

How to Setup FTP Server with VSFTPD on Ubuntu 22.04

Written by: [Bobbín Zachariah](#) | Last updated: August 22, 2022

[Installation](#)

Contents



Vsftpd (i.e. very secure FTP daemon) is an FTP server software for Linux and other Unix-like systems. An FTP server software facilitates the transfer of files from a client computer to the server and vice versa.

In this tutorial, you will learn how to set up FTP Server with **Vsftpd** on **Ubuntu 22.04** and enable secure file transfer (FTPS) via **TLS**.

Prerequisites

- An Ubuntu 22.04 Linux system
- A user with sudo capability
- An SSL-enabled FTP client such as FileZilla

Install FTP Server Vsftpd on Ubuntu

Vsftpd is available in the default Ubuntu package repository. You may begin by updating available packages with the command below.

```
sudo apt update
```

Next, run the following command to install Vsftpd.

```
sudo apt install vsftpd
```

Enter **y** if prompted to continue with the installation.

Once Vsftpd is successfully installed, you may check the version with the command below.

```
vsftpd -v
```

Also, verify the status of the Vsftpd server as follows.

```
sudo systemctl status vsftpd
```

```
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2021-03-12 12:18:25 UTC; 17min ago
     Main PID: 100074 (vsftpd)
        Tasks: 1 (limit: 1073)
      Memory: 648.0K
     CGroup: /system.slice/vsftpd.service
            └─100074 /usr/sbin/vsftpd /etc/vsftpd.conf
```

Check Vsftpd server status

The **vsftpd** service should already be active. Press **q** to return to the command prompt.

If the vsftpd service is not already active, you may start it with the next command.

```
sudo systemctl start vsftpd
```

Configure Vsftpd

There are a lot of options that you can configure for vsftpd but we will only examine the basics in this tutorial. Open the vsftpd configuration file with the following command.

```
sudo nano /etc/vsftpd.conf
```

You will see that the various vsftpd options are well explained in the configuration file. You only need to read the instructions to understand what you want to enable or

disable. Below are a few examples.

Configure anonymous FTP access

By default, anonymous FTP is disabled. We recommend that you leave this default setting as is. However, if for any reason you would like to enable anonymous FTP access for testing purposes, then change the value of the **anonymous_enable** option from NO to YES.

For now, leave it as is.

```
#  
# Allow anonymous FTP? (Disabled by default).  
anonymous_enable=NO  
#
```

Configure anonymous FTP access for vsftpd

Allow local users to log in

Local users are allowed to log in by default. If you would like to prevent local users from logging in to the Vsftpd server, then change the value of **local_enable** from YES to NO.

```
# Uncomment this to allow local users to log in.  
local_enable=YES  
#
```

Allow local users to login to the Vsftpd server

You could also allow only specific local users to log in to the Vsftpd server. To do that, ensure that **local_enable** is set to YES.

After that, add the following lines underneath.

```
userlist_enable=YES  
userlist_file=/etc/vsftpd.userlist  
userlist_deny=NO
```

Save and close the vsftpd.conf file.

Next, create the userlist file with the next command and enter the allowed users one

per line.

```
sudo nano /etc/vsftpd.userlist
```

Save and close the userlist file.

Restart vsftpd with:

```
sudo systemctl restart vsftpd
```

Enable FTP write command

To allow FTP users to create, delete, rename and save files, uncomment the **write_enable** option and make sure it is set to YES.

```
#  
# Uncomment this to enable any form of FTP write command.  
write_enable=YES  
#
```

Enable FTP write command

Before we go any further, let us login to the Vsftpd server to confirm that it is working. For now, save any changes and close the vsftpd configuration file.

Login to the Vsftpd Server

For this, let us create a test user and assign a password as follows.

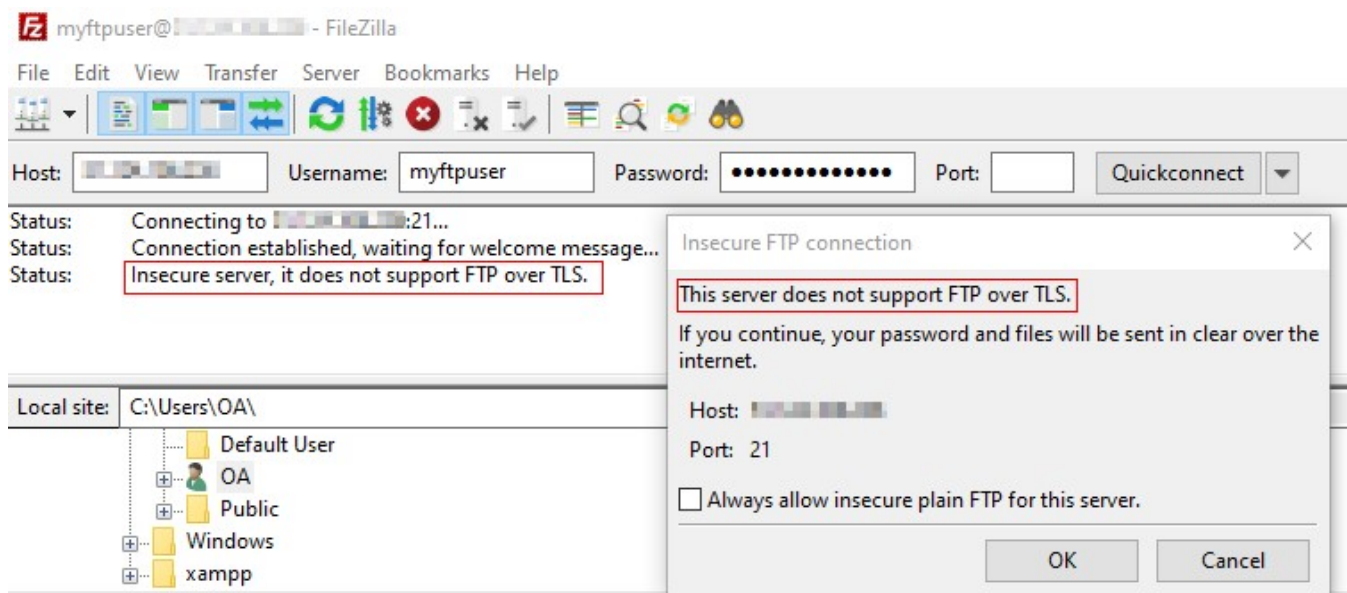
```
sudo useradd -m myftpuser
```

```
sudo passwd myftpuser
```

Note: If you enabled the vsftpd **userlist** earlier, do not forget to add the ftp user to `/etc/vsftpd.userlist` accordingly. By default users have ssh access, recommended to [disable shell access](#) for FTP users.

Now, launch an SSL-enabled FTP client such as FileZilla and then log in using the newly created test user.

In my case, FileZilla notified me that the server is insecure as it does not support FTP over TLS.



Insecure FTP server notification

Cancel the connection. Let us fix this in the next section.

Add TLS for secure file transfer

To enable secure file transfer via TLS, proceed as follows.

Firstly, open the vsftpd configuration file with the command below.

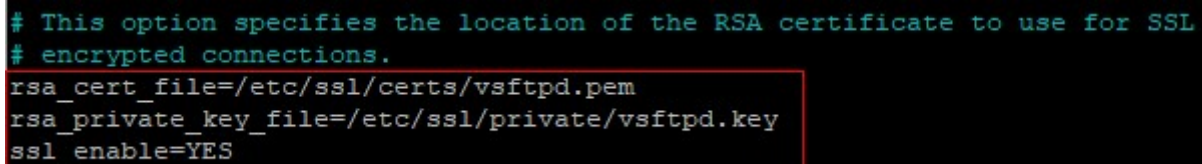
```
sudo nano /etc/vsftpd.conf
```

Next, look for the **rsa_cert_file** and **rsa_private_key_file** options and update the values as shown below.

```
rsa_cert_file=/etc/ssl/certs/vsftpd.pem  
rsa_private_key_file=/etc/ssl/private/vsftpd.key
```

Also, look for **ssl_enable** and change the value to YES.

```
ssl_enable=YES
```

A screenshot of a terminal window showing the configuration of the vsftpd.conf file. The text is as follows:

```
# This option specifies the location of the RSA certificate to use for SSL  
# encrypted connections.  
rsa_cert_file=/etc/ssl/certs/vsftpd.pem  
rsa_private_key_file=/etc/ssl/private/vsftpd.key  
ssl_enable=YES
```

The last three lines are enclosed in a red rectangular box.

Enable TLS/SSL for Vsftpd

Save and close the vsftpd configuration file.

Generate a private key and certificate

Now, you would need to create a private key and generate a TLS/SSL certificate with openssl. You can use the Let's Encrypt free SSL Certificate if you have a domain pointing to the FTP server.

To generate a private key, run:

```
sudo openssl genrsa -out /etc/ssl/private/vsftpd.key
```

Next, generate a certificate signing request with the command below. You would be prompted to provide some information such as your country, city, email address, etc. Please read the instructions carefully.

```
sudo openssl req -new -key /etc/ssl/private/vsftpd.key -out /etc/ssl/c
```

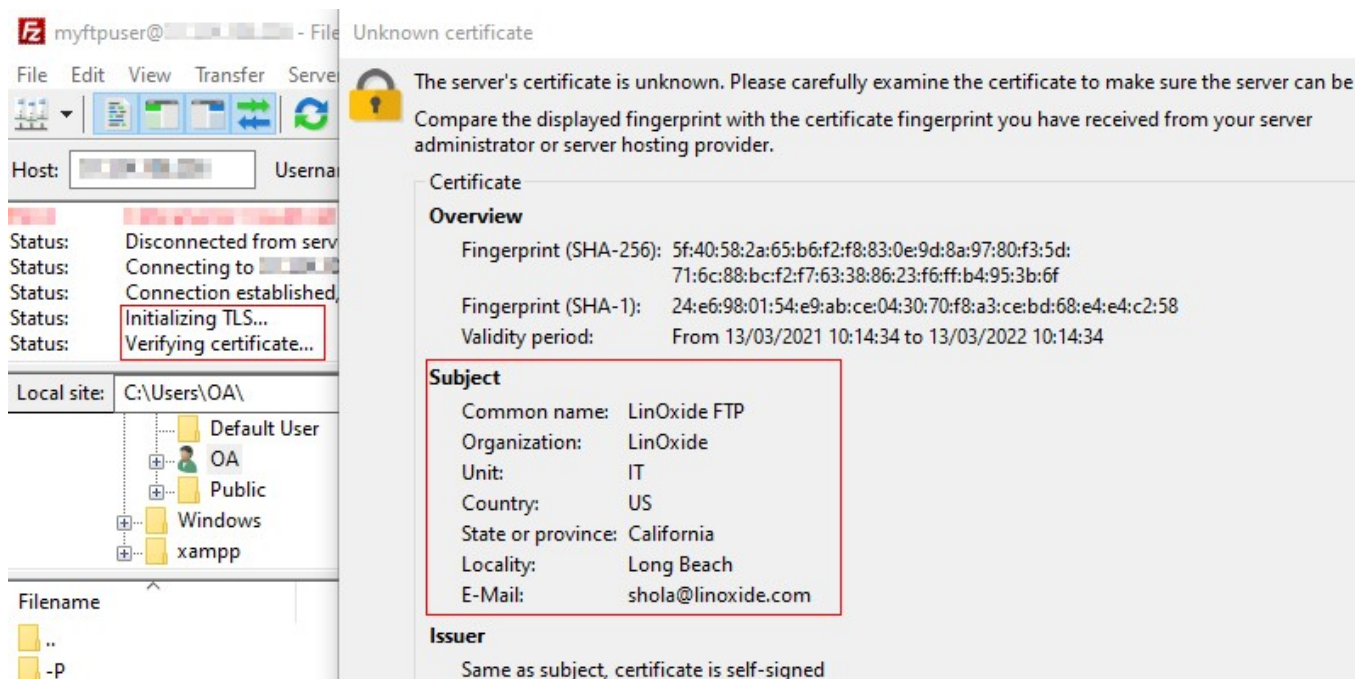
Now, generate and sign the certificate which will be valid for 365 days as follows.

```
sudo openssl x509 -req -days 365 -in /etc/ssl/certs/vsftpd.csr -signke
```

Restart vsftpd with:

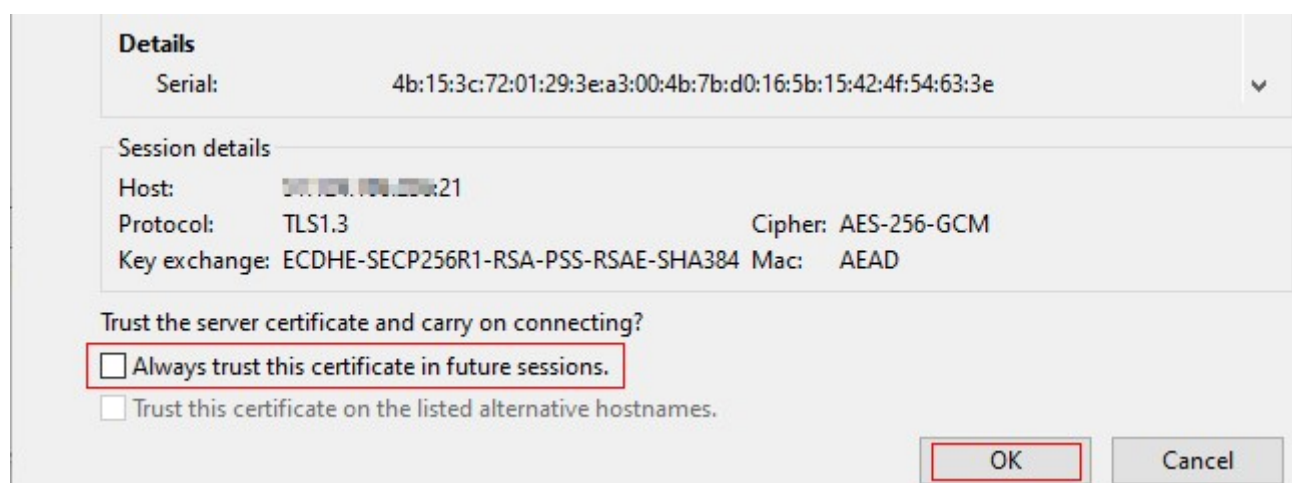
```
sudo systemctl restart vsftpd
```

Try to connect to the Vsftpd server again.



Secure FTP connection over TLS

Surely, FileZilla was able to connect securely via TLS this time around. You may safely choose the option to always trust this certificate in future sessions. Then click **OK** to proceed with the connection.



Trust self-signed certificate

If you try to connect to the FTP server via the command line which does not support FTP over TLS, you will get an error. For example:

```
ftp 192.168.100.168
```



```
220 (vsFTPd 3.0.3)
Name (██████████:root): myftpuser
530 Non-anonymous sessions must use encryption.
Login failed.
421 Service not available, remote server has closed connection
ftp>
```

FTP error without TLS

This is another proof that your Vsftpd server is indeed enabled for secure file transfer over TLS.

Conclusion

In this tutorial, we showed you how to configure FTP Server with Vsftpd on Ubuntu 22.04. We also described how to enable secure file transfer via the TLS protocol. We only covered basic Vsftpd options in this article but you can explore more options on the [vsftpd config options](#) manual page.