

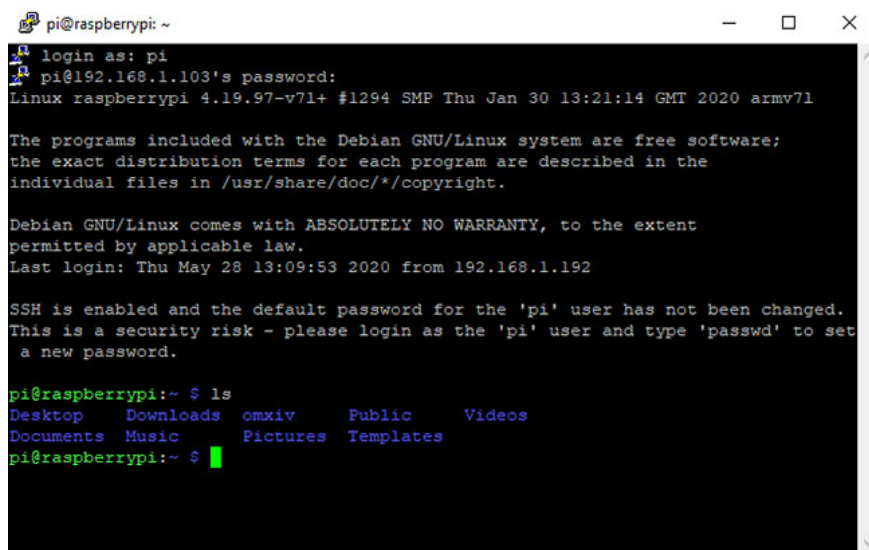
5 ways to use SSH in Windows

SSH (Secure Shell) is an encrypted network protocol used to connect devices over the network or the Internet. Several SSH options are available for Windows. Here's how to use SSH in Windows with native apps and third-party options.

SSH (Secure Shell) is an encrypted network protocol used to connect devices over the network or the Internet. Linux computers come with a built-in SSH tool, accessible using the Terminal command, but what about with Windows?

Several SSH options are available for Windows, including the built-in SSH tool. Here's how to use SSH in Windows with native apps and third-party options.

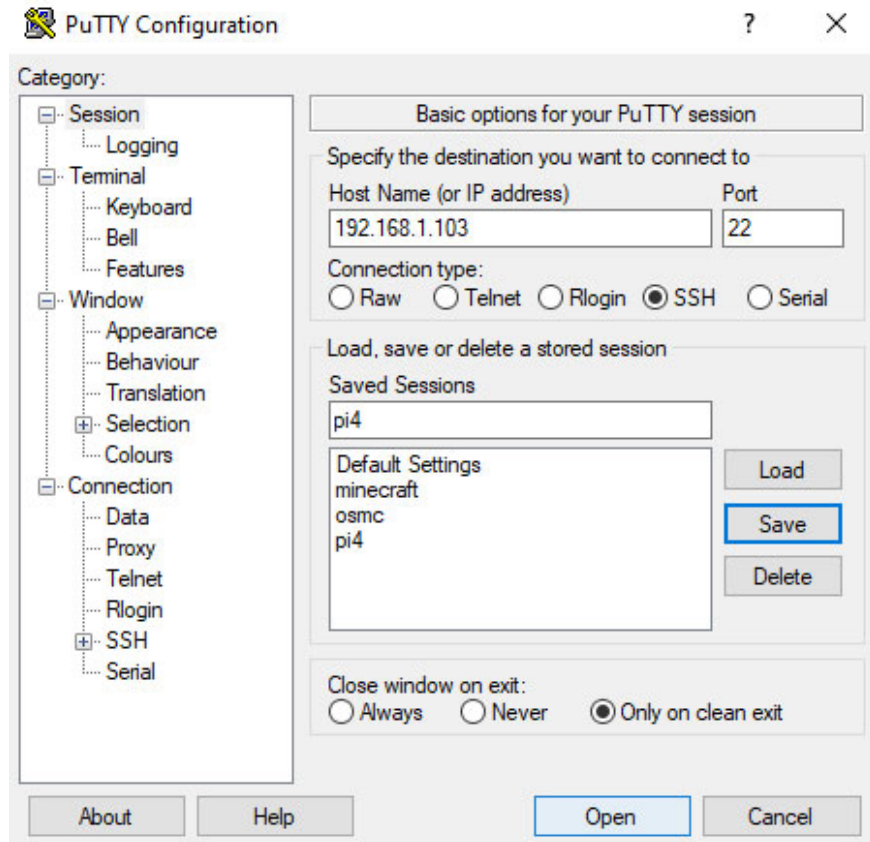
1. PuTTY for Windows desktop



PuTTY is the most popular application for connecting to SSH servers on Windows. PuTTY's interface may seem a little scary and complicated at the beginning, but when used, you will find it very simple.

To use PuTTY, all you need to do is launch **putty.exe**. Here, enter the hostname (or IP address) of the remote server, ensure the correct port and click **Open**. PuTTY will connect to the server, then prompt you to enter your username and password.

You can also save session information if desired. Click the **Default Settings** option, then select **Save** and PuTTY will use the saved settings each time it is opened. Or, set a different profile for each connection, enter a name in the **Saved Sessions** field and click **Save**.



Set different profiles for each connection

Download PuTTY (Free) [HERE](https://www.putty.org/)
<https://www.putty.org/>

See how to [install PuTTY](#) and [use PuTTY](#)

2. Use Windows PowerShell for SSH

```
pi@raspberrypi: ~
PS C:\WINDOWS\system32> ssh pi@192.168.1.103
The authenticity of host '192.168.1.103 (192.168.1.103)' can't be established.
ECDSA key fingerprint is SHA256:YKe/x4Trhc7tXultbZgiVDxi2L3xIPF5qOZ2dJ56xi4.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '192.168.1.103' (ECDSA) to the list of known hosts.
pi@192.168.1.103's password:
Linux raspberrypi 4.19.97-v7l+ #1294 SMP Thu Jan 30 13:21:14 GMT 2020 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu May 14 08:48:31 2020 from 192.168.1.37

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi: ~
```

Use Windows PowerShell for SSH

If you want a Windows command-line SSH tool built by Microsoft built into your operating system, you're in luck.

Windows PowerShell has gradually replaced the position of the Windows Command Prompt application since it was introduced in Windows 7. Recently, support for OpenSSH has been added, you can combine in PowerShell as follows:

1. Press **WIN + I** to open **Settings**.
2. Open **Apps > Apps & features** .
3. Click **Optional features**.
4. Click + **Add a feature** .
5. Browse the list to find **OpenSSH Client**.
6. Select and click **Install**.
7. Once done, restart Windows 10.

With OpenSSH added, you can use it by opening Windows PowerShell (right-click **Start > PowerShell**) and enter the connection command. For example:

```
ssh username@192.1.1.10
```

You will be prompted for a password. Please enter the password and agree to the security certificate.

3. Secure Shell for Google Chrome

Google provides an SSH client called **Secure Shell App** , which can be added to the Chrome browser. Just install the Secure Shell application from the Chrome Web Store. Although it runs in Chrome browser, it runs completely offline so you don't need Internet access to use it. Therefore, this tool works well with devices on the local network as well as with remote servers.

The Secure Shell App opens as a browser tab. Just enter the login and hostname (IP address) of the remote SSH server. You can also combine additional SSH command line arguments, if needed.

Like other Chrome web applications, Secure Shell App can be opened in a dedicated window to separate this application from the main browser.

Because Secure Shell is a Chrome web application, it is also available for macOS, Linux and even Chrome OS.

Download Secure Shell App for Google Chrome

<https://chrome.google.com/webstore/detail/secure-shell-app/pnhechapfajndjhompbnflclldabbghjo>

4. OpenSSH for Cygwin terminal

If you regularly use standard SSH commands on Linux, macOS and other similar UNIX systems, Cygwin has SSH support.

If you're new to SSH, you might want to use a graphical option like PuTTY. However, if you have any experience with command line operation, you will see that OpenSSH in Cygwin works just like on other platforms.

Cygwin is a great installation package, so you may just want to install OpenSSH. To do this, run the downloaded installer and when prompted to select a package, look for **OpenSSH**. Expand **Net** and in the **New** column , click

Skip so it displays the version to download.

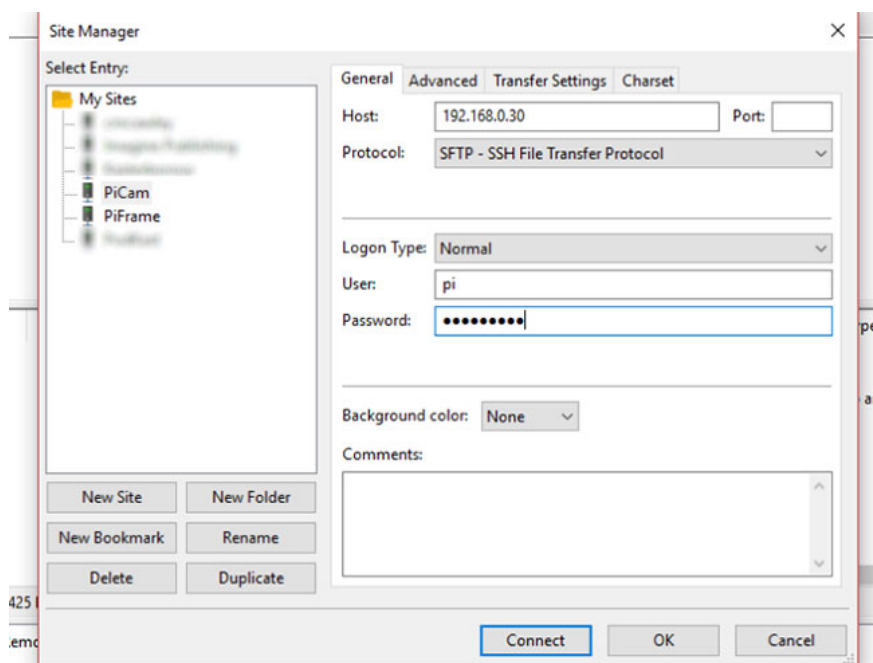
Click **Next** to continue, review the packages to be installed, and then click **Next** again.

After the installation process has finished, launch the Cygwin application in Terminal from the Start menu. To start an SSH connection, use the same ssh command that you already run on Linux and other UNIX-like operating systems.

While a good solution, Cygwin can be difficult to set up.

Download Cygwin (Free)
<http://cygwin.com/setup-x86.exe>

5. SSH over FTP with FileZilla



SSH over FTP with FileZilla

Typically, the main reason when using SSH to communicate with remote devices is to upload files. Typically, this is because you are managing a web server and want to upload a web application (e.g. WordPress).

FileZilla is an open source FTP (File Transfer Protocol) tool with support for SFTP (SSH File Transfer Protocol). Obviously, this makes FTP transmission a lot safer.

To use SSH in FileZilla :,

1. Open **File> Site Manager** to create a new connection.
2. Select **New site** to add a new site.
3. Select **SFTP** as the protocol.
4. Enter the server's IP address or hostname.
5. Add username and password.
6. Click on **Connect**.

File transfer will now be done via SSH.

Download FileZilla (Free)

<https://filezilla-project.org/download.php?platform=win64>

You finished reading the article "**5 ways to use SSH in Windows**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
