

Disable User API Access

Learn how to restrict API access for specific users in your Vultr account for enhanced security management.

Contents

01	Introduction	3
02	Vultr Customer Portal	3
03	Vultr API	3
04	Vultr CLI	4

How to Disable Vultr API Access for Users

Introduction

Disabling Application Programming Interface (API) access restricts users from accessing the Vultr account programmatically. This restriction applies to all linked API clients, such as the Linux cURL command, Vultr CLI, and modern programming language libraries.

Follow this guide to disable API access for users using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Select the user from the list and click the **Edit User** icon.
3. Click **Disable API** under **User API Key**.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) and note the target user ID.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users" \  
  -X GET \  
  -H "Authorization: Bearer ${VULTR_API_KEY}"
```

2. Send a `PATCH` request to the [Update User endpoint](#) and specify the user ID to disable API access for the target user.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}" \  
  -X PATCH \  
  -H "Authorization: Bearer ${VULTR_API_KEY}" \  
  -H "Content-Type: application/json" \  
  --data '{  
    "api_enabled" : false  
  }'
```

Visit the [Update User endpoint](#) to view additional attributes to add to your request.

Vultr CLI

1. List all users and note the target user ID.

CONSOLE

```
$ vultr-cli users list
```

2. Disable API access for the target user by specifying the user ID.

CONSOLE

```
$ vultr-cli users update <user-id> \  
  --api-enabled="false"
```

Run `vultr-cli users update --help` to view all options.



VULTR

