

GridPane with Windows CMD/PowerShell



([HTTPS://GRIDPANE.COM/BLOG/AUTHOR/GABRIEL-ADMIN/](https://gridpane.com/blog/author/gabriel-admin/)) **Gabriel**

(<https://gridpane.com/blog/author/gabriel-admin/>)

UPDATED ON 29TH JUNE 2020

4 min read

Index

- [Step 1: Check if ssh is installed](#)
- [Step 2: Create Your SSH Key Pair](#)
- [Step 3: Copy Your Public Key To Your Clipboard](#)
- [Step 4: Add Your Public Key To Your GridPane Settings](#)
- [Step 5: Push Your Public Key To Your Server](#)
- [Step 6: Connect To Your Server](#)

To get the most out of the GridPane platform, you'll often find the need to use SSH to log into your server and use our GPCLI (GridPane Command Line Interface) commands. GPCLI a powerful set of tools that allow you to customize not only your server but your WordPress installations as well.

For security reasons, SSH access is only available with the use of an SSH key and is restricted to the root user.

WARNING: The Peter Parker Principle applies here!

With great power comes great responsibility.

Not familiar with Spider-Man? In simple terms – the root user can do anything including deleting and breaking everything. Just a few bad keystrokes and everything can go away. Be careful with the commands you use and never share your Private



SSH Key with anyone!

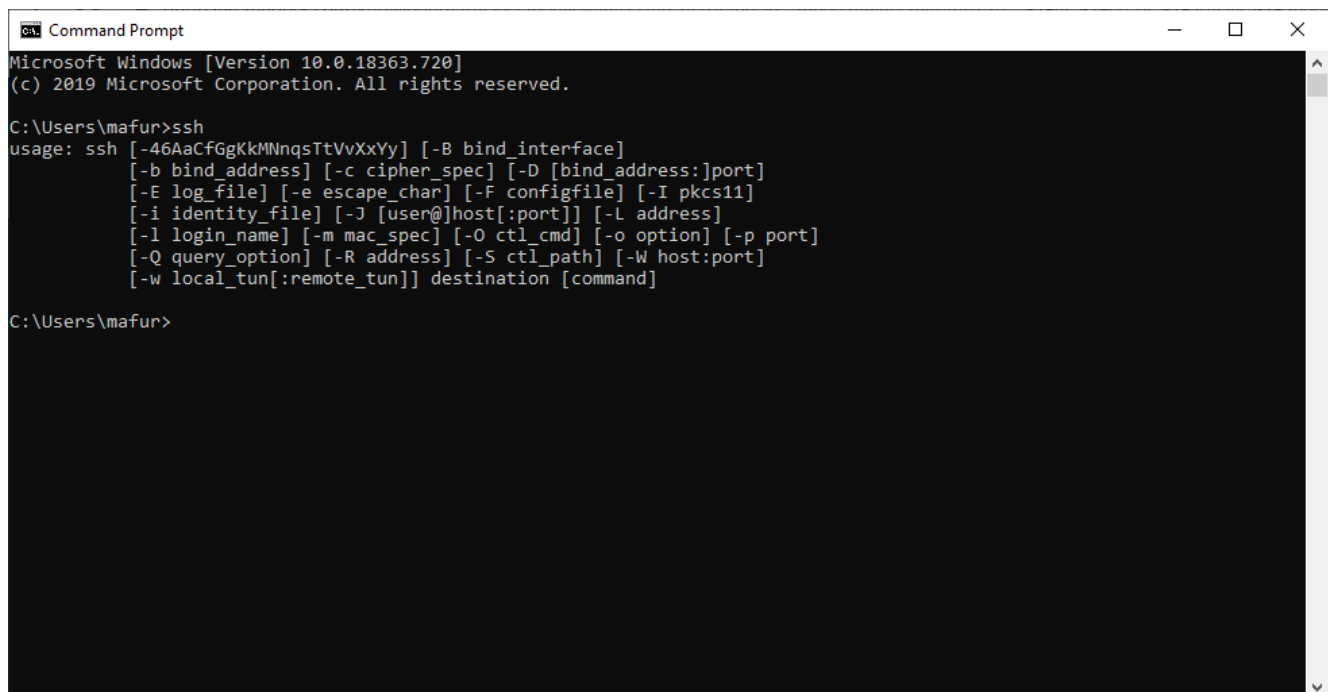
Step 1: Check if ssh client is installed

Make sure you have the latest updates of Windows if that is not possible, then at least you should have the Windows 10 Fall 2018 build update. From this update, Windows 10 now comes with a built-in ssh client!

To check if the client is working, fire up a Powershell or CMD window and type in this

```
ssh
```

If the client is installed, you should get the following reply:



```
Microsoft Windows [Version 10.0.18363.720]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\mafur>ssh
usage: ssh [-46AaCfGgKkMnQsTtVvXxYy] [-B bind_interface]
          [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
          [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
          [-i identity_file] [-J [user@]host[:port]] [-L address]
          [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
          [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
          [-w local_tun[:remote_tun]] destination [command]
```

If you do not get the above result please check if you have the above-mentioned update

- back to top ▲

Step 2: Create Your SSH Key Pair

Type the following command at the prompt then press enter.

```
ssh-keygen -b 4096
```

When prompted for the file in which to save the key, press enter. The default location will be created.

Keep default values and no need for a pass phrase.

Congratulations! You now have an SSH key. The whole process will look like this:

```
C:\Users\mafur>ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\mafur\.ssh/id_rsa):
C:\Users\mafur\.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\mafur\.ssh/id_rsa.
Your public key has been saved in C:\Users\mafur\.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:89FUK1MNRNyYvHNI+0oae0hDULkV+8ka5I05Ds9s1b8 mafur@DESKTOP-51QFD2R
The key's randomart image is:
+---[RSA 4096]-----+
|      . . . .o+o |
|      . . . +... |
|      . =*= . |
|      o=*O.o |
|      S.o B.B |
|      ooB==.. |
|      .o+O= . |
|      .*o . |
|      o..o.E |
+---[SHA256]-----+
C:\Users\mafur>
```

What does all this mean?

The key generating process has created two files.



id_rsa (this is your private key, do not lose or give this to anybody!)

id_rsa.pub (this is your public key, you copy this to servers or give to others to place onto servers for you to authenticate against using your private key)

These keys are store by default in

```
C:\Users<WINUSER>/.ssh/
```

The path might be different but you will always see it when generating the SSH Key

[back to top ▲](#)

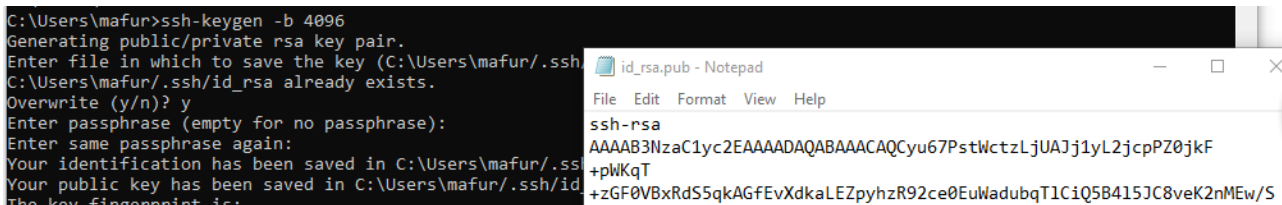
Step 3: Copy Your Public Key To Your Clipboard

We will use our good old notepad to get the contents of our public SSH key

You will need to run the following command. Remember to replace WINUSER with your own user

```
notepad C:\Users<WINUSER>/.ssh/id_rsa.pub
```

The output will look similar to this



The screenshot shows a Windows command prompt window with the following text:

```
C:\Users\mafur>ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (C:\Users\mafur/.ssh/id_rsa):
C:\Users\mafur/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in C:\Users\mafur/.ssh/id_rsa.
Your public key has been saved in C:\Users\mafur/.ssh/id_rsa.pub.
The key fingerprint is:
```

Next to it is a Notepad window titled "id_rsa.pub - Notepad" showing the contents of the public key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACyu67PstWctzLjUAJj1yL2jcpPZ0jkF
+pWkQT
+zGF0VBxRdS5qkAGfEvXdkaLEZpyhzR92ce0EuWadubqT1CiQ5B415JC8veK2nMEw/S
```

```

The key fingerprint is:
SHA256:89FUK1MNRyYvHNI+0oae0hDULkV+8ka5I05Ds9s1b8 mafur@DESKTOP-51QFD2R
The key's randomart image is:
+---[RSA 4096]-----+
|  . . . O + O |
|  . . . + . . . |
|  . = * = . |
|  o = * O . o |
|  S . o B . B |
|  ooB = = . |
|  . o + O = . |
|  . * O . |
|  o . . O . E |
+---[SHA256]-----+

C:\Users\mafur>notepad C:\Users\mafur\.ssh/id_rsa.pub

1NcmADIBSp/mJi8F0bBo6XoMJAWFs/xgzsikXcmc4eukueo0Au3Ky0jrsZvqsu/unNj
fzwrSDhSMM510+mWnCKXwFfXjYsXq1Q+BFX/DdNCji
+b14xPG4FWBJEMwetcgH/h3Bf7G0taTm2u9iJqWT/NLGrSPQf9jc6PtpvkAZ6wcEzUW
EwszR4t38eiFuNLn71eFceL41jhJLZCc7MDU/EnwjMKK0/D20qV5wwWB4k5r2npowQf
uIt1Ru4IAkPtT3TrsmE05ida80AtmW5H5KWiqyb9VmfkffWgNioPbdhoFf9v8rxedYK
rFX5jgo/QLwP4b7cDH3a
+LbWiNVNU3LzVzpfLEHDfwZxG3C2SmBArzbRydNo5yYmr-iIVA0KvdXN0kqW891duaI
NT5gV/YaAKozWop6EbzlhnKn9ckIJoau8GmS2XPtq9d476BWyYR95Sdgu7ZmlaMjNkI
qZDewUImF1t3j77evQpVQn8GMYkmpakzs
+iITKEVp0/LJ19y9+jCjFCN7ZikG1ycXnt18ewSmkPx0ZbR1YdNx4Zw5qK4mrWGtCCi
ep0SkgM17hDoxwQ== mafur@DESKTOP-51QFD2R

```

Now type CTRL+A then CTRL+C to copy the contents from notepad

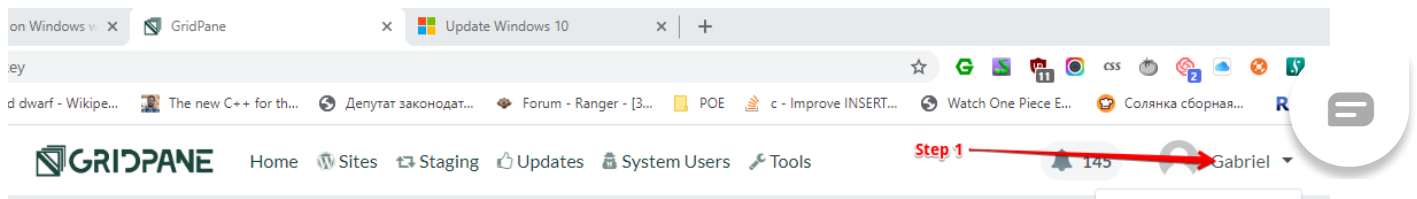
[back to top ▲](#)

Step 4: Add Your Public Key To Your GridPane Settings

Highlight the output of the previous command and press enter. This copies the data to your clipboard. You may find it useful to paste this into a Notepad document while you log into your GridPane account.

Once logged in, click on your name to display the dropdown menu.

- Select “Your Settings”
- Click on “SSH Keys” in the left menu
- Give your key a name
- Paste the public key into the large text field
- Click the green “Add Key” button



The screenshot shows the 'Add SSH Public Key' form in the GridPane settings. The left sidebar contains a 'SETTINGS' menu with 'SSH Keys' highlighted. The main form has two input fields: 'Name' and 'Public Key'. A red arrow labeled 'Step 3' points to the 'SSH Keys' menu item. Another red arrow labeled 'Name of Key' points to the 'Name' input field. A third red arrow labeled 'Step 2' points to the 'Public Key' input field. A fourth red arrow labeled 'Copy here the Key' points to the 'Public Key' input field. Below the input fields is a green 'Add Key' button. The right sidebar contains a 'Developer' menu with 'Your Settings' highlighted. Below the form is a section titled 'Active SSH Keys' with a table listing the keys. The table has columns 'Name' and 'Default'. The first row shows 'Gridpane-Gabriel-Win' with a toggle switch set to 'OFF'.

If you do this all correctly, your new key will appear below in the Active SSH Keys list.

The screenshot shows the 'Active SSH Keys' list. A red box highlights a new key entry. The entry has a name 'Test-Key-KB' and a toggle switch set to 'OFF'. The name 'test6' is visible above the key entry.

[back to top ▲](#)

Step 5: Push Your Public Key To Your Server

Now push the key to the public server as described in this article

[Add/Remove an SSH Key to/from an Active GridPane Server](#)

[\(https://gridpane.zendesk.com/hc/en-us/articles/\)](https://gridpane.zendesk.com/hc/en-us/articles/)

[back to top ▲](#)

Step 6: Connect To Your Server

To connect to the server, type the following in the terminal:

```
ssh root@ipaddress (mailto:root@ipaddress)
```

For my example, this is

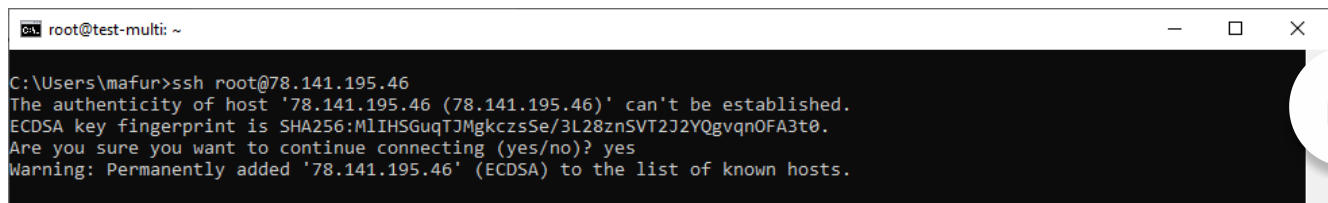
```
ssh root@78.141.195.46 (mailto:root@159.203.187.18)
```

Wait, root? But I did not name my key root! That doesn't matter. Every key, regardless of name, that is added to your GridPane Active SSH Keys is a root key.

If this is your first time connecting to this server, you will be asked if you want to continue connecting and add this IP address to your list of known hosts. Type yes.

If the private key on your machine matches the public key on the server, you will be authenticated and connect to the server.

The whole process looks like this:

A screenshot of a Windows terminal window titled 'root@test-multi: ~'. The terminal shows the command 'C:\Users\mafur>ssh root@78.141.195.46' being entered. The output shows the SSH connection process, including the authenticity of the host, the ECDSA key fingerprint, and a warning about adding the host to the list of known hosts. The terminal text is as follows:

```
root@test-multi: ~
C:\Users\mafur>ssh root@78.141.195.46
The authenticity of host '78.141.195.46 (78.141.195.46)' can't be established.
ECDSA key fingerprint is SHA256:MLIHSGuqTJMgkczsSe/3L28znSVT2J2YQgvqn0FA3t0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '78.141.195.46' (ECDSA) to the list of known hosts.
```


Quick Links

Documentation(<https://gridpane.com/kb/>)

Status(<https://status.gridpane.com/>)

Roadmap(<https://roadmap.gridpane.com/>)

Comparisons(<https://gridpane.com/comparisons/>)

Updates(<https://gridpane.com/updates/>)

Facebook Group(<https://www.facebook.com/groups/selfmanagedwordpress/>)

Connect With Us

(<https://gridpane.com>)
 (19) 4 SERVER
 ps:// (http ps://
 /w psi/ /w
 info@gridpane.com
 ww. /tw ww.
 fac itter you
 febo. co. ub
 ok.c m/g e.c
 om/ ridp om/
 grid ane grid
 e,) e)

GridPane is the world's first hosting control panel purpose-built for Serious WordPress Practitioners

© Copyright 2017-2020 – GridPane – Run WordPress the Right Way

Terms of Service (<https://gridpane.com/terms/>) – Privacy Policy (<https://gridpane.com/privacy/>) – GDPR

(<https://gridpane.com/gdpr-dpa/>)

Built with ❤ by S Bell (<https://sbell.co>)

