# **Setting Up an FTP Server on Ubuntu with vsftpd**

This guide will walk you through installing and configuring vsftpd to create an FTP server on your Ubuntu machine.

## **Step 1: Update Package List**

First, ensure your package list is up to date:

sudo apt update  
sudo apt upgrade

## **Step 2: Install vsftpd**

Now, install the vsftpd package:

sudo apt install vsftpd

Once installed, vsftpd will automatically start. You can check its status using:

sudo systemctl status vsftpd

## **Step 3: Configure vsftpd**

The main configuration file for vsftpd is located at /etc/vsftpd.conf. It's a good practice to back up the original configuration file before making any changes:

sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.bak

Now, open the configuration file for editing using your preferred text editor (e.g., nano or vim):

sudo nano /etc/vsftpd.conf

You'll need to uncomment or change certain lines to enable the desired functionality. Here are some common configurations:

1. Disable Anonymous Access (Recommended for Security):  
   Find the line anonymous\_enable=YES and change it to:  
   anonymous\_enable=NO
2. Enable Local User Access:  
   Ensure the following line is uncommented (or add it if missing) to allow local system users to log in:  
   local\_enable=YES
3. Enable Write Access:  
   Uncomment the following line to allow users to upload files:  
   write\_enable=YES
4. Chroot Jail (Security - Restrict Users to Their Home Directories):  
   This is highly recommended for security. It "jails" users to their home directories, preventing them from browsing the entire file system.  
   Uncomment the following line:  
   chroot\_local\_user=YES  
     
   Important Note for chroot\_local\_user=YES:  
   If you enable chroot\_local\_user=YES, vsftpd might refuse to start or allow logins if the user's home directory is writable by the user. This is a security measure. You have a few options:
   * Option A (Recommended): Create a non-writable parent directory and put the writable FTP directory inside it.  
     For example, if a user's home is /home/ftpuser, create /home/ftpuser/ftp and make /home/ftpuser owned by root and not writable by ftpuser.
   * **Option B (Less Secure but Simpler):** Add allow\_writeable\_chroot=YES to vsftpd.conf. This bypasses the security check but is generally not recommended unless you understand the risks.

Let's go with Option A for better security. We'll set this up in Step 5.

1. Passive Mode Port Range (Important for Firewalls):  
   For passive mode FTP to work correctly (which is common for many clients), you need to define a port range. Add these lines to the end of the file:  
   pasv\_min\_port=40000  
   pasv\_max\_port=50000  
     
   You can choose any range, but ensure it's not used by other services.
2. **Other useful settings (optional):**
   * **Log file:**  
     xferlog\_enable=YES  
     xferlog\_file=/var/log/vsftpd.log  
     xferlog\_std\_format=YES
   * **Message file (banner):**  
     ftpd\_banner=Welcome to my FTP service.

After making your changes, save the file (Ctrl+O, Enter, Ctrl+X in nano).

## **Step 4: Configure Firewall (UFW)**

If you're using UFW (Uncomplicated Firewall) on your Ubuntu server (which you should!), you need to allow FTP traffic.

sudo ufw allow OpenSSH # If you haven't already  
sudo ufw allow ftp  
sudo ufw allow 20/tcp # FTP Data Port  
sudo ufw allow 21/tcp # FTP Control Port  
sudo ufw allow 40000:50000/tcp # Passive Port Range (matching vsftpd.conf)  
sudo ufw enable # Enable UFW if it's not already

Confirm the firewall status:

sudo ufw status verbose

## **Step 5: Create a Dedicated FTP User and Directory (Recommended)**

It's best practice to create a dedicated user for FTP access rather than using your main system user, especially if you enabled chroot\_local\_user=YES.

Let's create a user named ftpuser with no shell access and a non-writable home directory, then a writable subdirectory for FTP files.

# Create the user with no home directory initially and no shell  
sudo useradd -m ftpuser -s /usr/sbin/nologin  
  
# Set a password for the new user  
sudo passwd ftpuser  
  
# Create the FTP directory structure  
# The user's home directory (/home/ftpuser) will be the chroot jail.  
# This directory must NOT be writable by the user.  
sudo mkdir /home/ftpuser/ftp  
  
# Set ownership of the chroot directory to root and make it not writable by others  
sudo chown root:root /home/ftpuser  
sudo chmod a-w /home/ftpuser  
  
# Set ownership of the writable FTP directory to the ftpuser  
sudo chown ftpuser:ftpuser /home/ftpuser/ftp

1. Now, ftpuser can log in, but they will be jailed to /home/ftpuser. Their writable directory will be /home/ftpuser/ftp.

## **Step 6: Restart vsftpd Service**

After making changes to the configuration file, you must restart the vsftpd service for the changes to take effect:

sudo systemctl restart vsftpd

If there are any errors, systemctl status vsftpd will show them. Common errors include incorrect syntax in the config file or issues with chroot permissions if allow\_writeable\_chroot=YES is not used.

## **Step 7: Test Your FTP Server**

You can test your FTP server from another machine or even from your Ubuntu server itself using an FTP client or the command line.

**From the command line (on another machine or your server):**

ftp your\_server\_ip\_address

Replace your\_server\_ip\_address with the actual IP address of your Ubuntu server. You'll be prompted for the username (ftpuser) and password you set.

Once logged in, try:

* ls to list files (you should see the ftp directory).
* cd ftp to enter the writable directory.
* put local\_file.txt to upload a file (create a dummy local\_file.txt first).
* get remote\_file.txt to download a file.
* bye to exit.

**Using a GUI FTP Client (e.g., FileZilla):**

* **Host:** your\_server\_ip\_address
* **Username:** ftpuser
* **Password:** your\_password
* **Port:** 21 (default)

You should be able to connect, navigate to the ftp directory, and transfer files.

That's it! You now have a basic and reasonably secure FTP server running on your Ubuntu machine.