FTP server is used to exchange files between computers over network . This guide helps you to setup ftp server on centos 7 . This guide contains configuration steps for both FTP and SFTP as well as user creation . Here i’ve used VSFTP package which is secure and less vulnerable .
1. [FTP Server](http://www.krizna.com/centos/setup-ftp-server-centos-7-vsftp/#FTP)
2. [SFTP Server](http://www.krizna.com/centos/setup-ftp-server-centos-7-vsftp/#SFTP)
3. [User creation](http://www.krizna.com/centos/setup-ftp-server-centos-7-vsftp/#user)

Setup FTP server on centos 7

**Step 1 »** Update your repository and install VSFTPD package .
[root@krizna ~]# yum check-update
[root@krizna ~]# yum -y install vsftpd
**Step 2 »** After installation you can find **/etc/vsftpd/vsftpd.conf** file which is the main configuration file for VSFTP.
Take a backup copy before making changes .
[root@krizna ~]# mv /etc/vsftpd/vsftpd.conf /etc/vsftpd/vsftpd.conf.org

Now open the file and make changes as below
[root@krizna ~]# nano /etc/vsftpd/vsftpd.conf

Find this line **anonymous\_enable=YES** ( Line no : 12 ) and change value to NO to disable anonymous FTP access.
anonymous\_enable=NO

Uncomment the below line ( Line no : 100 ) to restrict users to their home directory.
chroot\_local\_user=YES

and add the below lines at the end of the file to enable passive mode and allow chroot writable.
allow\_writeable\_chroot=YES
pasv\_enable=Yes
pasv\_min\_port=40000
pasv\_max\_port=40100
**Step 3 »** Now restart vsftpd service and make it start automatically after reboot.
[root@krizna ~]# systemctl restart vsftpd.service
[root@krizna ~]# systemctl enable vsftpd.service
**Step 4 »** Add FTP service in firewall to allow ftp ports .
[root@krizna ~]# firewall-cmd --permanent --add-service=ftp
[root@krizna ~]# firewall-cmd --reload
**Step 5 »** Setup SEinux to allow ftp access to the users home directories .
[root@krizna ~]# setsebool -P ftp\_home\_dir on
**Step 6 »** Now create an User for ftp access. Here **/sbin/nologin** shell is used to prevent shell access to the server .
[root@krizna ~]# useradd -m personel\_ftp -s /sbin/nologin
[root@krizna ~]# passwd personel\_ftp

mkdir /home/ftp\_user/www\_dev

mount --bind /var/www/dev/ /home/ftp\_user/www\_dev

After this the ftp user will be able to see the needed files in his home directory and use them in his ftp client as if they were local files.

If you need to make this *configuration permanent* you can either add the mount command in some startup script or you can just include a line in **/etc/fstab**:

/var/www/dev /home/ftp\_user/www\_dev none bind 0 0

Now user dave can able to login ftp on port 21 .
You can [filezilla](https://filezilla-project.org/%22%20%5Co%20%22Filezilla) or [winscp](http://winscp.net/eng/download.php%22%20%5Co%20%22Winscp%20download) client for accessing files.


SFTP server

SFTP ( Secure File Transfer Protocol ) is used to encrypt connections between clients and the FTP server. It is highly recommended to use SFTP because data is transferred over encrypted connection using SSH-tunnel on **port 22**.
Basically we need openssh-server package to enable SFTP .
Install openssh-server package, if its not already installed.
[root@krizna ~]# yum -y install openssh-server
**Step 7 »** Create a separate group for FTP access.
[root@krizna ~]# groupadd ftpaccess
**Step 8 »** Now open **/etc/ssh/sshd\_config** file and make changes as below.
Find and comment the below line ( Line no : 147 ).
#Subsystem sftp /usr/libexec/openssh/sftp-server

and add these lines below.
Subsystem sftp internal-sftp
Match group ftpaccess
ChrootDirectory %h
X11Forwarding no
AllowTcpForwarding no
ForceCommand internal-sftp
**Step 9 »** Now restart sshd service.
[root@krizna ~]# systemctl restart sshd

Now your SFTP server is configured and ready .

User creation

**Step 10 »** Create user jack with /sbin/nologin shell and ftpaccess group
[root@krizna ~]# useradd -m jack -s /sbin/nologin -g ftpaccess
[root@krizna ~]# passwd jack

Now assign root ownership for the home directory for chroot access and modify permission.
[root@krizna ~]# chown root /home/jack
[root@krizna ~]# chmod 750 /home/jack

Create a directory **www** inside home directory for writing and modify ownership .
[root@krizna ~]# mkdir /home/jack/www
[root@krizna ~]# chown jack:ftpaccess /home/jack/www
Now jack can use both ftp and sftp services . He can upload files in **www** directory .

If you are going to use FTP and SFTP together in the same server, you should follow above steps while creating users . For existing users add them to ftpaccess and make below changes.
[root@krizna ~]# usermod dave -g ftpaccess
[root@krizna ~]# chown root /home/dave
[root@krizna ~]# chmod 750 /home/dave
[root@krizna ~]# mkdir /home/dave/www
[root@krizna ~]# chown dave:ftpaccess /home/dave/www