Share files between two machines

When you're working on multiple machines (e.g., your laptop and a remote server), it's often useful to transfer files between them quickly. There are several straightforward methods to do this.
Here we present two options:

- a command line one (scp)
- a graphical one (FileZilla)

1. **Using scp (Secure Copy)**

scp is the simplest command-line tool for copying files over a secure SSH connection. It works on Windows (with PowerShell or Git Bash), Linux and macOS.

Copying from your local machine to a remote server:

```
> scp /path/to/local/file username@server:/path/to/remote/destination
```

- username → your login name on the server
- server → the server's IP address or domain name (e.g. jed.hpc.epfl.ch)
- ~ → shorthand for your home directory on either machine

Example:

```
> scp lab01.zip ruser@ jed.hpc.epfl.ch:~/DSD_LAB
```

- Note that the DSD_LAB directory here should already exist.

Copying from the server to your local machine:

```
> scp username@server:/path/to/remote/file /path/to/local/destination
```

Example:

```
> scp alice@192.168.1.10:~/work/report.txt    .
```

- The . means "copy into the current directory."

Copying entire directories:
Add the -r option to copy folders:

```
> scp -r ~/Projects alice@jed.hpc.epfl.ch:~/backup/
```

💡 **Tip:** You can put these commands into shell scripts for frequent transfers

When you use scp (or SSH) to connect to a server **for the first time**, you'll see a message like this:

```
The authenticity of host '192.168.1.10 (192.168.1.10)' can't be established.
ECDSA key fingerprint is SHA256:examplefingerprint.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

This is a **security check**: the server is sending you its SSH key fingerprint.

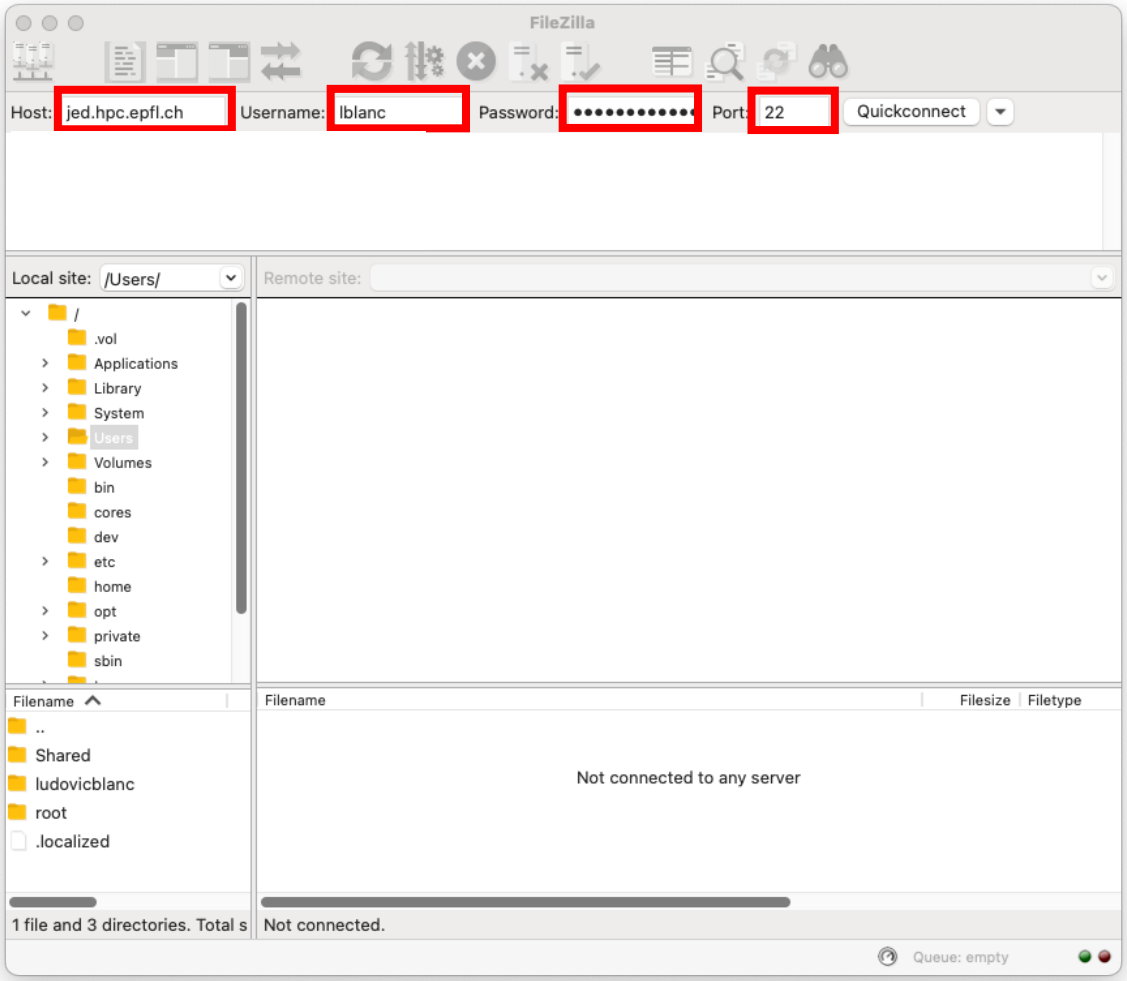
- Type yes and press **Enter** to continue.
- The server's key will be saved to your local ~/.ssh/known_hosts file.
- Next time you connect, the system will recognize the server automatically, so you won't see this prompt again (unless the server's key changes).

2. **Using FileZilla (Graphical Interface)**

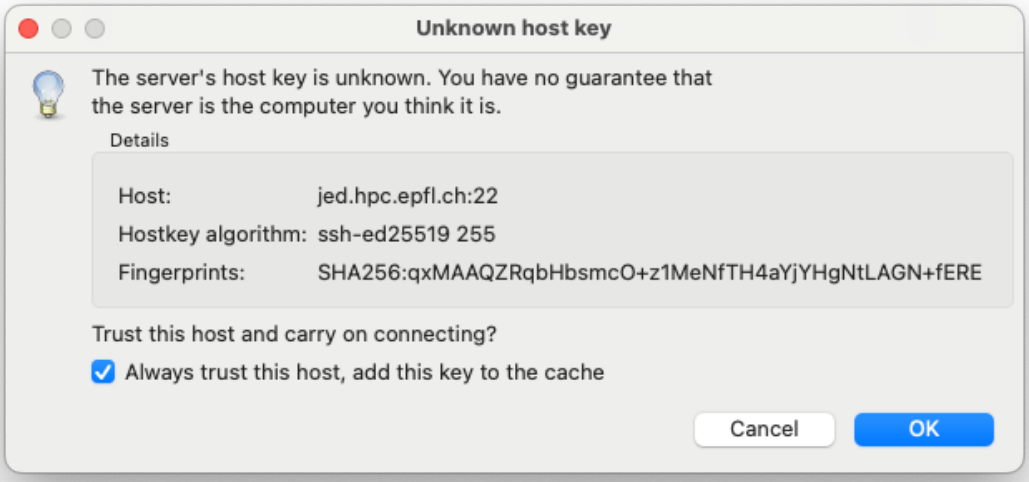
If you prefer a graphical interface, [FileZilla is a free FTP client] that also supports **SFTP** (secure file transfer over SSH).

1. Download and install FileZilla Client (not the server).
2. Open FileZilla and enter:
    - **Host:** your server's IP or domain
    - **Username:** your SSH login name (GASPAR)
    - **Password:** your SSH password (or configure an SSH key)
    - **Port:** usually 22 for SSH
3. Press Quickconnect.

.



When you use scp (or SSH) to connect to a server **for the first time**, you'll see a message like this:



Tick “Always trust this host, add this key to the cache” and press ok

1. Once connected, you can drag and drop files between your local system and the server. This is especially convenient for transferring multiple files or navigating complex directory structures