SFTP Configuration Setup

**✅ 1. Install OpenSSH Server**

Most Linux systems come with OpenSSH pre-installed, but if not:

sudo apt update && sudo apt install openssh-server -y # For Debian/Ubuntu

## ✅ ****2. Create a New SFTP Group (Optional but Recommended)****

sudo groupadd sftpusers

## ✅ ****3. Create a New User for SFTP Access****

sudo adduser newuser

### **Add User to** sftpusers **Group**

sudo usermod -aG sftpusers newuser

### **Create Directory Structure**

sudo mkdir -p /home/newuser/uploads

### **Set Correct Permissions**

#### 🔸 Home directory (must be owned by root):

sudo chown root:root /home/newuser

sudo chmod 755 /home/newuser

#### upload directory (must be owned by the user):

sudo chown newuser:sftpusers /home/newuser/uploads

### Step 5: Confirm Group Membership (optional)

groups username

You should see something like:

username : username sftpusers

Run this command to allow firewall

sudo ufw allow OpenSSH

sudo ufw enable

sudo ufw allow 22/tcp

sudo ufw enable

sudo ufw status

Go to the config file add this line

sudo nano /etc/ssh/sshd\_config

Match Group sftpusers

ChrootDirectory /home/%u

ForceCommand internal-sftp -d /uploads

PasswordAuthentication yes

X11Forwarding no

AllowTcpForwarding no

Change this line

#override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

You need to replace it with:

Subsystem sftp internal-sftp

sudo systemctl restart sshd

log checking

grep sftp /var/log/auth.log