# Secure FTP Server Setup using vsftpd with SSL/TLS Encryption – CentOS 9

**1. Objective**

The objective of this project is to set up a secure FTP server using vsftpd on CentOS 9. The server will use SSL/TLS encryption to protect data during transmission and ensure secure user access.

**2. Tools & Technologies Used**

- CentOS Stream 9  
- vsftpd  
- OpenSSL  
- firewall-cmd  
- WinSCP  
- systemctl

**3. System Requirements**

- CentOS Stream 9 installed  
- Internet connection to install packages  
- Root/sudo access to configure the system

**4. Step-by-Step Procedure**

1. Install vsftpd:  
 sudo dnf install vsftpd -y

2. Start and enable the vsftpd service:  
 sudo systemctl start vsftpd  
 sudo systemctl enable vsftpd

3. Create a new FTP user:  
 sudo useradd ftpuser  
 sudo passwd ftpuser

4. Create FTP directory and set permissions:  
 sudo mkdir -p /home/ftpuser/ftp/files  
 sudo chown -R ftpuser:ftpuser /home/ftpuser/ftp

5. Allow FTP through the firewall:  
 sudo firewall-cmd --add-service=ftp --permanent  
 sudo firewall-cmd --reload

6. Create SSL certificate:  
 sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \  
 -keyout /etc/ssl/private/vsftpd.key \  
 -out /etc/ssl/certs/vsftpd.crt

7. Set permissions for SSL files:  
 sudo chmod 600 /etc/ssl/private/vsftpd.key  
 sudo chmod 700 /etc/ssl/private

8. Edit /etc/vsftpd.conf and add:  
 ssl\_enable=YES  
 rsa\_cert\_file=/etc/ssl/certs/vsftpd.crt  
 rsa\_private\_key\_file=/etc/ssl/private/vsftpd.key

9. Enable passive mode and open firewall ports:  
 pasv\_enable=YES  
 pasv\_min\_port=40000  
 pasv\_max\_port=50000  
  
 sudo firewall-cmd --permanent --add-port=40000-50000/tcp  
 sudo firewall-cmd --reload

10. Restart vsftpd service:  
 sudo systemctl restart vsftpd

**5. Common Errors & Fixes**

• openssl: command not found – Install OpenSSL package using sudo dnf install openssl

• 500 OOPS: cannot load RSA certificate – Check certificate file path and file permissions

• Timeout or could not retrieve directory listing – Enable passive mode and open ports in the firewall

**6. Testing**

Connection tested using WinSCP client on Windows.  
Protocol: FTP  
Encryption: TLS/SSL Explicit encryption  
Port: 21  
Successful file transfer confirmed between client and server.

**7. Conclusion**

The secure FTP server was successfully set up using vsftpd on CentOS with SSL/TLS encryption. Passive mode was configured for smooth data transfer, and connection was successfully tested using WinSCP.

**8. Screenshots**

• FTP user creation

A screenshot of a computer screen

AI-generated content may be incorrect.

• vsftpd.conf edits

A screenshot of a computer

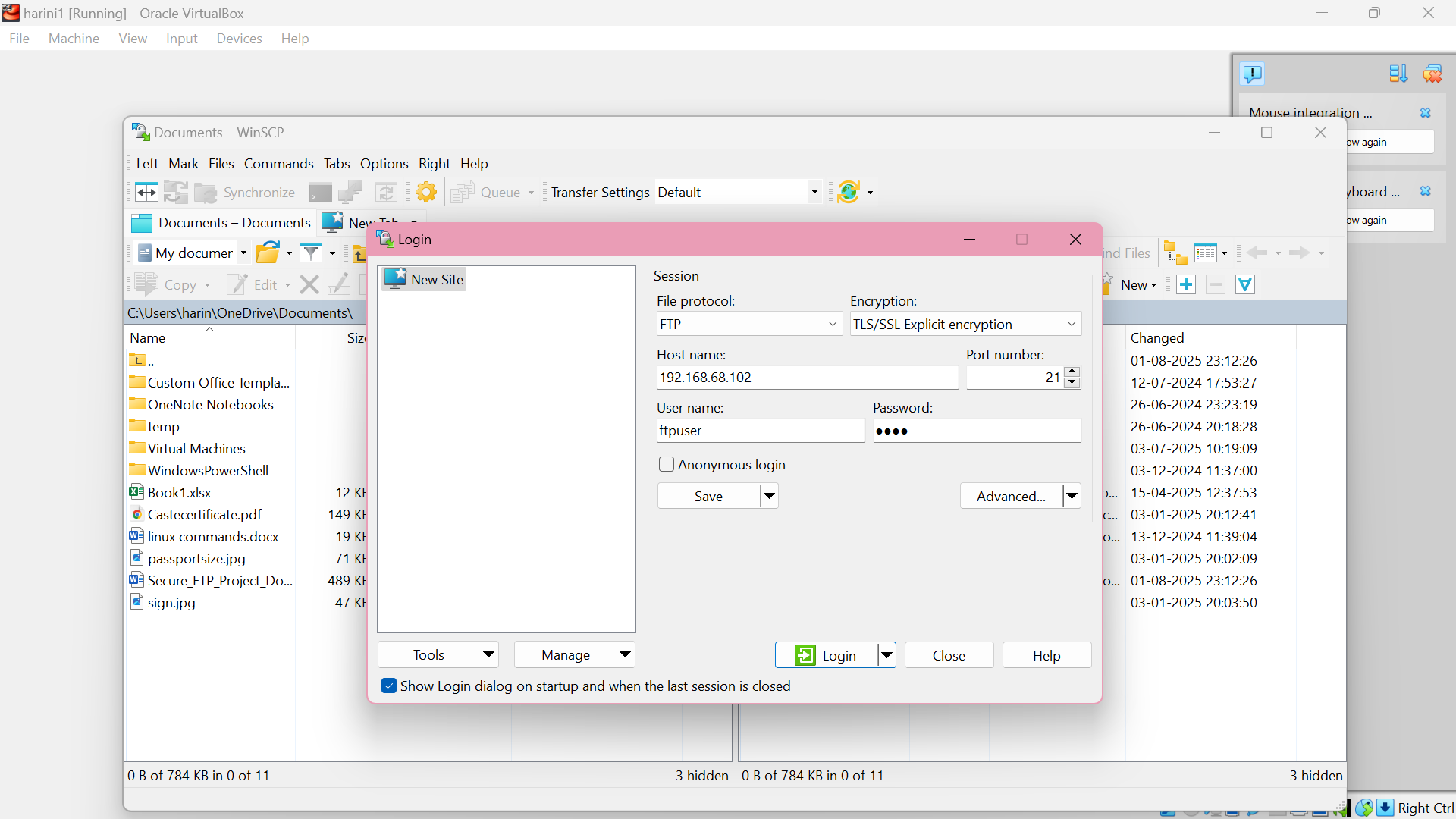
AI-generated content may be incorrect.

• SSL certificate generation

A computer screen with white text

AI-generated content may be incorrect.

• WinSCP file transfer success



A screenshot of a computer

AI-generated content may be incorrect.