# How To Use Filezilla to Transfer and Manage Files Securely on your VPS

[Getting Started](https://www.digitalocean.com/community/tags/getting-started)

* By Pablo Carranza

Published onOctober 17, 2013 718k views

### Introduction

Are you a recent cloud hosting convert and find yourself struggling to figure out how to best manage the files on your first virtual private server (VPS)? Do you find yourself intimidated by the command line? If so, you will be happy to learn that FileZilla provides a user-friendly graphical interface that can securely transfer files to-and-from, as well as move files around within, your VPS.

## Secure Communication

The two most common methods of securely transmitting information between two computers are the (i) Secure Shell (SSH) and (ii) Transport Layer Security (TLS), and its predecessor Secure Sockets Layer (SSL), cryptographic protocols. Both are public-key cryptography tunneling protocols that aim to create a secure, confidential exchange of data and connection across a network (particularly the internet). The encryption technologies used by both protocols are very reliable, and are (when configured correctly) nearly impossible for hackers to break into. However, while both protocols provide similar services, they are not the same. In fact, they have several significant differences that are beyond the scope of this article.

Today, [OpenSSH](http://www.openssh.org/) is a default software package found on Unix-like operating systems such as Mac OS X and Linux. Thus, programs or subsystems that are based on the SSH protocol will work “out-of-the-box” without having to go through the additional steps of either purchasing or creating the requisite SSL certificate needed for certain modes of secure data transmissions via TLS/SSL.

## FTP vs. SCP vs. SFTP vs. FTPS

When needing to upload or download files from your VPS in real time, you essentially have the following options:

1. [File Transfer Protocol (FTP)](https://www.digitalocean.com/community/articles/what-is-ftp-and-how-is-it-used);
2. Secure Copy Program (SCP);
3. SSH File Transfer Protocol (SFTP); or
4. FTP over TLS/SSL (FTPS).

### FTP \*not secure

Among the various file-transfer options, one should never, ever, ever connect to a remote server via FTP; SCP and SFTP are just as easy to use, but provide much more security. In addition, while FTP requires the installation of FTP server software such as [vsFTP](https://www.digitalocean.com/community/articles/how-to-set-up-vsftpd-on-ubuntu-12-04) or [ProFTP](https://www.digitalocean.com/community/articles/how-to-set-up-proftpd-on-ubuntu-12-04), both SCP and SFTP utilize the SSH protocol and, as a result, will work “out-of-the-box” when connecting to a remote Unix-like machine, such as Mac OS X or Linux.

### SCP vs. SFTP

Given that both SCP and SFTP utilize the SSH protocol in connecting to another computer, the two methods are fairly equal in regard to security. SFTP has a slight edge in regard to efficiency, because an interrupted file-transfer can resume where it left off in the event of a broken connection that is later re-established.

### SFTP vs. FTPS

SFTP should not be confused with FTPS, because the two methods are incompatible with each other. While FTPS can provide equal security, it does require additional steps to deploy if one does not already have an SSL certificate.

## SFTP Clients

There are several quality SFTP clients out there: [Cyberduck](http://en.wikipedia.org/wiki/Cyberduck), [Filezilla](http://en.wikipedia.org/wiki/Filezilla) or [WinSCP](http://winscp.net/), to name a few. This article, however, will focus on Filezilla – an open-source (i.e. free) FTP client for Windows, Mac OS X and Linux. In addition to being able to download the program, the [filezilla-project.org](https://filezilla-project.org/) site also contains a documentation [Wiki](https://wiki.filezilla-project.org/Main_Page) and a [Support Forum](https://forum.filezilla-project.org/).

## Key-based Authentication

With SFTP, you have two user-authentication options when connecting to a cloud server: (i) passwords or (ii) SSH keys. For a discussion on the benefits of SSH keys over passwords and/or instructions on setting up password-less logins on your server, please refer to [How To Create SSH Keys with PuTTY to Connect to a VPS](https://www.digitalocean.com/community/articles/how-to-create-ssh-keys-with-putty-to-connect-to-a-vps).

## SFTP via SSH2 Key-based Authentication

FileZilla has a built-in key management page in the Settings dialog, which allows you to save your Public (SSH) Key and to (securely) automate the process of connecting to a remote server.

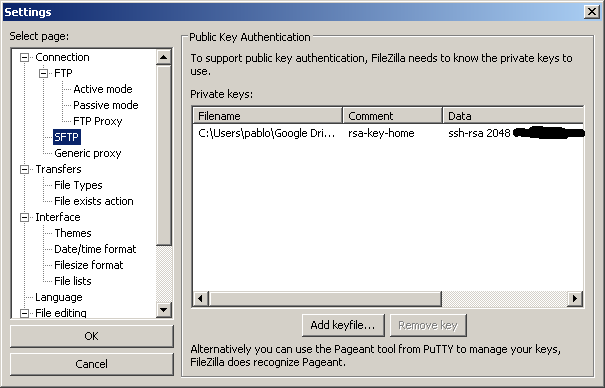
### Prequisite

If you have yet to create an SSH key pair, you can do so by following one of two [DigitalOcean tutorials](https://www.digitalocean.com/community/articles):

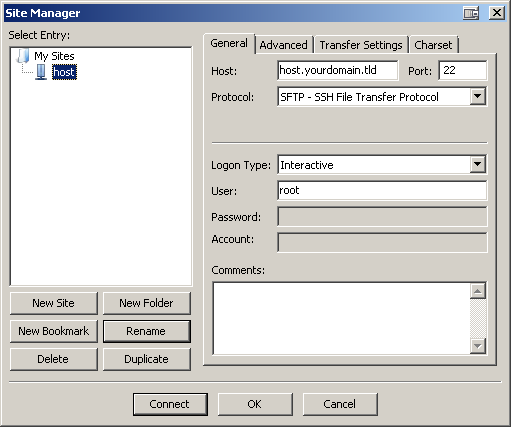
* Windows users: [How To Create SSH Keys with PuTTY to Connect to a VPS](https://www.digitalocean.com/community/articles/how-to-create-ssh-keys-with-putty-to-connect-to-a-vps)
* Mac OSX & Linux users: [How To Set Up SSH Keys](https://www.digitalocean.com/community/articles/how-to-set-up-ssh-keys--2)

Follow these steps once you have an SSH key pair that you would like to use to connect to your VPS:

1. Open the FileZilla client.
2. From the top of the home screen, click on Edit and select Settings.
3. On the left side of the menu, expand the Connection section and highlight SFTP.



1. Click on the [Add keyfile…] button and browse your local machine’s directories and select your Private Key file.
2. Then, again from the top of FileZilla’s home screen, click on File and select Site Manager.
3. Finally, on the left side of the Site Manager, click on the New Site button and type a unique name under My Sites that will allow you to easily identify this particular remote server in the future.



1. Now, under the General tab, fill in the Host (with either an IP address or [FQDN](https://www.digitalocean.com/community/articles/how-to-set-up-a-host-name-with-digitalocean)) and Port fields (default is 22).
2. In the Protocol dropdown menu, select SFTP - SSH File Transfer Protocol.
3. In the Logon Type dropdown menu, select Interactive.

Note for PuTTY users with passphrase-protected public keys: If your original .ppk file is password-protected, FileZilla will convert your .ppk file to an unprotected one when importing the key into FileZilla. As of version 3.0.10, a password-protected key file is not yet supported.

If a password-protected key file is desired, FileZilla is able to utilize [PuTTY](http://www.chiark.greenend.org.uk/~sgtatham/putty/)’s [Pageant](http://the.earth.li/~sgtatham/putty/0.63/htmldoc/Chapter9.html" \l "pageant) tool.

1. Simply run Pageant; in your system tray, you will see the Pageant icon appear.
2. Right-click on the icon and select Add Key and select your private key (.ppk) file.
3. Then, follow the prompt to enter your passphrase.
4. Finally, launch FileZilla and connect to your virtual private server via SFTP using SSH2 with a username and an empty password (do not forget to close pageant when you are done).

## Editing Text Files

In managing your VPS, you will inevitably encounter a situation where some programming (text) files require edits. FileZilla does not carry a built-in text editor, which gives you the freedom of using any text editor of your choice. A popular editor among Windows users is [Notepad++](http://notepad-plus-plus.org/) because it is lightweight and can work with many of today’s popular [programming languages](http://en.wikipedia.org/wiki/Notepad%2B%2B" \l "Programming_languages).

By default, FileZilla is configured to utilize your local system’s default editor. If you do not wish to make Notepad++ your system’s default text editor, but would nevertheless like to use it to edit HTML, XML, Python, CSS, PHP & other programming files on your VPS:

1. From the FileZilla home screen, click on Edit and select Settings.
2. Along the left side of the Settings window, highlight File editing.
3. Then, select the radio button associated with Use custom editor and click on the Browse button.
4. Find your desired editor’s executable (.exe on Windows machines), double-click on it, and click the OK button to save your changes & close the Settings window.

<p><div class=“author”>Article submitted by: <a href=“https://plus.google.com/107285164064863645881?rel=author” target=“\_blank”>Pablo Carranza</a> </div></p>

https://www.digitalocean.com/community/tutorials/how-to-use-filezilla-to-transfer-and-manage-files-securely-on-your-vps