3 Ways to Use SSH on Windows to Log Into Linux Server

Last Updated: June 12th, 2022 Xiao Guoan (Admin) 9 Comments Linux Server

This tutorial is going to show you 3 ways to log into Linux server on Windows via SSH.

What's SSH?

SSH stands for **S**ecure **Sh**ell, which was invented in 1995 to replace the insecure Telnet (Telecommunication Network). It's now the primary way for system administrators to securely log into remote Linux servers over the public Internet. Although it looks and acts the same as Telnet, all communications over the SSH protocol is encrypted to prevent packet sniffing.

If you are running a Linux or Mac computer, SSH client is installed by default. You can open up a terminal window and run the `ssh` command like below to connect to a remote Linux server.

```
ssh username@12.34.56.78
```

Now let's discuss how to use SSH on Windows.

Method 1: Windows 10's Built-in SSH Client

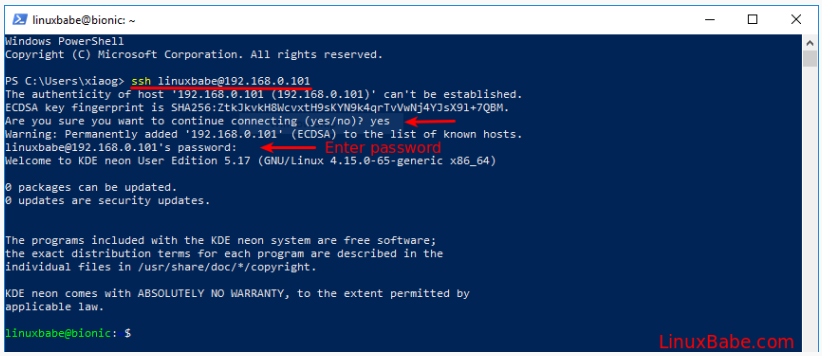
The Microsoft PowerShell team decided to port OpenSSH (both the client and the server) to Windows in 2015. It finally arrived in Windows 10's Fall Creator Update in 2017 and is enabled by default in the April 2018 Update.

To use the OpenSSH client on Windows 10, simply open a PowerShell window or a command prompt window and run the `ssh` command. For example, if I want to connect to my Ubuntu desktop in the LAN, I would run

```
ssh linuxbabe@192.168.0.101
```

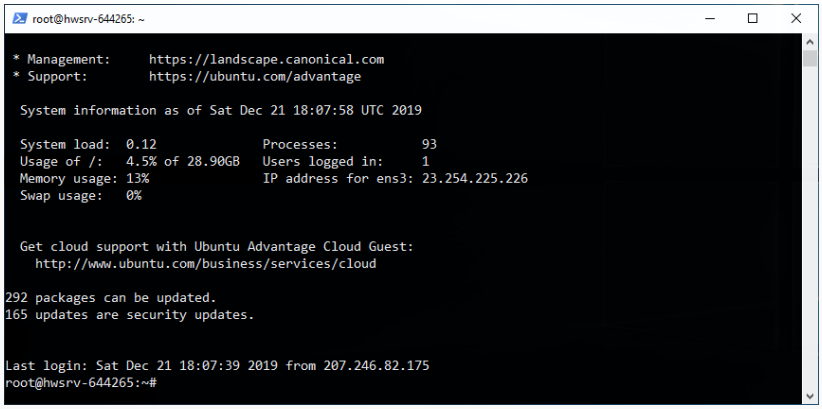
`linuxbabe` is the username on my Ubuntu desktop and `192.168.0.101` is the private IP address for my Ubuntu desktop. The first time you connect to a Linux computer, you will be prompted to accept the host key. Then enter your password to login. After login, you can run Linux commands to do administrative tasks.

Note that if you want to paste a password into the PowerShell window, you need to right-click the mouse and press Enter.



To log out from the Linux box, run the `exit` command or press `Ctrl+D`.

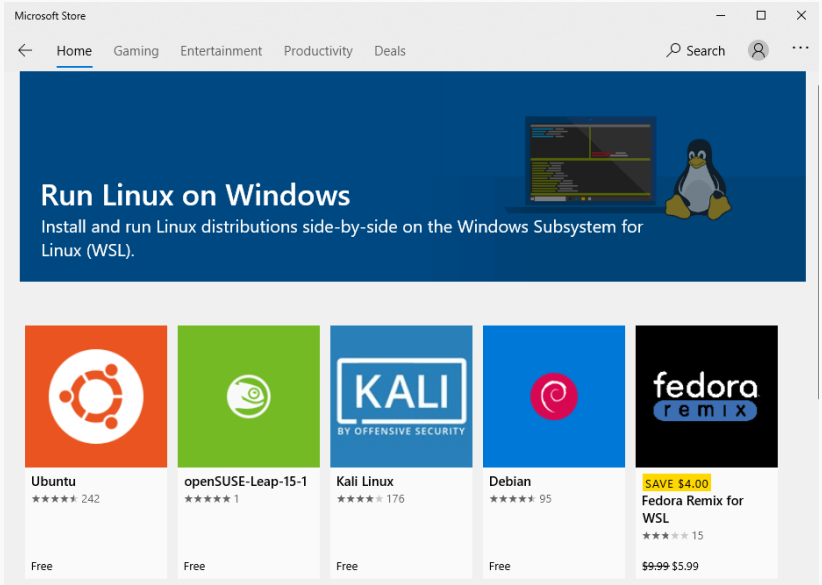
The default font size in PowerShell Window is very small. To change it, right-click the titlebar and select `properties`, then you can change the font size, and the background color.



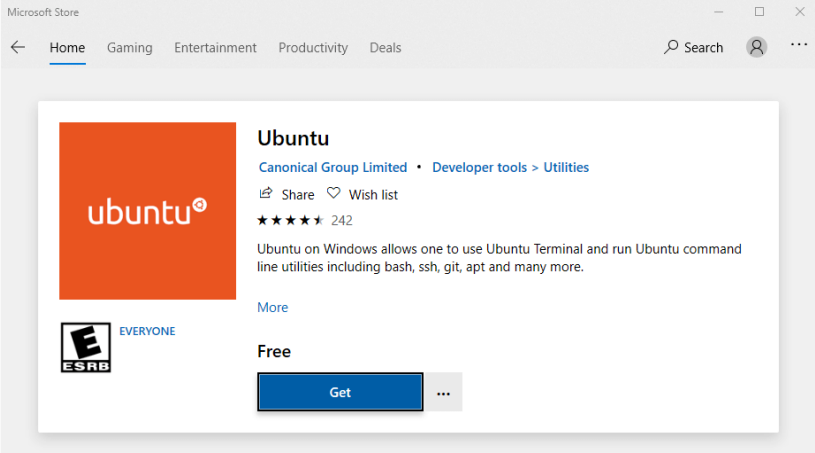
Method 2: Use SSH in Windows Subsystem for Linux

Windows Subsystem for Linux (WSL) enables you to run native Linux command-line tools directly on Windows 10. If you are a system administrator, WSL is probably an overkill for just using SSH because it would install and run a Linux distro (without graphical user interface) on your Windows 10 desktop. WSL is created for web developers or those who need to work on open-source projects. You can use not only SSH but also other Linux command line tools (Bash, sed, awk, etc).

Open the Microsoft Store and enter `WSL` in the search box. Select `Run Linux on Windows` and install a Linux distro of your choice.

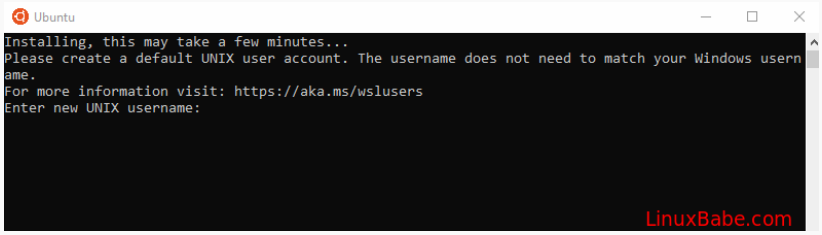


For example, I choose **Ubuntu** and click the `Get` button to install it.



Once your Linux distro is installed, open the `Control Panel` and select `Programs` -> `Turn Windows features on or off`. Tick on the checkbox of Windows Subsystem for Linux to enable this feature. (You may need to reboot your Windows PC for this change to take effect.)

Next, you can launch the Linux distro from the start menu by search the distro's name. The first time you launch it, you need to create a user and set a password.



After that, you can use the ssh command like below to connect to a Linux server or PC that runs a SSH server.

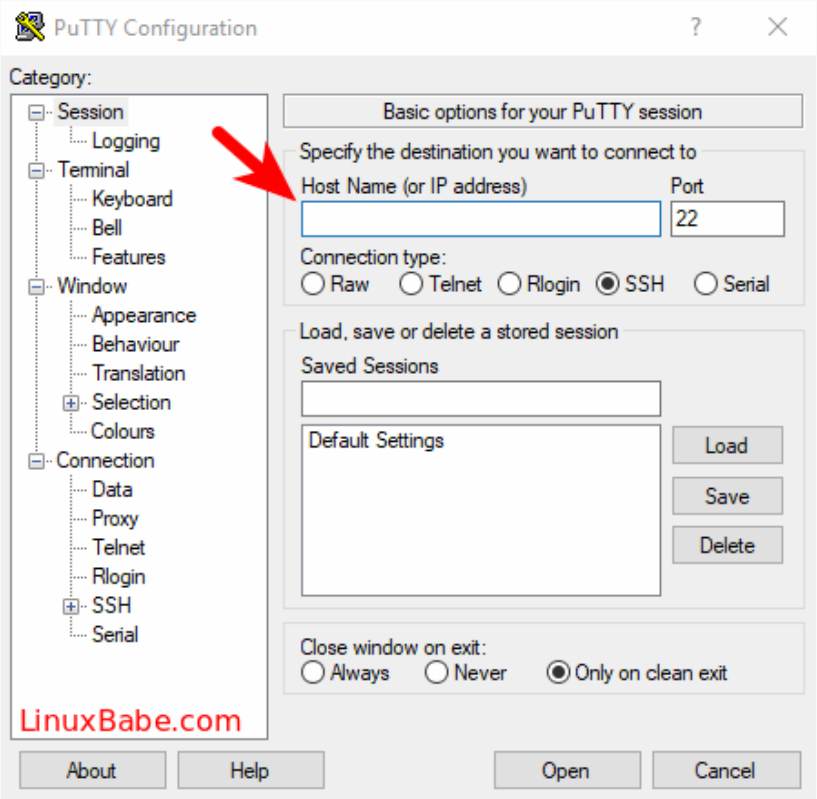
```
ssh linuxbabe@192.168.0.101
```

Method 3: Use Putty

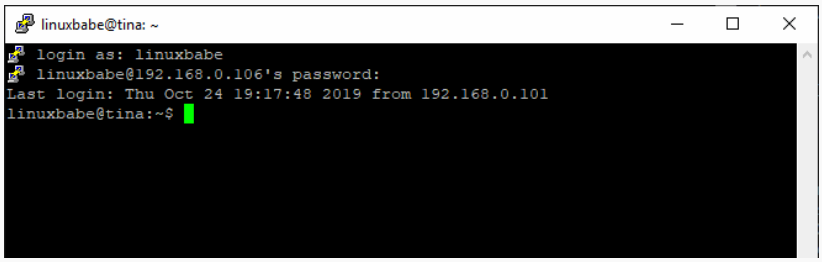
Putty is a well-known and the most popular SSH client on Windows before the arrival of Windows OpenSSH client and

Windows Subsystem for Linux. To use SSH with Putty, you need to download the Putty program from the official website and install it.

Launch Putty from the Start menu. Then enter the IP address or hostname of the Linux box and click the `Open` button to connect to it.



Accept the host key and you will be prompted to enter the username and password.



Please note that when you type in your password, the cursor doesn't move, but it's actually accepting your password. To paste text into Putty, first press `Ctrl+C` to copy the text, then go to Putty window and press the right button of your mouse.

How to Set Up SSH Key on Windows 10 (Optional)

There’re mainly two ways of authenticating user login with OpenSSH server:

- password authentication
- public-key authentication: also known as **passwordless SSH login** because you don’t need to enter your password.

To set up public-key authentication on Windows 10, follow the instructions below.

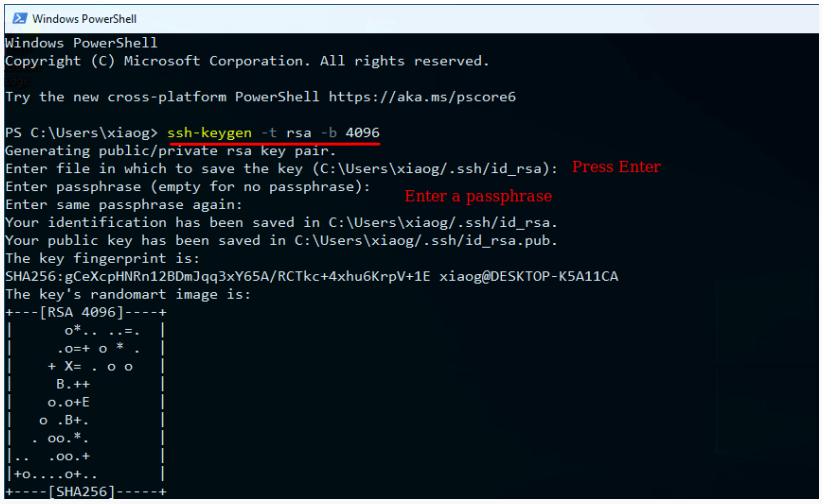
Open Windows Powershell, and run the following command to generate SSH keypair.

```
ssh-keygen -t rsa -b 4096
```

Where:

- `-t` stands for `type`. The above command generates an RSA type keypair. RSA is the default type.
- `-b` stands for `bits`. By default, the key is 3072 bits long. We use a 4096 bits key for stronger security.

When asked which file to save the key, you can simply press `Enter` to use the default file. Next, you can enter a passphrase to encrypt the private key, but you will need to enter this passphrase every time when you log into the Linux server. If you don’t want it, you can press Enter, so it will have no passphrase.



- The private key (your identification) will be saved in the **.ssh/id_rsa** file under your user directory.
- The public key will be saved in the **.ssh/id_rsa.pub** file.

Now we need to upload the public key to remote Linux server. You can display the public key in the Powershell with the following command.

```
cat .ssh/id_rsa.pub
```

Then log in to your server via password authentication, and run the following command to create a `.ssh` directory under your home directory.

```
sudo mkdir ~/.ssh
```

Create the authorized_hosts file

```
sudo nano ~/.ssh/authorized_keys
```

Copy your SSH public key and paste it to this file. Save and close the file. To save a file in Nano text editor, press `Ctrl+O`, then press `Enter` to confirm. To close a file, press `Ctrl+X`.

Next, change the permission of this file.

```
sudo chmod 600 ~/.ssh/authorized_keys
```

Log out of your Linux server.

```
exit
```

Now you can SSH into your server without entering a password.

Next Step

I hope this article helped you use SSH on Windows. You might also want to protect SSH service from hacking, I recommend setting up public-key authentication or two-factor authentication.

- 2 Simple Steps to Set up Passwordless SSH Login on Ubuntu
- Set Up SSH Two-Factor Authentication (2FA) on Ubuntu Server

Also, you can enable automatic security updates on your Linux server to patch vulnerabilities.

- Set Up Automatic Security Update (Unattended Upgrades) on Ubuntu

If you want FTP access to the Ubuntu server, you can set up pure-FTPd server.

- How to Set Up a Secure FTP Server with Pure-FTPd on Ubuntu