How to Connect Your Push3 Gateway to a SFTP Server

To connect to your Gateway UI, use its IP. Find it by logging into your https://api.ekmpush.com/ account, navigate to your Gateway MAC Address on the left-hand side, and click on the displayed IP (e.g., LAN IP: 192.168.0.3) under 'LAN IP':

Log into your Gateway UI, navigate to Settings > SFTP/Archive, and select *Enable SFTP*. Next, you will find explanations on how to connect using either *User/Password* or *Perform client authentication using public/private key*.

For our example server, the login details are as follow:

Host: 192.168.0.10

User: test

Password: Test123

Using *User/Password* Authentication

If you only have the IP, username, and password of your remote server where you want to save your files, you can fill them into the corresponding inputs, like this::

- **Host:** 192.168.0.10
- **User:** test
- **Password:** Test123
-

Finally, press the '**Apply**' button to save the filled configurations.

You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.

Using a Private Key for Authentication

If you already have experience with Private/Public Keys and don't need to follow the next steps because you already have your own Private Key, select *Perform client authentication using public/private key*. Copy your Private Key (yes, it is the Private Key; we are not wrong 😉) and paste it into the *Private Key* blank space. Also, ensure that your Public Key is added to your remote server in `~/.ssh/authorized_keys` . Finally, press the '**Apply**' button to save the filled configurations. Wait at least 15 minutes to check if the data has been successfully saved to the server.

If you don't have enough experience, don't stress! We're here to help you. This is a more advanced guide where we'll explain how you cancreate your own keys using Linux or Windows.

Create your Private Key in Linux

You can create your **Private Keys** on your server or on another Linux server by following these instructions:

1. Open your terminal and run: `ssh-keygen -m PEM`
2. If you don't want to create it with a passphrase (password), simply press ENTER every time the terminal prompts you. You will see something like:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/myLaptop/.ssh/id_rsa):(Simply press
ENTER)
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/myLaptop/.ssh/id_rsa
Your public key has been saved in /home/myLaptop/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iB5mwc8jFw7jeb31tNWlp2OLKsosDoS1OzWuThNkzLM myLaptop@myLaptop
The key's randomart image is:
+---[RSA 3072]----+
|   o_ o .    .o..|
|  ..E= = oo .. .o|
|   .+.Xo+.o.o o +|
|    +B+*+  o + = | | +B+ooS . + |
|   +o+.          |
|    o.           |
|   .o            |
|    .o           |
+----[SHA256]-----+
```

After this, you have to save the **Public Key** in the *authorized_keys* file. If you create your keys on the same server where you want to save files, you can run `cat ~/.ssh/id_rsa.pub > .ssh/authorized_keys`

If you want to add extra security to your key, you can create it with a passphrase (password):

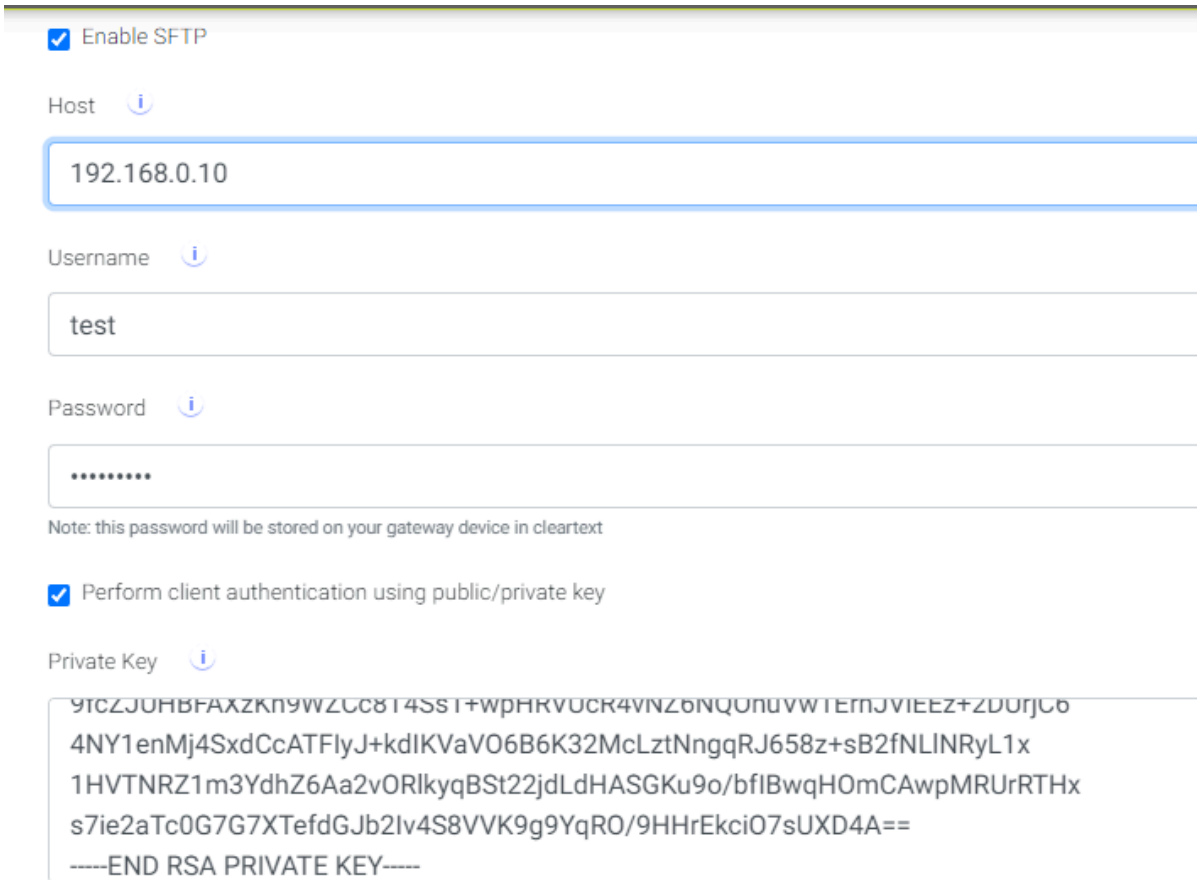
```
Generating public/private rsa key pair.
```

```
Enter file in which to save the key (/home/myLaptop/.ssh/id_rsa):(Simply press
ENTER)
Enter passphrase (empty for no passphrase): YOUR_SECURE_PASSWOR_HERE
Enter same passphrase again:REPEAT_YOUR_SECURE_PASSWOR_HERE
Your identification has been saved in /home/myLaptop/.ssh/id_rsa
Your public key has been saved in /home/myLaptop/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:iB5mwc8jFw7jeb31tNWlp2OLKsosDoS1OzWuThNkzLM myLaptop@myLaptop
The key's randomart image is: +---[RSA 3072]----+
|   o_ o .    .o..|
|  ..E= = oo .. .o|
|   .+.Xo+.o.o o +|
|    +B+*+  o + = |
| +B+ooS . +      |
|   +o+.          |
|    o.           |
|   .o            |
|    .o           | +----[SHA256]-----+
```

Finally, copy your **Private Key**. You can view it in the console by running: `cat ~/.ssh/id_rsa` . Copy the file content and paste it into the Gateway UI (in this example, we are using 192.168.0.3). Navigate to Settings > SFTP/Archive and select *Enable SFTP*.

- **Host:** 192.168.0.10
- **User:** test
- **Password:** If you added a passphrase (password), you have to add it here; if not, leave the space blank.
- Select: *Perform client authentication using public/private key*
    - Paste your ***Private Key*** in the Private Key box.

If you've used a passphrase, you should see something similar to:

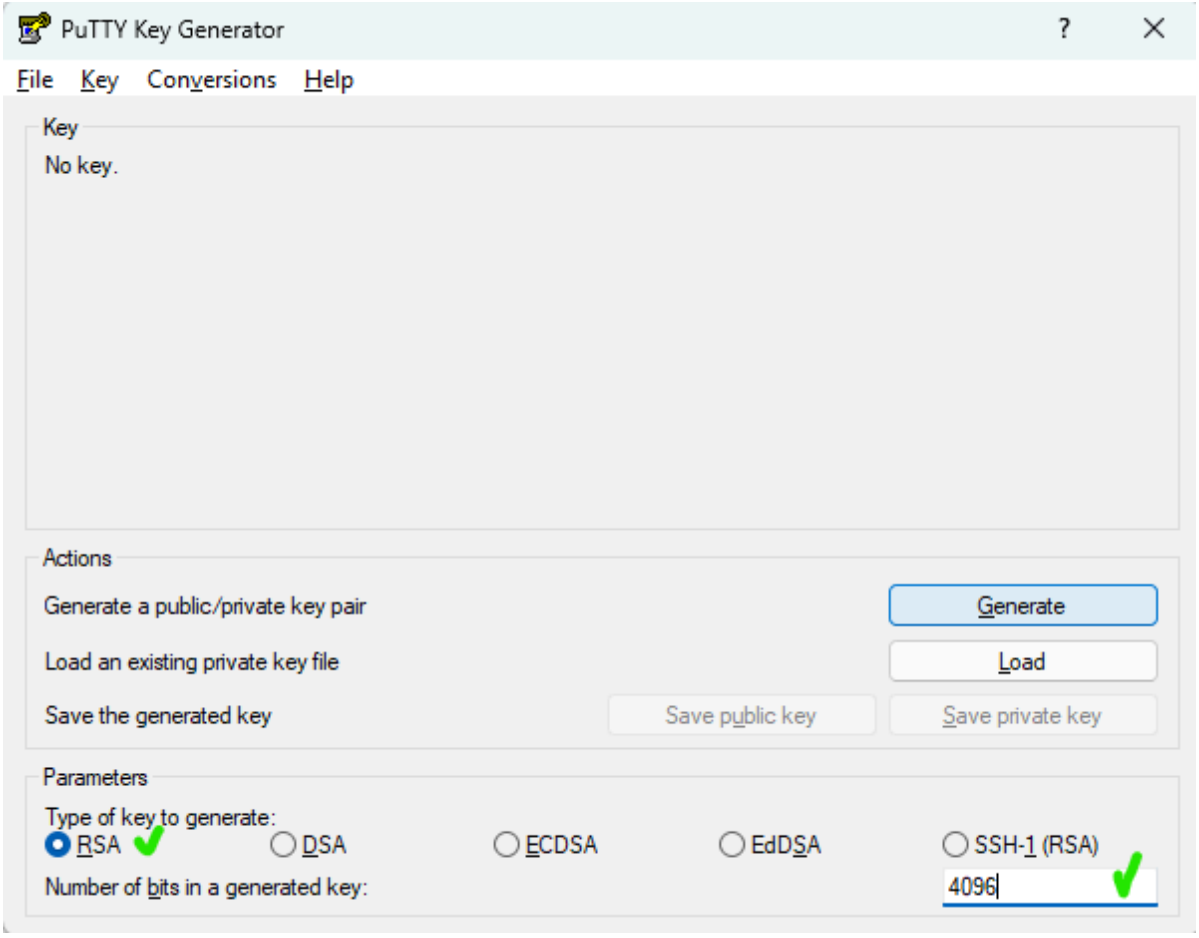


You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.

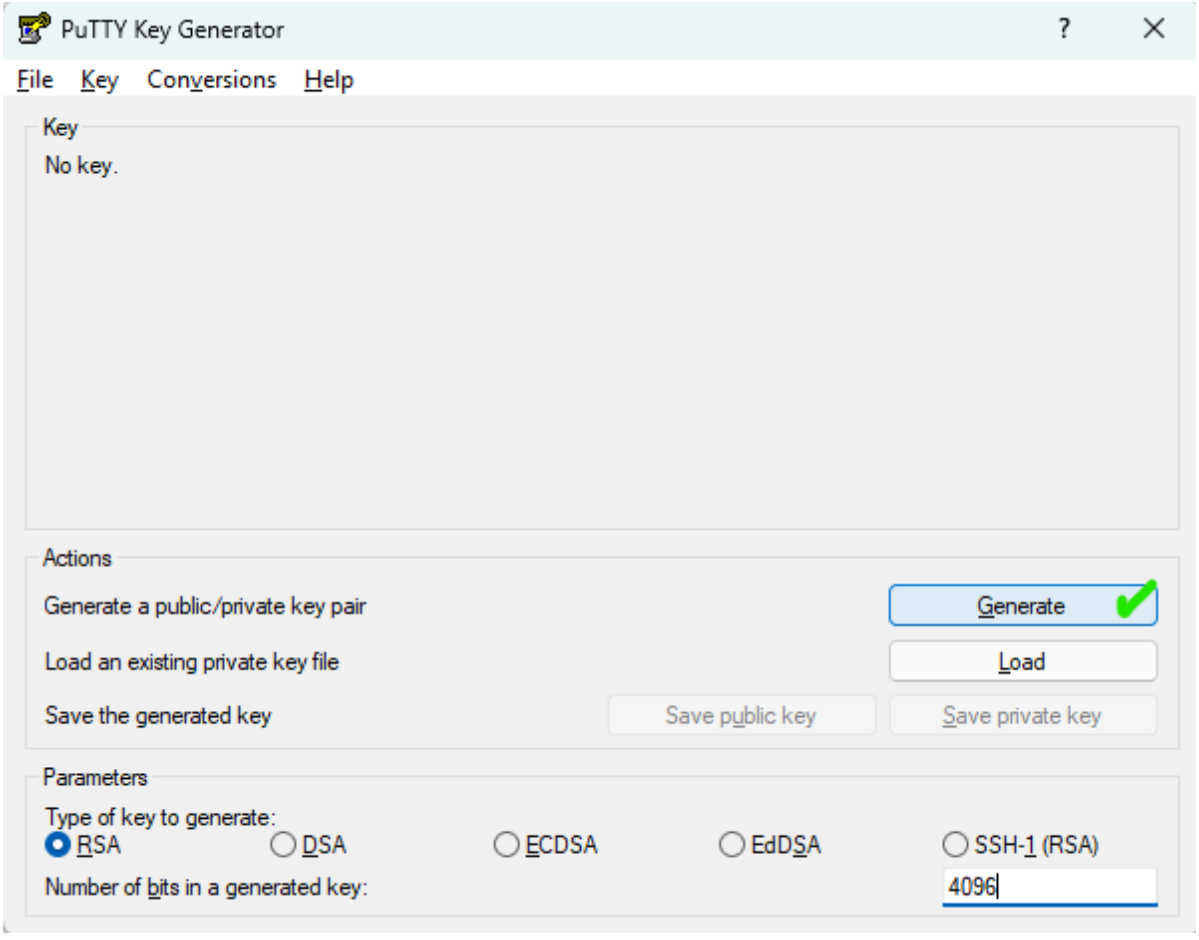
Create your Private Key in Windows using putty

You can create your **Private Keys** on your Windows computer by following these instructions:

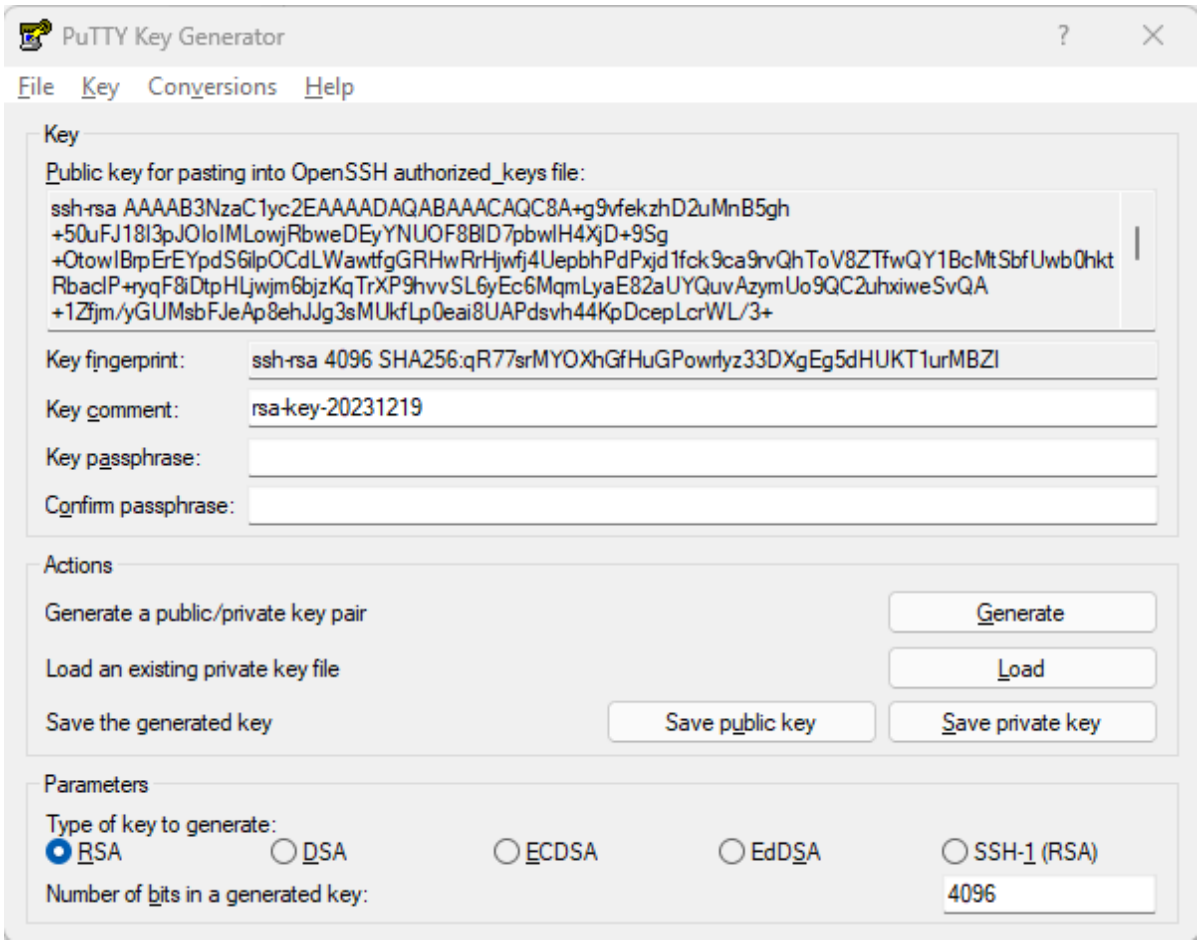
1. Download the `puttygen.exe` software from its official web page: https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
2. Execute it.
3. At this point, you can create your key using RSA with either 2048 or 4096 bits in the 'Number of bits in a generated key'.



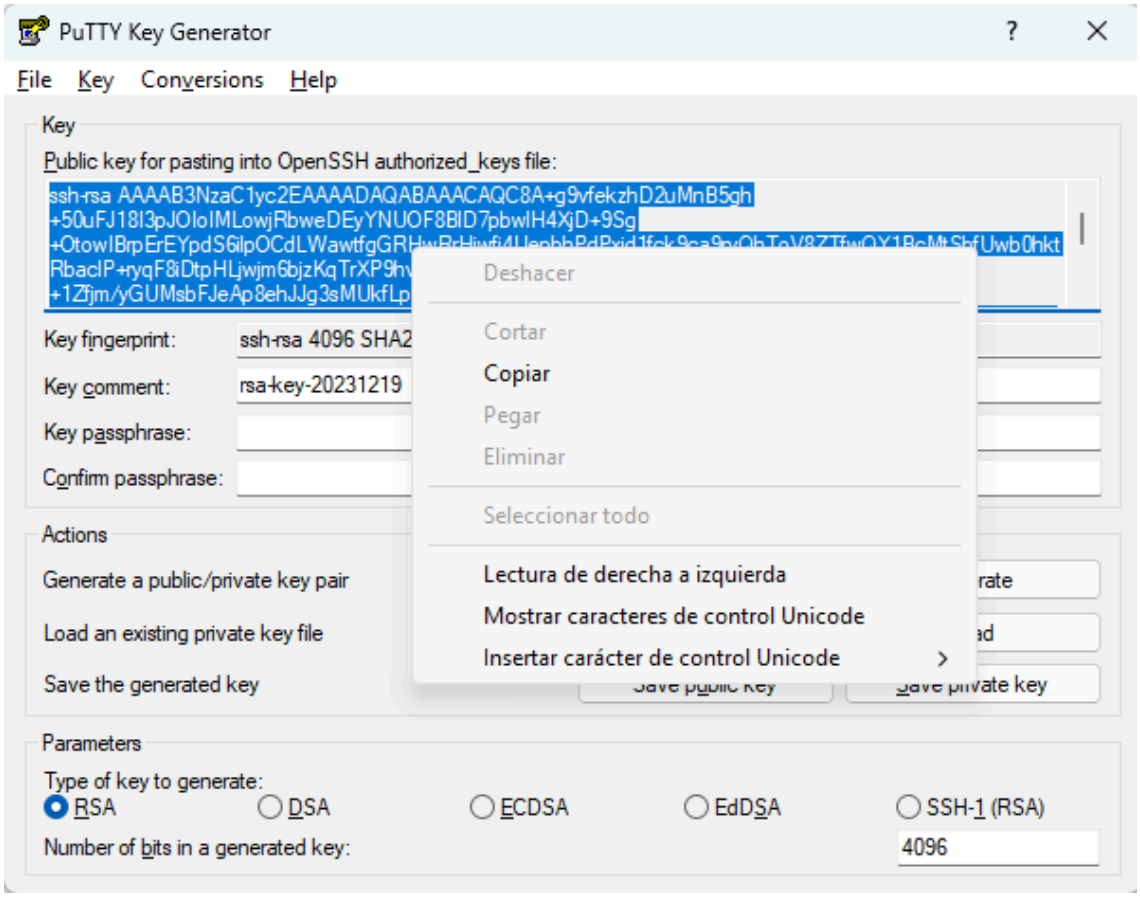
4. After selecting these two options, press the 'Generate' button, and then move your mouse over the blank area.



5. You should see something similar to:

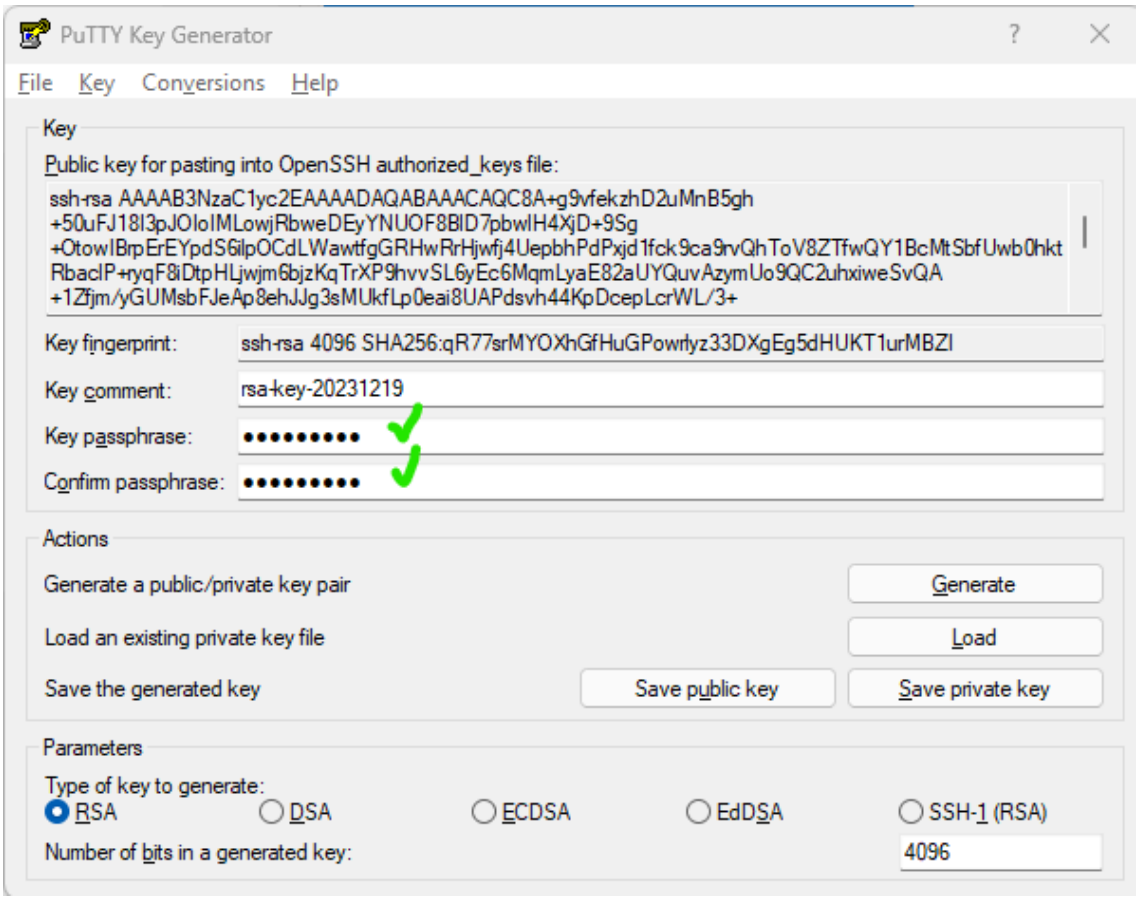


6. Select and copy the entire box that says: *Public key for pasting into OpenSSH authorized_keys files.*



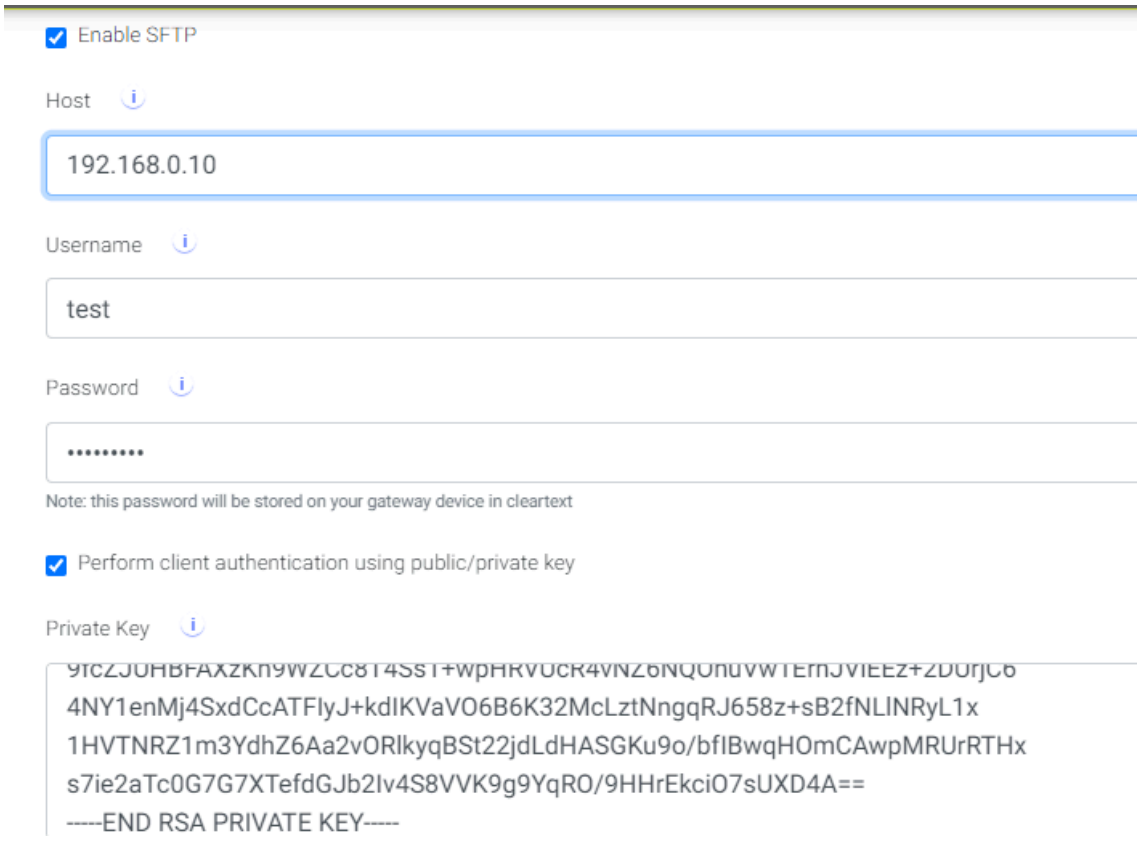
   - Paste it in your remote server on: `~/.ssh/authorized_keys` .

7. If you want to enhance the key security by adding a passphrase (password), enter the passphrase in the provided input:



8. Export your **Private Key**: Go to Conversions > Export OpenSSH Key and save it in a secure place.
9. Finally, copy the content of your converted **Private Key** and paste it into the Gateway UI (in this example, we are using 192.168.0.3). Navigate to Settings > SFTP/Archive and select *Enable SFTP*.
    - **Host:** 192.168.0.10
    - **User:** test
    - **Password:** If you added a passphrase (password), you have to add it here; if not, leave the space blank.
    - Select: *Perform client authentication using public/private key*
        - Paste your ***Private Key*** in the Private Key box.

    If you've used a passphrase, you should see something similar to:



You have to wait for at least 15 minutes to check if the data has been successfully saved to the server.