

How to use SSH keys

Connect to an instance using an SSH key

You must provide an **SSH key** when you create a GPU instance with FluidStack. Once the instance is running, that SSH key is used to authenticate for remote command-line access to the instance.

Generate a public/private key pair

✕ Supported public key formats:

- ssh-rsa
- ssh-dss (DSA)
- ssh-ed25519
- ecdsa keys with NIST curves

If you already have a public/private key pair of a supported format, you can use that pair instead of generating a new one.

Follow the steps below to generate a key pair with a command-line tool called **ssh-keygen**. This tool is pre-installed on nearly all operating systems.

Use any supported format for your key pair. The tabs below contain instructions for generating a key pair with either the **RSA** algorithm or **ECDSA** algorithm.

RSA **ECDSA with NIST curves**

1 Generate the key pair

Enter the following command in your CLI shell:

```
$ ssh-keygen -t ecdsa -b 256 -f ~/.ssh/id_ecdsa_256
```

If prompted to enter a filename, press **Enter** to save the key pair to the default location (`~/.ssh/`). When prompted to enter a passphrase, you can optionally do so to increase security.

2 Confirm that your key pair was created

Enter the following command to confirm that your key pair was created:

```
$ ls ~/.ssh
```

In the output, you should see `id_ecdsa_256` (the file that contains your private key) and `id_ecdsa_256.pub` (the file that contains your public key).

3 View your public key

Open the `id_ecdsa_256.pub` file in a plaintext editor, or enter the command below to output it to your terminal:

```
$ cat ~/.ssh/id_ecdsa_256.pub
```

🔔 With any public/private key pair that you generate, your public key can be shared freely. Your private key should be just that—private! Take care not to share it with others, or in public repositories such as in GitHub.

Create an SSH key

Use your public key to create an SSH key on your FluidStack account. If you don't have a public key, see: [Generate a public/private key pair](#).

☆ In this context, "creating an SSH key" means "storing (adding) a copy of your public key on your FluidStack account." The stored SSH key is identical to your public key.

> Use the FluidStack Dashboard

∨ Use the FluidStack API

Create an SSH key by using the **Create an SSH key** endpoint.

```
POST /ssh_keys
curl -X POST https://platform.fluidstack.io/ssh_keys \
  -H "api-key: <api-key>" \
  -H "Content-Type: application/json" \
  -d '{
  "name": "my_ssh_key",
  "public_key": "<my_public_key>"
}'
```

☆ Make sure to replace the `<api-key>` value with your API key, the `<public-key>` value with your public key, and the `name` of `my_ssh_key` with the unique SSH key name you'd like to use.

If your POST request is successful, the endpoint responds with a JSON object that

- [Generate a public/private key pair](#)
- [Create an SSH key](#)
- [View existing SSH keys](#)
- [Delete an SSH key](#)
- [Connect to an instance with an SSH key](#)

echoes the `name` and `public_key` that you sent:

```
Response example
1 {
2   "name": "my_ssh_key",
3   "public_key": "<your_public_key>"
4 }
```

View existing SSH keys

> Use the FluidStack Dashboard

▼ Use the FluidStack API

View SSH keys that have been added to your FluidStack account by using the [List SSH keys](#) endpoint:

```
GET /ssh_keys
curl https://platform-fluidstack.io/ssh_keys \
-H "api-key: <api-key>"
```

If your GET request is successful, the endpoint responds with a JSON array of objects. Each object in the JSON array represents an SSH key, including its `name` and `public_key`:

```
Example response
1 [
2   {
3     "name": "my_ssh_key",
4     "public_key": "<public_key>"
5   },
6   {
7     "name": "another_ssh_key",
8     "public_key": "<public_key>"
9   }
10 ]
```

Delete an SSH key

🔔 Deleting an SSH key removes the ability to authenticate to instances with that key.

> Use the FluidStack Dashboard

▼ Use the FluidStack API

Delete an SSH key by using the [Delete an SSH key](#) endpoint. Replace the text `{ssh_key_name}` with the name of the key you want to delete:

```
DEL /ssh_keys/{ssh_key_name}
curl -X DELETE https://platform-fluidstack.io/ssh_keys/{ssh_key_name} \
-H "api-key: <api-key>"
```

Connect to an instance with an SSH key

Use your private key to authenticate when connecting to a running instance via SSH. The instance has an SSH key associated with it, provided when that instance was created. The private key must correspond to that SSH key.

```
Connect to your instance with SSH
$ ssh -i <path_to_your_private_key> <username>@<ip_address>
```

Examples:

```
RSA ECDSA
$ ssh -i ~/.ssh/id_rsa ubuntu@192.0.2.0
```

Was this page helpful? Yes No

Get started

- Home
- Quickstart
- API overview

Account management

- Dashboard >

Instances

- Manage >
- Configurations
- Operating systems

SSH

- What is SSH?
- How to use SSH keys

SDKs

- Python >

API reference

- Instances >
- SSH Keys >
- Configurations >