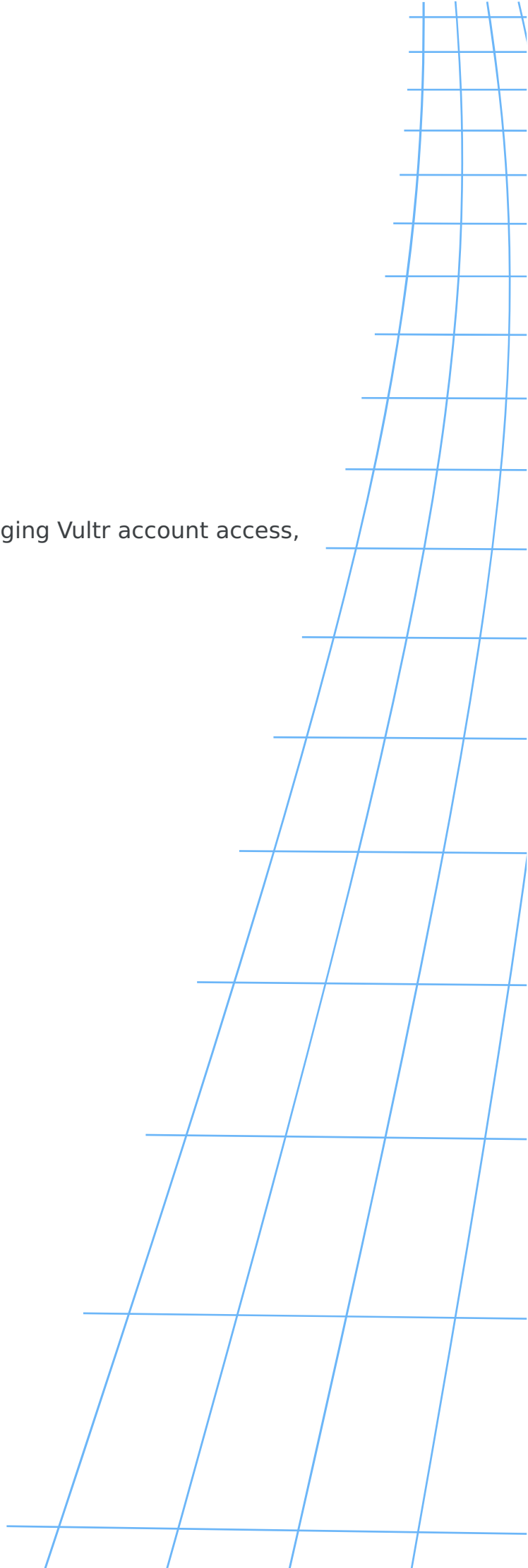


Other

Administrative and security settings for managing Vultr account access, compliance, and authentication.



Contents

01	Users	4
	Manage Users	6
	Add User	8
	Delete Users	13
	Update Users	17
	Add Service User	22
	FAQ	26
	API Access	29
	Disable User API Access	31
	Enable User API Access	35
	Manage API Access Controls	39
	Regenerate User API Key	42
	IP Address Whitelisting	45
	List IP Addresses	47
	Add IP Addresses	50
	Removed IP Addresses	54
	Single Sign-On	58
	Google Accounts	60
	Microsoft Entra ID	72
	Okta	88
	OneLogin	99
	FAQ	109
02	Compliance	112
	Data Center Compliance Artifacts	114
	Vultr Compliance Artifacts	118
	FAQ	122
03	SSH Keys	126
	Add SSH Keys	128
	Delete SSH Keys	133
	Update SSH Keys	138
	FAQ	143

04	API	147
	Disable API Access	149
	Enable API Access	152
	Manage API Access Control	155
	FAQ	158
	Current User API Key Management	161
	Create New API Key	163
	Delete API Key	167
	List API Key	171
	Rotate API Key	174
	Other Users API Key Management	178
	Delete API Key	180
	Create New API Key	184
	List API Key	188
	Rotate API Key	192
05	Sub Accounts	197
	Create a Sub Account	199
	Monitor Sub Accounts	204
	Activate a Sub Account	208
	FAQ	213
06	Manage Notifications	219
07	Account Logs	223

Users

Manage user accounts and control access permissions to your Vultr resources.

Contents

01	Manage Users	6
	Add User	8
	Delete Users	13
	Update Users	17
	Add Service User	22
	FAQ	26
	API Access	29
	Disable User API Access	31
	Enable User API Access	35
	Manage API Access Controls	39
	Regenerate User API Key	42
	IP Address Whitelisting	45
	List IP Addresses	47
	Add IP Addresses	50
	Removed IP Addresses	54
02	Single Sign-On	58
	Google Accounts	60
	Microsoft Entra ID	72
	Okta	88
	OneLogin	99
	FAQ	109

Manage Users

Learn how to create, manage, and control user accounts and permissions within your Vultr account.

Contents

01	Add User	8
02	Delete Users	13
03	Update Users	17
04	Add Service User	22
05	FAQ	26
06	API Access	29
	Disable User API Access	31
	Enable User API Access	35
	Manage API Access Controls	39
	Regenerate User API Key	42
	IP Address Whitelisting	45
	List IP Addresses	47
	Add IP Addresses	50
	Removed IP Addresses	54

Add User

Learn how to add additional users to your Vultr account with custom permissions and access controls

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Add Vultr Account Users

Introduction

Vultr allows you to create individual user accounts within your organization's account, enabling team members to access services using their own login credentials. You can assign specific permissions to each user, controlling which actions they are authorized to perform and which resources they can access. Implementing user accounts with defined roles and access levels helps enforce organizational security policies and ensures proper management of your Vultr services.

Follow this guide to add new users using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Click **Add New User**.
3. Enter the user's **First Name**, **Last Name** and **Email** address.
4. Customize the user permissions as required and click **Add User**.
5. An email will be sent to the provided address with a link to set the password for the user account.
6. After the user is created, select their profile from the users list to retrieve the API key.

Vultr API

1. Send a `POST` request to the [Create User endpoint](#) to create a user.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users" \  
-X POST \  
-H "Authorization: Bearer ${VULTR_API_KEY}" \  
-H "Content-Type: application/json" \  
--data '{  
  "email" : "user@example.com",  
  "first_name" : "Example",  
  "last_name" : "User",  
  "password" : "example-password",  
  "api_enabled" : true,  
  "acls" : [  
    "manage_users",  
    "subscriptions_view",  
    "subscriptions",  
    "provisioning",  
    "billing",  
    "support",  
    "abuse",  
    "dns",  
    "upgrade",  
    "objstore",  
    "loadbalancer"  
  ]  
'
```

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

2. Send a `GET` request to the [Get Users endpoint](#) to view all users.

CONSOLE

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

Vultr CLI

1. Create a new user by specifying the name, email, password, and user access control settings.

CONSOLE

```
$ vultr-cli users create --email="vultrcli@vultr.com" --  
name="Vultr-cli" \  
  --password="Password123" --api-enabled="true" --  
acl="manage_users,billing"
```

Run `vultr-cli users create --help` to view additional available options.

2. List all users.

CONSOLE

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

Delete Users

Learn how to remove users from your Vultr account to manage access permissions and team membership.



Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Delete Vultr Account Users

Introduction

Deleting a user removes the user's sign-in information and permissions from your Vultr account. After removing an account, users can no longer log in or access any resources. This action is important if a user has left your organization.

Follow this guide to delete users using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Identify the user from the list.
3. Click the **Delete User** icon to remove the user.
4. Click **Delete User** in the confirmation prompt to permanently delete the user.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to view all users 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 `DELETE` request to the [Delete User endpoint](#) and specify the user ID to delete the target user.

CONSOLE

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

Vultr CLI

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

CONSOLE

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

2. Delete the target user by specifying the user ID.

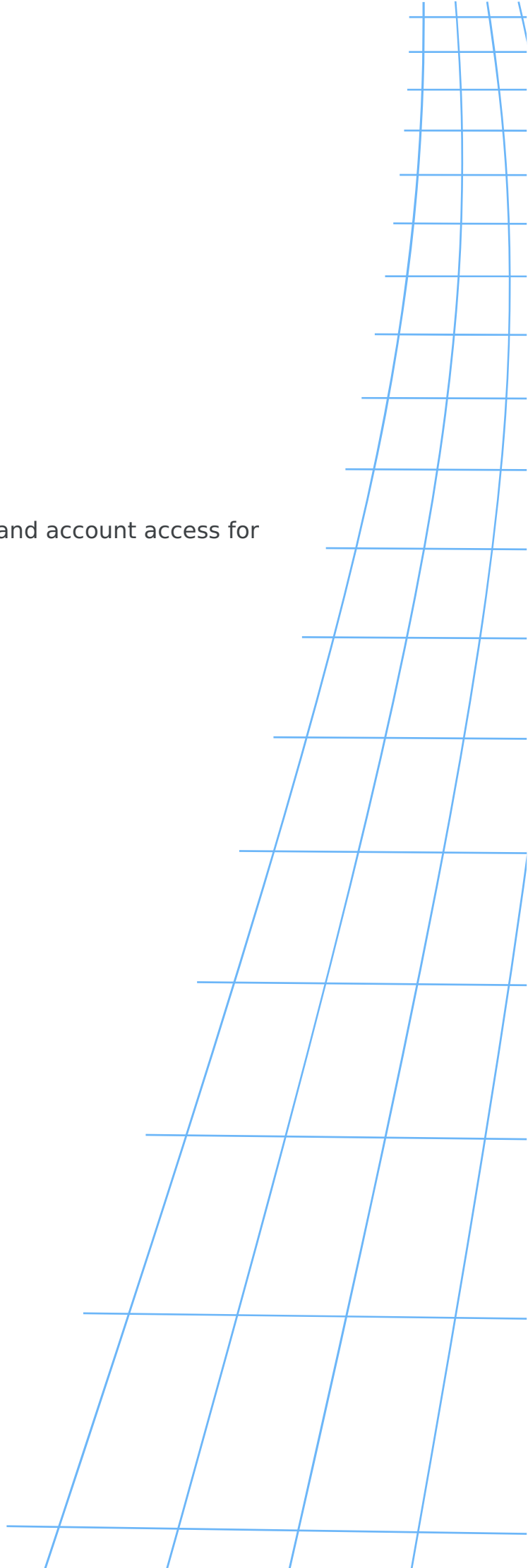
CONSOLE

```
$ vultr-cli users delete <user-id>
```

Run `vultr-cli users delete --help` to view additional available options.

Update Users

Learn how to modify user permissions, roles, and account access for team members on your Vultr account



Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Update Vultr Account Users

Introduction

Updating Vultr user account details involves changing their names, email, password, and permissions. Changing the information is necessary if the user's password is compromised or if you want to limit or add more permissions to their account.

Follow this guide to update user details using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Identify the user from the list.
3. Click the **Edit User** icon to edit the user details.
4. Update the user's details and click **Update Profile**.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to view all users 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 update the target user details.

```
CONSOLE

$ curl "https://api.vultr.com/v2/users/{user-id}" \
  -X PATCH \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
  --data '{
    "name" : "{new_user_name}",
    "email" : "{new_user_email_address}",
    "password" : "{new_user_password}",
    "api_enabled" : true,
    "acls" : [
      "manage_users",
      "subscriptions_view",
      "subscriptions",
      "provisioning",
      "billing",
      "support",
      "abuse",
      "dns",
      "upgrade",
      "objstore",
      "loadbalancer"
    ]
  }'
```

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. Update the target user details by specifying the user ID.

CONSOLE

```
$ vultr-cli users update <user-id> \  
--name="<new_user_name>" \  
--email="<new_user_email_address>" \  
--password="<new_user_password>" \  
--api-enabled true \  
--  
acl="manage_users,subscriptions_view,subscriptions,provisioning,billing"
```

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

Add Service User

A guide for adding and managing additional user accounts with specific permissions to your Vultr account

Contents

01 Introduction	10
-----------------	----

How to Add Vultr Service Account Users

Introduction

Service users on Vultr are dedicated, API-only accounts intended for secure, automated access to cloud resources. Unlike standard users, service users are not permitted to log into the web portal and do not support OAuth, SSO, or password resets. Authentication is exclusively handled via a one-time API key, which cannot be retrieved after creation—making it essential to store securely.

Follow this guide to add new users using the Vultr API.

1. Send a `POST` request to [Create User endpoint](#) to create a new service user for your Vultr account.

CONSOLE

```
$ curl -X POST "<https://api.vultr.com/v2/users>" \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
  -d '{
    "email": "automation@company.com",
    "first_name": "Automation",
    "last_name": "Bot",
    "password": "SecurePassword123!",
    "api_enabled": true,
    "service_user": true,
    "acls": ["subscriptions_view", "provisioning", "dns"]
  }'
```

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

 Note

The API key will be displayed only once after generation. Please store it securely, as it cannot be retrieved later.

2. Send a `GET` request to the [Get Users endpoint](#) to confirm the service user creation.

CONSOLE

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

FAQ

A comprehensive resource providing answers to common questions about Vultr's services, features, and platform usage.

Contents

01	Introduction	10
02	Does Vultr support multi-user logins?	28
03	Can I create new users using the Vultr API?	28
04	Can additional user accounts manage other users?	28

Frequently Asked Questions (FAQs) for Vultr Users

Introduction

These are the frequently asked questions for Vultr Users.

Does Vultr support multi-user logins?

Vultr allows you to create new users to share account resource management without sharing your master login credentials. You can set up users with limited access to portions of your Vultr account including the ability to administer servers, deploy instances, manage billing, open support tickets, and more.

Can I create new users using the Vultr API?

You can create, update, and delete Vultr account users using the Vultr API and Vultr CLI.

Can additional user accounts manage other users?

Yes. if you enable **Manage Users** permission for a user, the user can add or edit other user accounts. However, users with the **Manage Users** permission enabled can access all root user functions. For further granularity, set this permission to off and toggle the individual permissions.

API Access

Documentation for managing API access controls, permissions, and security settings for Vultr's API infrastructure.

Contents

01	Disable User API Access	31
02	Enable User API Access	35
03	Manage API Access Controls	39
04	Regenerate User API Key	42
05	IP Address Whitelisting	45
	List IP Addresses	47
	Add IP Addresses	50
	Removed IP Addresses	54

Disable User API Access

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

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

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.

Enable User API Access

A guide explaining how to grant API access permissions to sub-users in your Vultr account

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Enable Vultr API Access for Users

Introduction

Application Programming Interface (API) access allows users to access the Vultr account programmatically. The Vultr API works with various clients, such as the Linux cURL command, Vultr CLI, and modern programming language libraries.

Follow this guide to enable 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 **Enable 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 enable 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" : true  
  }'
```

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. Enable API access for the target user by specifying the user ID.

CONSOLE

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

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

Manage API Access Controls

Learn how to configure and manage API access permissions for users on your Vultr account.

Contents

01 Introduction	10
-----------------	----

How to Manage Vultr API Access Control for Users

Introduction

Access control enforces permissions for users, systems, and services that interact with the Vultr Application Programming Interface (API). This mechanism enhances security by allowing or blocking a range of IP addresses that can access the API.

Follow this guide to manage API access control for users using the 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. Enter the IP addresses you want to permit and click **Add**.
4. Select an IP from the list and click **Remove** to delete the entry from the list.

Regenerate User API Key

Learn how to regenerate a users API key in the Vultr control panel for enhanced account security.

Contents

01 Introduction	10
-----------------	----

How to Regenerate Vultr API Key for Users

Introduction

A Vultr account Application Programming Interface (API) key authenticates requests to the Vultr API. You should regenerate the Vultr account API key periodically to reduce the risk of unauthorized access or if you suspect an authorized person has access to the key.

Follow this guide to regenerate API keys for users using the 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 the **Generate new API key** icon to generate a new key under the **User API Key** section.

IP Address Whitelisting

Manage access to your Vultr account by controlling which IP addresses can log in to the control panel.

Contents

01	List IP Addresses	47
02	Add IP Addresses	50
03	Removed IP Addresses	54

List IP Addresses

A guide explaining how to retrieve the IP whitelist associated with a specific user account on Vultr



Contents

01 Introduction	10
-----------------	----

How to Get the IP Whitelist for a User

Introduction

Retrieving the IP whitelist for a user allows authorized administrators to review which public IP addresses are permitted to access the Vultr account. This operation is restricted to root users or those with the `manage_users` permission, ensuring that only privileged roles can manage access controls. The whitelist supports only public IPs—private addresses are not accepted—and enforces valid subnet sizes: `/8` to `/32` for IPv4 and `/20` to `/128` for IPv6. Additionally, the API is idempotent, meaning adding the same IP multiple times has no adverse effect, which simplifies automation and scripting.

Follow this guide to get the IP whitelist for a user using the Vultr API.

1. Send a `GET` request to the [Get Users endpoint](#) to view all users and note the user id for the target user.

CONSOLE

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

2. Send a `GET` request to the [List User IP Whitelist endpoint](#) to list all whitelisted IP addresses for a user's whitelist.

CONSOLE

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

Add IP Addresses

Learn how to add IP addresses to your accounts whitelist for secure access management

Contents

01 Introduction	10
-----------------	----

How to Add IP Addresses to a User's Whitelist

Introduction

Adding an IP address or subnet to a user's whitelist allows authorized administrators to define which public IPs are permitted to access the Vultr platform on that user's behalf. This action is restricted to root users or those granted the `manage_users` permission, maintaining strict access control. Only public IP addresses are allowed, with valid subnet ranges of `/8` to `/32` for IPv4 and `/20` to `/128` for IPv6. The operation is idempotent—repeated additions of the same IP or subnet do not result in errors, making it safe for use in automated access management scripts.

Follow this guide to add IP addresses for a user's whitelist using the Vultr API.

1. Send a `GET` request to the [Get Users endpoint](#) to view all users and note the user id for the target user.

CONSOLE

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

2. Send a `POST` request to the [Add IP to User Whitelist endpoint](#) to add IP addresses in the user's whitelist.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/ip-  
whitelist" \  
-X POST \  
-H "Authorization: Bearer ${VULTR_API_KEY}" \  
-H "Content-Type: application/json" \  

```

```
--data '{
  "subnet" : "8.8.8.0",
  "subnet_size" : 24
}'
```

3. Send a `GET` request to the [List User IP Whitelist endpoint](#) to list confirm the addition of IP addresses.

CONSOLE

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

Removed IP Addresses

A guide explaining how to remove IP addresses from a users whitelist in the Vultr control panel

Contents

01 Introduction	10
-----------------	----

How to Remove IP Addresses from a User's Whitelist

Introduction

Removing an IP address or subnet from a user's whitelist allows authorized administrators to revoke access for specific public IPs. This action helps maintain tight security controls by ensuring only trusted sources can interact with the Vultr account. Access to this endpoint is restricted to root users or those with the `manage_users` permission. Only public IPs can be removed—private IP addresses are not supported, and valid subnet sizes must be respected. This operation enables precise control over access policies, supporting secure and flexible user management.

Follow this guide to remove IP addresses from a user's whitelist using the Vultr API.

1. Send a `GET` request to the [Get Users endpoint](#) to view all users and note the user id for the target user.

CONSOLE

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

2. Send a `DELETE` request to the [Remove IP from User Whitelist endpoint](#) to remove IP addresses from a user's IP whitelist.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/ip-  
whitelist" \  
-X DELETE \  
-H "Authorization: Bearer ${VULTR_API_KEY}" \  
"
```

```
-H "Content-Type: application/json" \  
--data '{  
  "subnet" : "8.8.8.0",  
  "subnet_size" : 24  
'
```

3. Send a `GET` request to the [List User IP Whitelist endpoint](#) to list confirm the removal of IP addresses.

CONSOLE

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

Single Sign-On

Securely access your Vultr account using third-party identity providers through Single Sign-On (SSO) authentication.

Contents

01	Google Accounts	60
02	Microsoft Entra ID	72
03	Okta	88
04	OneLogin	99
05	FAQ	109

Google Accounts

A guide for setting up Vultrs Single Sign-On integration with Google accounts to streamline authentication across services.

Contents

01	Introduction	10
02	Set up Google Account Integration	62
03	Set up Vultr Single Sign-On	69

How to Integrate Vultr Single Sign-On with Google Accounts

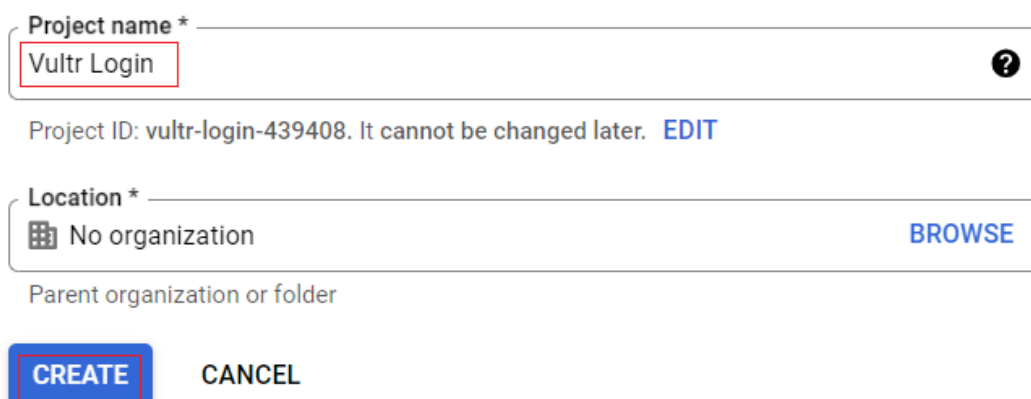
Introduction

Single Sign-On (SSO) is a service that lets you authenticate to multiple websites and applications using one set of login credentials. SSO eliminates the need for multiple logins, hence providing a better user experience. Vultr SSO integrates well with Google SSO service, a user integration platform that allows users to sign in to multiple applications.

Follow this guide to integrate Vultr SSO with Google using the Vultr Customer Portal.

Set up Google Account Integration

1. Log in to your [Google API Console account](#).
2. Create a Google Cloud project, such as `Vultr Login`.



The screenshot shows a Google Cloud Project creation form. The 'Project name' field is filled with 'Vultr Login' and has a red border. Below it, the 'Project ID' is 'vultr-login-439408'. The 'Location' field is set to 'No organization' and has a 'BROWSE' button. At the bottom, there are 'CREATE' and 'CANCEL' buttons.

Project name *
Vultr Login ?

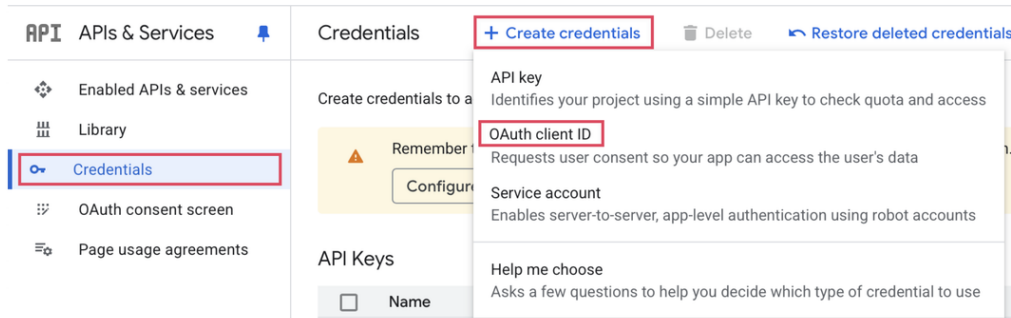
Project ID: vultr-login-439408. It cannot be changed later. [EDIT](#)

Location *
No organization BROWSE

Parent organization or folder

CREATE CANCEL


3. Navigate to the **Credentials** under **APIs & Services**. Then, click **Create Credentials** and select **OAuth client ID**



4. Click **Configure consent screen**.

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.

 To create an OAuth client ID, you must first configure your consent screen

[Configure consent screen](#)

5. Click **Get started** to configure your application.



Google Auth Platform not configured yet
Get started to configure your application's identity and manage credentials
for calling Google APIs and Sign-in with Google. [Learn more](#)

[Get started](#)

6. Name your app, such as **Vultr Login**, and enter the support email. Click **Next**.

1 App Information

App name *
Vultr Login
The name of the app asking for consent

User support email *
admin@example.com
For users to contact you with questions about their consent. [Learn more](#)

Next

2 Audience

3 Contact Information

4 Finish

Create Cancel

7. Select the target audience and click **Next**.

✓ App Information

2 Audience

Internal ⓘ
Only available to users within your organization. You will not need to submit your app for verification. [Learn more about user type](#)

External ⓘ
Available to any test user with a Google Account. Your app will start in testing mode and will only be available to users you add to the list of test users. Once your app is ready to push to production, you may need to verify your app. [Learn more about user type](#)

Next

3 Contact Information

4 Finish

Create Cancel

8. Enter the contact information and click **Next**.

The screenshot shows a vertical progress bar on the left with four steps: 1. App Information (checked), 2. Audience (checked), 3. Contact Information (active), and 4. Finish. The active step is highlighted with a blue circle and a vertical line. The 'Contact Information' section contains a text input field labeled 'Email addresses *' with the value 'admin@example.com' and a close button. Below the input field is a note: 'These email addresses are for Google to notify you about any changes to your project.' A 'Next' button is highlighted with a red box. At the bottom, there are 'Create' and 'Cancel' buttons.

9. Check the **I agree to the Google API Services: User Data Policy** box, then click **Continue**.

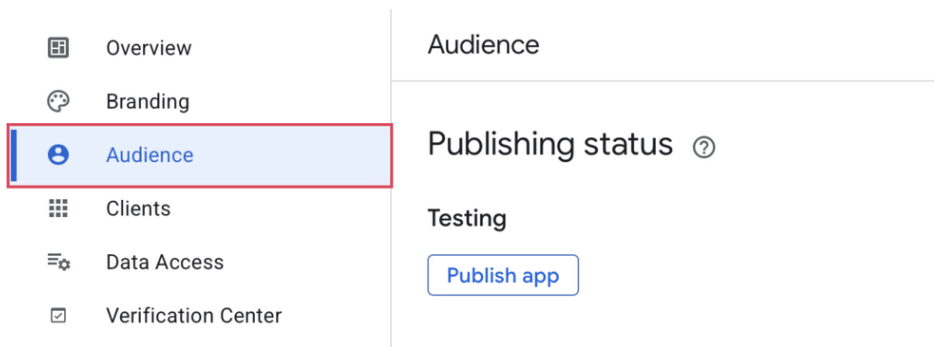
The screenshot shows the same vertical progress bar as in the previous step, but now step 4, 'Finish', is active and highlighted with a blue circle and a vertical line. The 'Finish' section contains a checkbox that is checked, with the text 'I agree to the [Google API Services: User Data Policy](#)'. A 'Continue' button is highlighted with a red box. At the bottom, there are 'Create' and 'Cancel' buttons.

10. After completing the required fields, click **Create**.

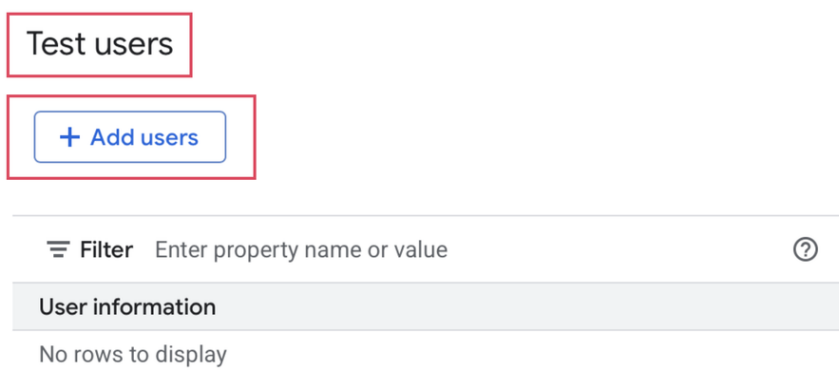
- ✓ App Information
- |
- ✓ Audience
- |
- ✓ Contact Information
- |
- ✓ Finish

[Create](#) [Cancel](#)

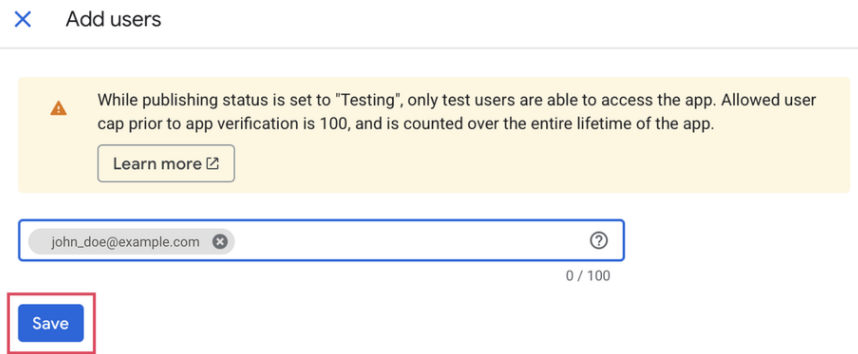
11. Navigate to **Audience**.



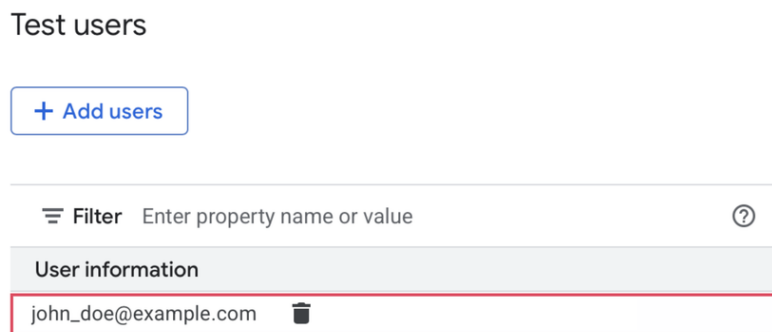
12. Scroll down to **Test users**, and click **Add users**.



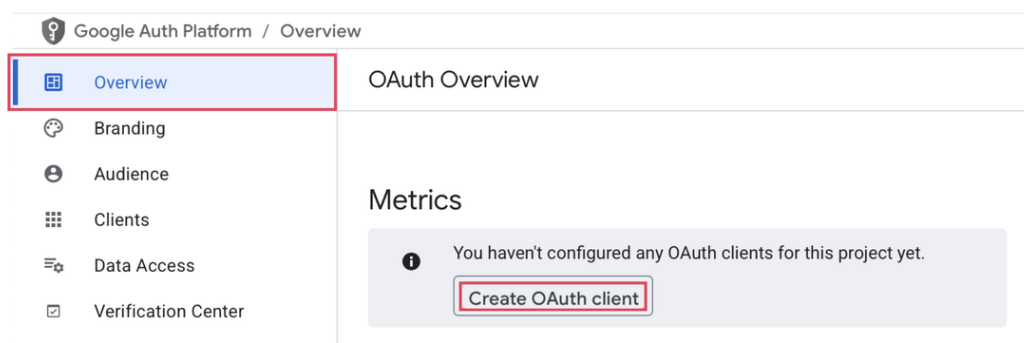
13. Enter the user's email address and click **Save**.



14. Verify the added Test user's email address.



15. Navigate to **Overview** and click **Create OAuth client** to generate and configure OAuth credentials for your project.



16. Choose **Web Application** as the application type. You will be prompted to fill in several fields.

← Create OAuth client ID

A client ID is used to identify a single app to Google's OAuth servers. If your app runs on multiple platforms, each will need its own client ID. See [Setting up OAuth 2.0](#) for more information. [Learn more](#) about OAuth client types.



17. Enter `https://my.vultr.com` under **Authorized JavaScript origins**. Then, enter `https://my.vultr.com/` and `https://my.vultr.com/openid/` under **Authorized redirect URIs** and click **Create**.

Name *
Web client 1

The name of your OAuth 2.0 client. This name is only used to identify the client in the console and will not be shown to end users.

i The domains of the URIs you add below will be automatically added to your [OAuth consent screen](#) as [authorized domains](#).

Authorized JavaScript origins ⓘ
For use with requests from a browser

URIs 1 *
`https://my.vultr.com`

+ Add URI

Authorized redirect URIs ⓘ
For use with requests from a web server

URIs 1 *
`https://my.vultr.com/`

URIs 2 *
`https://my.vultr.com/openid/`

+ Add URI

Note: It may take 5 minutes to a few hours for settings to take effect

Create Cancel

18. Copy the **Client ID** and **Client Secret** in the next screen.

OAuth client created

The client ID and secret can always be accessed from Credentials in APIs & Services

i OAuth access is restricted to the [test users](#) listed on your [OAuth consent screen](#)

Client ID	15439 s.googleusercontent.com	
Client secret	ziNB8_CEQDZ47S03j0Q	
Creation date	October 23, 2024 at 9:15:03 AM GMT+3	
Status	Enabled	


DOWNLOAD JSON

[OK](#)

Set up Vultr Single Sign-On

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Click **Begin Setup** under **Single Sign-On**.

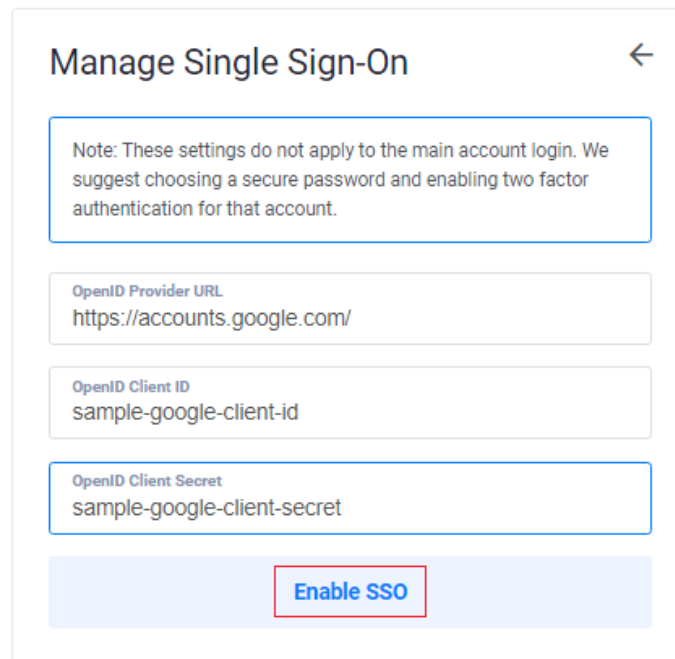
Single Sign-On



Vultr supports third party single sign-on via OpenID Connect. Once configured, all users on the account will need to sign in via OpenID. [Learn more](#).

[Begin Setup](#)

3. Enter the Google **Client ID**, **Client Secret**, and `https://accounts.google.com/` in the **OpenID Provider URL** and click **Enable SSO**.



Manage Single Sign-On

Note: These settings do not apply to the main account login. We suggest choosing a secure password and enabling two factor authentication for that account.

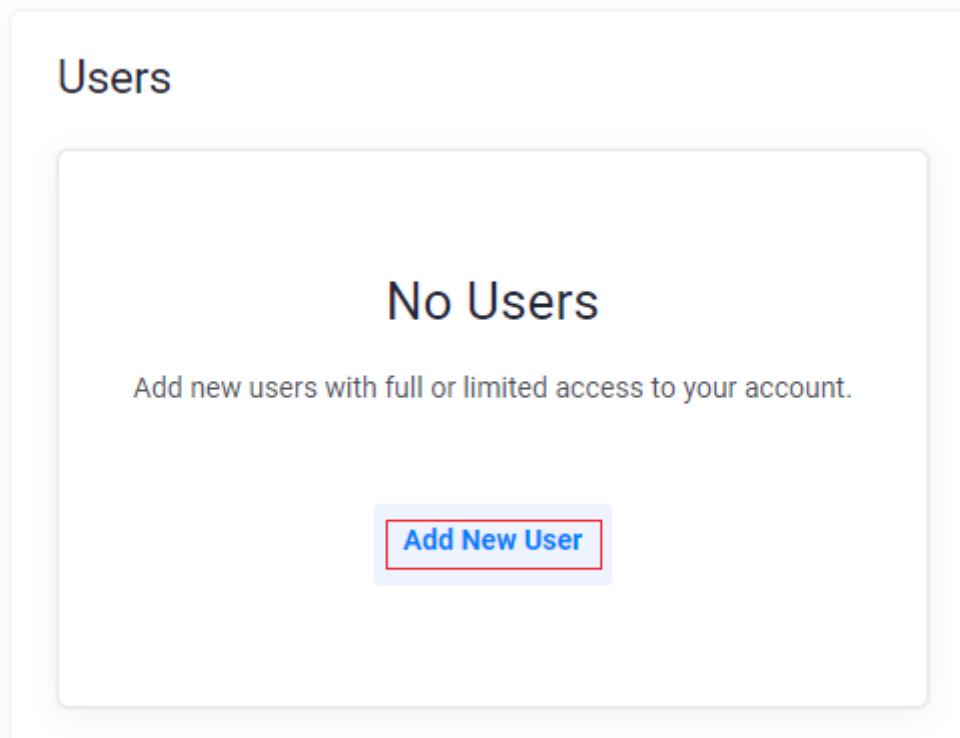
OpenID Provider URL
https://accounts.google.com/

OpenID Client ID
sample-google-client-id

OpenID Client Secret
sample-google-client-secret

Enable SSO

4. Click **Add New User** to create a new user account.



Users

No Users

Add new users with full or limited access to your account.

Add New User

5. Enter the user details, including the **Name** and **Email**. Then, customize the user permissions and click **Add User**.

This will create a new <https://my.vultr.com> log in with limited privileges to manage your account

Name	John Doe
Email	john_doe@example.com

Users will log in via SSO, passwords are not available.

- | | |
|--|--|
| Manage Users ? | <input type="checkbox"/> OFF |
| Manage Servers ? | <input checked="" type="checkbox"/> ON |
| Manage Vultr Kubernetes Engines ? | <input type="checkbox"/> OFF |
| Receive AUP/ToS Notifications ? | <input checked="" type="checkbox"/> ON |
| Receive Maintenance Notifications | <input type="checkbox"/> OFF |

Add User

- Use your Google account to log in to Vultr through the Vultr [SSO Login page](#).

Microsoft Entra ID

A guide for integrating Vultrs Single Sign-On functionality with Microsoft Entra ID to enable unified authentication credentials across services.

Contents

01	Introduction	10
02	Set up Microsoft Entra ID Integration	74
03	Set up Vultr Single Sign-On	69

How to Integrate Vultr Single Sign-On with Microsoft Entra ID

Introduction

Single Sign-On (SSO) is a service that lets you authenticate to multiple websites and applications using one set of login credentials. SSO eliminates the need for multiple logins, hence providing a better user experience. Vultr SSO integrates well with Microsoft Entra ID, a cloud-based identity and access management service.

Follow this guide to integrate Vultr SSO with Microsoft Entra ID using the Vultr Customer Portal.

Set up Microsoft Entra ID Integration

Create a Microsoft Entra ID Account User

1. Log in to your [Microsoft Azure account](#).
2. Select **Microsoft Entra ID** under **Azure Services**.

Azure services



Create a resource



Microsoft Entra ID



SQL databases



Virtual machines

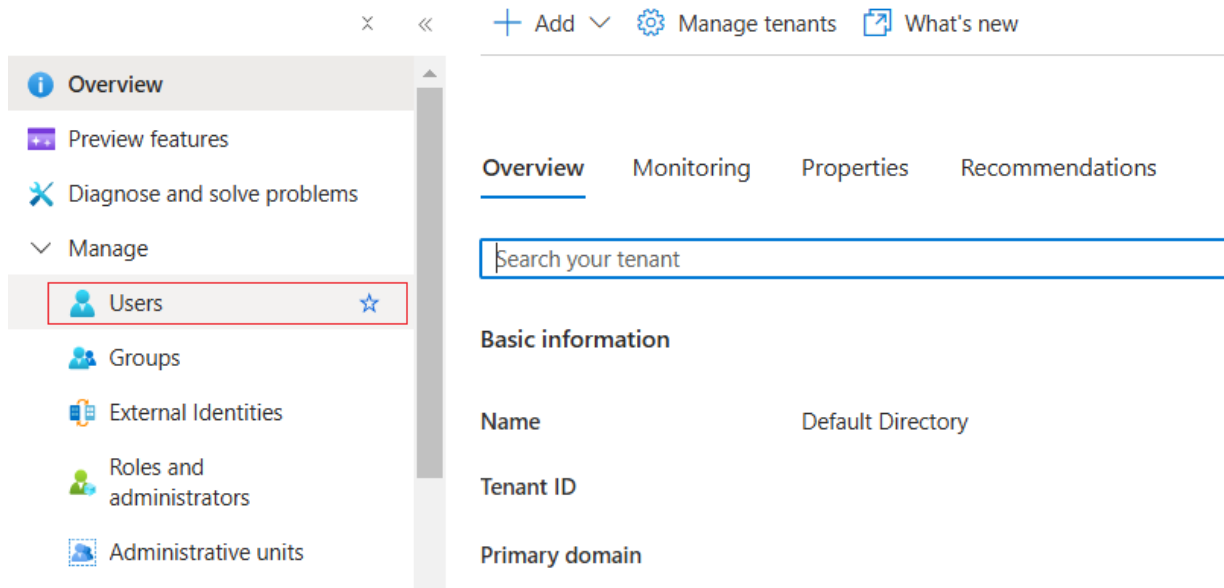


Quickstart Center

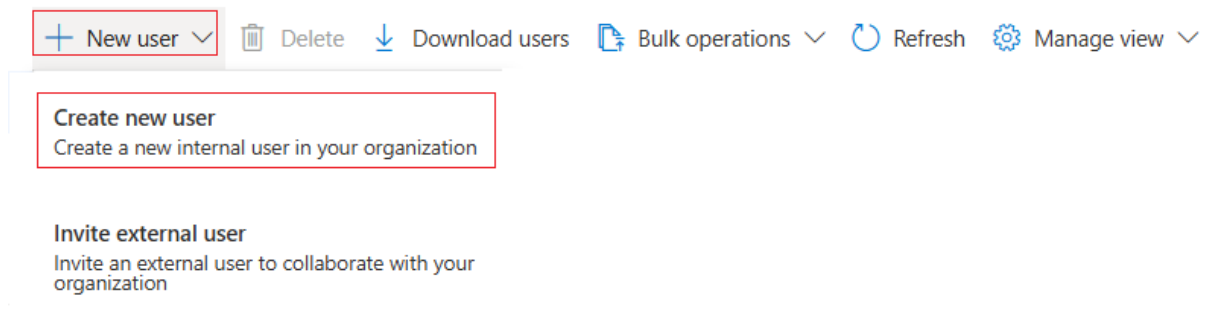


Azure AI services

3. Click **Users** under **Manage**.



4. Click **New user**, then select **Create new user**.



5. Enter the user details. Then, auto-generate and copy the user's password. After that, click **Review + create**.

Create new user ...

Create a new internal user in your organization

Basics Properties Assignments Review + create

Create a new user in your organization. This user will have a user name like alice@contoso.com. [Learn more](#)

Identity

User principal name *

john_doe @ francisndungu83gmail... 

Domain not listed? [Learn more](#)

Mail nickname *

john_doe

Derive from user principal name

Display name *

John Doe

Password *

.....  

Auto-generate password

Account enabled ⓘ

[Review + create](#)

[< Previous](#)

[Next: Properties >](#)

- Review the user's details and click **Create**. Copy the **User principal name**. You'll use the value as an email address to set up a new Vultr SSO user.

Create new user ...

Create a new internal user in your organization

Basics

User principal name

john_doe@example.onmicrosoft.com 


Display name

John Doe

Mail nickname

john_doe

Password

..... 

Account enabled

Yes

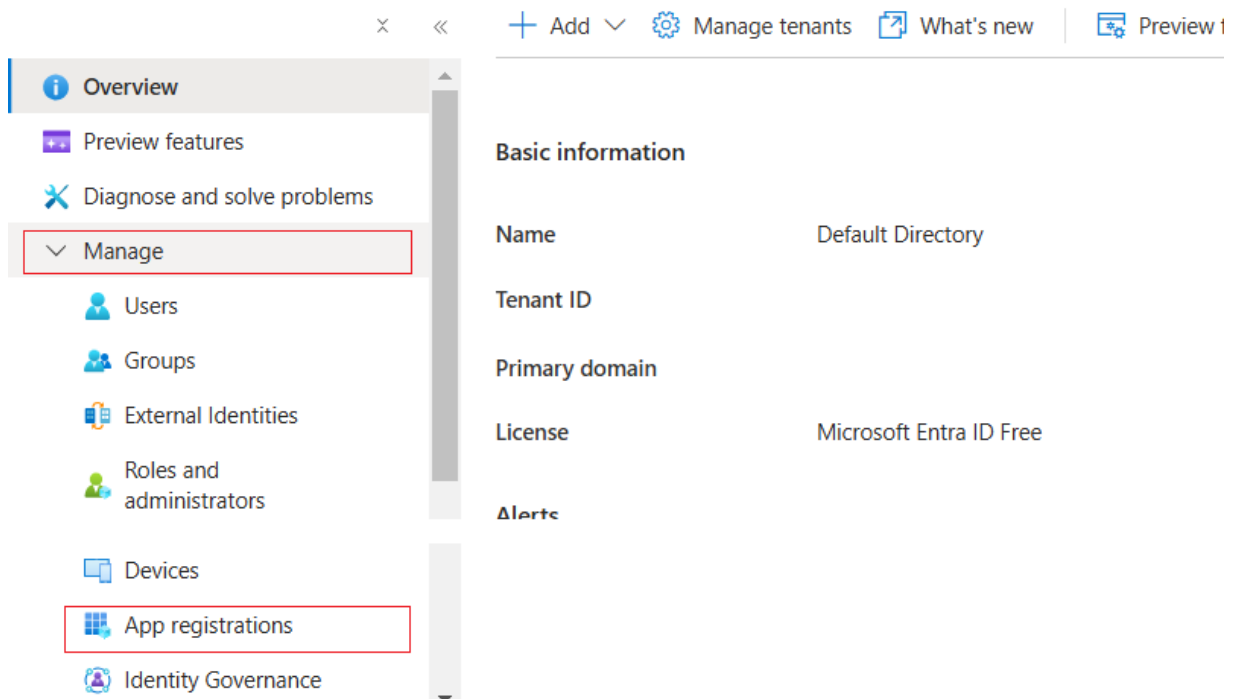
[Create](#)

[< Previous](#)

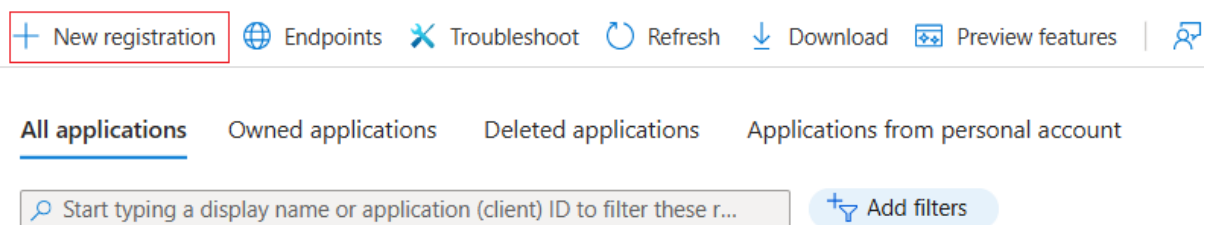
[Next >](#)

Create a Microsoft Entra ID Application

1. Select **App registrations** under **Manage**.



2. Click **New registration**.



3. Name your App, for instance, `Vultr ss0`. Then, select **Web** from the drop-down menu, set the **Redirect URI** to `https://my.vultr.com/openid/`, and click **Register**.

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

By proceeding, you agree to the [Microsoft Platform Policies](#)

4. Navigate to **Manage** and select **API permissions** in the new App page. Then, click **Add a permission**.

Manage

- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

i The "Admin consent required" column shows the default value for an organization. However organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admin all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission
✓ Grant admin consent for Default Directory

API / Permissions name	Type	Description
▼ Microsoft Graph (1)		
User.Read	Delegated	Sign in and read user profile


5. Click **Microsoft Graph**.

Request API permissions


Select an API

Microsoft APIs APIs my organization uses My APIs


Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Service Management**

Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

6. Click **Delegated permissions**.

Request API permissions

[< All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

7. Search and set the following permissions in the search box.

- **Directory:** Set `Directory.Read.All` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<input checked="" type="checkbox"/> Directory (1)	
<input type="checkbox"/> Directory.AccessAsUser.All ⓘ Access directory as the signed in user	Yes
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes
<input type="checkbox"/> Directory.ReadWrite.All ⓘ Read and write directory data	Yes
<input type="checkbox"/> DirectoryRecommendations	

- **Group:** Set `Group.Read.All` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<input type="checkbox"/> Group-Conversation	
<input checked="" type="checkbox"/> Group (1)	
<input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups	Yes
<input type="checkbox"/> Group.ReadWrite.All ⓘ Read and write all groups	Yes

- **User:** Set `User.Read` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
> UserTimelineActivity	
<div style="background-color: #e6f2ff; padding: 2px;"> ✓ User (1) </div>	
<input type="checkbox"/> User.DeleteRestore.All ⓘ Delete and restore users	Yes
<input type="checkbox"/> User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/> User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/> User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/> User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/> User.Read ⓘ Sign in and read user profile	No
<input type="checkbox"/> User.Read.All ⓘ Read all users' full profiles	Yes

- **email:** Set `email` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<div style="background-color: #e6f2ff; padding: 2px;"> ✓ OpenId permissions (1) </div>	
<input checked="" type="checkbox"/> email ⓘ View users' email address	No

- **offline_access:** Set `offline_access` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>▼ OpenId permissions (1)</p>	
<input checked="" type="checkbox"/> offline_access ⓘ Maintain access to data you have given it access to	No

- **openid**: Set `openid` permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>▼ OpenId permissions (1)</p>	
<input checked="" type="checkbox"/> openid ⓘ Sign users in	No

- **profile**: Set `profile` permissions and click **Add permissions** to save all the permissions.

Select permissions expand all

i The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the value in your organization, or in organizations where this app will be used. [Learn more](#)

Permission	Admin consent required
<p>▼ OpenId permissions (1)</p>	
<input checked="" type="checkbox"/> profile ⓘ View users' basic profile	No

Add permissions

Discard

8. Click **Grant admin consent for Default Directory**.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission Grant admin consent for Default Directory

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	⚠ Not granted for Default ...
email	Delegated	View users' email address	No	...
Group.Read.All	Delegated	Read all groups	Yes	⚠ Not granted for Default ...
offline_access	Delegated	Maintain access to data you have given it access to	No	...
openid	Delegated	Sign users in	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...

9. Navigate to **Certificates & secrets** and click **New client secret**.

- Overview
- Quickstart
- Integration assistant
- Diagnose and solve problems
- Manage
- Branding & properties
- Authentication
- Certificates & secrets
- Token configuration
- API permissions
- Expose an API
- App roles
- Owners

Credentials enable confidential applications to identify themselves to the authentication service (when using a certificate scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret).

i Application registration certificates, secrets and federated credentials can be found in the tabs below

Certificates (0) Client secrets (0) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be used to access resources.

+ New client secret

Description	Expires	Value ⓘ
No client secrets have been created for this application.		

10. Name the client secret. For instance, `Vultr SSO Secret`, set the expiration period, and click **Add**.

✕

Add a client secret

Description

Expires

Add




Cancel

11. Copy the Azure **Client Secret** value to your clipboard because the Azure Portal won't display the value again.

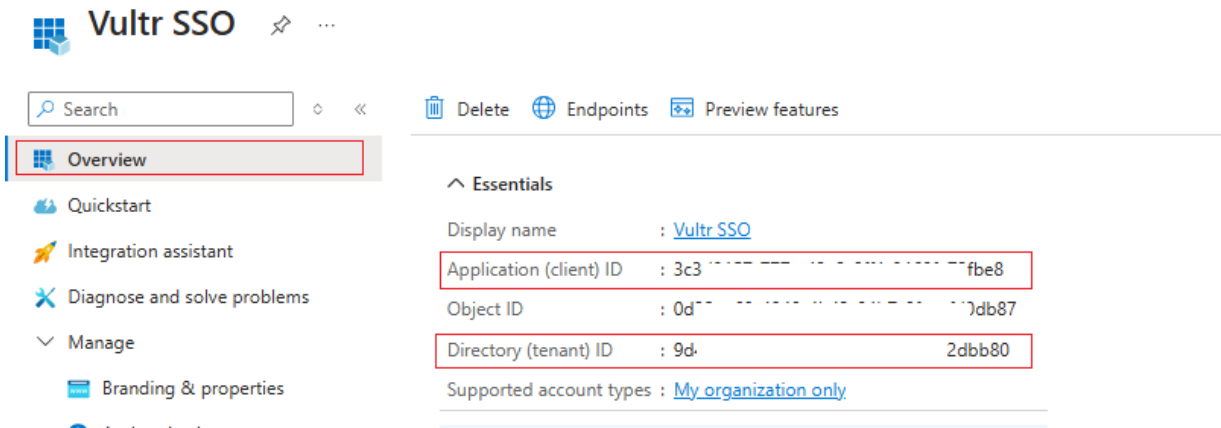
Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Secret ID
Vultr SSO Secret	4/28/2025	N3k8Q~-Ge4j6 Zg... 	414: 4ccd74  

12. Navigate to **Overview** and copy the **Application (client) ID** and **Directory (tenant) ID**.



Vultr SSO

Search

Delete Endpoints Preview features

Overview

Quickstart

Integration assistant

Diagnose and solve problems

Manage

Branding & properties

Essentials

Display name : [Vultr SSO](#)

Application (client) ID : 3c3...f8be8

Object ID : 0d...db87

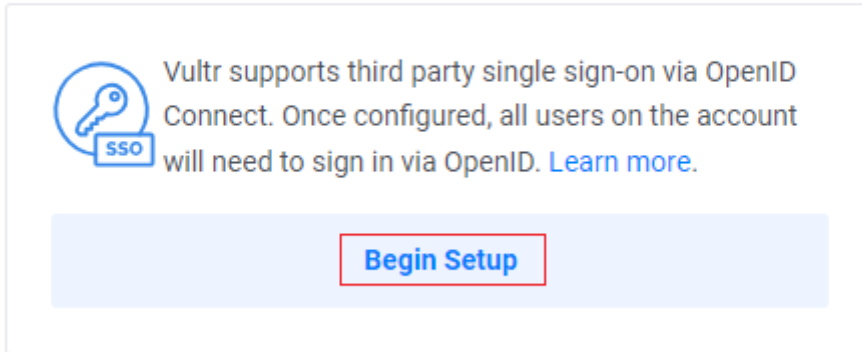
Directory (tenant) ID : 9d...2dbb80

Supported account types : [My organization only](#)

Set up Vultr Single Sign-On

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Click **Begin Setup** under **Single Sign-On**.

Single Sign-On

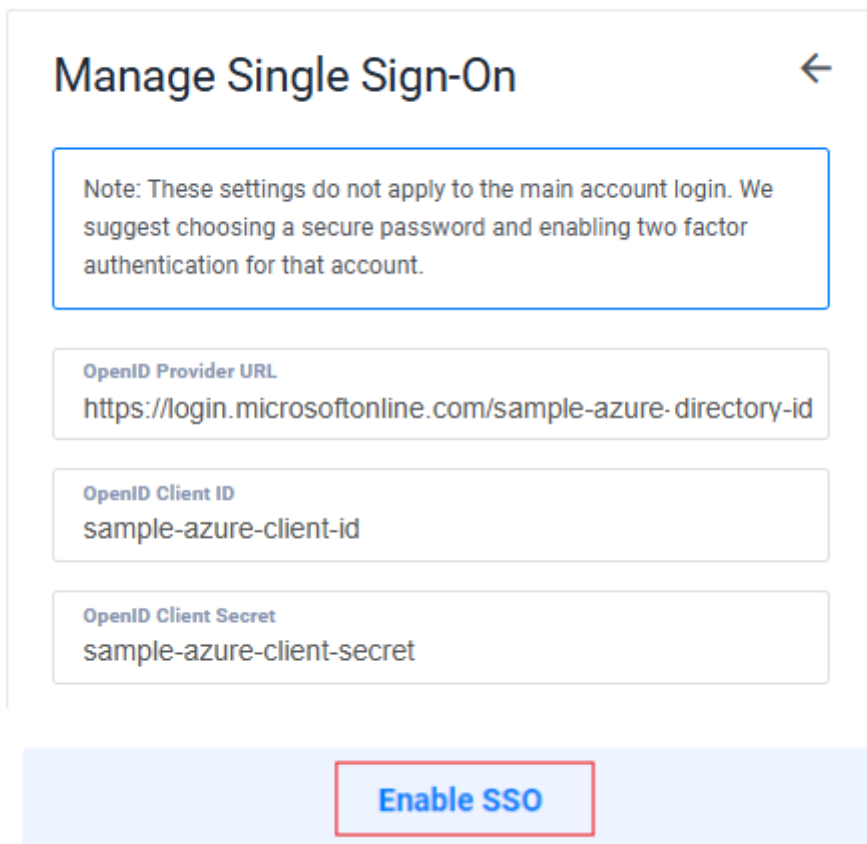


Vultr supports third party single sign-on via OpenID Connect. Once configured, all users on the account will need to sign in via OpenID. [Learn more.](#)

[Begin Setup](#)

3. Enter **Microsoft Entra ID Credentials** and specify `https://login.microsoftonline.com/directory-tenant-id` (For example, `https://login.microsoftonline.com/963-542b-48b-8e75-1a`) as the OpenID Provider URL. Then, click **Enable SSO**.

Single Sign-On Enabled



Manage Single Sign-On

Note: These settings do not apply to the main account login. We suggest choosing a secure password and enabling two factor authentication for that account.

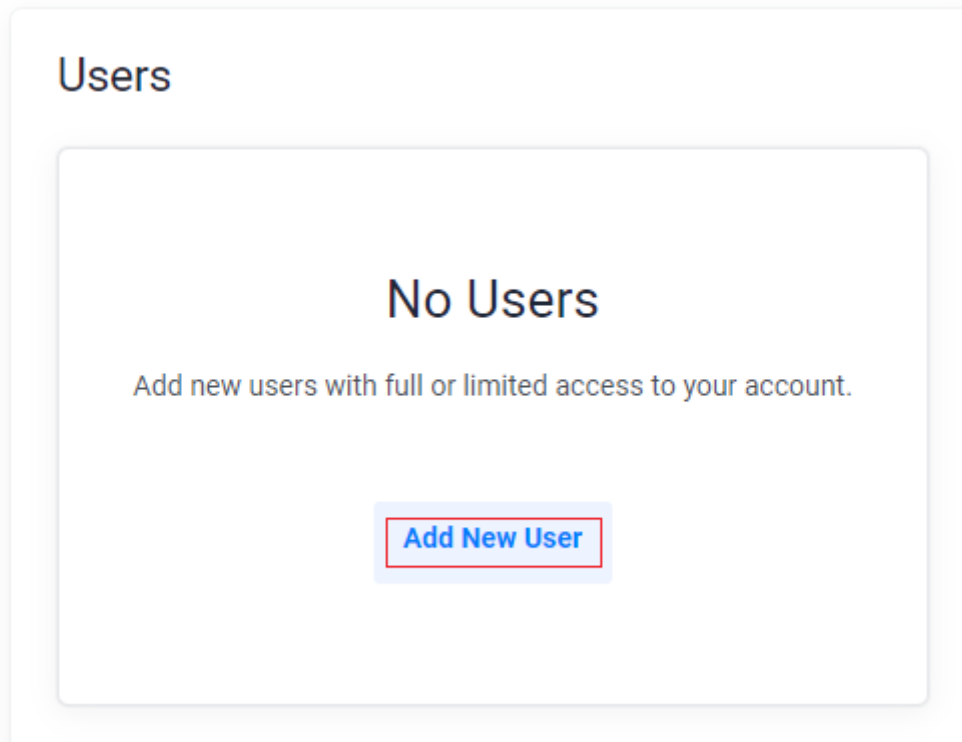
OpenID Provider URL
`https://login.microsoftonline.com/sample-azure-directory-id`

OpenID Client ID
`sample-azure-client-id`

OpenID Client Secret
`sample-azure-client-secret`

[Enable SSO](#)

4. Click **Add New User** to create a new user account.



5. Enter the user details, including the **Name** and **Email**. Then, customize the user permissions and click **Add User**.





Add User Profile

This will create a new <https://my.vultr.com> log in with limited privileges to manage your account

Name
John Doe

Email
johndoe@example.onmicrosoft.com

Users will log in via SSO, passwords are not available.

- Manage Users  OFF
- Manage Servers  ON
- Manage Vultr Kubernetes Engines  OFF
- Receive AUP/ToS Notifications  OFF
- Receive Maintenance Notifications OFF

[Add User](#)

- Use your Microsoft Entra ID user account to log in to Vultr through the Vultr [SSO Login page](#).

Okta

A guide for configuring Vultrs Single Sign-On integration with Okta identity provider for centralized authentication management.

Contents

01	Introduction	10
02	Set up Okta Account Integration	90
03	Set up Vultr Single Sign-On	69

How to Integrate Vultr Single Sign-On with Okta

Introduction

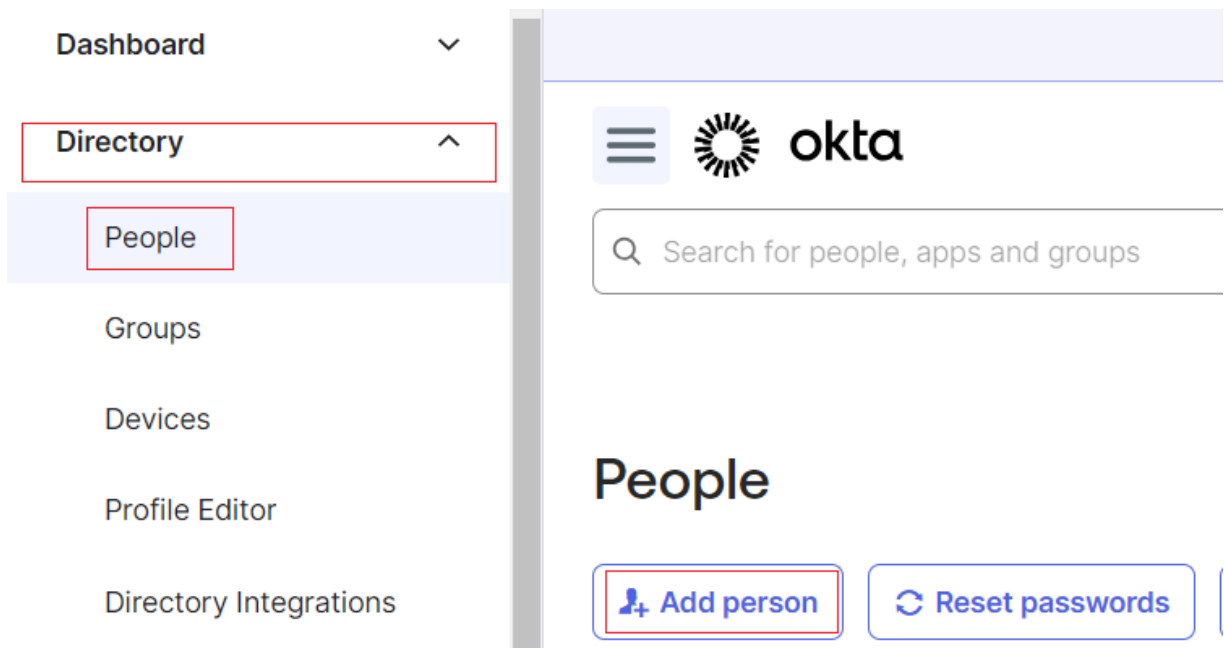
Single Sign-On (SSO) is a service that lets you authenticate to multiple websites and applications using one set of login credentials. SSO eliminates the need for multiple logins, hence providing a better user experience. Vultr SSO integrates well with Okta, a secure identity cloud solution for unifying logins for apps and devices.

Follow this guide to integrate Vultr SSO with Okta using the Vultr Customer Portal.

Set up Okta Account Integration

Create an Okta Account User

1. Log in to your [Okta account](#).
2. Select **People** under **Directory** and click **Add person** to add a new user.



3. Enter the user's details, including the **First name**, **Last name**, and **Username**.

Add Person

User type ?	<input type="text" value="User"/>
First name	<input type="text" value="John"/>
Last name	<input type="text" value="Doe"/>
Username	<input type="text" value="john_doe@example.com"/>
Primary email	<input type="text" value="john_doe@example.com"/>

4. Set the user's password and click **Save**.

Secondary email (optional)

Groups (optional) You haven't added any [groups](#)

Activation

I will set password

User must change password on first login

Do not send unsolicited or unauthorized activation emails. [Read more](#)

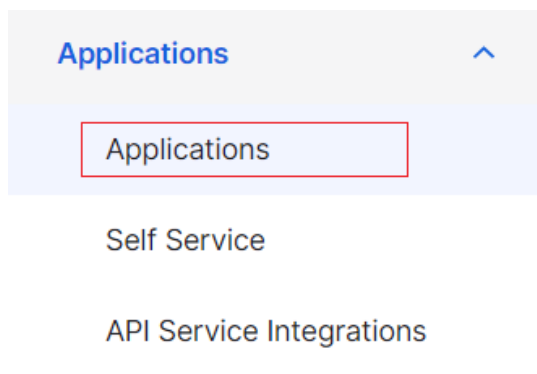
Save

Save and Add Another

Cancel

Create an Okta Application

1. Navigate to **Applications** and click **Create App Integration**.




Applications

Create App Integration

2. Select **OIDC - OpenID Connect** as the Sign-in method and **Web Application** as the application type. Then, click **Next**.

Create a new app integration

- Sign-in method** **OIDC - OpenID Connect**
[Learn More](#)  Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for application only supports SAML.
- Application type** **Web Application**
Server-side applications where authentication and tokens are handled by the server (for example, Go, Java, ASP.Net, Node.js, PHP)

Cancel

Next




3. Enter your preferred app name, such as `Vultr Login`.

New Web App Integration

General Settings

App integration name

Logo (Optional)



4. Enter `https://my.vultr.com/openid/` in the **Sign-in redirect URIs** and **Sign-out redirect URIs** fields and allow user access to the application.

New Web App Integration

General Settings

Sign-in redirect URIs Allow wildcard * in sign-in URI redirect.

[Learn More](#)

Sign-out redirect URIs


Assignments

Controlled access Allow everyone in your organization to access

Limit access to selected groups

Skip group assignment for now

5. Copy the **Client ID** and **Client secret** in the next screen.



Vultr Login

Active ▾ View Logs

[General](#) [Sign On](#) [Assignments](#) [Okta API Scopes](#) [Application Rate Limits](#)

Client Credentials Edit

Client ID Copy

Public identifier for the client that is required for all OAuth flows.

Client authentication Client secret Public key / Private key

CLIENT SECRETS

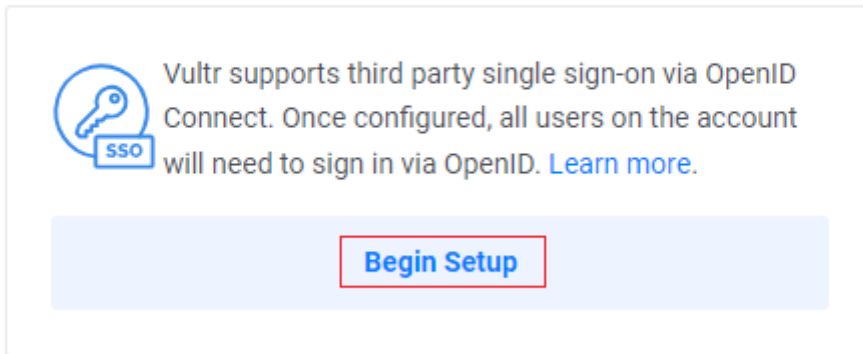
Generate new secret

Creation date	Secret	Status
Oct 22, 2024	<input type="text" value="....."/> Copy Eye	Active ▾

Set up Vultr Single Sign-On

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Click **Begin Setup** under **Single Sign-On**.

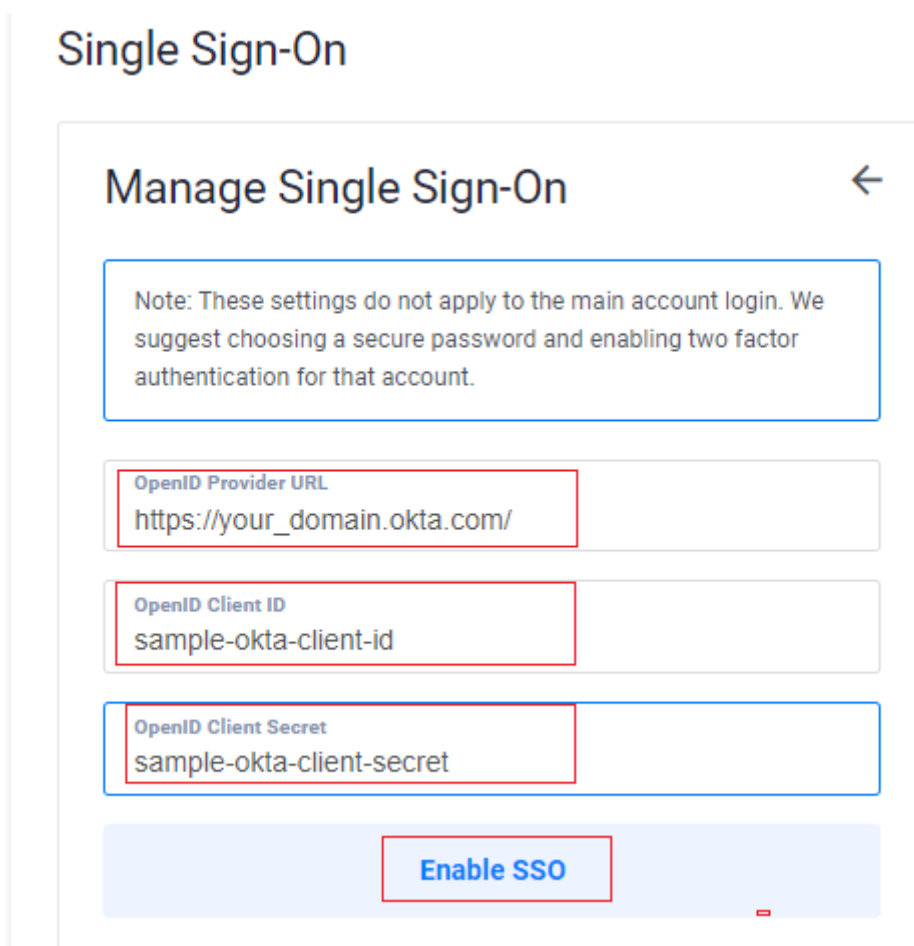
Single Sign-On



Vultr supports third party single sign-on via OpenID Connect. Once configured, all users on the account will need to sign in via OpenID. [Learn more.](#)

[Begin Setup](#)

3. Enter Okta Credentials and click **Enable SSO**.



Single Sign-On

Manage Single Sign-On

Note: These settings do not apply to the main account login. We suggest choosing a secure password and enabling two factor authentication for that account.

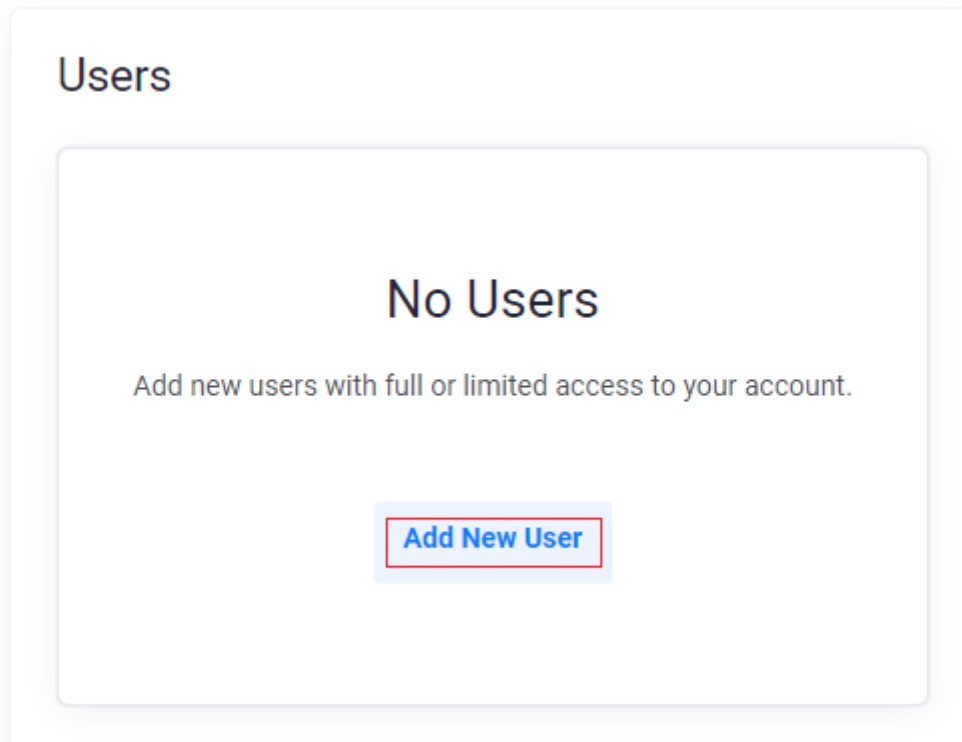
OpenID Provider URL
https://your_domain.okta.com/

OpenID Client ID
sample-okta-client-id

OpenID Client Secret
sample-okta-client-secret

[Enable SSO](#)

4. Click **Add New User** to create a new user account.



5. Enter the user details, including the **Name** and **Email**. Then, customize the user permissions and click **Add User**.

This will create a new <https://my.vultr.com> log in with limited privileges to manage your account

Name	John Doe
Email	john_doe@example.com

Users will log in via SSO, passwords are not available.

Manage Users ?	<input type="checkbox"/> OFF
Manage Servers ?	<input checked="" type="checkbox"/> ON
Manage Vultr Kubernetes Engines ?	<input type="checkbox"/> OFF
Receive AUP/ToS Notifications ?	<input checked="" type="checkbox"/> ON
Receive Maintenance Notifications	<input type="checkbox"/> OFF

Add User

6. Use your Okta user account to log in to Vultr through the Vultr [SSO Login page](#).

OneLogin

A comprehensive guide for configuring and implementing Vultrs Single Sign-On (SSO) integration with OneLogin identity provider.

Contents

01	Introduction	10
02	Set up OneLogin Account Integration	101
03	Set up Vultr Single Sign-On	69

How to Integrate Vultr Single Sign-On with OneLogin

Introduction

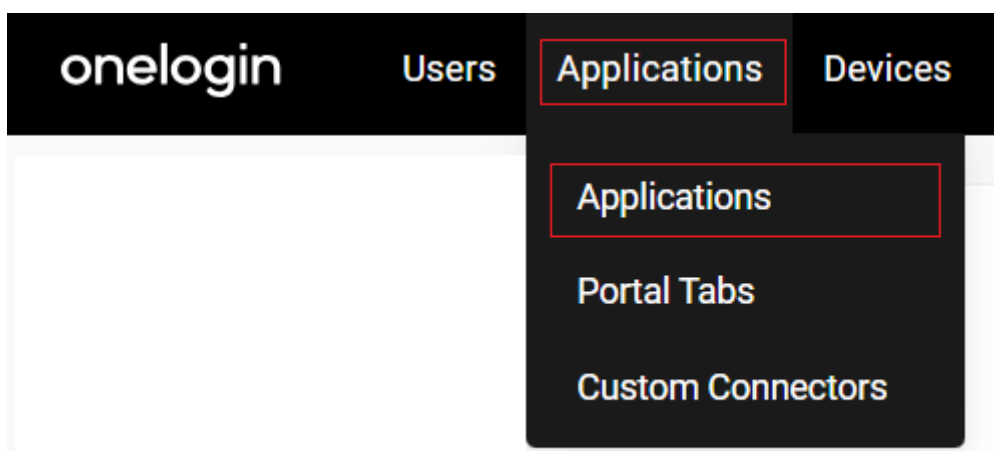
Single Sign-On (SSO) is a service that lets you authenticate to multiple websites and applications using one set of login credentials. SSO eliminates the need for multiple logins, hence providing a better user experience. Vultr SSO integrates well with OneLogin, a market-leading identity and access management solution.

Follow this guide to integrate Vultr SSO with OneLogin using the Vultr Customer Portal.

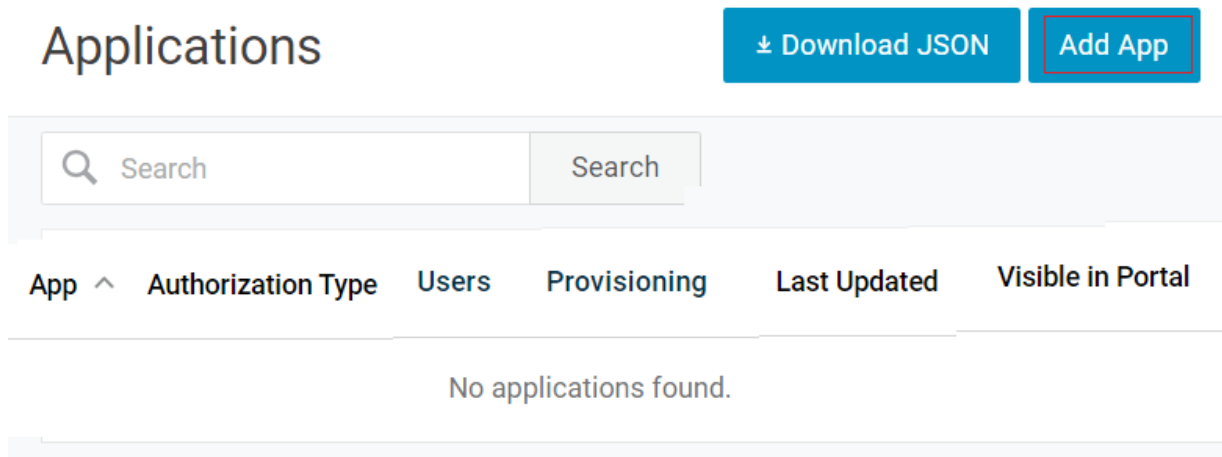
Set up OneLogin Account Integration

Create a OneLogin Application

1. Log in to your [OneLogin account](#).
2. Go to **Applications** and select **Applications**.

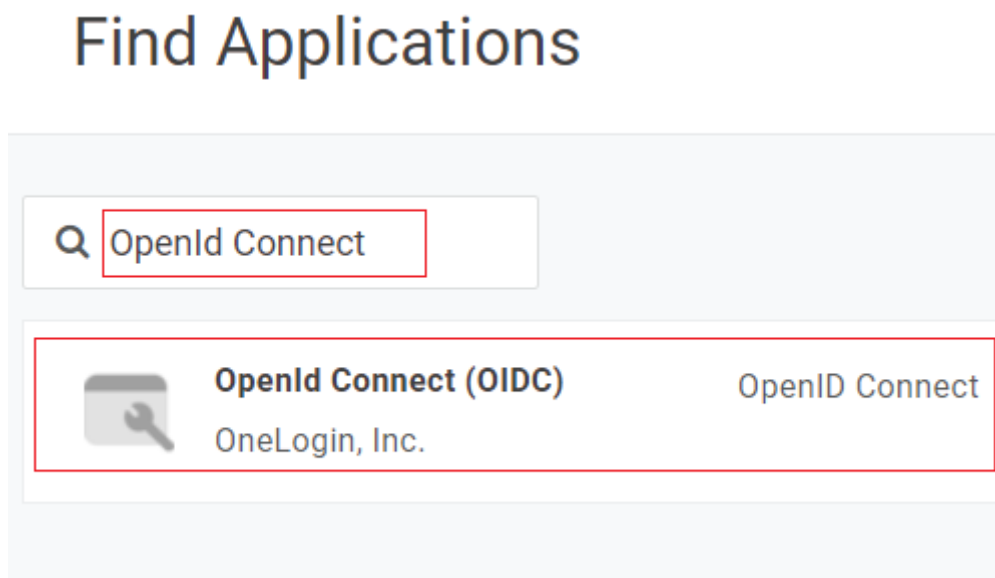


3. Click **Add App**.



The screenshot shows the 'Applications' page in OneLogin. At the top right, there are two buttons: 'Download JSON' and 'Add App'. The 'Add App' button is highlighted with a red box. Below the buttons is a search bar with a magnifying glass icon and the text 'Search'. Below the search bar is a table with columns: 'App', 'Authorization Type', 'Users', 'Provisioning', 'Last Updated', and 'Visible in Portal'. The table is currently empty, with the text 'No applications found.' centered below the columns.

4. Enter the **OpenId Connect** keyword in the search box. Then click **OpenId Connect (OIDC)** in the search result.



The screenshot shows the 'Find Applications' page in OneLogin. The search bar contains the text 'OpenId Connect'. Below the search bar, a search result is displayed, highlighted with a red box. The result is for 'OpenId Connect (OIDC)' by OneLogin, Inc. The result includes an icon of a calendar with a wrench, the text 'OpenId Connect (OIDC)', and the text 'OpenID Connect'.

5. Customize your app **Display Name**, **Icon**, and **Description**. Then, click **Save** at the top.

[Cancel](#) [Save](#)

Portal

Display Name

Visible in portal

- Click **Configuration** in the new navigation menu. Then, enter `https://my.vultr.com/openid/` in the **Login Url**, **Redirect URI's**, and **Post Logout Redirect URIs** fields, and click **Save**.

[Applications /](#)
OpenId Connect (OIDC) [More Actions](#) [Save](#)

Info	Application details
Configuration	Login Url <input type="text" value="https://my.vultr.com/openid/"/>
Parameters	Redirect URI's <input type="text" value="https://my.vultr.com/openid/"/>
Rules	Post Logout Redirect URIs <input type="text" value="https://my.vultr.com/openid/"/>
SSO	
Access	

- Click **SSO** in the navigation menu. Then, copy the **Client ID**, **Client Secret**, and **Issuer URL**. You must click the **Show client secret** to

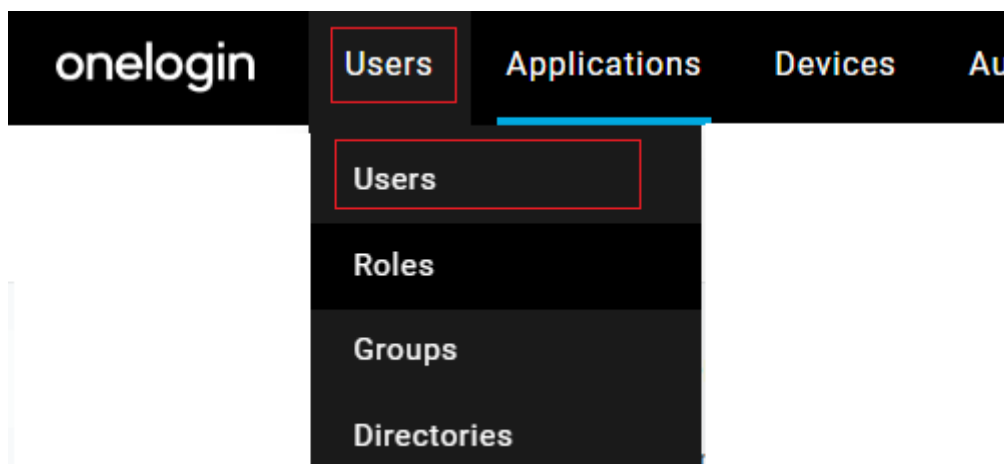
display the value. Then, select **POST** under **Token Endpoint Authentication Method** and click **Save**.

The screenshot shows the OneLogin configuration interface. On the left, a sidebar contains navigation options: Info, Configuration, Parameters, Rules, **SSO**, Access, and Users. The main content area is titled 'Enable OpenID Connect' and includes a 'More Actions' dropdown and a 'Save' button. The configuration fields are as follows:

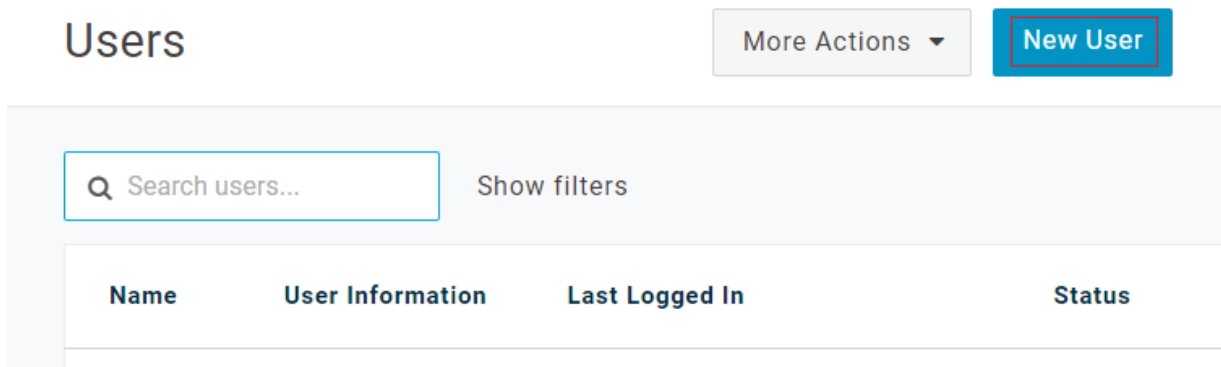
- Client ID:** 9df69...
- Client Secret:** Show client secret (with a 'Regenerate client secret' link)
- Issuer URL:** https://example.onelogin.com/oidc/2 Well-known Configuration
- Application Type:** Web
- Token Endpoint Authentication Method:** POST

Create a OneLogin User

1. Navigate to **Users** and select **Users**.

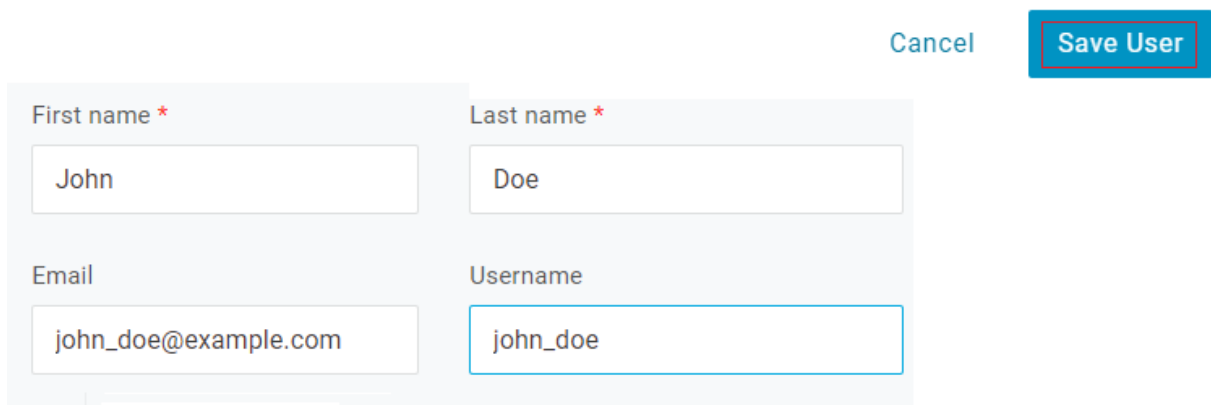


2. Click **New User**.



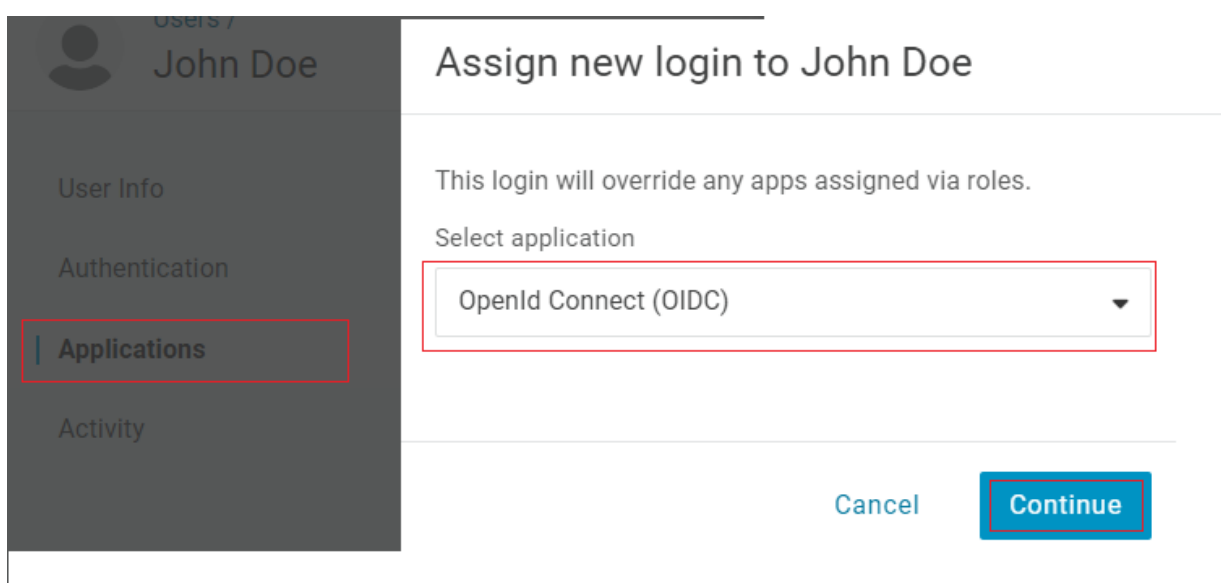
The screenshot shows the 'Users' management page. At the top left is the title 'Users'. To its right is a 'More Actions' dropdown menu and a blue 'New User' button. Below this is a search bar with the placeholder text 'Search users...' and a 'Show filters' link. Underneath is a table header with columns: 'Name', 'User Information', 'Last Logged In', and 'Status'.

3. Customize the user details, including the **Name** and **Email** address and click **Save User**.



The screenshot shows the user details form. It has four input fields: 'First name *' (containing 'John'), 'Last name *' (containing 'Doe'), 'Email' (containing 'john_doe@example.com'), and 'Username' (containing 'john_doe'). At the top right of the form are 'Cancel' and 'Save User' buttons, with 'Save User' highlighted in blue.

4. Select **Applications** in the new navigation menu and click the **+** to assign an application to the user. Select the OpenId Connect App you created earlier and click **Continue**.



The screenshot shows a dialog box titled 'Assign new login to John Doe'. On the left is a navigation menu with options: 'User Info', 'Authentication', 'Applications' (highlighted with a red box), and 'Activity'. The main content area contains the text 'This login will override any apps assigned via roles.' followed by 'Select application' and a dropdown menu showing 'OpenId Connect (OIDC)' (highlighted with a red box). At the bottom right are 'Cancel' and 'Continue' buttons, with 'Continue' highlighted in blue.

5. Click **Save** in the next screen.

Edit OpenId Connect (OIDC) login for John Doe

- Allow the user to sign in
 Hide this app in Portal

Groups

Select Groups ▼ Add

Added Items

[Reset login](#) ([What's this?](#))

Cancel

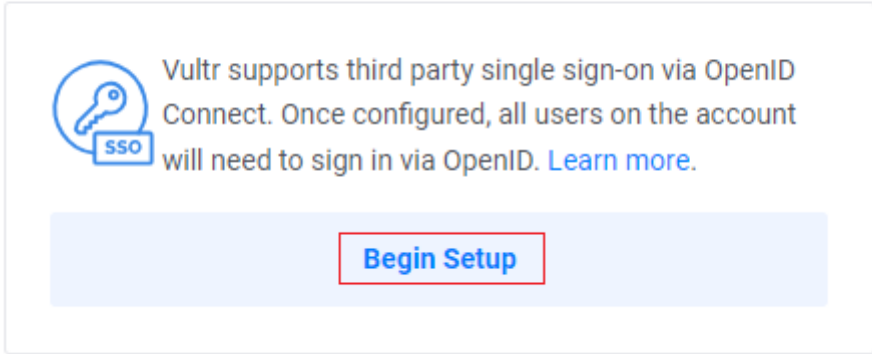
Delete

Save

Set up Vultr Single Sign-On

1. Navigate to **Account** and select **Users** under **OTHER**.
2. Click **Begin Setup** under **Single Sign-On**.

Single Sign-On



Vultr supports third party single sign-on via OpenID Connect. Once configured, all users on the account will need to sign in via OpenID. [Learn more.](#)

Begin Setup

3. Enter OneLogin Credentials and click **Enable SSO**.

Single Sign-On

Manage Single Sign-On ←

Note: These settings do not apply to the main account login. We suggest choosing a secure password and enabling two factor authentication for that account.

OpenID Provider URL
https://sample.onelogin.com/oidc/2

OpenID Client ID
your_onelogin_client_id

OpenID Client Secret
your_one_login_secret

[Enable SSO](#)

4. Click **Add New User** to create a new user account.

Users

No Users

Add new users with full or limited access to your account.

[Add New User](#)

5. Enter the user details, including the **Name** and **Email**. Then, customize the user permissions and click **Add User**.

This will create a new <https://my.vultr.com> log in with limited privileges to manage your account

Name	John Doe
Email	john_doe@example.com

Users will log in via SSO, passwords are not available.

Manage Users ?	<input type="checkbox"/> OFF
Manage Servers ?	<input checked="" type="checkbox"/> ON
Manage Vultr Kubernetes Engines ?	<input type="checkbox"/> OFF
Receive AUP/ToS Notifications ?	<input checked="" type="checkbox"/> ON
Receive Maintenance Notifications	<input type="checkbox"/> OFF

[Add User](#)

6. Use your OneLogin user account to log in to Vultr through the Vultr [SSO Login page](#).

FAQ

A comprehensive resource addressing common questions about Vultr's Single Sign-On authentication system.

Contents

01	Introduction	10
02	Which Single Sign-On providers does Vultr support?	111
03	Do I incur additional charges if I enable SSO??	111
04	What is the main difference between Single Sign-On (SSO) and Two-factor Authentication (2FA)?	111

Frequently Asked Questions (FAQs) for Vultr Single Sign-On

Introduction

These are the frequently asked questions for Vultr Single Sign-On.

Which Single Sign-On providers does Vultr support?

Vultr Single Sign-On (SSO) works with all major OpenID Connect providers including OneLogin, Okta, Google, Azure, and more. Ensure your provider is compatible with OpenID Connect before linking your account.

Do I incur additional charges if I enable SSO??

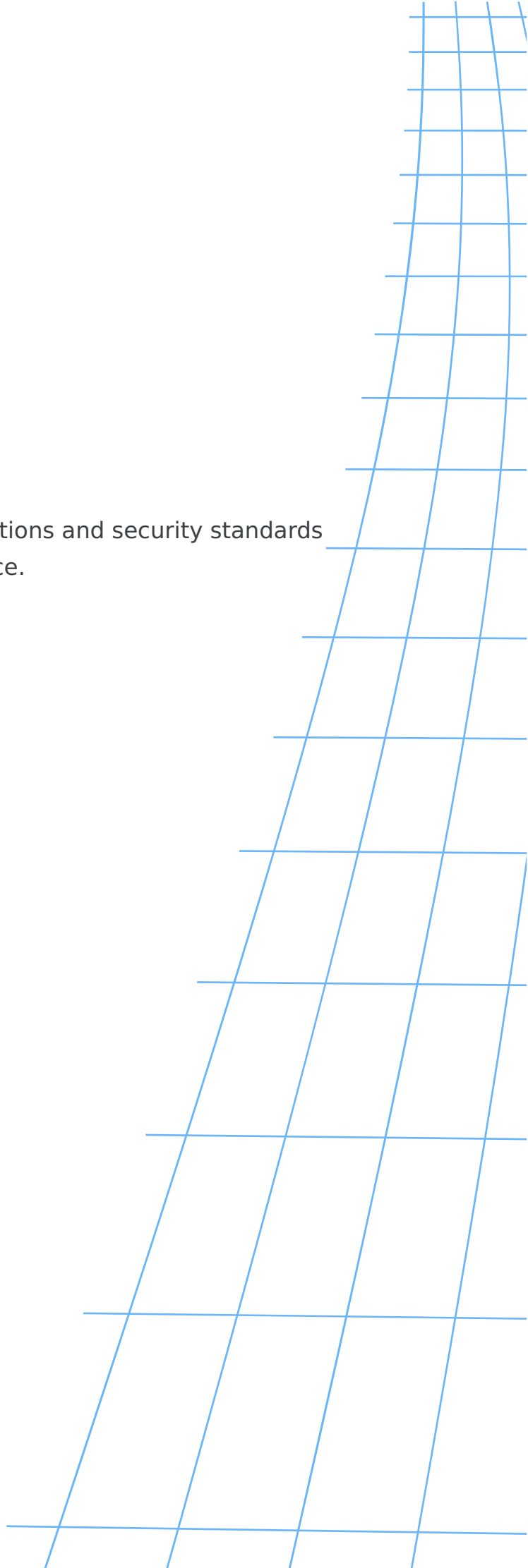
No, you won't incur additional charges after enabling SSO in your account.

What is the main difference between Single Sign-On (SSO) and Two-factor Authentication (2FA)?

SSO focuses on convenience by allowing users to access multiple applications with a single login, while 2FA focuses on security by requiring multiple forms of authentication to grant users access to a resource.

Compliance

Vultr's framework for meeting industry regulations and security standards to ensure data protection and legal compliance.



Contents

01	Data Center Compliance Artifacts	114
02	Vultr Compliance Artifacts	118
03	FAQ	122



[Vultr Docs](#) > [Platform Documentation](#)

Data Center Compliance Artifacts

Access and review compliance documentation for Vultr's data centers to verify regulatory adherence and security standards.

Contents

01 Introduction	10
-----------------	----

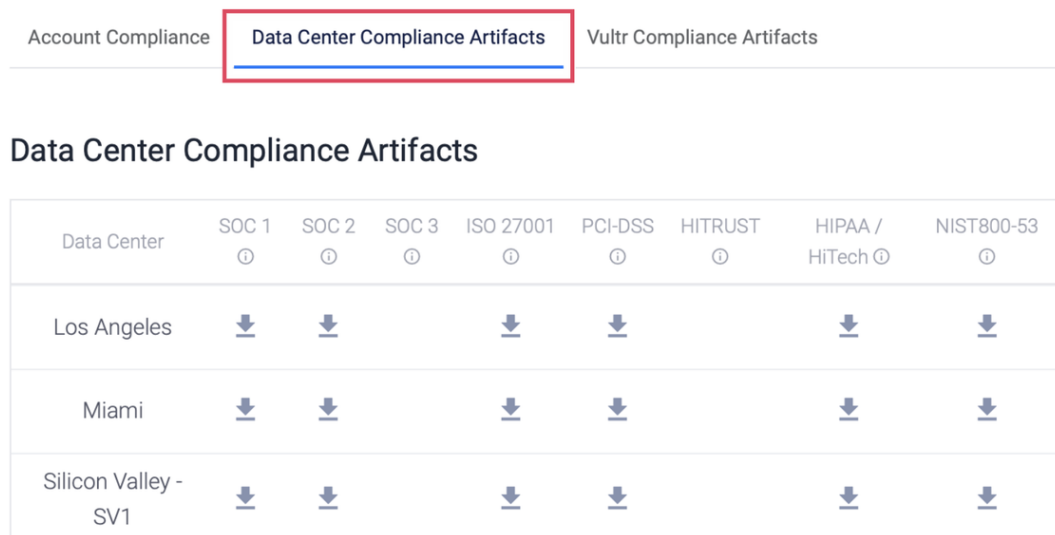
How to View Vultr Data Center Compliance Artifacts

Introduction

Vultr Data Center Compliance Artifacts demonstrate that Vultr meets specific requirements. Third-party auditors provide these artifacts after testing and verifying Vultr's compliance with different global and regional industry-specific security standards and regulations.

Follow this guide to view Data Center Compliance Artifacts using the Vultr Customer Portal.

1. Navigate to **Account** and select **Compliance** under **OTHER**.
2. Select **Data Center Compliance Artifacts**.



Data Center	SOC 1	SOC 2	SOC 3	ISO 27001	PCI-DSS	HITRUST	HIPAA / HiTech	NIST800-53
Los Angeles	↓	↓		↓	↓		↓	↓
Miami	↓	↓		↓	↓		↓	↓
Silicon Valley - SV1	↓	↓		↓	↓		↓	↓

3. Choose your target Data Center, such as Miami, and click the download icon to get the compliance report.

[Account Compliance](#)[Data Center Compliance Artifacts](#)[Vultr Compliance Artifacts](#)

Data Center Compliance Artifacts

Data Center	SOC 1 ⓘ	SOC 2 ⓘ	SOC 3 ⓘ	ISO 27001 ⓘ	PCI-DSS ⓘ	HITRUST ⓘ	HIPAA / HiTech ⓘ	NIST800-53 ⓘ
Los Angeles	↓	↓		↓	↓		↓	↓
Miami	↓	↓		↓	↓		↓	↓
Silicon Valley - SV1	↓	↓		↓	↓		↓	↓

4. Use Adobe software to accept the terms and view the compliance report.

Vultr Compliance Artifacts

Access and review Vultr's compliance documentation and certificates that demonstrate adherence to industry standards and regulations.

Contents

01 Introduction	10
-----------------	----

How to View Vultr Compliance Artifacts

Introduction


Vultr Compliance Artifacts demonstrate that Vultr meets specific requirements. Third-party auditors provide these artifacts after testing and verifying Vultr's compliance with different global and regional industry-specific security standards and regulations.

Follow this guide to view Vultr Compliance Artifacts using the Vultr Customer Portal.

1. Navigate to **Account** and select **Compliance** under **OTHER**.
2. Select **Vultr Compliance Artifacts**.

Account Compliance Data Center Compliance Artifacts **Vultr Compliance Artifacts**

Vultr Compliance Artifacts

Compliance	Description	Last Audit Date	Download
SOC 2 Type 2 - AICPA Trust Service Criteria with Added HIPAA Security Rule	<p>The SOC 2+ report evaluates Constant's information system relevant to security, availability, confidentiality and the HIPAA Security rules.</p> <p>The SOC 2 report is a clickwrapped PDF. Please use an Adobe branded PDF viewer for access and to accept the terms of use.</p>	12/31/2024	


3. Select your target compliance from the list, review the **Description**, and **Last Audit Date**. Then, click the download icon.

Account Compliance

Data Center Compliance Artifacts

Vultr Compliance Artifacts

Vultr Compliance Artifacts

Compliance	Description	Last Audit Date	Download
SOC 2 Type 2 - AICPA Trust Service Criteria with Added HIPAA Security Rule	The SOC 2+ report evaluates Constant's information system relevant to security, availability, confidentiality and the HIPAA Security rules. The SOC 2 report is a clickwrapped PDF. Please use an Adobe branded PDF viewer for access and to accept the terms of use.	12/31/2024	

4. Use Adobe software to accept the terms and view the compliance report.

FAQ

A collection of common questions and answers about Vultr's compliance policies, certifications, and security practices.

Contents

01	Introduction	10
02	Are Vultr services GDPR compliant?	124
03	What is Vultr's role with respect to GDPR?	124
04	Does Vultr offer a Data Processing Addendum?	124
05	How can I delete or retrieve the data I have with Vultr?	125
06	How can I view Vultr Data Center Compliance information?	125

Frequently Asked Questions (FAQs) for Vultr Compliance

Introduction

These are the frequently asked questions for Vultr data Compliance.

Are Vultr services GDPR compliant?

Vultr is committed to transparent and secure handling of all personal data on our network. Our processes go through an extensive procedural and legal review to ensure we fully meet the requirements set forth in the EU General Data Protection Regulation (GDPR) legislation.

What is Vultr's role with respect to GDPR?

Vultr acts as a data controller and a data processor. Vultr acts as a data controller for customer information that we collect to process payments and provide customer support. When a customer uses our services to process personal data, Vultr acts as a data processor.

Does Vultr offer a Data Processing Addendum?

If GDPR applies to your organization and you need a DPA to satisfy GDPR requirements, Vultr will provide a DPA for eSignature. Please contact your account manager and/or [create a support ticket](#).

How can I delete or retrieve the data I have with Vultr?

We've created a step-by-step document that shows you how to delete all your hosted data in our Vultr Docs section. Please review the [Vultr Data Portability Guide](#) for more information.

How can I view Vultr Data Center Compliance information?

Visit the Vultr [Datacenter Compliance information page](#) for more information.

SSH Keys

Securely access your Vultr instances without passwords by storing and managing your public SSH keys.

Contents

01	Add SSH Keys	128
02	Delete SSH Keys	133
03	Update SSH Keys	138
04	FAQ	143

Add SSH Keys

Learn how to add and manage SSH keys to your Vultr account for secure, password-free server access

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Add Vultr SSH Keys

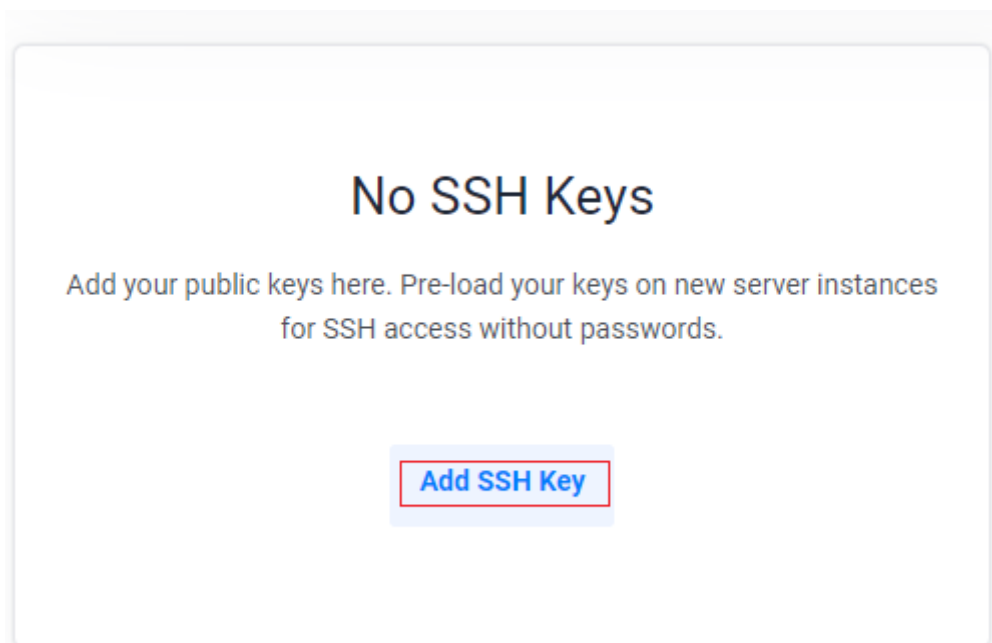
Introduction

A Vultr account Secure Shell (SSH) key authenticates and establishes a secure connection between a client application like Putty or Filezilla and cloud compute instances. SSH keys are more secure than passwords because they're long, complex, and less prone to brute-force attacks.

Follow this guide to add SSH keys using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **SSH Keys** under **OTHER**.
2. Click **Add SSH Key**.



3. Enter the SSH Key details and click **Add SSH Key**.

test-ssh-key

SSH Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAAdSdfsfYVgWDrDXbK2vAhcUpEserwr69u
SDliV3io0buWx2Nt97ctKa9Xgh4rJ7jk+RZY424581Bw4b1MC6N
bZosddfdfvJNdsfsdfjBw5fcBOJlQNYNZMI3KQP1Ht96X6uREYS
AIiF57YQ== john-doe
```

Vultr API

1. Send a `POST` request to the [Create SSH key endpoint](#) to create an SSH key.

```
CONSOLE
$ curl "https://api.vultr.com/v2/ssh-keys" \
  -X POST \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
  --data '{
    "name" : "{ssh_key_name}",
    "ssh_key" : "{ssh_public_key_value} {email_address}"
  }'
```

Visit the [Create SSH key endpoint](#) to view additional attributes to add to your request.

2. Send a `GET` request to the [List SSH Keys endpoint](#) to view all SSH keys.

CONSOLE

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

Vultr CLI

1. Create a new SSH Key.

CONSOLE

```
$ vultr-cli ssh-keys create \  
  --name="<ssh_key_name>" \  
  --key="<ssh_public_key_value> <email_address>"
```

Run `vultr-cli ssh-keys create --help` to view additional available options.

2. List all SSH keys.

CONSOLE

```
$ vultr-cli ssh-keys list
```

Delete SSH Keys

Learn how to permanently remove SSH keys from your Vultr account when they're no longer needed.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Delete Vultr SSH Keys

Introduction







Deleting a Secure Shell (SSH) key removes the public key from your Vultr account. After deleting the key, you can no longer log in to your account using the corresponding private key. This action is necessary if you've inactive or compromised keys.

Follow this guide to delete SSH keys using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **SSH Keys** under **OTHER**.
2. Select the SSH key from the list and click the **Delete SSH Key** icon.

SSH Keys

Name	Date Created		
test-ssh-key	14-10-2024 10:23:30		
test-ssh-key2	14-10-2024 10:24:00		
test-ssh-key3	14-10-2024 10:24:12		

3. Click **Delete SSH Key** in the confirmation prompt to permanently delete the target SSH Key.

📘 Delete SSH Key?

Are you sure you want to delete this key? This will not remove the key from any machines that already have it.

SSH Key: test-ssh-key

Delete SSH Key

Cancel

Vultr API

1. Send a `GET` request to the [List SSH Keys endpoint](#) and note the target SSH key's ID.

CONSOLE

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

2. Send a `DELETE` request to the [Delete SSH Key endpoint](#) and specify the ID to delete the target SSH key.

CONSOLE

```
$ curl "https://api.vultr.com/v2/ssh-keys/{ssh-key-id}" \  
  -X DELETE \  
  -H "Authorization: Bearer ${VULTR_API_KEY}"
```

Vultr CLI

1. List all SSH keys and note the target SSH key ID.

CONSOLE

```
$ vultr-cli ssh-keys list
```

2. Delete the target SSH Key by specifying the ID.

CONSOLE

```
$ vultr-cli ssh-keys delete <ssh-key-id>
```

Update SSH Keys

A guide explaining how to modify or replace existing SSH keys in your Vultr account for secure server access

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10
04	Vultr CLI	11

How to Update Vultr SSH Keys

Introduction







Updating a Secure Shell (SSH) key means replacing the public key from your Vultr account. Before updating the key, ensure you have a fresh SSH key pair. Then, keep the private key on your local device and copy the public key to your clipboard.

Follow this guide to update SSH keys using the Vultr Customer Portal, API, or CLI.

Vultr Customer Portal

1. Navigate to **Account** and select **SSH Keys** under **OTHER**.
2. Select the SSH key from the list and click the **Edit SSH Key** icon.

SSH Keys

Name	Date Created		
test-ssh-key	14-10-2024 10:23:30		
test-ssh-key2	14-10-2024 10:24:00		
test-ssh-key3	14-10-2024 10:24:12		

3. Enter the SSH Key details and click **Update SSH Key**.

Name
test-ssh-key

SSH Key
ssh-rsa AAAAB3NzaC1yc2EA....

Update SSH Key

Vultr API

1. Send a `GET` request to the [List SSH Keys endpoint](#) to view all SSH keys and note the target SSH key's ID.

CONSOLE

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

2. Send a `PATCH` request to the [Update SSH Key endpoint](#) to update the target SSH key.

CONSOLE

```
$ curl "https://api.vultr.com/v2/ssh-keys/{ssh-key-id}" \
  -X PATCH \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
  --data '{
    "name" : "{updated_ssh_key_name}",
    "ssh_key" : "{updated_ssh_public_key_value}"
  }'
```

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

Vultr CLI

1. List all SSH keys and note the target SSH key's ID.

CONSOLE

```
$ vultr-cli ssh-keys list
```

2. Update the target SSH Key by specifying the ID.

CONSOLE

```
$ vultr-cli ssh-keys update <ssh-key-id> \  
--name="<updated_ssh_key_name>" \  
--key="<updated_ssh_public_key_value> <email_address>"
```

Run `vultr-cli ssh-keys update --help` to view additional available options.

FAQ

A comprehensive guide addressing common questions about managing and using SSH keys with Vultr services.

Contents

01	Introduction	10
02	Why are SSH keys important?	145
03	How do I secure my SSH keys?	145
04	How do I generate an SSH key?	145
05	Can I use a single SSH key with multiple servers?	146

Frequently Asked Questions (FAQs) for Vultr SSH Keys

Introduction

These are the frequently asked questions for Vultr SSH keys.

Why are SSH keys important?

Unlike passwords, Vultr SSH keys are more secure and less susceptible to brute-force attacks and eavesdropping. SSH keys encrypt data between the client and the server.

How do I secure my SSH keys?

You should protect your SSH private keys with a passphrase and avoid sharing them with unauthorized users.

How do I generate an SSH key?

You can use a key generator, such as `ssh-keygen` for Linux and PuTTYgen for Windows to create SSH keys. SSH keys are a public-private key pair. You should share the public key with the remote server and keep the private key locally on your computer. Visit the guide on how to [generate SSH Keys](#) for more information.

Can I use a single SSH key with multiple servers?

Yes, you can use the same SSH key with multiple servers. However, if the key is compromised, the attacker gains access to all servers using it. Therefore, consider creating different keys for your servers.

API

Programmatic interface for automating and managing Vultr resources through HTTP requests.

Contents

01	Disable API Access	149
02	Enable API Access	152
03	Manage API Access Control	155
04	FAQ	158
05	Current User API Key Management	161
	Create New API Key	163
	Delete API Key	167
	List API Key	171
	Rotate API Key	174
06	Other Users API Key Management	178
	Delete API Key	180
	Create New API Key	184
	List API Key	188
	Rotate API Key	192

Disable API Access

Learn how to disable API access to your Vultr account for enhanced security.

Contents

01 Introduction	10
-----------------	----

How to Disable Vultr API Access

Introduction

Disabling Application Programming Interface (API) access prevents your Vultr account from being accessed programmatically. This restriction applies to all connected API clients, including the Linux cURL command, Vultr CLI, and programming language libraries.

Follow this guide to disable API access for your account using the Vultr Customer Portal.

1. Navigate to **Account** and select **API** under **OTHER**.
2. Click **Disable API** under **Personal Access Token**.

Enable API Access

Learn how to enable and configure API access to automate and manage your Vultr resources programmatically.

Contents

01 Introduction	10
-----------------	----

How to Enable Vultr API Access

Introduction

Application Programming Interface (API) access allows you to interact with your Vultr account programmatically. The Vultr API supports various tools, including the Linux cURL command, the Vultr CLI, and libraries for modern programming languages.

Follow this guide to enable and manage API access for your account using the Vultr Customer Portal.

1. Navigate to **Account** and select **API** under **OTHER**.
2. Click **Enable API** under **Personal Access Token**.

Manage API Access Control

Learn how to configure and manage API access control settings to secure your Vultr accounts API interactions.

Contents

01 Introduction	10
-----------------	----

How to Manage Vultr API Access Control

Introduction

Access control enforces permissions for systems and services that interact with the Vultr Application Programming Interface (API). This mechanism enhances security by allowing or blocking specific IP address ranges from accessing your account via the API.

Follow this guide to manage API access control for your account through the Vultr Customer Portal.

1. Navigate to **Account** and select **API** under **OTHER**.
2. Under **Access Control**, enter the IP addresses you want to permit and click **Add**.
3. Select an IP from the list and click **Remove** to delete the entry from the list.

FAQ

A collection of common questions and answers about managing and using Vultr API keys for platform automation and integration.

Contents

01	Introduction	10
02	What should I do if I suspect my API key is compromised?	160
03	Which clients are supported by the Vultr API key?	160
04	How should I store API keys securely?	160

Frequently Asked Questions (FAQs) for Vultr API Key

Introduction

These are the frequently asked questions for Vultr API Key.

What should I do if I suspect my API key is compromised?

If you suspect your API key has been compromised or observe any suspicious activity, regenerate the key immediately to revoke access and secure your account.

Which clients are supported by the Vultr API key?

The Vultr API key can be used with various clients, including Postman, the Linux cURL command, the Vultr CLI, and libraries for popular programming languages.

How should I store API keys securely?

Store API keys in environment variables or encrypted configuration files. Avoid hard-coding keys into your source code, and consider using a separate API key for each project to improve security and manageability.

Current User API Key Management

Securely manage Vultr current user API keys: create, list, delete, and rotate easily.

Contents

01	Create New API Key	163
02	Delete API Key	167
03	List API Key	171
04	Rotate API Key	174

Create New API Key

Create a new Vultr current user API key securely via portal or API.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Creating a new API Key for the current user allows you to manage access more securely, issue separate credentials for different integrations, and support key rotation without disrupting existing workflows.

Follow this guide to create a new API key for the current user in the Vultr Customer Portal or via Vultr API..

Vultr Customer Portal

1. Navigate to **Dashboard** and select **Vultr API** under **Orchestration**.
2. In **User Access Tokens** section, enter a **Name**, choose an API key **Expiry** option, and set the **Expiry On** date.
3. Click **Add Key**.
4. Copy the new API key and store it securely.

Vultr API

1. Send a `POST` request to the [Create API Key endpoint](#) to generate a new API key for your current user account.

CONSOLE

```
$ curl "https://api.vultr.com/v2/apikeys" \  
  -X POST \  
  -H "Authorization: Bearer ${VULTR_API_KEY}" \  
  -H "Content-Type: application/json" \  
  -d '{  
    "name": "<api-key-name>",  
    "expire": true,  
    "date_expire": "2030-01-01T00:00:00Z"  
  }'
```

The response returns the new API key in plain text. Copy and store it securely, as you cannot view or recover it later from the portal or API.

Delete API Key

Generate a new Vultr current user API key securely using portal or API.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Deleting a current user API key is an important security measure to prevent unauthorized access. Remove keys that are no longer needed or may be compromised to maintain secure account access.

Note

Deleting an API key immediately revokes its access. Any applications, scripts, or integrations using the deleted key will stop working. Ensure you have updated all workloads to use a replacement key before deleting an old key to avoid service interruptions.

Follow this guide to delete an API key for current user in the Vultr Customer Portal or via Vultr API.

Vultr Customer Portal

1. Navigate to **Dashboard** and select **Vultr API** under **Orchestration**.
2. In **User Access Tokens** section, locate the key you want to remove and click **Delete**.
3. Click **OK** to confirm the deletion.

Vultr API

1. Send a `GET` request to the [List API Keys endpoint](#) to retrieve all available API keys for the current user.

CONSOLE

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

Note the `id` of the API key you want to delete.

2. Send a `DELETE` request to the [Delete API Key endpoint](#) to remove the API key by ID.

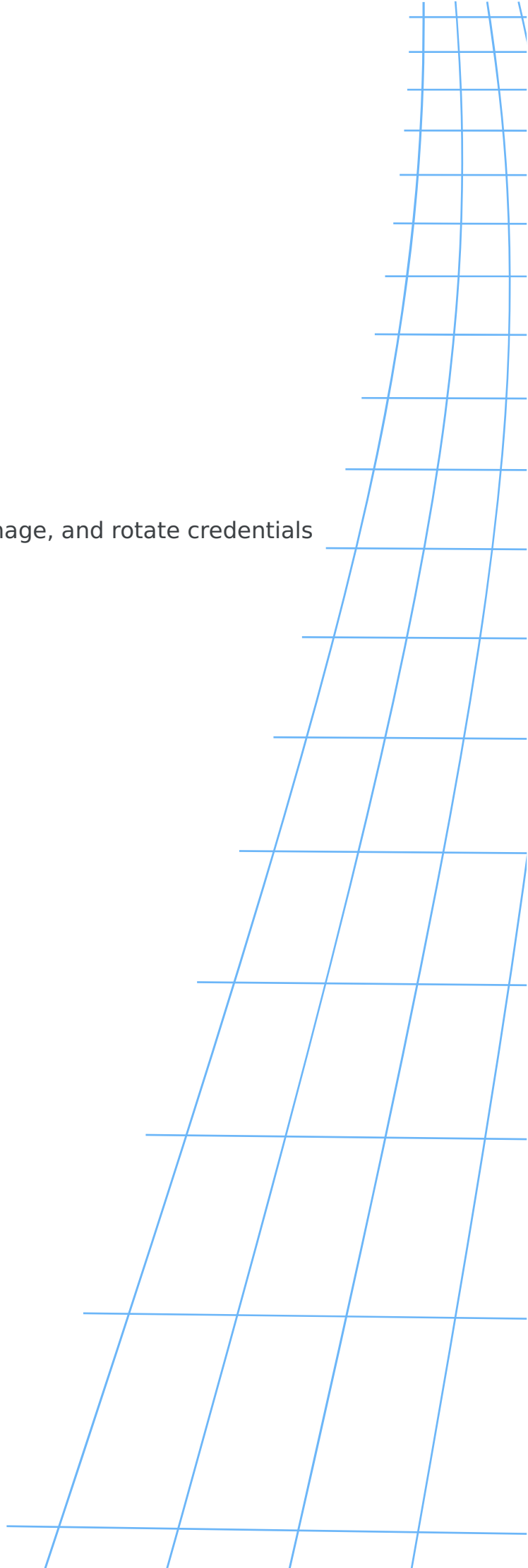
CONSOLE

```
$ curl "https://api.vultr.com/v2/apikeys/{apikey-id}" \  
  -X DELETE \  
  -H "Authorization: Bearer ${VULTR_API_KEY}"
```

An HTTP response of `204 No Content` confirms that your API key is deleted.

List API Key

List Vultr current user API keys to review, manage, and rotate credentials securely.



Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Listing API keys for the current user allows you to review active credentials, view access control, and manage key rotation securely. Regularly reviewing keys ensures you maintain proper access control and detect unused or compromised keys. Follow this guide to list your current user API keys in the Vultr Customer Portal or through the Vultr API.

Vultr Customer Portal

1. Navigate to **Dashboard** and select **Vultr API** under **Orchestration**.
2. In the **User Access Tokens** section, view all API keys associated with your current logged in user account, including their names, creation dates, and expiry information.

Vultr API

1. Send a `GET` request to the [List API Keys endpoint](#) to list all API keys for your current user account.

CONSOLE

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

2. (Optional) Send a `GET` request to the [Get API Key endpoint](#) to retrieve detailed information for a single API key by using its ID.

CONSOLE

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

Rotate API Key

Rotate Vultr current user API keys securely with zero downtime using portal or API.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Regularly rotating API keys is a security best practice that reduces the risk of unauthorized access and credential compromise. This guide provides a safe, zero-downtime workflow to rotate your current user API key using the Vultr Customer Portal or the Vultr API. Follow these steps to rotate a current user API Key, ensuring your applications and automation continue to function without interruption.

Vultr Customer Portal

1. Navigate to **Dashboard** and select **Vultr API** under **Orchestration**.
2. In **User Access Tokens** section, enter a **Name**, choose an API key **Expiry** option, and set the **Expiry On** date.
3. Click **Add Key**.
4. Update all applications, scripts, and automation to use the new API key.
5. After verifying that all workloads successfully authenticate with the new API key, delete the old key in **User Access Tokens** section.

Vultr API

1. Send a `POST` request to the [Create API Key endpoint](#) to generate a new API key for your current user account.

CONSOLE

```
$ curl "https://api.vultr.com/v2/apikeys" \  
  -X POST \  
  -H "Authorization: Bearer ${VULTR_API_KEY}" \  
  -H "Content-Type: application/json" \  
  -d '{  
    "name": "<api-key-name>",  
    "expire": true,  
    "date_expire": "2030-01-01T00:00:00Z"  
  }'
```

The response returns the new API key in plain text. Copy and store it securely, as this is the only time you can view it.

2. Update your applications, scripts, and automation to use the new API key, then validate that they work correctly.
3. Send a `GET` request to the [List API Keys endpoint](#) to view all API keys for the current user and identify the old key's ID.

CONSOLE

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

4. Send a `DELETE` request to the [Delete API Key endpoint](#) to delete the old API key.

CONSOLE

```
$ curl "https://api.vultr.com/v2/apikeys/{apikey-id}" \  
  -X DELETE \  
  -H "Authorization: Bearer ${VULTR_API_KEY}"
```

An HTTP response of `204 No Content` confirms that your API key is deleted.

Other Users API Key Management

Manage other users' Vultr API keys: create, list, delete, and rotate securely.

Contents

01	Delete API Key	180
02	Create New API Key	184
03	List API Key	188
04	Rotate API Key	192

Delete API Key

Delete Vultr user API keys with admin access to maintain security and prevent misuse.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Deleting a user's API key is an important security practice to prevent unauthorized access and reduce the risk of compromised credentials. When an API key is no longer in use, or after you generate a replacement during credential rotation, remove the old key to keep your environment secure.

Note

When managing API Keys for other users:

- You must have root or administrator credentials in Vultr to perform these actions.
- Deleting a API key immediately invalidates it. Applications, scripts, and integrations using the deleted API key will lose access.
- Update all workloads to use a replacement API key before deleting the old API key to avoid service interruptions.

Follow this guide to delete a user API key using the Vultr Customer Portal or the Vultr API.

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. In the **User Access Tokens** section, locate the key you want to remove and click **Delete**.
4. Click **OK** to confirm the deletion.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to list all users.

CONSOLE

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

Note the `id` of the user whose API key you want to delete.

2. Send a `GET` request to the [List User API Keys endpoint](#) to list the API keys for that user.

CONSOLE

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

Note the `id` of the API key you want to delete.

3. Send a `DELETE` request to the [Delete User API Key endpoint](#) to remove the key by ID.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/apikeys/  
{apikey-id}" \  
  -X DELETE \  
  -H "Authorization: Bearer ${VULTR_API_KEY}"
```

The API responds with `204 No Content` to confirm successful deletion.

4. Send a `GET` request to the [List User API Keys endpoint](#) again to verify the key no longer appears in the response.

CONSOLE

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

Confirm that the deleted key ID no longer appears in the output.

Create New API Key

Create and manage Vultr API keys for other users with admin credentials securely.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Creating an additional API key for a user allows you to isolate access per integration, improving security and simplifying credential management. This enables better access control and easier rotation of credentials.

Note

This guide covers creating API Keys for other users linked to the same Vultr account and requires root or administrator credentials to perform these actions

Follow this guide to create a user API key using the Vultr Customer Portal or Vultr API.

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. In **User Access Tokens** section, enter a **Name**, choose an API key **Expiry** option, and set the **Expiry On** date.
4. Click **Add Key** to create the new API key.
5. Copy and store the new API key securely, as you cannot view it again.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to list all users.

CONSOLE

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

Note the `id` of the user for whom you want to create an API key.

2. Send a `POST` request to the [Create User API Key endpoint](#) and specify the user ID to create a new API key for the target user.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/apikeys" \
-X POST \
-H "Authorization: Bearer ${VULTR_API_KEY}" \
-H "Content-Type: application/json" \
--data '{
  "name": "<api-key-name>",
  "expire": true,
  "date_expire": "2030-01-01T00:00:00Z"
}'
```

The response includes the newly generated API key in plain text. This is the only time the key is visible. Copy and store it in a secure location as you cannot view or recover it later from the portal or API.

List API Key

List Vultr user API keys with admin access to audit, monitor, and manage credentials.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Listing a user's API keys allows you to audit active credentials, monitor usage, and manage key rotation effectively. Regularly reviewing API keys helps maintain security by identifying unused or outdated credentials.

Note

This guide covers listing API Keys for other users. You must have root or administrator account credentials in Vultr to perform these actions.

Follow this guide to list a user's API keys in the Vultr Customer Portal or through the Vultr API.

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. Scroll to the `User Access Tokens` section to view all API keys associated with the user.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to list all users.

CONSOLE

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

Note the `id` of the user whose API keys you want to list.

2. Send a `GET` request to the [List User API Keys endpoint](#) to list all keys for that user.

CONSOLE

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

3. (Optional) Send a `GET` request to the [Get User API Key endpoint](#) to retrieve details for a single key by ID.

CONSOLE

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

Rotate API Key

Rotate Vultr user API keys with admin access to maintain security and avoid downtime.

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

Introduction

Regularly rotating API keys is a critical security practice that reduces the risk of unauthorized access. A safe rotation process ensures your workloads keep running without downtime while you replace old keys with new ones.

Note

This guide covers managing API Keys for other users. You must have root or administrator account credentials in Vultr to perform these actions.

Follow this guide to rotate a specific user's API key using the Vultr Customer Portal or the Vultr API.

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. In **User Access Tokens** section, enter a **Name**, choose an API key **Expiry** option, and set the **Expiry On** date.
4. Click **Add Key** to create the new API key.
5. Update your applications, scripts, and automation to use the new API key.
6. After you confirm that workloads authenticate with the new key, delete the old key in **User Access Tokens** section.

Vultr API

1. Send a `GET` request to the [Get Users endpoint](#) to list all users.

CONSOLE

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

Note the `id` of the user whose API key you want to rotate.

2. Send a `POST` request to the [Create User API Key endpoint](#) to generate a new key for that user.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/apikeys" \
  -X POST \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
  --data '{
    "name": "<api-key-name>",
    "expire": true,
    "date_expire": "2030-01-01T00:00:00Z"
  }'
```

The response includes the new API key in plain text. Copy and store it securely, as this is the only time you can view it.

3. Update your applications, scripts, and automation to use the new API key, then validate that they work correctly.
4. Send a `GET` request to the [List User API Keys endpoint](#) to view all keys for the user.

CONSOLE

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

Identify the `id` of the old API key you want to remove.

5. Send a `DELETE` request to the [Delete User API Key endpoint](#) to delete the old key.

CONSOLE

```
$ curl "https://api.vultr.com/v2/users/{user-id}/apikeys/
{apikey-id}" \
```

```
-X DELETE \  
-H "Authorization: Bearer ${VULTR_API_KEY}"
```

The response returns `204 No Content` to confirm successful deletion.

6. Send another `GET` request to the [List User API Keys endpoint](#) to verify that the old key no longer appears in the response.

CONSOLE

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

Sub Accounts

Manage separate accounts with unique credentials and permissions under your primary Vultr account for team collaboration and access control.

Contents

01	Create a Sub Account	199
02	Monitor Sub Accounts	204
03	Activate a Sub Account	208
04	FAQ	213

Create a Sub Account

Learn how to create a sub-account to manage separate billing and resources under your main Vultr account

Contents

01	Introduction	10
02	Vultr Customer Portal	10
03	Vultr API	10

How to Create a Vultr Sub-Account

Introduction

Vultr Sub-Accounts is an account management feature that lets you create, monitor, and manage multiple accounts attached to your Vultr account. A Sub-Account is an independent Vultr user account that's linked to a parent Vultr account. A Sub-Account shares the parent account's billing information, allowing you to set up an account linking structure to separate specific user accounts with centralized billing to your main Vultr account.

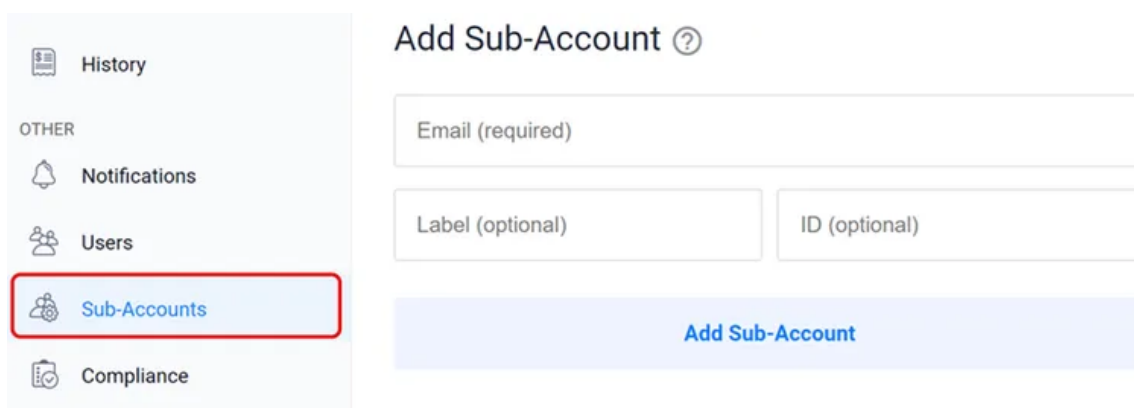
Follow this guide to create a Sub-Account using the Vultr Customer Portal or API.

Note

The Vultr Sub-Accounts feature is not enabled by default. Please [contact Vultr Sales](#) to enable the Sub-Accounts feature on your Vultr account if it's not available on your account.

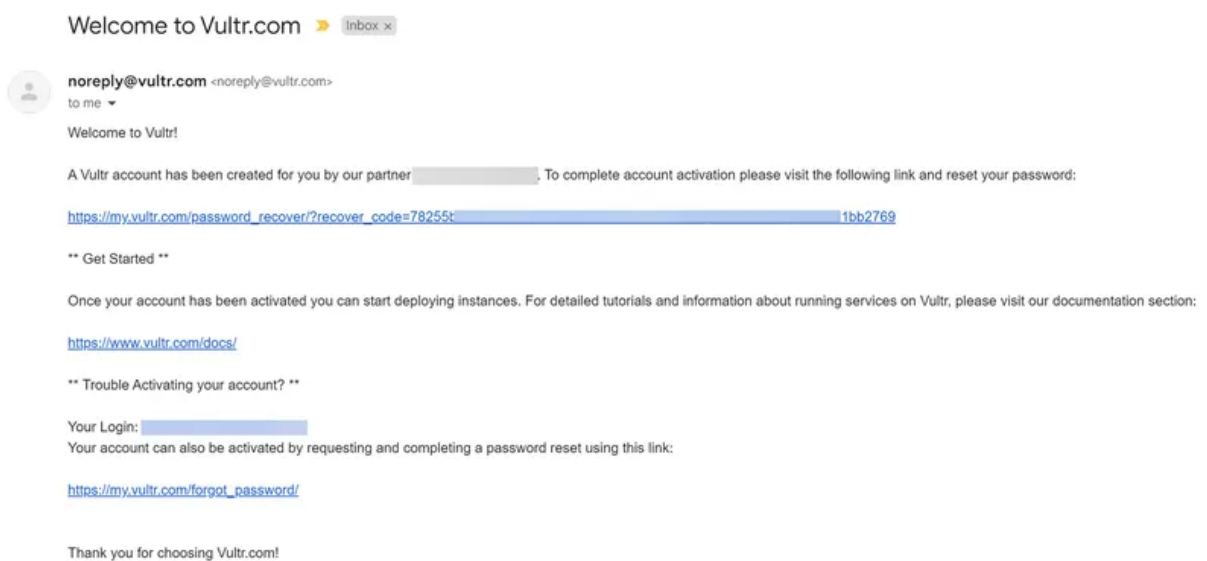
Vultr Customer Portal

1. Navigate to **Account**.
2. Find and Click **Sub-Accounts** within the **OTHER** section.



The screenshot displays the Vultr Customer Portal interface. On the left, a sidebar menu lists various options: History, OTHER, Notifications, Users, Sub-Accounts (highlighted with a red border), and Compliance. The main content area is titled 'Add Sub-Account' with a help icon. It contains three input fields: 'Email (required)', 'Label (optional)', and 'ID (optional)'. Below these fields is a blue button labeled 'Add Sub-Account'.

3. Fill in your Sub-Account information in the **Email** and **Label** fields respectively.
4. Enter your desired ID value in the **ID** field. For example, `1` translates to the user ID `1` depending on your desired identification scheme.
5. Click **Add Sub-Account** to create the Sub-Account and send an invitation email to the specified email address.
6. Open your email inbox, locate the new account invitation email from `noreply@vultr.com`, and open it.



7. Click the recovery link in the **Welcome to Vultr.com** email to set up the new Sub-Account and reset the password.

Vultr API

1. Send a `POST` request to the [Create Sub-Account endpoint](#) to create a new Sub-Account.

```
CONSOLE
$ curl "https://api.vultr.com/v2/subaccounts" \
  -X POST \
  -H "Authorization: Bearer ${VULTR_API_KEY}" \
  -H "Content-Type: application/json" \
```

```
--data '{
  "email" : "{subaccount_email}",
  "subaccount_name" : "{subaccount_label}",
  "subaccount_id" : "{custom_subaccount_ID}"
}'
```

2. Send a `GET` request to the [List Sub-Accounts endpoint](#) to view all Sub-Accounts for your account.

CONSOLE

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

Monitor Sub Accounts

Learn how to track and monitor the activity and resource usage of your Vultr sub-accounts from the parent account dashboard.

Contents

01 Introduction	10
-----------------	----

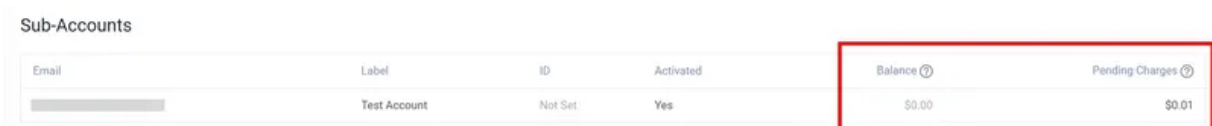
How to Monitor Vultr Sub-Accounts

Introduction

Monitoring Sub-Accounts allows you to view all active child accounts, pending charges, and the account balance for each account. You can view the Sub-Account email addresses, IDs, activation status, and billing charges, allowing you to monitor the status of each Sub-Account attached to your parent Vultr account.

Follow this guide to monitor Sub-Accounts using the Vultr Customer Portal.

1. Navigate to **Account**.
2. Find and click **Sub-Accounts** within the **OTHER** section.
3. Review the list of all Sub-Accounts attached to your parent account.



Email	Label	ID	Activated	Balance ⓘ	Pending Charges ⓘ
	Test Account	Not Set	Yes	\$0.00	\$0.01

For every Sub-Account:

- **Balance:** Represents the Sub-Account's billing balance. The balance value is ZERO for newly created Sub-Accounts. A positive balance means that a payment has previously been made directly to the account to cover all pending charges. A negative balance represents pre-existing charges incurred by the Sub-Account before attachment to your parent account.
- **Pending Charges:** The real-time Sub-Account charges that will be billed to your parent Vultr account at the end of the billing cycle. For example, if a Sub-Account user deploys a new Vultr Cloud Compute instance, the real-time usage costs display in the **Pending Charges** section. These charges are directly billed to your parent Vultr account at the end of the billing cycle.

  **Note**

The Vultr Sub-Accounts billing information updates whenever the child account incurs new charges. Please contact [Vultr Support](#) to set up billing limits for each Sub-Account attached to your Vultr account.

Activate a Sub Account

Learn how to activate a sub-account to access its resources and billing information in your Vultr customer portal

Contents

01 Introduction	10
-----------------	----

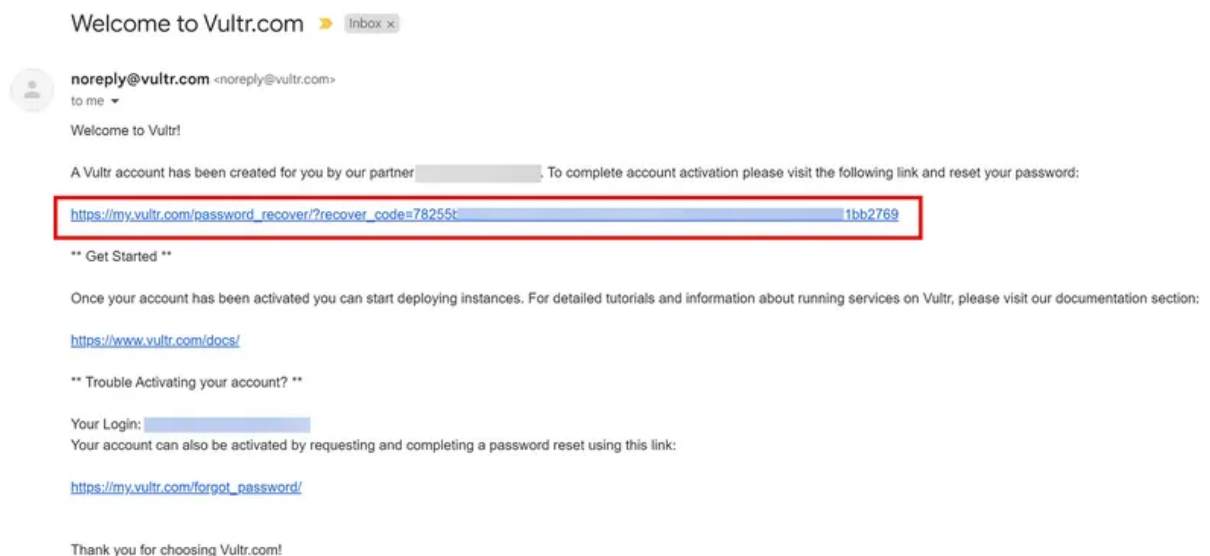
How to Activate a Vultr Sub-Account

Introduction

Activating a Vultr Sub-Account allows you to change the account password, deploy, and manage Vultr Cloud resources. To activate a new Vultr Sub-Account associated with your main account, ensure that the Sub-Account has been created and is marked as inactive in your parent account, then open the invitation email in your inbox.

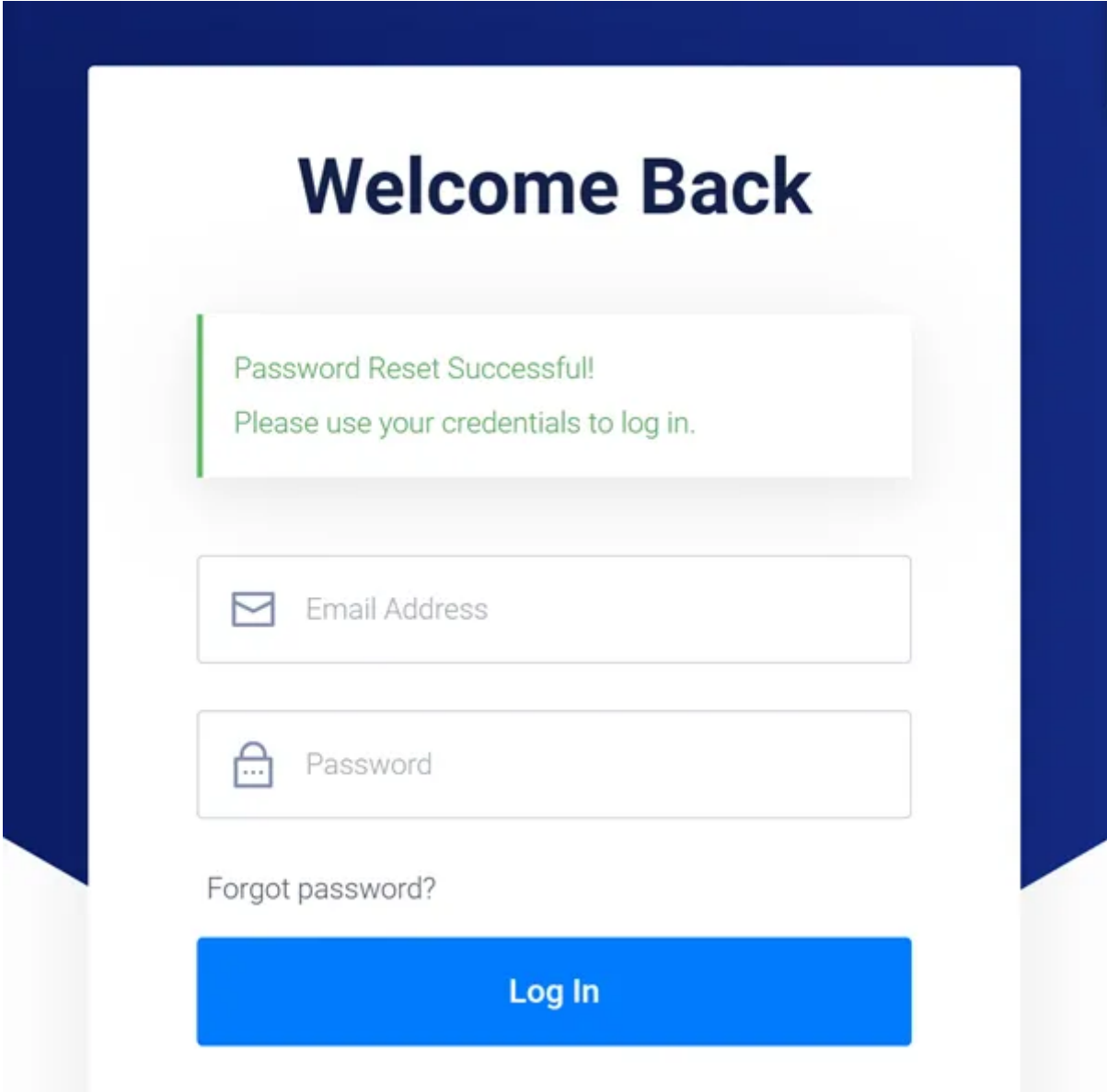
Follow this guide to activate a Vultr Sub-Account by completing the account activation process using the Vultr Customer Portal.

1. Open the **Welcome to Vultr.com** verification email in your inbox.



2. Find and click the password reset link in the email body to redirect to the Vultr account password setup page.
3. Enter a new strong password in the **Password** field.

4. Repeat the password in the **Confirm New Password** field to verify that your passwords match.
5. Check the **I agree to the Terms of Service** option to accept the Vultr terms of service agreement.
6. Click **Reset Password** to activate the new Vultr Sub-Account password and be redirected to the Vultr Customer Portal login page.




The screenshot displays a login interface with a dark blue header and footer. The main content area is white and features a large, bold, dark blue heading "Welcome Back". Below the heading is a green-bordered box containing the text "Password Reset Successful!" and "Please use your credentials to log in." in green. Underneath this box are two input fields: the first is labeled "Email Address" with an envelope icon, and the second is labeled "Password" with a lock icon. Below the password field is a link that says "Forgot password?". At the bottom of the form is a prominent blue button with the text "Log In" in white.

7. Enter your Vultr Sub-Account **Email Address** and **Password** in the respective fields.
8. Click Log in or press Enter to log in and activate the Sub-Account.

9. Navigate to the **Vultr Sub-Accounts** management page using the parent account and verify that the new Sub-Account's **Activated** value changes from **No** to **Yes**.

Sub-Accounts

Email	Label	ID	Activated	Balance ⓘ	Pending Charges ⓘ
[REDACTED]	Test Account	Not Set	Yes	\$0.00	\$0.00



FAQ

A comprehensive resource addressing common questions about managing and using Vultr Sub-Accounts.

Contents

01	Introduction	10
02	How many Sub-Accounts can I create and attach to my account?	215
03	What information is shared or inherited by the Sub-Accounts attached to my Vultr account?	215
04	Can I delete a Vultr Sub-Account?	216
05	How many users can a single Vultr Sub-Account support?	216
06	If my parent Vultr account is suspended, do the Sub-Accounts stay active?	216
07	Can I attach existing Vultr accounts as Sub-Accounts to my Vultr account?	216
08	Can I restrict Sub-Accounts to specific budget caps per billing cycle?	217
09	Can I edit the Vultr Sub-Account information details?	217
010	What is a parent account in Vultr Sub-Accounts?	217
011	What's a child account in Vultr Sub-Accounts?	217
012	How are Sub-Accounts different from Vultr Account Users?	218
013	What are the benefits of using Vultr Sub-Accounts?	218

Frequently Asked Questions (FAQs) for Vultr Sub-Accounts

Introduction

These are the frequently asked questions for Vultr Sub-Accounts.

How many Sub-Accounts can I create and attach to my account?

You can create and attach an unlimited number of sub-accounts to your parent Vultr account. Upon activation, all charges incurred by every Sub-Account display in your billing information and are directly billed to your Vultr account at the end of each billing cycle.

What information is shared or inherited by the Sub-Accounts attached to my Vultr account?

All Vultr Sub-Accounts attached to your parent account share the same company or organization name and use your billing account as the default payment method. Navigate to **Account > Profile > Company Details** to update the company information to share with all Sub-Accounts attached to your account.

Can I delete a Vultr Sub-Account?

You cannot delete a Vultr Sub-Account directly. Please open a new [Vultr support ticket](#)) and include your target Sub-Account email address and ID to detach it from your account. Detaching a Sub-Account may not delete it as a Vultr account because it functions as a standalone profile on its own. To permanently delete the Sub-Account, please open a new Vultr support ticket using the child account and submit a service deactivation request.

How many users can a single Vultr Sub-Account support?

Each Vultr Sub-Account supports an unlimited number of additional users with limited or full access to the account. In this case, an entire organization department can use a single Vultr Sub-Account with multiple users sharing different access privileges.

If my parent Vultr account is suspended, do the Sub-Accounts stay active?

Yes, Sub-Accounts stay active and keep running until your parent Vultr account is restored. You will be required to enter a new payment method at the end of a billing cycle if the parent Vultr account is not restored.

Can I attach existing Vultr accounts as Sub-Accounts to my Vultr account?

No, you cannot attach existing Vultr user accounts directly as Sub-Accounts. Please contact Vultr Support to set up the necessary authorization to attach an existing Vultr account as a Sub-Account linked to your parent account. Verify

that the existing Vultr account is accessible and can authorize adoption requests from your parent Vultr account before contacting Vultr Support.

Can I restrict Sub-Accounts to specific budget caps per billing cycle?

You cannot restrict sub-accounts directly in your parent account. Please contact Vultr Support to restrict specific Sub-Accounts to a specific budget per quota to meet your billing procedure and plans at the end of each billing cycle.

Can I edit the Vultr Sub-Account information details?

You cannot edit the Vultr Sub-Account information directly. Please contact Vultr Support to modify the information of Sub-Accounts attached to your Vultr account.

What is a parent account in Vultr Sub-Accounts?

A parent account is your main Vultr account. All sub-accounts use your parent account as the default payment method. The parent account inherits all billing charges for the attached Sub-Accounts at the end of a billing cycle.

What's a child account in Vultr Sub-Accounts?

A child account is a Vultr Sub-Account with full functionality and access to all Vultr Cloud services. You can use a child account to deploy any type of infrastructure resources, with all charges billed to your parent account.

How are Sub-Accounts different from Vultr Account Users?

Sub-Accounts are independent Vultr User Accounts, directly linked to a single parent account, while Vultr Account Users are secondary users with access to a single account. You can create additional Vultr account users in a single Sub-Account, allowing you to create an organizational structure with a centralized billing account.

What are the benefits of using Vultr Sub-Accounts?

By using Vultr Sub-Accounts, you benefit from:

- Centralized billing management for multiple accounts.
- Enhanced account security and management.
- Independent resource deployment and management.

Manage Notifications

Learn how to configure and customize your account notifications to stay informed about important events on the Vultr platform.

Contents

01 Introduction	10
-----------------	----

How to Manage Notifications on Vultr

Introduction

Vultr provides customizable notifications to keep you informed about key events affecting your infrastructure. These alerts can help you stay ahead of potential issues, monitor resource usage, and keep track of billing activity. You can configure email notifications for maintenance, outages, bandwidth usage, and new invoices, ensuring your team receives timely updates.

Follow this guide to manage your notification settings using the Vultr Customer Portal.

1. Navigate to **Account** and select **Notifications** under **OTHER**.
2. Toggle email alerts **ON** for scheduled maintenance events and real-time outage notifications for affected instances or regions..

Maintenance and Outage Notifications

Send E-mails for Outage and Maintenance



3. For **Bandwidth** notifications, choose from the default thresholds or set a custom percentage.

Bandwidth Preferences

Send E-mail notifications when bandwidth usage exceeds a percentage of the [global bandwidth pool allotment](#).

Send E-mails at 75%, 90% and 100% Usage OFF

Send E-mails at a Custom Percentage of Usage ON

%

4. Select how you would like to receive notifications when a new invoice is generated, then click **Save** to apply your selection.

Invoice Preferences

New Invoice Notification
By E-mail

Account Logs

A comprehensive record of all actions and changes made to your Vultr account for security monitoring and troubleshooting purposes.

Contents

01 Introduction	10
-----------------	----

How to List Logs for a Vultr Account

Introduction

Logs provide detailed records of user actions across your account, capturing events such as logins, web portal interactions, and API requests. These logs offer valuable insight into account usage and help monitor security, track changes, and troubleshoot issues across your infrastructure. To access the List Logs API endpoint, you must either be the root user or have the appropriate ACL permission.

Follow this guide to retrieve the activity of users for your Vultr account using the Vultr API.

1. [Retrieve the API key](#) for your Vultr account from the Vultr Customer Portal.
2. Send a `GET` request to the List Logs endpoint.

CONSOLE

```
$ curl "https://api.vultr.com/v2/logs?
start_time=<START_TIME>&end_time=<END_TIME>&log_level=<LOG_LE
VEL>&resource_type=<RESOURCE_TYPE>&resource_id=<RESOURCE_ID>"
\
-X GET \
-H "Authorization: Bearer ${VULTR_API_KEY}"
```

- `<START_TIME>` - e.g., `2025-07-17T00:00:00Z`
- `<END_TIME>` - e.g., `2025-07-17T18:19:59Z`
- `<LOG_LEVEL>` - One of: `info`, `debug`, `warning`, `error`, `critical`
- `<RESOURCE_TYPE>` - e.g., `instances`, `load-balancers`, `kubernetes`, etc.
- `<RESOURCE_ID>` - UUID of the specific resource.
- `{VULTR_API_KEY}` - Your Vultr API key.

The response output looks similar to the one below.

```
{
  "logs": [
    {
      "resource_id": "xb671a46-66ed-4dfb-b839-543f2c6c0b63",
      "resource_type": "instances",
      "log_level": "debug",
      "message": "Success",
      "timestamp": "2025-06-26T16:45:06+00:00",
      "metadata": {}
    }
  ],
  "meta": {
    "continue_time": "2025-06-26T12:24:03Z",
    "returned_count": 5000,
    "unreturned_count": 3524,
    "total_count": 8524
  }
}
```

- To grant non-root users access to your account's activity logs, enable the `activity_logs` ACL for them by sending a `PATCH` request to the [Update User endpoint](#).

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" : true,
  "acls" : [
    "activity_logs"
  ]
}'
```

Note

As per our Terms of Service, Vultr retains customer activity logs for 30 days. Contact [Customer Support](#) if you require a retention period longer

than 30 days, as additional charges may apply. When specifying `start_time` and `end_time` in your API request, ensure that the selected time range falls within this retention window. Requests outside this period may return no results. Currently, the `max_query_series` limit is set to 5000, meaning a maximum of 5000 log entries can be returned per request, regardless of the specified date range.



VULTR

