# Configure FTP

You can use `scp` instead, taking advantage of the added security and already-configured users on your system. It works a lot like `ssh`

Copy a file from a remote host to your local host -

```
scp -i ~/.ssh/some_key -P 22 username@123.123.123.12:/home/username/test .
```

If you still need or want FTP, you can follow the steps below to configure the FTP server and then connect with Filezilla.

## Installing Very Secure FTP Daemon

I am using an Ubuntu 19.04 server in this guide, depending on your system your steps may vary slightly.

Assuming you have nothing installed, run `sudo apt-get update && sudo apt install vsftpd` to install vsftpd (Very Secure FTP Daemon). Navigate to the home directory of the user you wish to enable FTP access, and run the following.

```
# Login as your sudo user
sudo su USER

# Create FTP Directory
mkdir /home/USER/ftp
sudo chown nobody:nogroup /home/USER/ftp
sudo chmod a-w /home/USER/ftp
```

## Create User FTP Directories

Create a directory where files can be uploaded, you can name this directory whatever you want. Give this directory permissions so you can upload files to it via FTP clients like FileZilla.

```
mkdir /home/USER/ftp/files
sudo chown USER:USER /home/USER/ftp/files
sudo chmod 777 /home/USER/ftp/files
```

## Configure vsftpd Settings

If you have a firewall enabled, be sure you open the TCP ports 20, 21, 990, and 40000-50000 before you continue.

Add the following to `/etc/vsftpd.conf`

```
# FTP Initial Configuration Options
pasv_min_port=40000
pasv_max_port=50000
user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=40000
pasv_max_port=40000
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
pasv_promiscuous=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH
```

Run `echo "USER" | sudo tee -a /etc/vsftpd.userlist && sudo systemctl restart vsftpd` to add your user to the userlist file we configured above and restart the service

`tail -f /var/log/syslog` in another console to see a live feed of service logs when restarting instead of checking the status with `sudo systemctl status`

Change or modify the following values, when editing these files I like to comment out the default value, and create a separate value in an organized list with my custom settings. This is useful later should I want to refer back to the default value I can just search it up in my file, and keeps things organized so when I can pick things back up quickly. You can do this however you see fit. The result of my modified values within `vsftpd.conf` is below.

```
# Values Modified During FTP Setup
chroot_local_user=YES
write_enable=YES
ssl_enable=YES
```

Run `sudo systemctl restart vsftpd` to restart the service and test your connection <u>using Filezilla</u>.

## Debugging FTP Connections

If you're having issues with your FTP connection, check on the service with the following commands
`sudo systemctl -l status vsftpd`  `sudo tail -f /var/log/vsftpd.log`

To test FTP connections via commandline, run the following
`ftp -p IPADDRESS`

You cannot connect to FTP via commandline using this method if you have enabled SSL/TLS because your connection will *not* be encrypted under TLS. Use Filezilla or another encrypted connection method instead.

## Notes

Here's a working config file, with some comments on some extra settings I found on the manpages for vsftpd.conf

```
# *Example config file /etc/vsftpd.conf.bak
# *Don't forget to backup your default /etc/vsftpd.conf.bak
#
# Custom FTP configuration for basic server configuration
#
# These settings should be refined for security
# Firewall should be used and reflect the settings in this file
# For more security, use keys and disable password authentication
# +Restrict FTP access to a list of approved IP's with distributed keys


# FTP Custom Configuration Options

# Set chroot user options
chroot_local_user=YES
user_sub_token=$USER

# Set Directory FTP Will Default Into
local_root=/home/$USER/ftp
write_enable=YES
# If you can't write with Write_enable=YES, check directory permissions
# Create .../ftp/files and chmod 777 .../ftp/files
```

```
# Passive FTP Connection Settings
pasv_promiscuous=YES
pasv_min_port=40000
pasv_max_port=50000


# userlist_enable=YES tells vsftpd to read /etc/vsftpd.userlist
# /etc/vsftpd.userlist should contain one user per line
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
# Sets the userlist to be a whitelist or a blacklist
# userlist_deny=YES will deny FTP for any user on the list
userlist_deny=NO
# Enable logs for failed FTP connections due to userlist errors
# userlist_log=YES


# Enable dual logs fot vsftpd in /var/log/
# log/xferlog - stardard parsable log
# log/vsftpd.log - vsftpd formatted logs
dual_log_enable=YES


# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
# Other Settings For SSL
ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
require_ssl_reuse=NO
ssl_ciphers=HIGH


# Default vsftpd.conf Values
```

```
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.

# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.

secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
connect_from_port_20=YES
use_localtime=YES
dirmessage_enable=YES
local_enable=YES
anonymous_enable=NO
listen_ipv6=YES
listen=NO
```

Modifying the values below during setup of TLS encryption caused vsftpd to crash on startup..

These values were obtained following this tutorial. Just noting this in case I missed something here, so I can revisit it later.

```
# Working values, establishes TLS connection via Filezilla FTP
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

# Modified values from generating ssl cert that are crashing vsftpd
# rsa_cert_file=/etc/ssl/private/vsftpd.pem
# rsa_private_key_file=/etc/ssl/private/vsftpd.pem
```

Revision #14
Created 7 April 2019 12:41:45 by Shaun Reed
Updated 18 December 2021 15:20:07 by Shaun Reed