Install and configure SSH server

What this exercise is about

The objective of this lab is to guide you through the installation and configuration of SSH server that supports SFTP and generate the key-pair (public-private) using PuTTy key generator.

What you should be able to do

At the end of this lab you should be able to:

- Install freeSSHd server
- Create users in freeSSHd server
- Install PuTTYgen and generate key pair (public and private) using it

Introduction

SSH over FTP (SFTP) is a network protocol that provides a mechanism for file transfer over a reliable data stream. SFTP runs on a secure SSH channel on port 22 and encrypts all traffic using either user name and password authentication or public key authentication. Public key authentication uses a pair of computer generated keys, one public and one private.

You will install the freeSSHd server and configure it to create users as a prerequisite for the **FTP Adapter – SFTP support** lab.

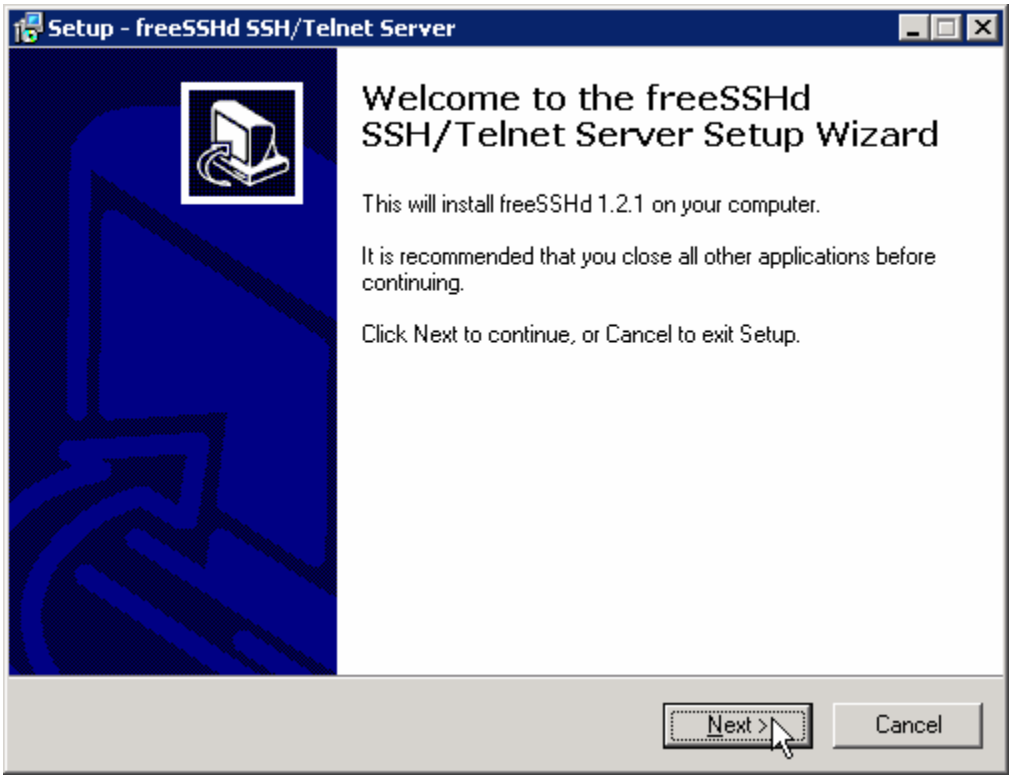
Part 1: Install and configure freeSSHd server

This part of the lab describes the steps for installing the SSH server, freeSSHd, and then guides you with the configuration setup.

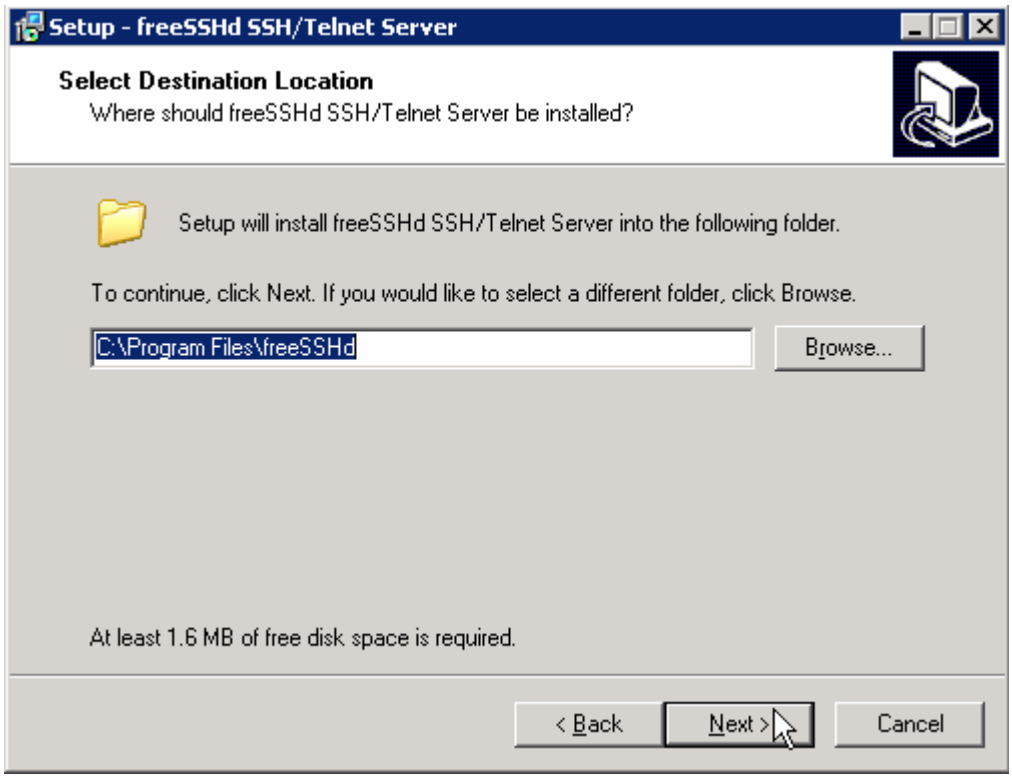
____ 1. Go to the http://www.freesshd.com/?ctt=download and download the latest stable version of freeSSHd onto your local machine

____ 2. Double click the downloaded **freeSSHd.exe** file to start the installation

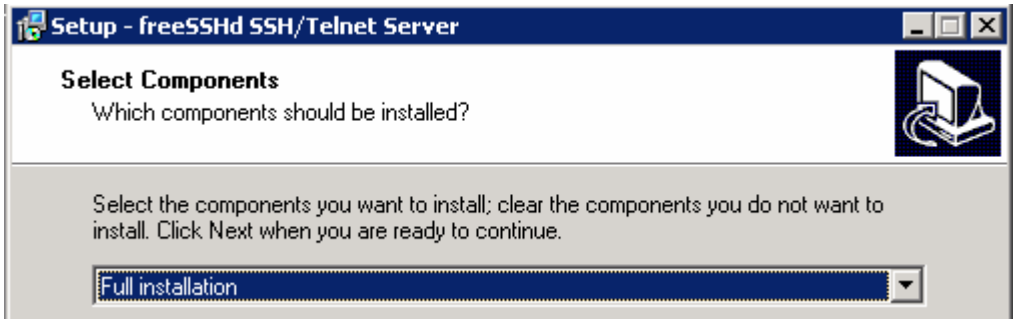
____ 3. Follow the instructions on the Welcome screen and click **Next**



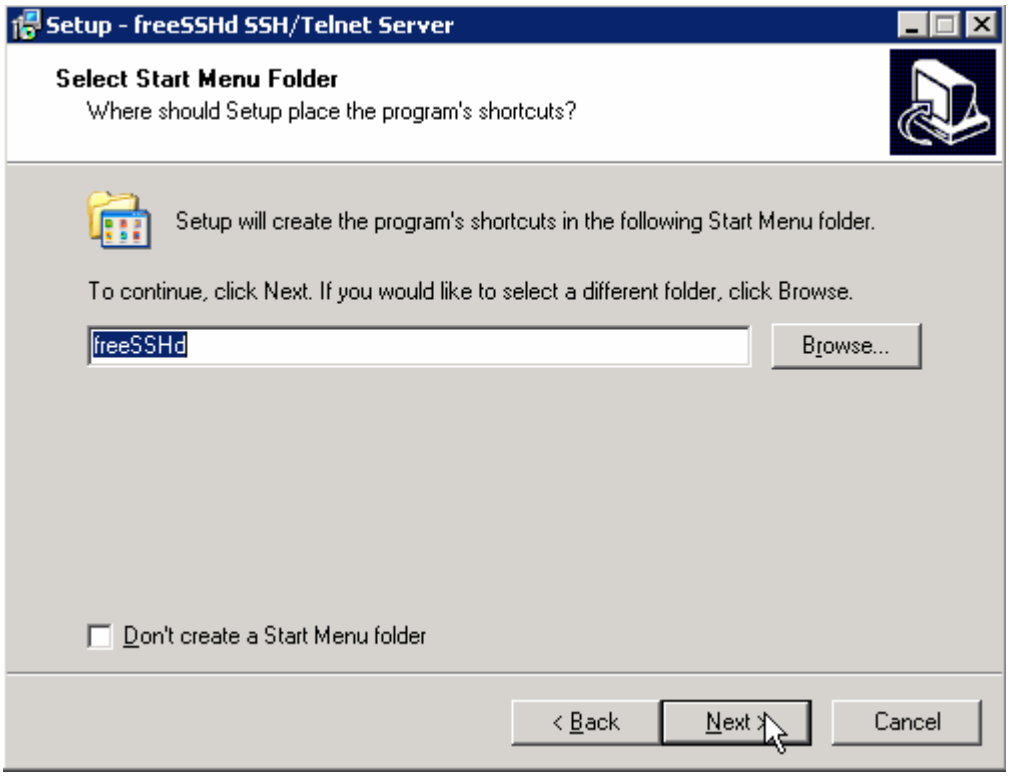
____ 4. Accept the default value or Browse and select the location of your choice for and click **Next**



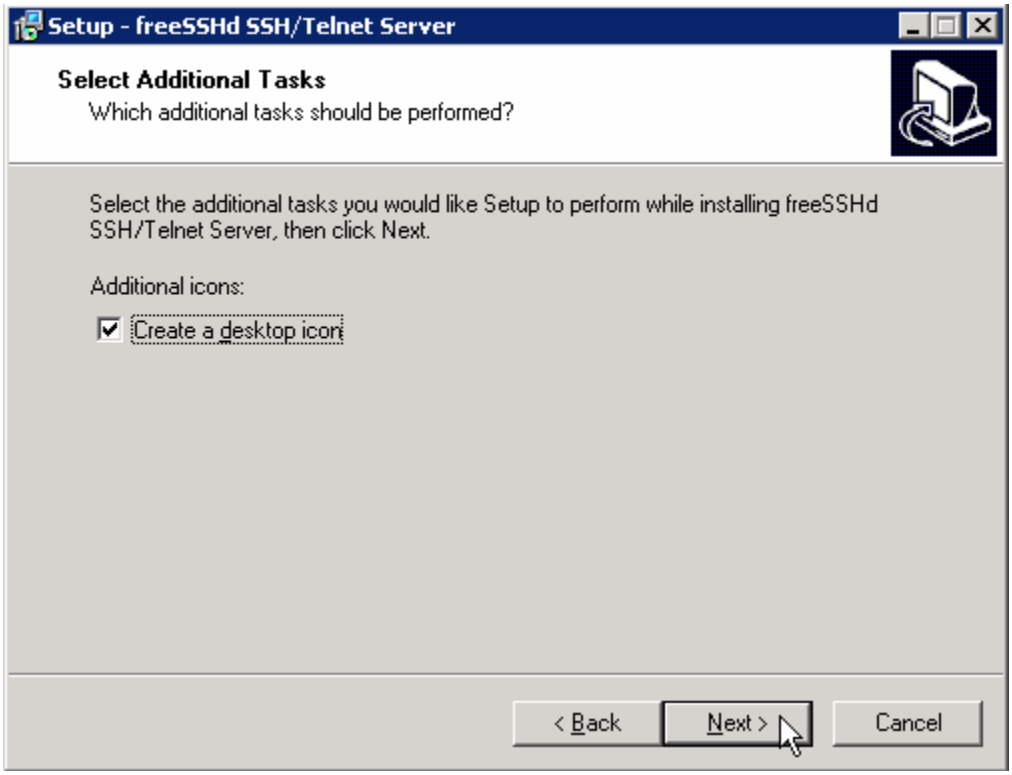
____ 5. Ensure that the **Full Installation** is selected and click **Next**



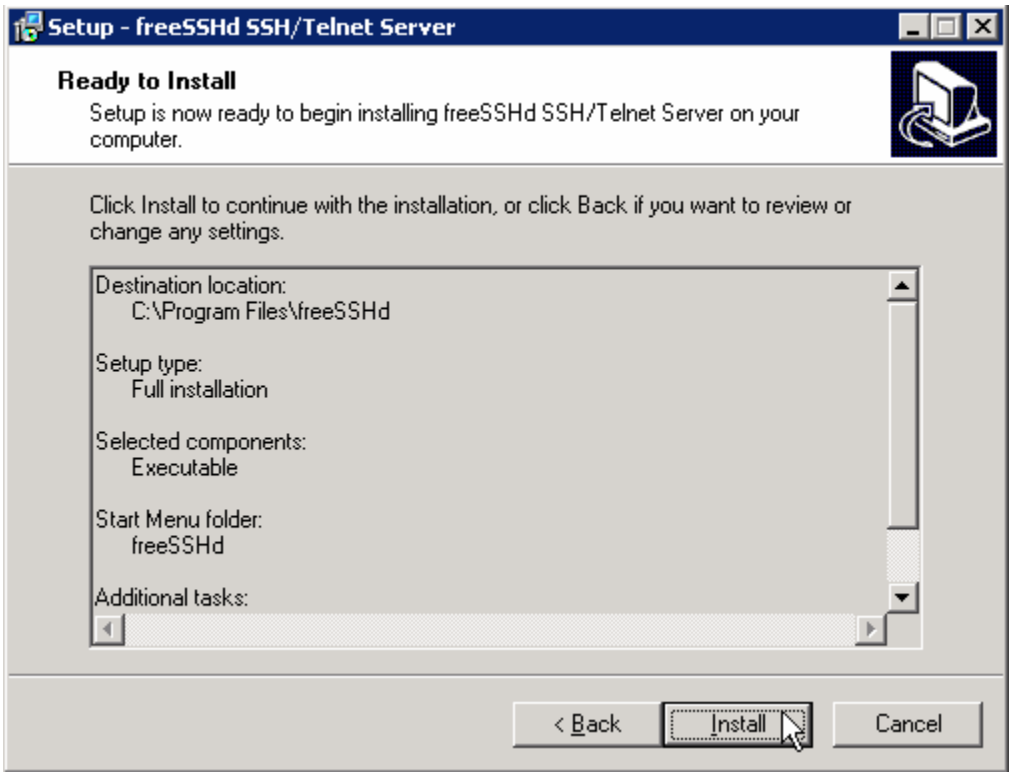
____ 6. Click **Next** on the next screen to accept the default start menu folder



____ 7. Accept the defaults on the next screen to create a desktop icon and click **Next**

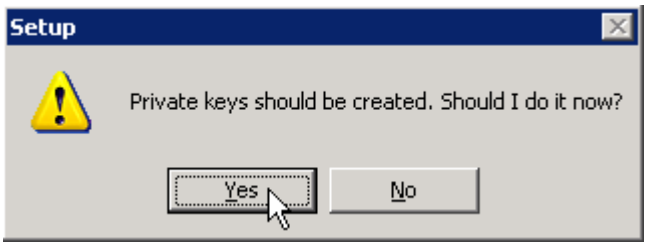


____ 8. Verify and click **Finish** on the summary screen. The installation takes less than a minute depending upon the system resources

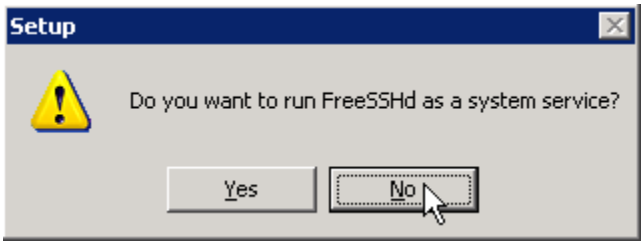


____ 9. Click Close in Try Other Product screen

____ 10. Select **Yes** from the Setup pop-up window to create Private keys



____ 11. Click **No** in the next Setup window shown below:

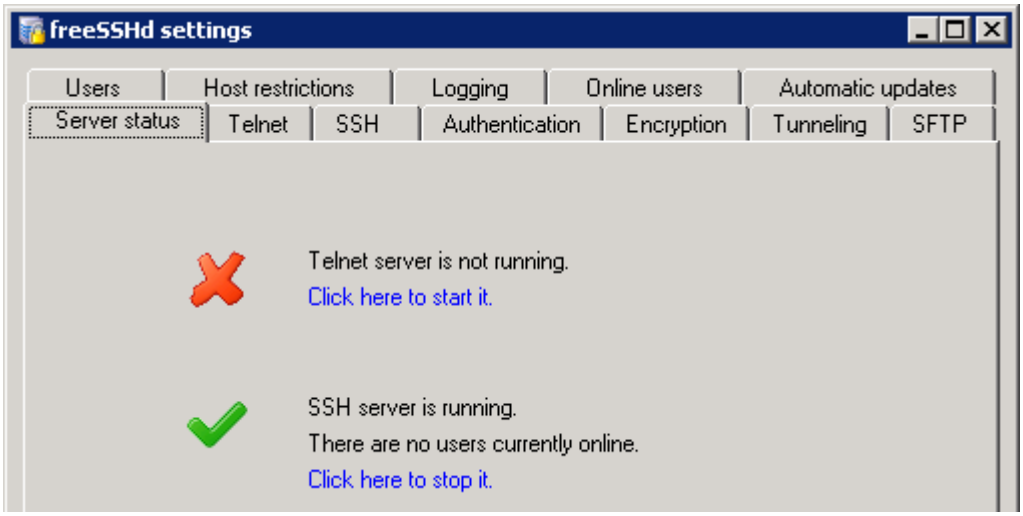


____ 12. Click **Finish** to exit setup

____ 13. Select **Start > Programs > freeSSHd > freeSSHd**

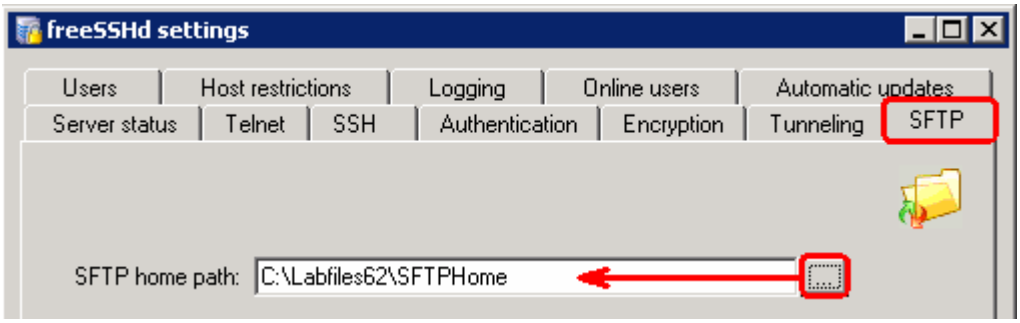
____ 14. Click the **FreeSSHDService (** **)** icon at the bottom tray

____ 15. The freeSSHd settings window is opened:

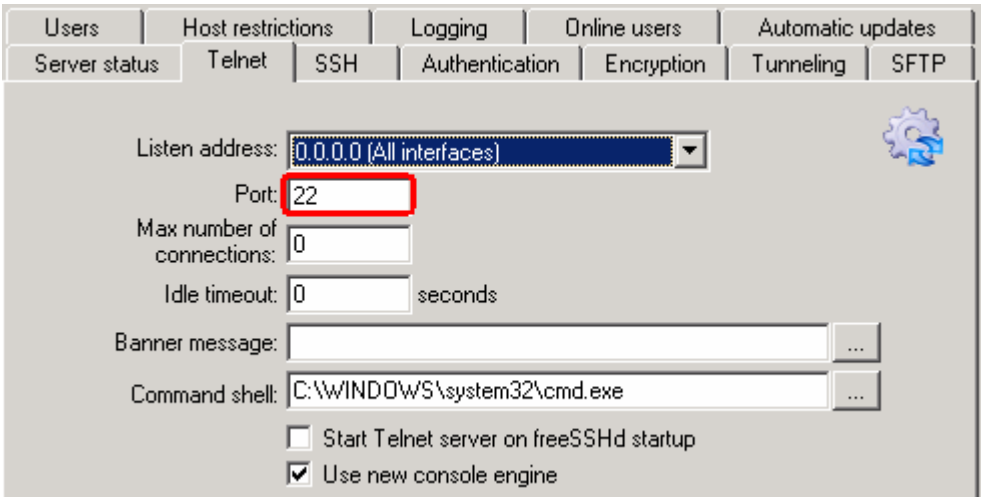


____ 16. Click **SFTP** tab from the top. Browse and select **C:\Labfiles62\SFTPHome** as SFTP home.

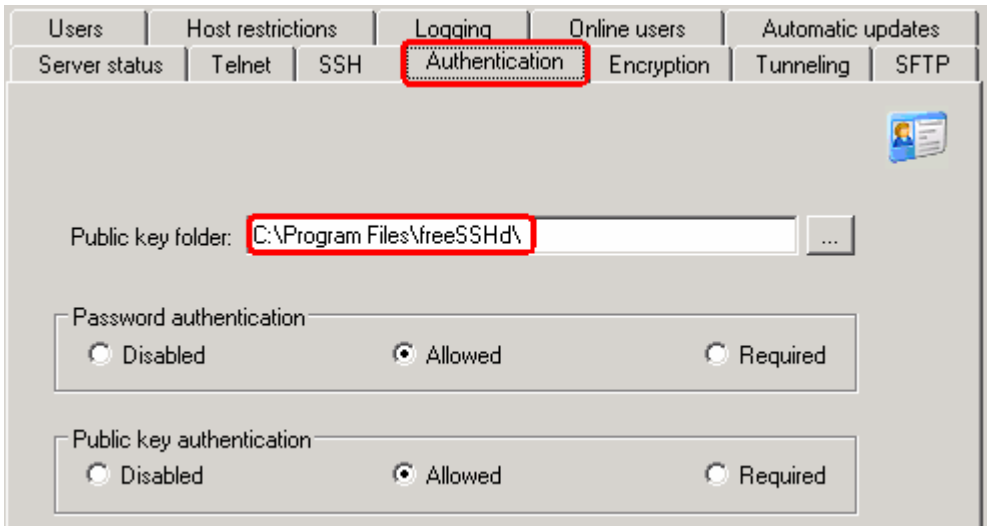
Note: Make a note of this directory as this is going to be the home directory for all the users that you will define later in this lab.



____ 17. Click **Telnet** tab from the top and ensure that the **Port** number is **22**



____ 18. Click the **Authentication** tab. Browse and select or accept the default Public key folder. Make a note of this folder as you are going to use this while generating the public/private key later in this lab.



____ 19. Add a user without public key authentication: **sftpuser1**

__ a. Click **Users** tab from the top of the settings window

__ b. Click **Add…**

__ c. Provide the values as shown below in the User properties window:

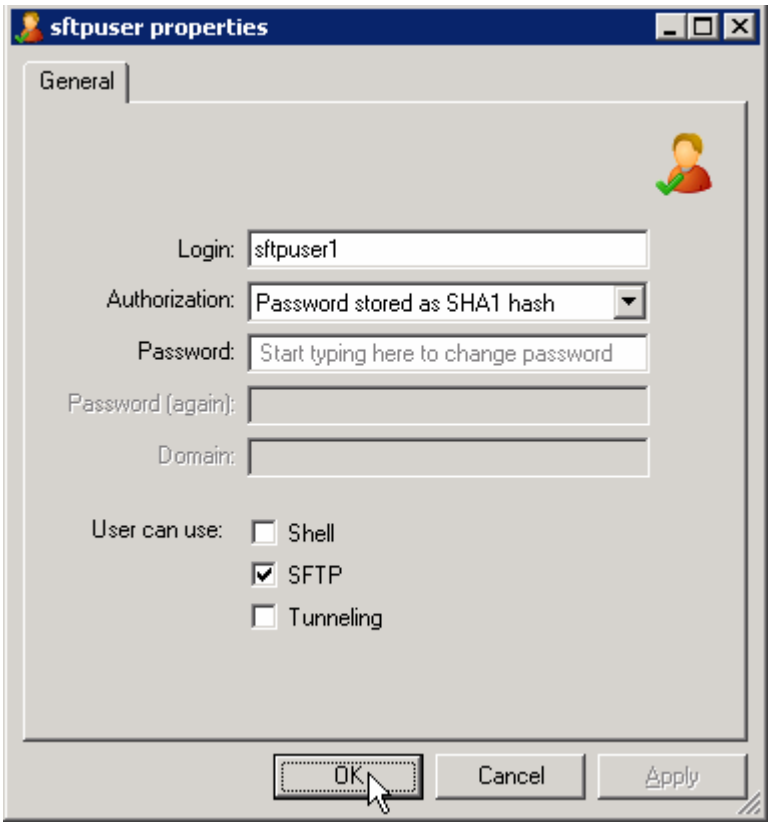
1) Login: enter any value, for Ex: **sftpuser1** (This is the user name to connect to your FTP server)

2) Authentication: select **Password stored as SHA1 hash** from the drop down menu

3) Password: enter any value, for Ex: **password**

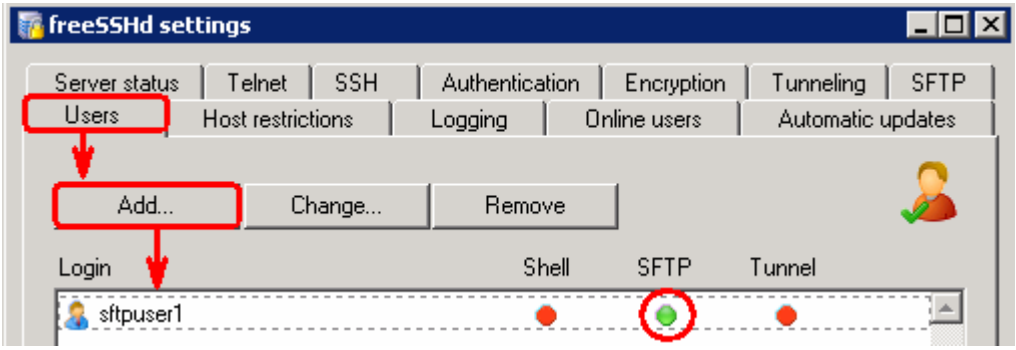
4) Password (again): enter the same value entered for the above field

5) Select the box next to **SFTP**



6) Click **OK**

__ d. You should now see **sftpuser1** added under Users tab



____ 20. Add another user with public and private key authorization: **sftpuser2**

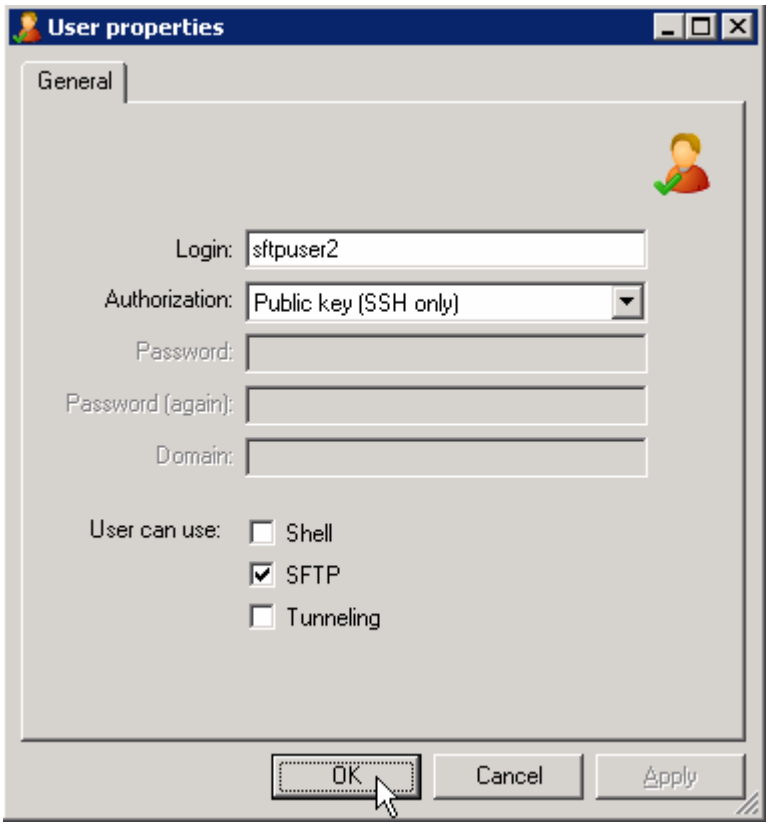
__ a. Under **Users** tab, click **Add…**

__ b. Provide the values as shown below in the User properties window:

1) Login: enter any value, for Ex: **sftpuser2** (This is the user name to connect to your FTP server)

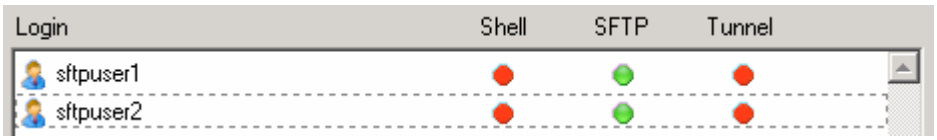
2) Authentication: select **Public key (SSH only)** from the drop down menu

3) Select the box next to **SFTP**



4) Click **OK**

__ c. You should see one more user, **sftpuser2**, added under Users tab

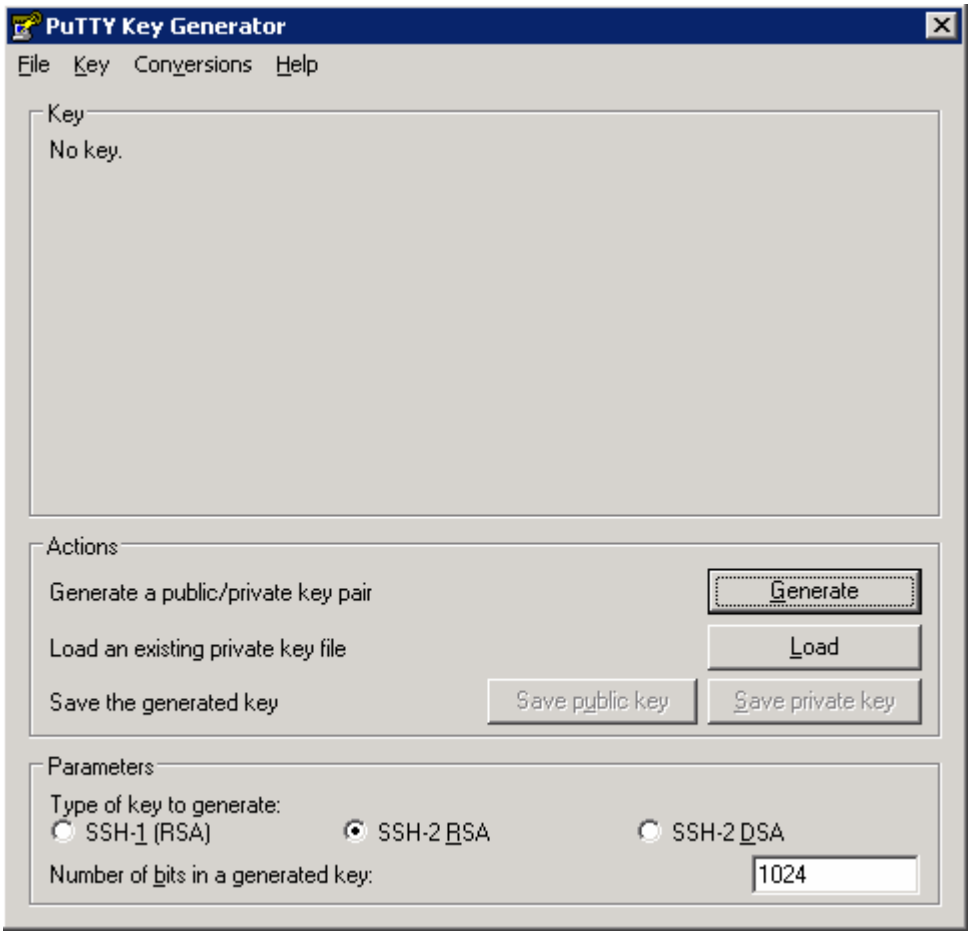


____ 21. Use PuTTY generator to generate public-private key pair

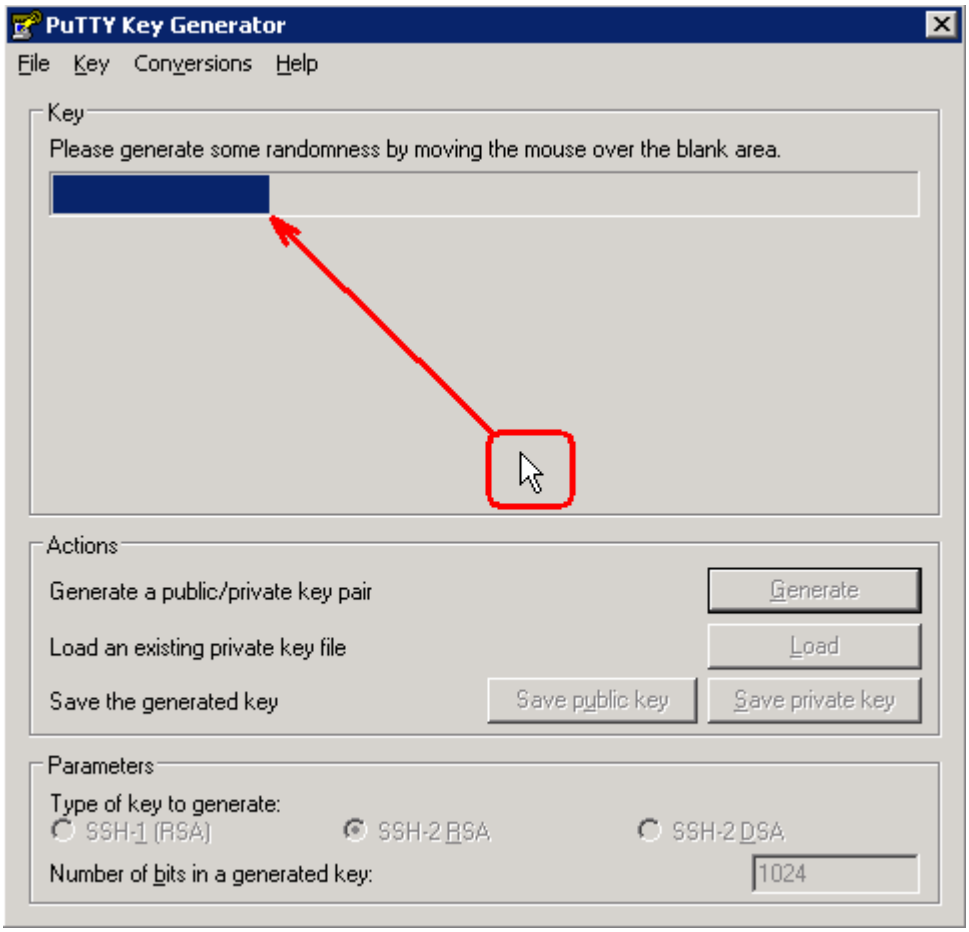
__ a. Go to the http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html and download the PuTTYgen (puttygen.exe) file onto your local machine.

__ b. Double click the downloaded **puttygen.exe** file to start the key generation

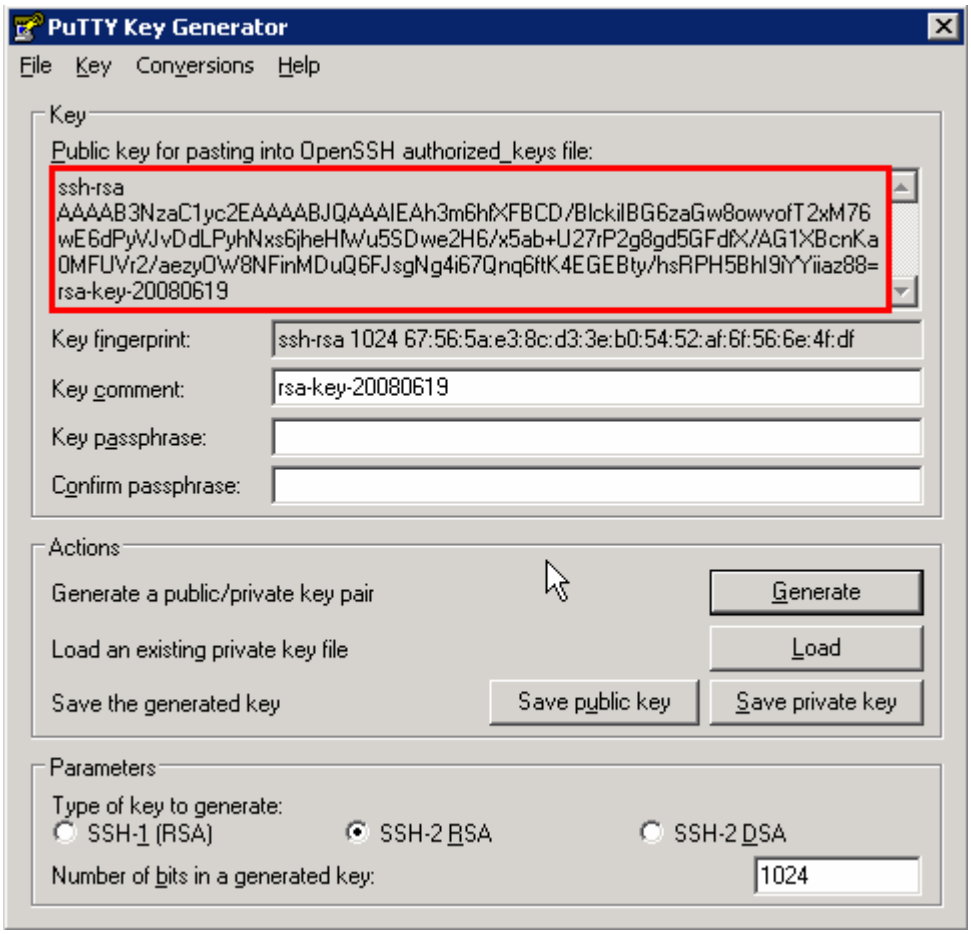
__ c. You should see the 'PuTTY Key Generator' window:



__ d. Click **Generate** and keep moving your curser inside the window to create some randomness

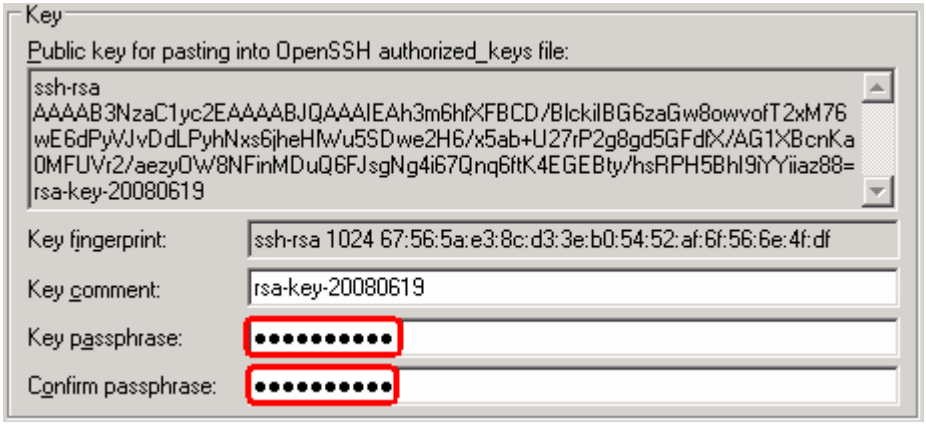


__ e. You should see the generated key as shown below:



__ f. Enter any value for Key Passphrase, for Ex: **passphrase**

__ g. Enter the same value for Confirm Passphrase, for Ex: **passphrase**



__ h. From the main menu, select **Conversions > Export OpenSSH key**

__ i. Browse and select any location to save this private key and provide any name for the file, for Ex: location - **C:\Labfiles62\SFTP** and file name – **PrivateKey.ppk**

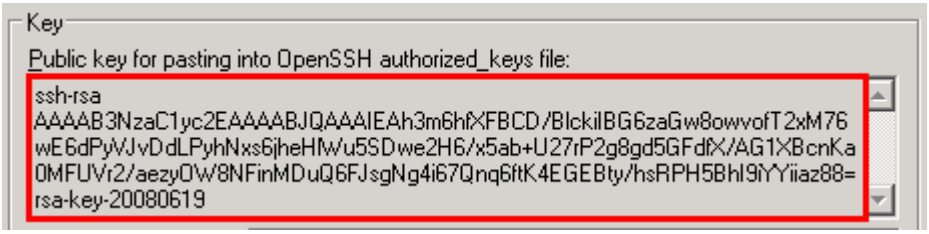
Note: Make a note of this file name and the path provided here.

__ j. Open a windows explorer and browse to your Public key folder, **C:\Program Files\freeSSHd**, and create a file with exactly same as the user name, **sftpuser2**, without any file extension

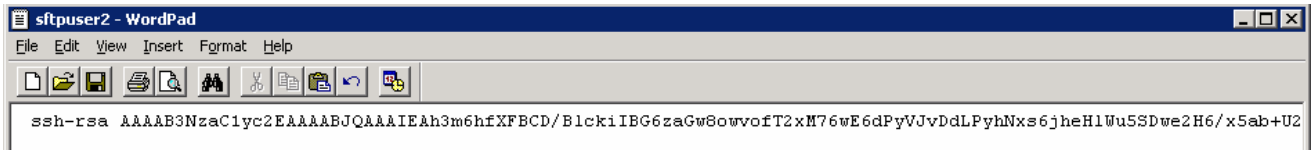
---

Note: The file name should match the user name that you created with public key authorization in the previous steps of this lab.

__ k. Copy the public key from PuTTY Key Generator window



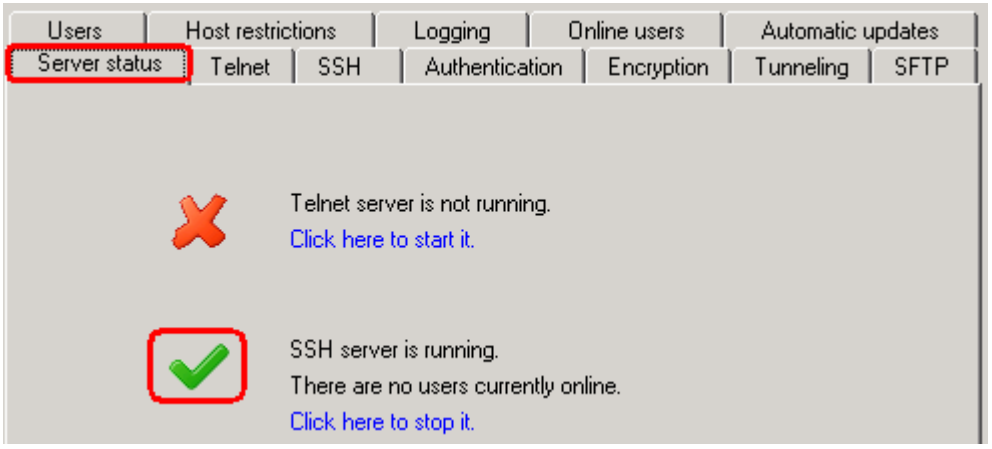
__ l. Open the above created file, **sftpuser2**, (using word pad or note pad) and paste the public key into that file



__ m. Save changes into that file and close it

____ 22. Make sure that the server is running:

__ a. Click **Server status** tab and you should see 'SSH server is running':



What you did in this exercise

In this lab, you installed the freeSSHd server and created two users. Then you continued to install and configure the PuTTYgen to generate key pair as a prerequisite for the FTP Adapter – SSH support lab.