

How to create SSH key on Windows

Protecting your connections and data integrity is where Secure Shell (SSH) keys excel. SSH keygen is commonly used to gain secure access to remote servers and cloud services.

You should have an SSH key if you regularly access remote servers using your Windows device.

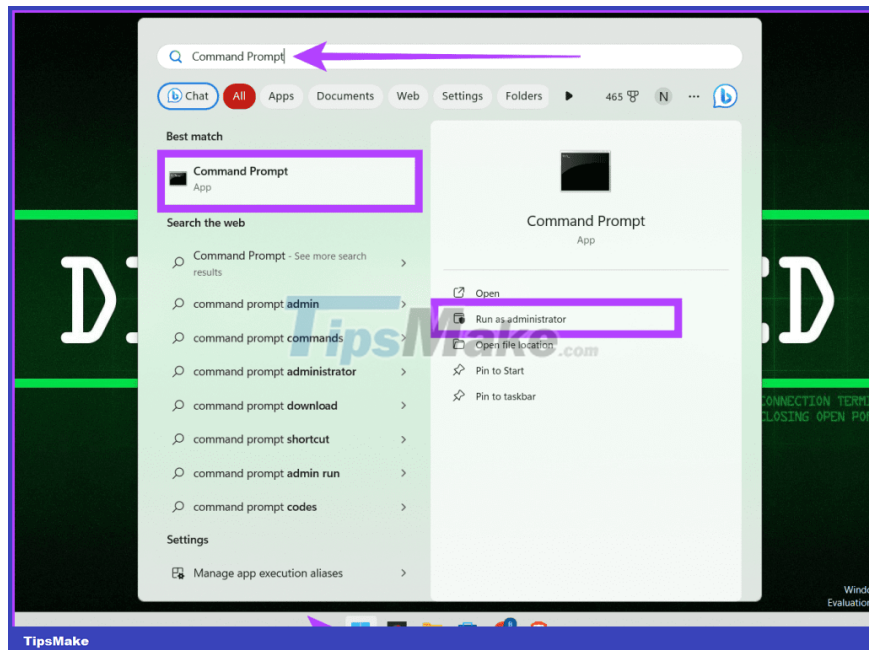
Besides remote servers, you can also use these security keys to grant access to your employees at work where you are likely to be exposed to a data breach, e.g. , data center, etc. This article will guide you through easy steps to create SSH keys on Windows.

Creating an SSH key on Windows is very simple, you can use 1 of the 3 methods listed below.

1. Use Command Prompt

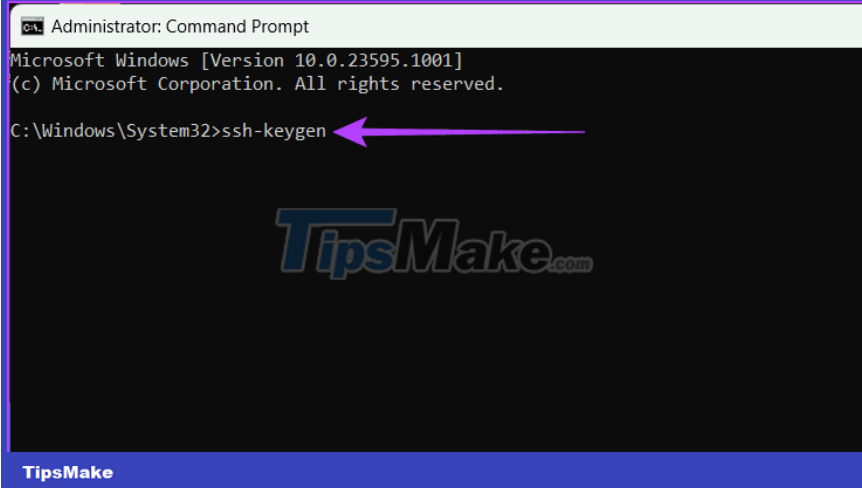
Generating SSH keys with the help of the command line is quick and easy. Follow the steps outlined below.

Step 1: Click the Start button. Search for **Command Prompt** and select **Run as administrator** . Click **Yes** when prompted to let CMD make the changes to your computer.



Step 2: Type the following command and press **Enter** on the keyboard:

ssh-keygen



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

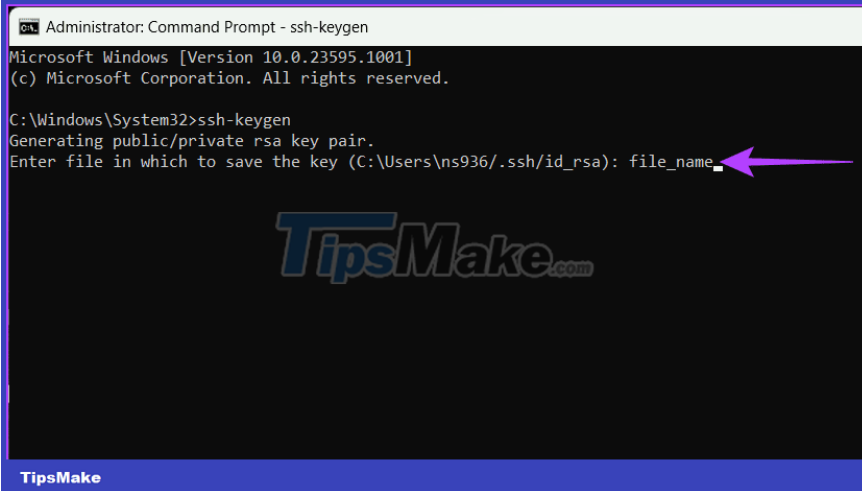
C:\Windows\System32>ssh-keygen
```

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The text inside the window includes the Windows version information and the command "ssh-keygen" being entered at the prompt. A purple arrow points to the command. A "TipsMake.com" watermark is visible in the center of the window.

Step 3: Enter the key storage file name and press **Enter** :

file_name

Tip : You can also set a custom path here to store the key in the default location (*C:Users[username]*) .



```
Administrator: Command Prompt - ssh-keygen
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ns936/.ssh/id_rsa): file_name_
```

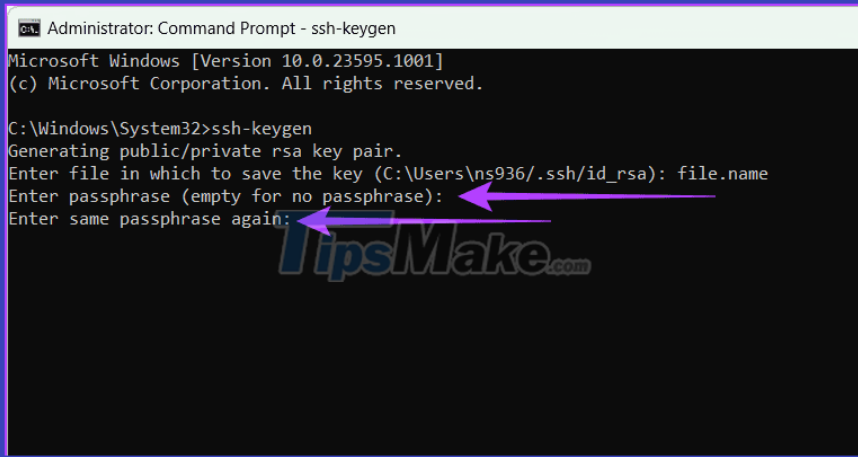
The screenshot shows the Command Prompt window after the "ssh-keygen" command has been executed. It displays the progress of generating a public/private RSA key pair and prompts the user to enter a file name to save the key. A purple arrow points to the "file_name_" prompt. A "TipsMake.com" watermark is visible in the center of the window.

Step 4: Enter the passphrase to secure your key and press **Enter** to save the changes.

Note : You can press **Enter** twice to skip this step and directly save the key without a password.

Your private key and public key are securely stored. A confirmation message with additional key information is now displayed on the screen. You can proceed to close this window.

You can use this to generate multiple SSH keys with different file names.

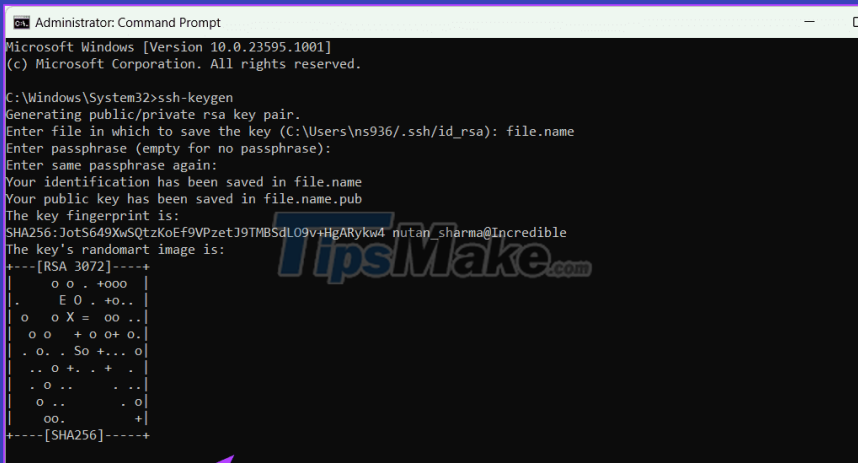


```
Administrator: Command Prompt - ssh-keygen
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ns936/.ssh/id_rsa): file.name
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

TipsMake

Step 5: Type **exit** and press **Enter** on the keyboard to close the CMD window.



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\ns936/.ssh/id_rsa): file.name
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in file.name
Your public key has been saved in file.name.pub
The key fingerprint is:
SHA256:JotS649XwSQtzKofF9VPzetJ9TMBSDLO9v+HgARYkw4 nutan_sharma@Incredible
The key's randomart image is:
+--[RSA 3072]-----+
  |  o o . +ooo |
  |   E 0 . +o.. |
  |  o o X = oo . |
  | o o . + o o+ o |
  | . o . . So +... |
  | .. o +. . + . |
  | - o .. . . . |
  | o .. . . o |
  | oo. . . . + |
  +----[SHA256]-----+
```

TipsMake

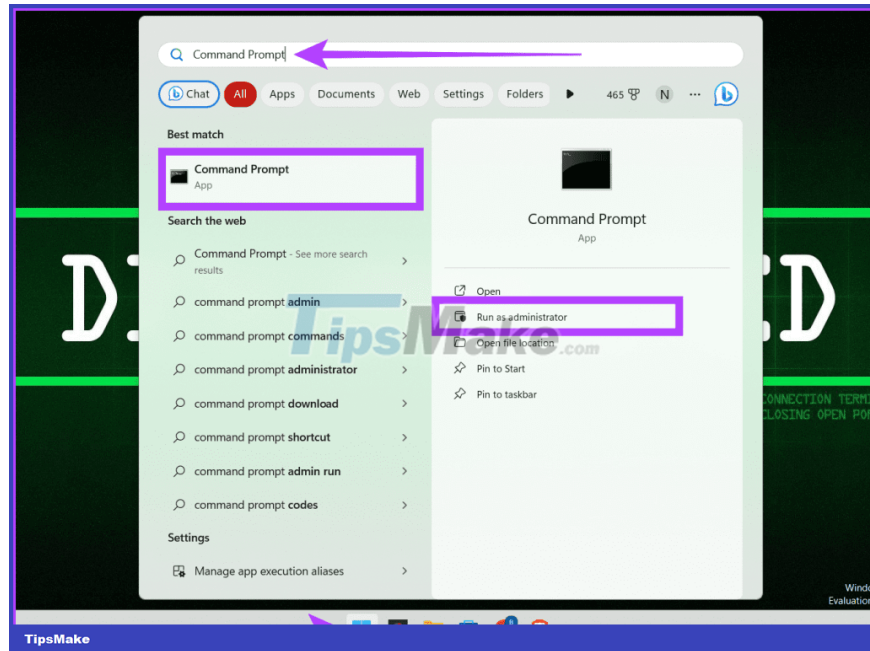
2. Use WSL

Generating SSH keys using Windows Subsystem for Linux (WSL) gives you many advantages. You can get the benefits of Linux tools and the ease of working on a Windows computer. Furthermore, it provides a smooth and secure way to handle SSH authentication.

Install WSL and Linux distribution

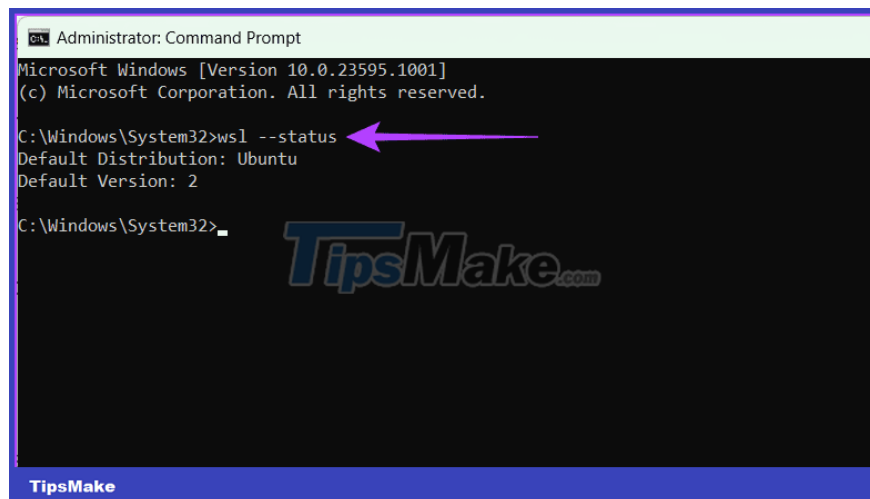
Follow the steps below to install and set up WSL and Linux distribution on your Windows device.

Step 1: Click on the Windows icon and find **Command Prompt** . Click **Run as administrator** and select **Yes** when prompted.



Step 2: Windows 11 comes pre-installed with WSL. You can check it by typing the command mentioned below and pressing **Enter** .

```
wsl --status
```



If you are using Windows 10, install WSL using one of the methods below:

1. **Microsoft Store**

Download Windows Subsystem for Linux (WSL) from the Microsoft Store.

1. **Command line interface**

Enter the command mentioned below and press **Enter** on your keyboard.

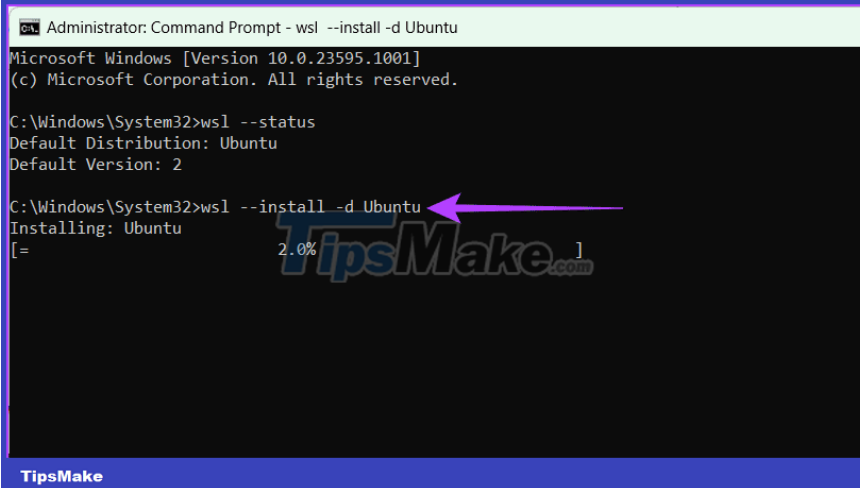
```
wsl --install
```

Step 3: After installing WSL on your computer, you can download any Linux operating system using Microsoft Store or command line interface.

The article is using Command Prompt to download Ubuntu for this tutorial. Enter the command below and press **Enter** on your keyboard to do so.

```
wsl --install -d Ubuntu
```

Note : If you want to install Kali Linux, write **kali-linux** in the command above.



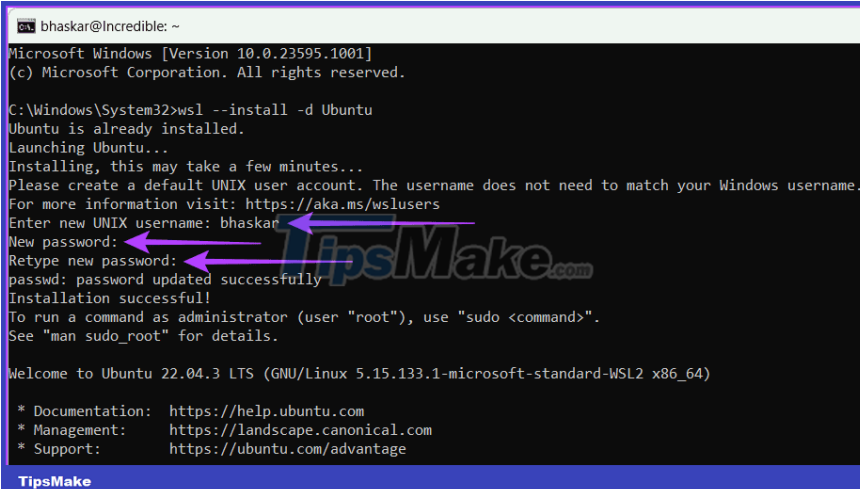
```
Administrator: Command Prompt - wsl --install -d Ubuntu
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>wsl --status
Default Distribution: Ubuntu
Default Version: 2

C:\Windows\System32>wsl --install -d Ubuntu
Installing: Ubuntu
[= 2.0%
```

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - wsl --install -d Ubuntu". The prompt shows the status of WSL, then the command to install Ubuntu, and the progress of the installation. A purple arrow points to the command line. A "TipsMake.com" watermark is visible in the center.

Step 4: Enter UNIX username and password.



```
bhaskar@Incredible: ~
Microsoft Windows [Version 10.0.23595.1001]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>wsl --install -d Ubuntu
Ubuntu is already installed.
Launching Ubuntu..
Installing, this may take a few minutes..
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: bhaskar
New password:
Retype new password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 x86_64)

* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
```

The screenshot shows the same Command Prompt window after the installation. It displays the progress of launching Ubuntu, prompts for a UNIX username and password, and shows the successful completion of the installation. A purple arrow points to the username input. A "TipsMake.com" watermark is visible in the center.

Step 5: Close the UNIX window by typing **exit** and pressing **Enter**. Repeat the process to close the CMD window.

```
Administrator: Command Prompt
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>wsl --install -d Ubuntu
Ubuntu is already installed.
Launching Ubuntu...
Installing, this may take a few minutes...
Please create a default UNIX user account. The username does not need to match your Windows username.
For more information visit: https://aka.ms/wslusers
Enter new UNIX username: bhaskar
New password:
Retype new password:
passwd: password updated successfully
Installation successful!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 x86_64)

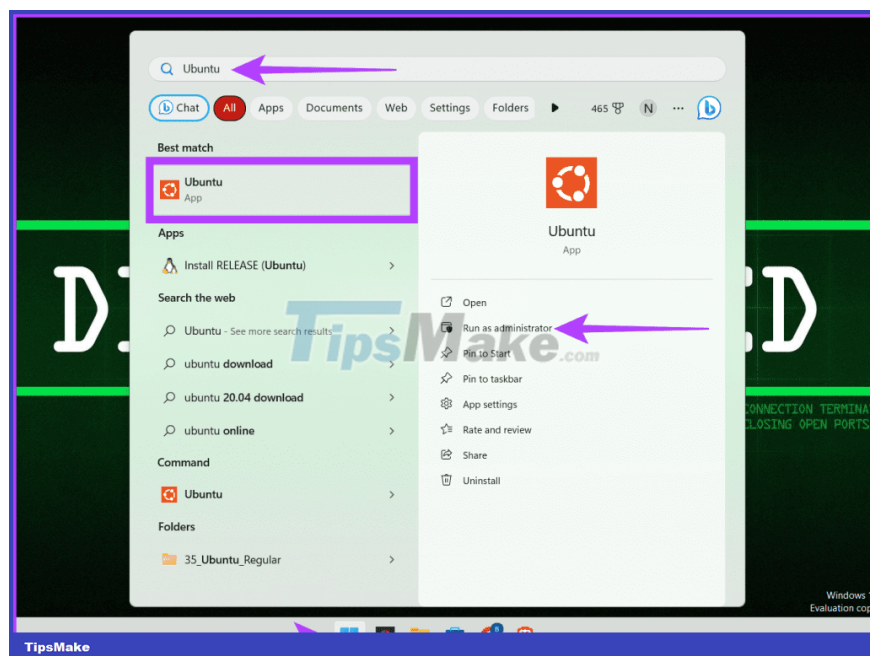
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This message is shown once a day. To disable it please create the
/home/bhaskar/.hushlogin file.
bhaskar@incredible:~$ exit
logout
The operation completed successfully.
```

You have successfully installed WSL and the Linux operating system. To generate SSH key using WSL, follow the steps below.

Generate SSH key using WSL

Step 1: Click on the Windows icon . Search for **Ubuntu** and select **Run as administrator** . When prompted, click **Yes**.

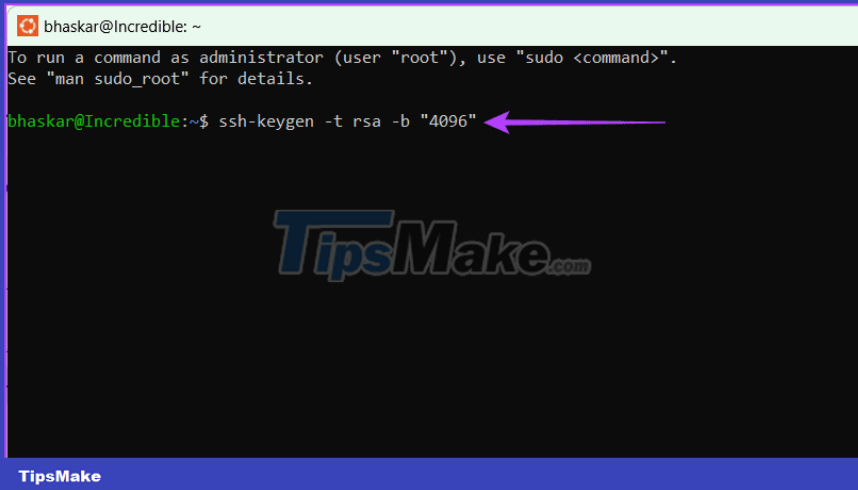


Step 2: Enter the command below to generate SSH key and press **Enter** .

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

```
bhaskar@Incredible: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bhaskar@Incredible:~$ ssh-keygen -t rsa -b "4096" ←
```



TipsMake

Step 3: Provide the desired path and press the **Enter** key . If not, press the **Enter** key to save the file in the default location.

Step 4: Enter the passphrase you want to use and press **Enter** . You need to do this twice to confirm.

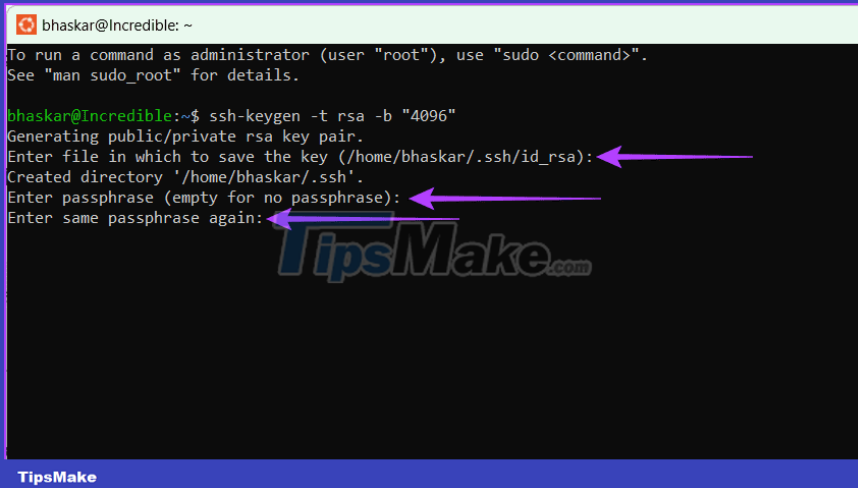
Note : You won't be able to see anything you type as you enter your password, but the tool will save it as you type, so make sure there are no typos.

Alternatively, if you don't want to use any passphrase, you can simply press **Enter** twice.

Warning : You should not use a blank passphrase for security reasons.

```
bhaskar@Incredible: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bhaskar@Incredible:~$ ssh-keygen -t rsa -b "4096"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bhaskar/.ssh/id_rsa): ←
Created directory '/home/bhaskar/.ssh'.
Enter passphrase (empty for no passphrase): ←
Enter same passphrase again: ←
```



TipsMake

Step 5: Finally type **exit** and press **Enter** to close the window.

```

bhaskar@Incredible: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bhaskar@Incredible:~$ ssh-keygen -t rsa -b "4096"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/bhaskar/.ssh/id_rsa):
Created directory '/home/bhaskar/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bhaskar/.ssh/id_rsa
Your public key has been saved in /home/bhaskar/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:9CNLheBw190o3ygs+VL1d2XyVoqmKuj+fCP21+22Ak bhaskar@Incredible
The key's randomart image is:
+--[RSA 4096]--+
  . o . . . o
  + o . o .
  . o . o o
  . o .oo.o o
  S . . . =
  o.o++ . +
  Eo* . o
  + +o0 o .
  . * = o =
+--[SHA256]-----

```

You have successfully created an SSH key. Visit the website where you hosted it to check. There, you will find two keys. You can differentiate them by extension:

1. Public keys have the .pub extension.
2. Private keys do not have extensions.

Code explanation

A typical SSH command that can help you generate an SSH key is as follows:

```
ssh-keygen -t rsa -N "" -b "2048" -C "key comment" -f path/root_name
```

Below is the meaning of each symbol or character in the command.

1. **-t rsa** : Specify the type of key to generate, in this case rsa. RSA (Rivest–Shamir–Adleman) is a secure and widely used algorithm for public key cryptography.
2. **-N ""** : Set the passphrase to an empty string, meaning the key will not be protected. Therefore, anyone with access to the private key file can use it without a password.
3. **-b '2048'** : This defines the key size, set to 2048 bits. You should use a larger key size because it provides better security.

Note : Larger key sizes will take more time to create and use.

1. **-C 'key comment'** : Allows you to add comments to the generated key file. This can be useful in real-life situations because you will be working with multiple SSH keys to access different remote devices.
2. **-f path/root_name** : Specify the path and file name for the generated key pair. The file name will have **root_name** provided with the extension .pub for the public key and .pem for the private key (for example: root_name.pub and root_name.pem).

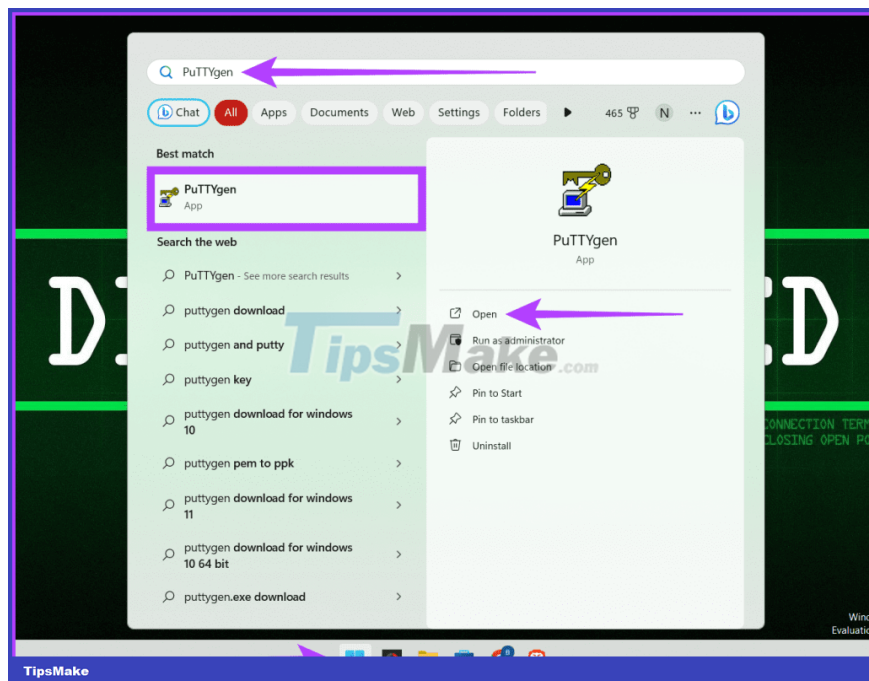
3. Use PuTTY

PuTTY is one of the old-fashioned free and open source terminal emulators, serial console and network file transfer applications. It supports several network protocols, including SSH, Telnet, rlogin, and raw socket

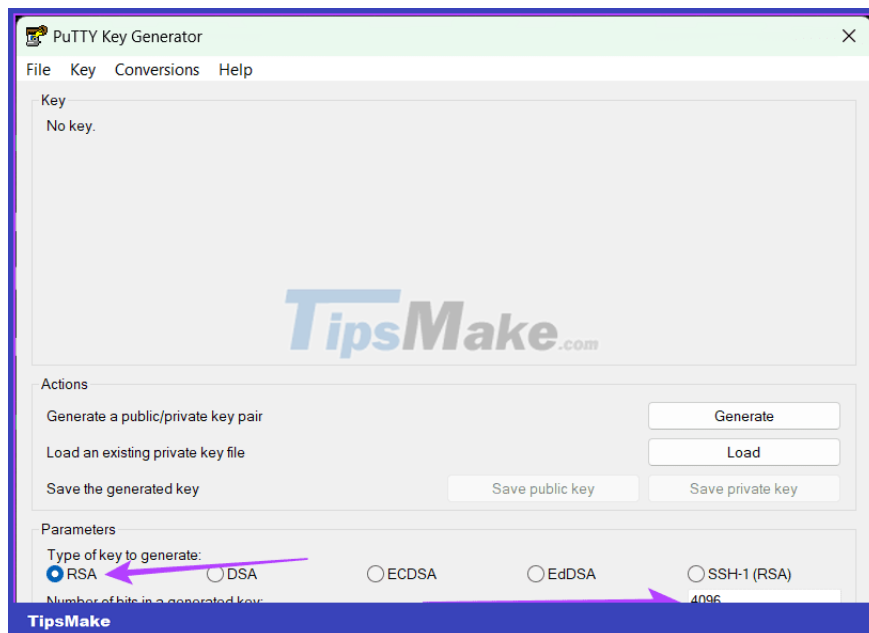
connections. Follow the steps described below to generate SSH keys on Windows using PuTTY.

Step 1: Launch a web browser and visit the official PuTTY website. Download and install PuTTY.

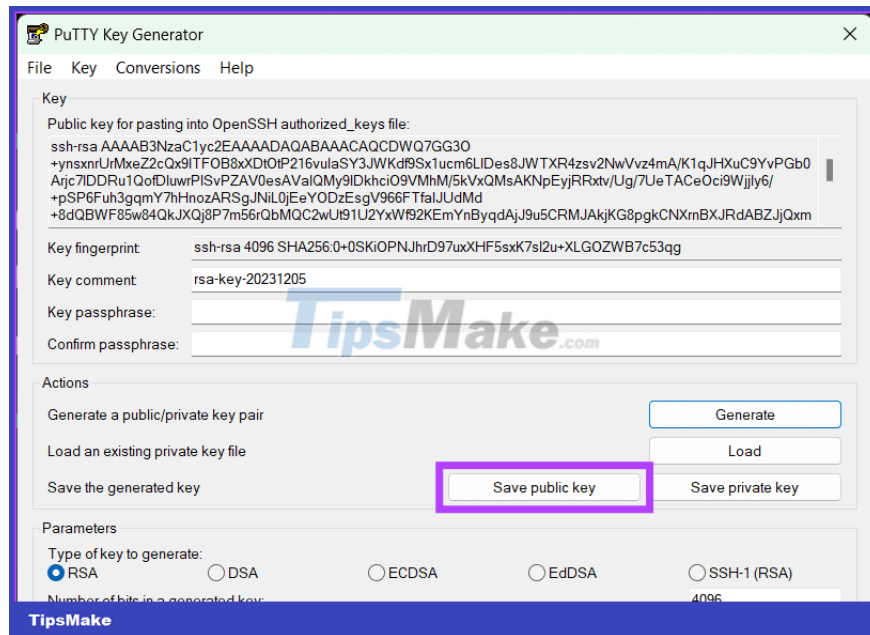
Step 2: Press the keyboard shortcut **Windows + S** to open Windows Search, type **PuTTYgen** and click **Open**.



Step 3: In the **Type of key to generate** section, select a type (for example, RSA). Enter the desired number of bits into the generated key. Click the **Generate** button.

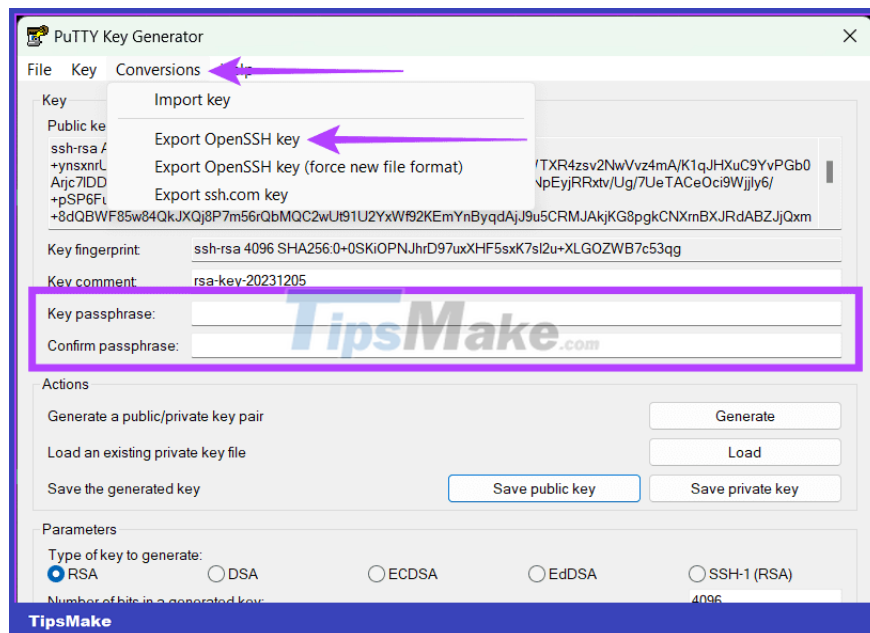


Step 4: Click **Save public key** and choose a location to save the file. Rename the file using the key type and add the '.pub' extension (e.g. id_rsa.pub for RSA).



Step 5: Finally, enter the passphrase and confirm it. Go to the **Conversions** tab at the top and click **Export OpenSSH key** for the private key.

Step 6: Choose a location to save the private key and remember that no extension is used after the file name. Furthermore, you should use a name similar to the public key (e.g. id_rsa).



You finished reading the article "**How to create SSH key on 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.