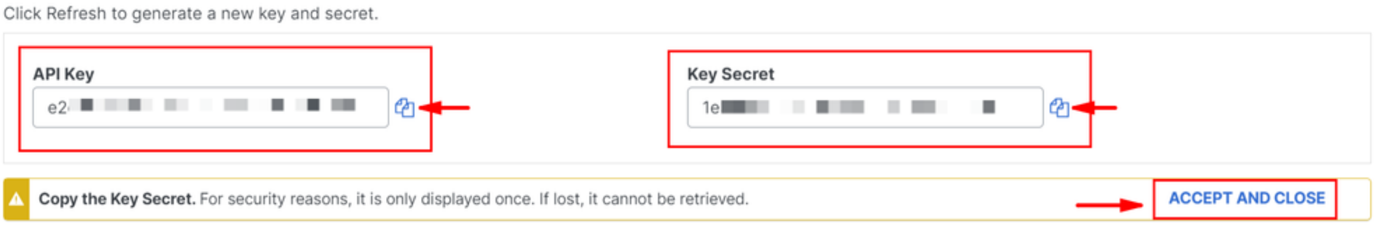
2 selected — Remove All

| Scope | | |
|---|---|---|
| Policies / Destination Lists | Read / Write | ✕ |
| Policies / Destinations | Read / Write | ✕ |

Expiry Date
- ● Never expire
- ○ Expire on May 21 2024

*Create your API Key 4*

- Copy the API Keyand the **Key Secret** and then click on ACCEPT AND CLOSE



Click Refresh to generate a new key and secret.

API Key: e2[redacted]

Key Secret: 1e[redacted]

**Copy the Key Secret.** For security reasons, it is only displayed once. If lost, it cannot be retrieved.

*Create your API Key 5*

**Note**: There is only one opportunity to copy your API secret. Secure Access does not save your API secret and you cannot retrieve it after its initial creation.

## 2.Generate an API Access Token

In order to generate the API Access Token, make a Token Authorization Request:

**Token Authorization Request**

Use the Secure Access API credentials that you created for your organization to generate an API access token.

- In the curl sample, substitute your Secure Access API key and secret

```
curl --user key:secret --request POST --url https://api.sse.cisco.com/auth/v2/token -H Content-Type: ap
```

- Copy and save the generated Bearer API Token

**Note**: A Secure Access OAuth 2.0 access token expires in one hour (3600 seconds). It is recommend that you do not refresh an access token until the token is nearly expired.

## 3.Manage Destination Lists

There are multiple ways to manage destination lists which include:

**Get all Destination Lists**

Open windows command prompt or Mac terminal to run the command:

```
curl -L --location-trusted --request GET --url https://api.sse.cisco.com/policies/v2/destinationlists -
```

Snippet from sample output:

```
{"id":23456789,"organizationId":1234567,"access":"none","isGlobal":false,"name":" Test Block list","thi
{"destinationCount":2,"domainCount":2,"urlCount":0,"ipv4Count":0,"applicationCount":0}
```

Make a note of the **destinationListId** which is listed under "**id**" field of the output which is used further for GET, POST or DELETE requests specific to this destination list.

### Get all destinations within a Destination List

- Get the destinationListId using this earlier mention step, Get all Destination Lists

Open windows command prompt or Mac terminal to run the command:

```
curl -L --location-trusted --request GET --url https://api.sse.cisco.com/policies/v2/destinationlists/d
```

Sample Output:

```
{"status":{"code":200,"text":"OK"},"meta":{"page":1,"limit":100,"total":3},"data":
[
{"id":"415214","destination":"cisco.com","type":"domain","comment":null,"createdAt":"2024-02-20 09:15:4
]}
```

### Create a new Destination List

Open windows command prompt or Mac terminal to run the command:

```
curl -L --location-trusted --request POST --url https://api.sse.cisco.com/policies/v2/destinationlists
```

**Note**: Replace 'Destination List Name' with the desired name.

Sample Output:

```
{"id":23456789,"organizationId":1234567,"access":"none","isGlobal":false,"name":"API List 1","thirdpart
```

### Add destinations to a Destination List

- Get the destinationListId using this earlier mention step, Get all Destination Lists

Open windows command prompt or Mac terminal to run the command:

```
curl -L --location-trusted --request POST --url https://api.sse.cisco.com/policies/v2/destinationlists/
```

Sample Output:

```
{"status":{"code":200,"text":"OK"},"data":{"id":17804929,"organizationId":1234567,"access":"none","isGl
{"destinationCount":3}}}
```

### Delete a Destination List

- Get the destinationListId using this earlier mention step, Get all Destination Lists

Open windows command prompt or Mac terminal to run the command:

```
curl -L --location-trusted --request DELETE --url https://api.sse.cisco.com/policies/v2/destinationlist
```

Sample Output:

```
{"status":{"code":200,"text":"OK"},"data":[]}
```

### Delete destinations from a Destination List

- Get the destinationListId using this earlier mention step, Get all Destination Lists
- Get the **id** of the particular destination within the list which needs to be deleted using this earlier mentioned step, Get all destinations within a destination list

Open windows command prompt or Mac terminal to run the command:

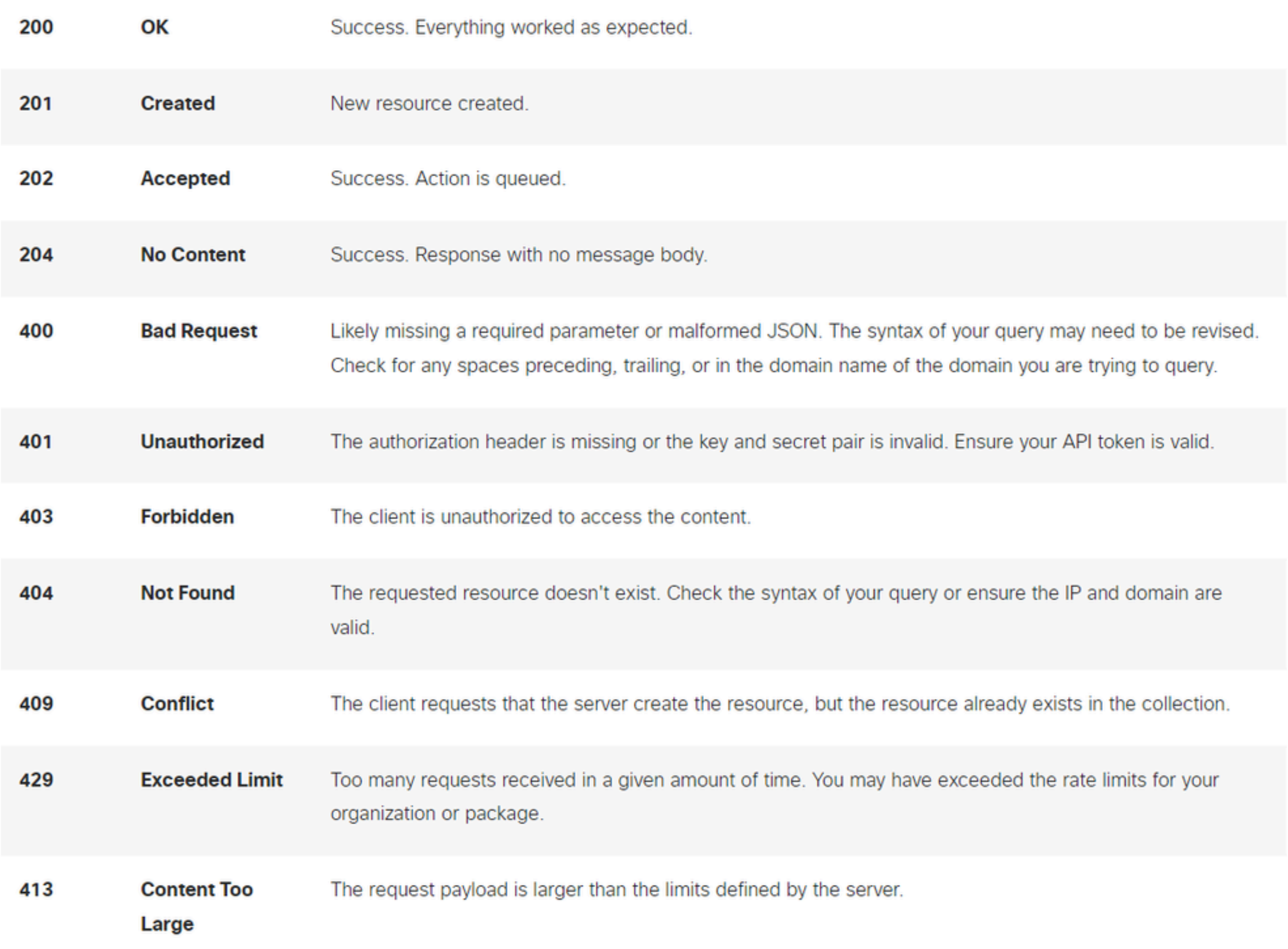
```
curl -L --location-trusted --request DELETE --url https://api.sse.cisco.com/policies/v2/destinationlist
```

Sample Output:

```
{"status":{"code":200,"text":"OK"},"data":{"id":17804929,"organizationId":1234567,"access":"none","isGl
```

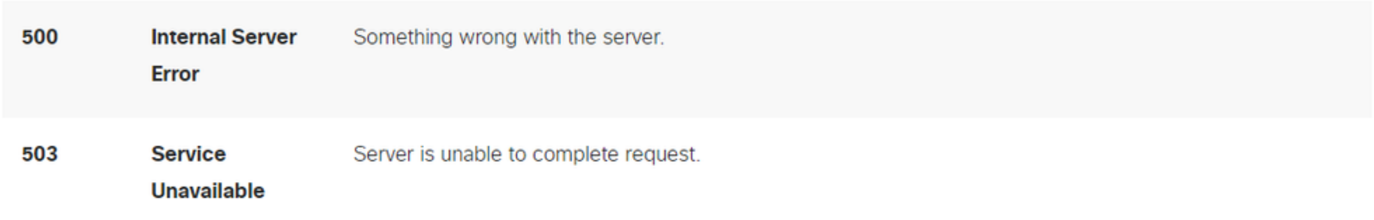
## Troubleshoot

The Secure Access API endpoints use HTTP response codes to indicate success or failure of an API request. In general, codes in the 2xx range indicate success, codes in the 4xx range indicate an error that resulted from the provided information, and codes in the 5xx range indicate server errors. The approach to resolve the issue would depend on the response code that is received:



| | | |
|---|---|---|
| **200** | **OK** | Success. Everything worked as expected. |
| **201** | **Created** | New resource created. |
| **202** | **Accepted** | Success. Action is queued. |
| **204** | **No Content** | Success. Response with no message body. |
| **400** | **Bad Request** | Likely missing a required parameter or malformed JSON. The syntax of your query may need to be revised. Check for any spaces preceding, trailing, or in the domain name of the domain you are trying to query. |
| **401** | **Unauthorized** | The authorization header is missing or the key and secret pair is invalid. Ensure your API token is valid. |
| **403** | **Forbidden** | The client is unauthorized to access the content. |
| **404** | **Not Found** | The requested resource doesn't exist. Check the syntax of your query or ensure the IP and domain are valid. |
| **409** | **Conflict** | The client requests that the server create the resource, but the resource already exists in the collection. |
| **429** | **Exceeded Limit** | Too many requests received in a given amount of time. You may have exceeded the rate limits for your organization or package. |
| **413** | **Content Too Large** | The request payload is larger than the limits defined by the server. |

*REST API - Response codes 1*



| | | |
|---|---|---|
| **500** | **Internal Server Error** | Something wrong with the server. |
| **503** | **Service Unavailable** | Server is unable to complete request. |

*REST API - Response codes 2*

Additionally while troubleshooting API related errors or problems, here are the Rate Limits to be aware of:

- [Secure Access API Limits]

# Related Information

- [Cisco Secure Access User Guide]
- [Cisco Technical Support and Downloads]
- [Add Secure Access API Keys]
- [Developers User Guide]