This guide explains how to generate your security keys and configure your software to access our secure file exchange server (SFTP).

Prerequisites

To connect, we do not use a password, but an **SSH key pair** (a public key that you give us, and a private key that you keep).

Step 1: Generate your SSH key pair

🍎 On macOS / Linux

1. Open the **Terminal** application.
2. Copy and paste the following command and press **Enter**:

```
ssh-keygen -t rsa -b 4096 -C "your-email@partner.com"
```

3. The terminal will ask where to save the key. Press **Enter** to accept the default location.
4. It will ask for a passphrase. You can press **Enter** twice to skip one (simpler for automation), or set one for extra security.

Your keys are created in the hidden folder `/Users/your_name/.ssh/` :

- `id_rsa` : This is your **PRIVATE KEY**. (Never share it with anyone.)
- `id_rsa.pub` : This is your **PUBLIC KEY**.

🪟 On Windows (10 and 11)

1. Open the Start menu and type **PowerShell**.
2. Copy and paste the following command and press **Enter**:

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

3. Press **Enter** at each prompt to accept the defaults.

Your keys are created in the folder `C:\Users\YourName\.ssh\` :

- `id_rsa` : This is your **PRIVATE KEY**.
- `id_rsa.pub` : This is your **PUBLIC KEY**.

Step 2: Send us your public key

1. Go to the folder where the keys were created.
2. Open the file ending in `.pub` (e.g. `id_rsa.pub`).

3. Email us that file.

⚠️ **IMPORTANT:** Never send us the file with no extension (your private key). Keep it safe—it is your “passport” for access.

Partner import — server addresses

Use the host that matches your environment (**staging** vs **production** tests). Your **username** is provided by your Swile contact.

Step 3: Connect with FileZilla

We recommend the free **FileZilla Client** software, but any SFTP-compatible client works (WinSCP, Cyberduck, Transmit).

1. Download and install FileZilla Client.
2. Open FileZilla and go to **File** > **Site Manager** (or the icon at the top left).
3. Click **New Site** and name it (e.g. “SFTP exchange”).
4. Configure the **General** tab as follows:

Field	Value
Protocol	**SFTP - SSH File Transfer Protocol** (Very important!)
Host	For partner import SFTP, use the **Staging** or **Production** host from *Partner import — server addresses* above; otherwise *(the address we provided by email)*
Port	`22`
Logon Type	**Key file**
User	*(The username we provided by email)*
Key file	Click “Browse” and select your **private key** file (`id_rsa`) generated in step 1.

> *Note: If FileZilla asks to convert the key to another format, click “Yes”.*

5. Click **Connect**.

FAQ / Troubleshooting

I cannot see my keys in the .ssh folder
Folders whose names start with a dot are often hidden.

- *On Mac:* In Finder, press `Cmd + Shift + .` to show hidden files.
- *On Windows:* In File Explorer, open the “View” tab and enable “Hidden items”.

Error “Permission denied (publickey)”
This usually means:

- You are not using the correct private key.
- We have not yet enabled your access with the public key you sent us.
- The username is incorrect.

Can I use the same key on several computers?
Yes. You can copy your private key file (`id_rsa`) to another computer or server to automate uploads.