SSH Key & Login (OpenSSH)

Last update: Jan 9, 2026.

Introduction

On PowerShell (Windows), Terminal.app (Mac), or terminal applications of Linux, you can generate SSH keys using the OpenSSH ssh-keygen command from the command line.

Key generation using ssh-keygen

Ed25519, ECDSA-384, ECDSA-256, RSA 4096 bits keys can be used. Please use Ed25519 if you have no preference.

Run the "ssh-keygen" command in a command line environment (such as Windows PowerShell, Terminal.app (Mac), or a terminal on Linux Xorg environment (e.g. xterm, gnome-terminal)). When creating the key, you can set a passphrase for the private key. Please set it properly.

The public key will be generated as a file under .ssh directory. For example, in case of Ed25519 key, the filename will be ~/.ssh/id_ed25519.pub.

The contents of the generated public key file (this file contains only one line) should be uploaded according to the instruction in "How to set your password and put your public key" page. After the completion of this step, you can login to our server (ccfep.ims.ac.jp) via SSH.

Ed25519

```
ssh-keygen -t ed25519
```

ECDSA-384

```
ssh-keygen -t ecdsa -b 384
```

ECDSA-256

```
ssh-keygen -t ecdsa -b 256
```

RSA 4096 bits

```
ssh-keygen -t rsa -b 4096
```

Login

After uploading the public key according to "How to set your password and put your public key", please execute following command on terminal (PowerShell, Terminal.app etc.).

```
ssh (user id)@ccfep.ims.ac.jp
```

Please replace (user id) part with your 3-letters id assigned by RCCS. You will need to input passphrase if a passphrase is set for the private key.

You can specify private key file name with "-i" option. (NOTE: files such as ~/.ssh/id_ed25519, ~/.ssh/id_ecdsa, and ~/.ssh/id_rsa will be referenced even if not specified.)

```
ssh -i ~/.ssh/id_ed25519 (user id)@ccfep.ims.ac.jp
```

Ed25519 example

We will show a sample SSH setting using Ed25519 key in this page.
The procedure itself is common among Windows PowerShell, Mac Terminal.app, and various Linux terminal emulators.
You need to type (or paste) red-colored texts. Blue-colored texts are mere comments or notes.
Some strings, such as "user" and "hostname", are system-dependent.

First, we generate a new key pair.

```
user@hostname ~ % ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/user/.ssh/id_ed25519): (press enter is default loc is OK)
Enter passphrase (empty for no passphrase): (input password for this key)
Enter same passphrase again: (input password for this key, again)
Your identification has been saved in /Users/user/.ssh/id_ed25519 (private key file)
Your public key has been saved in /Users/user/.ssh/id_ed25519.pub (public key file)
The key fingerprint is:
SHA256:**************************************** user@hostname.domain
The key's randomart image is:
+--[ED25519 256]--+
|            |
|            |
|            |
|            |
|  (skipped)    |
|            |
|            |
|            |
|            |
+----[SHA256]-----+
user@hostname ~ %
```

You need to upload contents of public key ~/.ssh/id_ed25519.pub (/Users/user/.ssh/id_ed25519.pub) to this website according to the guide in this page. The location of key files can be found in the ssh-keygen log. The public key file (.pub) is a text file and it should contain single-line text. You should upload that line. You MUST NOT upload private key file (~/.ssh/id_ed25519 here).

The key pair generated here can be used for other software such as WinSCP, cyberduck, and FileZilla.

Once you uploaded the public key, let's login to login server.

```
user@hostname ~ % ssh uid@ccfep.ims.ac.jp (uid is a three-letter ID provided by RCCS (e.g. xxx))
The authenticity of host 'ccfep.ims.ac.jp (133.48.230.13)' can't be established.
ED25519 key fingerprint is SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI. (some other string might be shown; see below)
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes (required upon first login)
Warning: Permanently added 'ccfep.ims.ac.jp' (ED25519) to the list of known hosts.
Enter passphrase for key '/Users/user/.ssh/id_ed25519': (input password used at ssh-keygen step)
[uid@ccfep* ~]$ (you can login to one of login server if you input correct password.)
```

Most of the strings other than passphrase one are first-time only. You won't see those confirmation messages on second and subsequent login attempts.

Tips

Some tips about login.

How to access generated public key file with Finder? (Mac)

Files begin with . (dotfiles), such as .ssh, are not normally displayed in the Finder. They can be displayed on Finder by pressing " Command + Shift + . " keys.

If you want to hide them, press " Command + Shift + . " again.
The public key file (.pub file) is just a text file, so you can open it with TextEdit.

Host fingerprint

After the "*** key fingerprint is" message, one of following fingerprints will be displayed.

- wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJllxWehryCtStIp1Dir (SHA256)

Configuration file (~/.ssh/config)

You can save settings in ~/.ssh/config file. You can omit domain name (.ims.ac.jp), username (e.g. xxx) by using following example.
Blue-colored "uid" must be replaced with your user ID (three-letter ID provided by RCCS).
If you have more than one keys, you may need to specify key file with "IdentityFile" keyword.

```
Host ccfep
  HostName ccfep.ims.ac.jp
  User uid
```