

OpenSSH

A secure protocol for remote server access that comes pre-installed on Vultr instances, allowing encrypted connections from your local machine.

Contents

01	Introduction	3
02	Connect to an Instance Using the Default User Credentials	3
03	Connect to an Instance Using SSH Keys	4

How To Connect to a Vultr Optimized Cloud Compute Instance Using SSH

Introduction

OpenSSH is a connection protocol that enables SSH access to an instance. It is pre-installed and active on Vultr Optimized Cloud Compute instances by default to enable secure connections.

Follow this guide to connect to a Vultr Optimized Cloud Compute instance using SSH on your workstation.

Connect to an Instance Using the Default User Credentials

1. Open your instance's management page.
2. Note the default credentials within the **Overview** tab and copy the user password to your clipboard.
3. Open a new terminal or command prompt application on your workstation.
4. Connect to your Vultr Optimized Cloud Compute instance using SSH.

CONSOLE

```
$ ssh username@SERVER-IP
```

5. Enter `yes` and press `ENTER` when prompted to add the instance's public key to your known hosts.

```
The authenticity of host '192.0.2.123 (192.0.2.123)' can't be established.  
ED25519 key fingerprint is SHA256:gTA0uCiCa3Us4tpVaVHVk9d3q0jKrsqXP0sAFQbB8xw.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

6. Enter your instance user's password when prompted and press **ENTER** to log in.

```
username@SERVER-IP's password:
```

7. View the active user in your SSH session.

```
CONSOLE
```

```
$ whoami
```

Connect to an Instance Using SSH Keys

Note

Generate an SSH key on your workstation and add it to your instance during deployment. Adding an SSH key using the Vultr Customer Portal after deployment will result in data loss and wipe your instance to install the new key.

1. Open a new terminal or command prompt application on your workstation.
2. Connect to your Vultr Optimized Cloud Compute instance using a specific SSH key on your workstation.

```
CONSOLE
```

```
$ ssh -i /path/to/private/key username@SERVER-IP
```

3. Enter **yes** and press **ENTER** when prompted to add the instance's public key to your known hosts.

```
The authenticity of host '192.0.2.123 (192.0.2.123)' can't be established.  
ED25519 key fingerprint is SHA256:gTA0uCiCa3Us4tpVaVHVk9d3q0jKrsqXP0sAFQbB8xw.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

4. View the active user in your SSH session.

CONSOLE

```
$ whoami
```



VULTR

