

Set up VS Code Remote Development

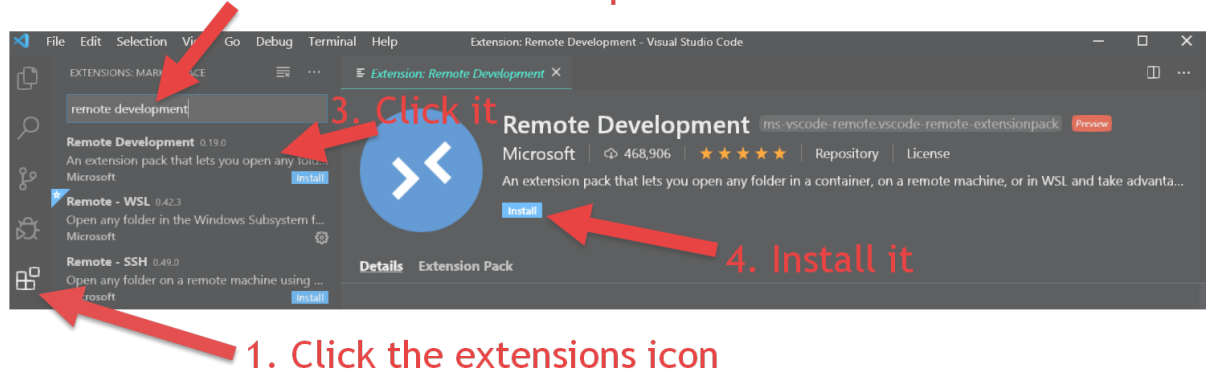
Microsoft released an extension for VS Code called remote development that let you connect to a VM remotely and access/edit files directly from VS code. <https://code.visualstudio.com/docs/remote/remote-overview>

Fortunately both MacOS and Windows users can follow mostly the same steps for setting this up.

Installing the Extension

Open VS Code in a new window and search for `remote development` in the extensions menu.

2. search for the "remote development" extension



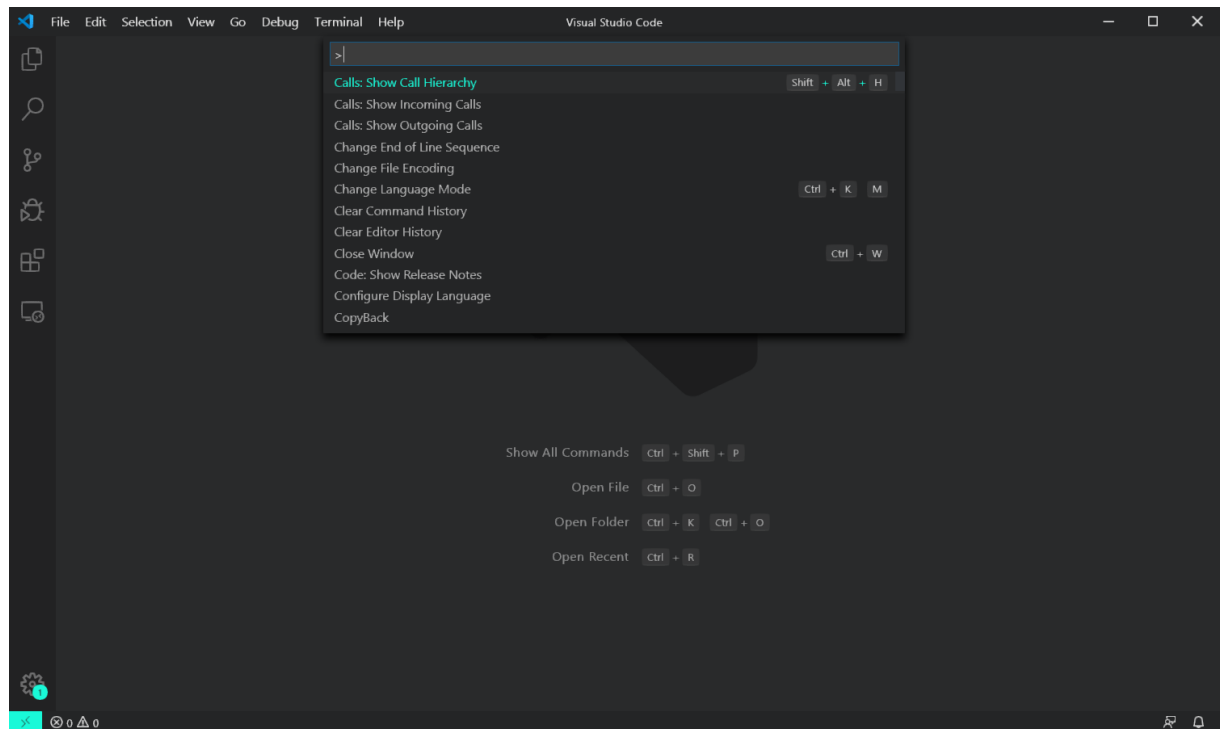
Adding a new host

Once it's installed close the extension menu (just click the icon again) and close the *Extension: Remote Development* tab. Then press the following keys simultaneously:

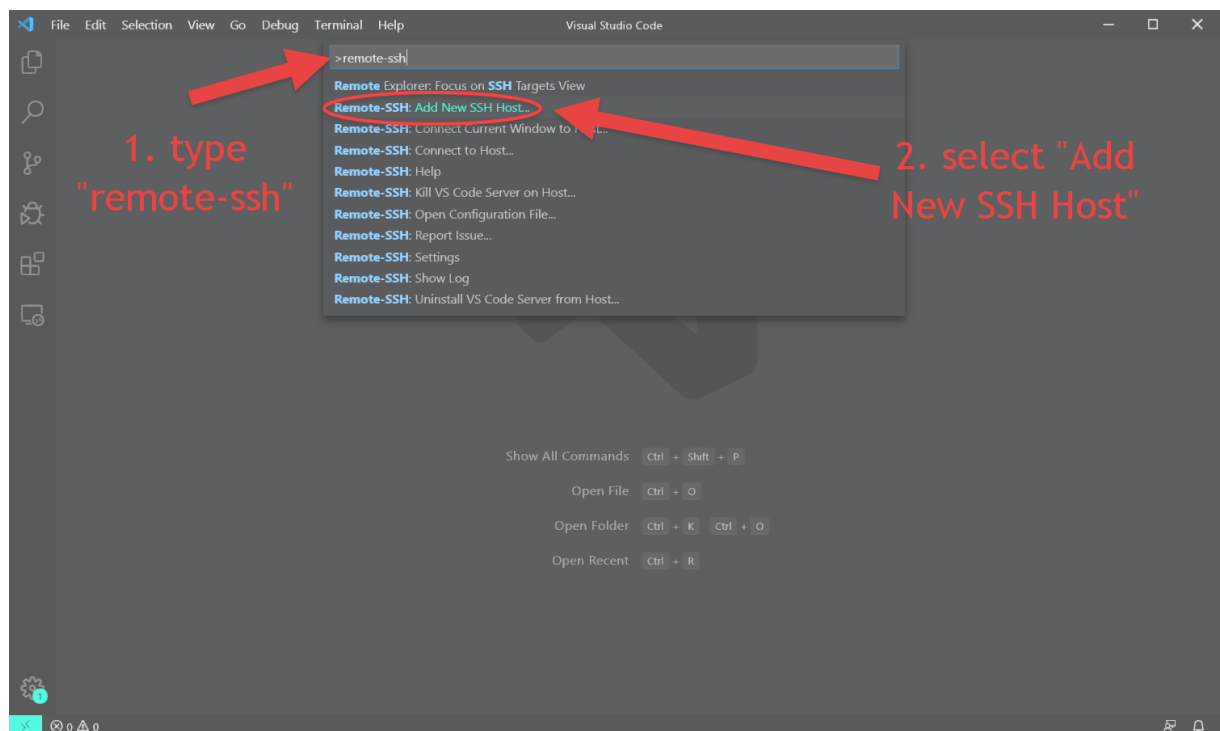
`ctrl+shift+p` (Windows)

`cmd+shift+p` (MacOS)

This will open the **command palette**. You should see this menu popup:



Type this: `remote-ssh` into the menu and choose `Remote-SSH: Add New SSH Host`



SSH command

You'll be presented with a prompt to enter your SSH command. Windows users may not be familiar with this command so ensure you type it in correctly.

Windows Users

Windows user should remember that file paths use backslashes unlike mac and linux (which use forward slashes)

```
"C:\Users\your-computer-username\path\to\key"
```

SSH command breakdown

```
ssh -i /path/to/private/key username@public_ip
```

ssh this is the command for the **ssh** program

-i this flag means you're passing an **identity file** (a private key)

/path/to/private/key this is the path to your private key

username the username you used for Azure

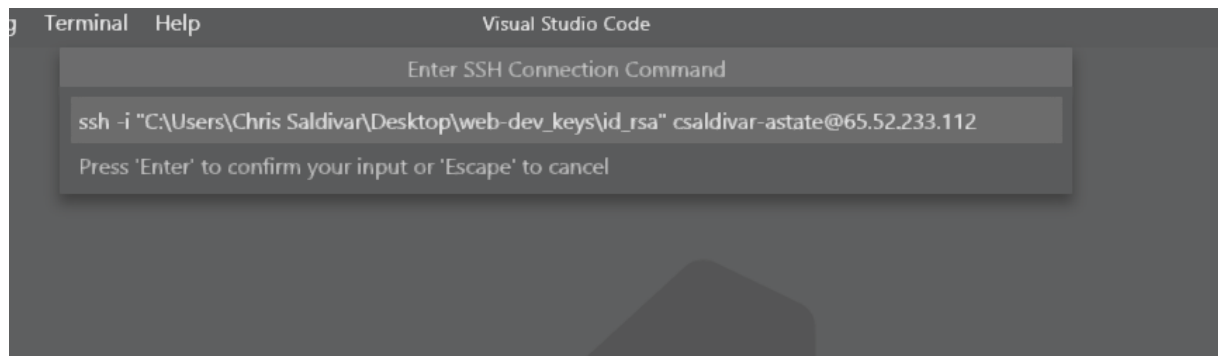
public_ip your VM's public IP

If there are any spaces in your path you have to wrap your path in quotes!

My command

This is the ssh command I had to use on my Windows machine. If there are any spaces in your path you **must** put quotes around your path.

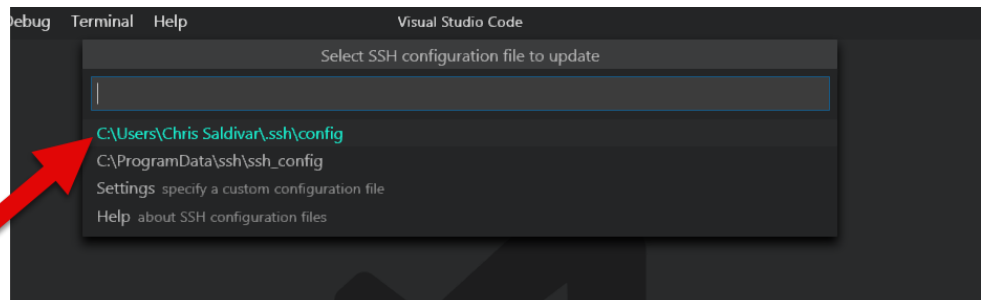
```
ssh -i "C:\Users\Chris Saldivar\Desktop\web-dev_keys\id_rsa" csaldivar-astate@65.52.233.112
```



Once you've entered your command, double check it and then press Enter.

SSH config file

Then you'll be presented with a dialog box to update your **SSH configuration file**. This is a file that contains all of the SSH configs you've set up (you likely don't have any but this will still create the config file for you).



Choose the
first one

You should select the first option that places the file in your home directory.

Connecting to the Host

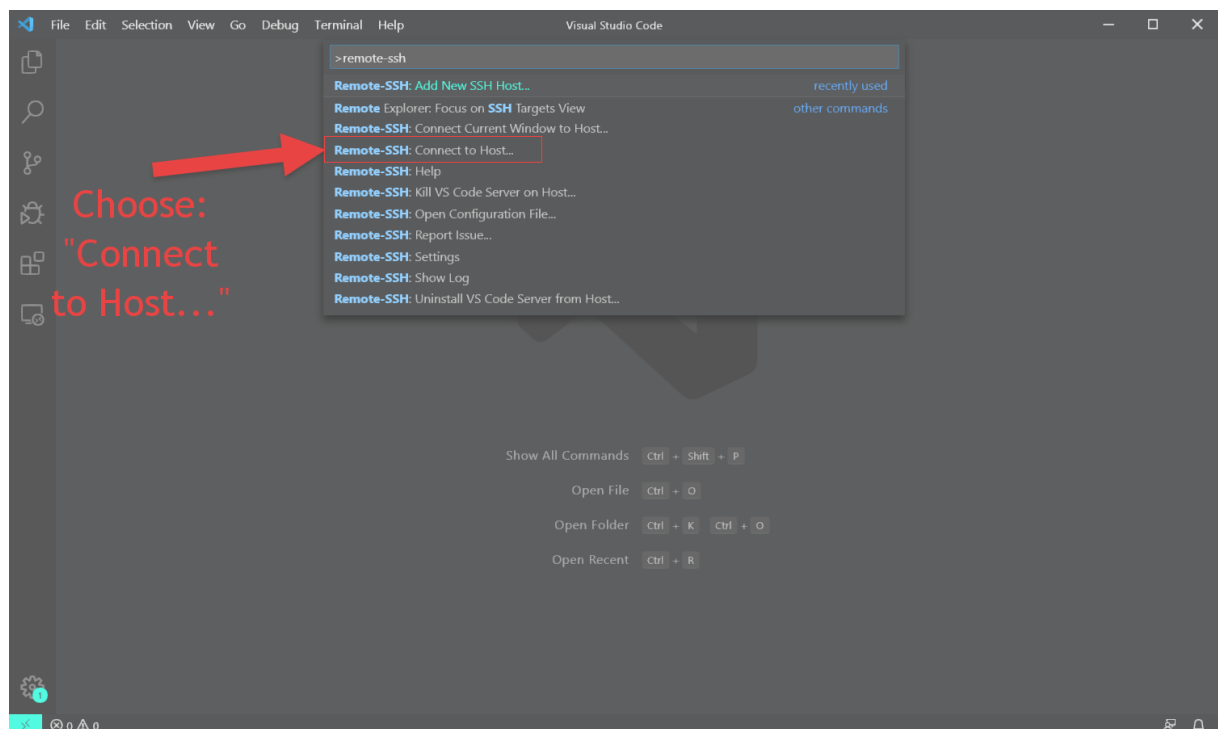
You'll see a popup in the lower left corner that has a button marked "Connect" but as far as I can tell this doesn't do anything. So just hit the little "X" in the notification box.

Enter the keyboard shortcut to open the **command palette** again.

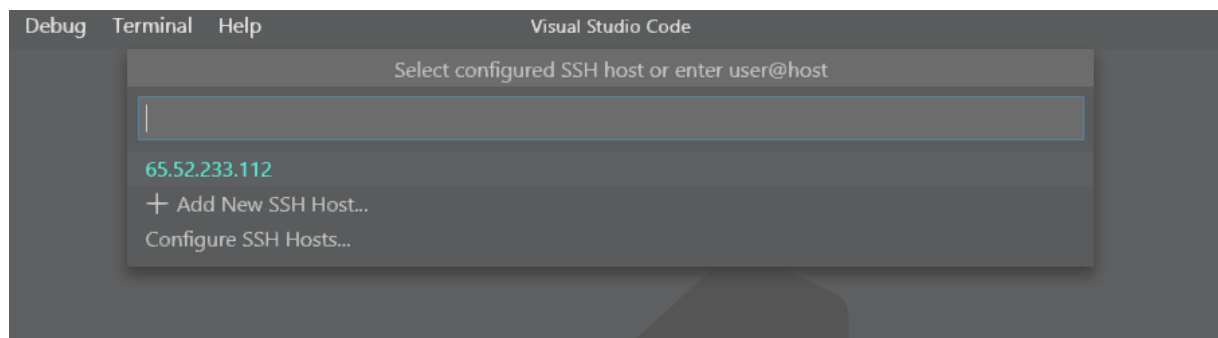
ctrl+shift+p (Windows)

cmd+shift+p (MacOS)

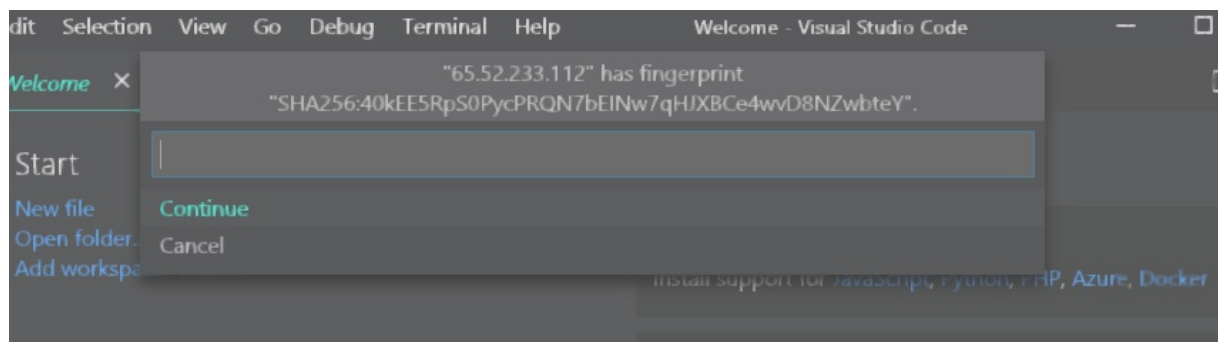
And type in: `remote-ssh` then choose "**Connect to Host**"



This will open a new dialog box that has the host you've just added. It will be your VM's public IP. Click it.

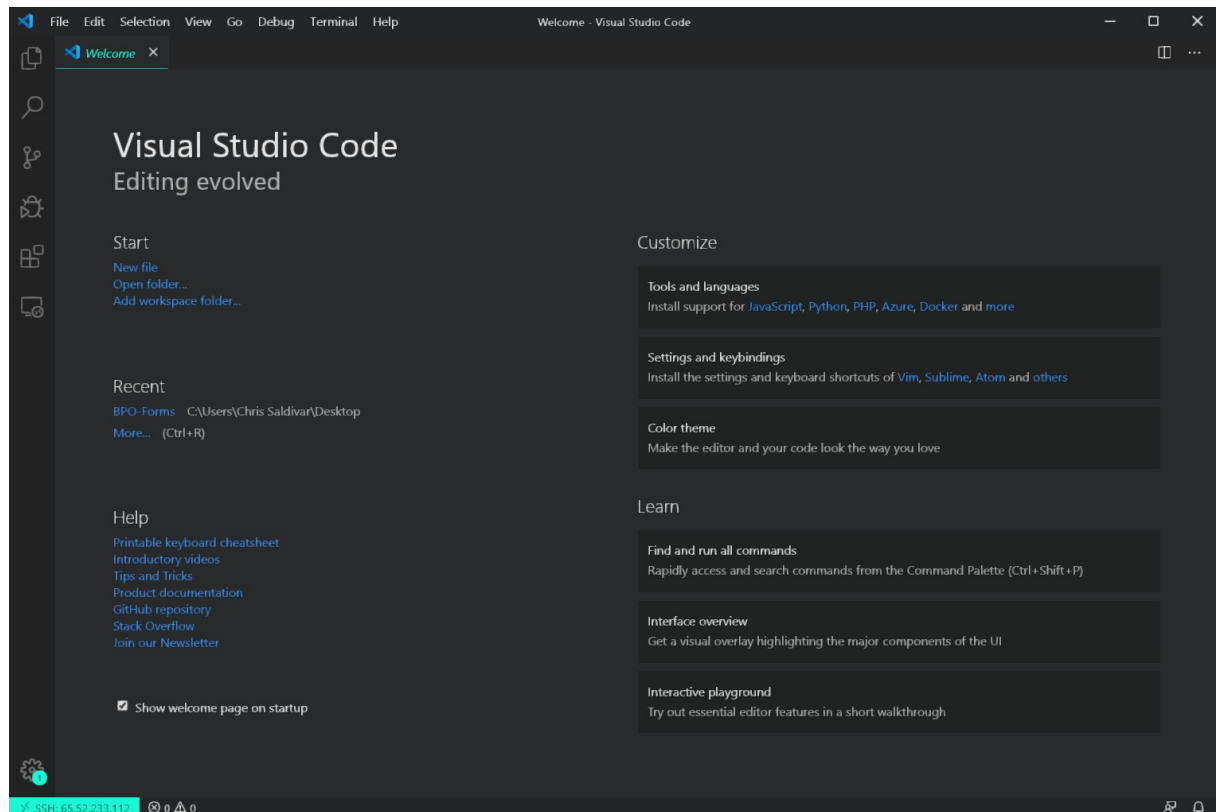


If this is the first time you've connected to the VM on this machine you will get a prompt like this:

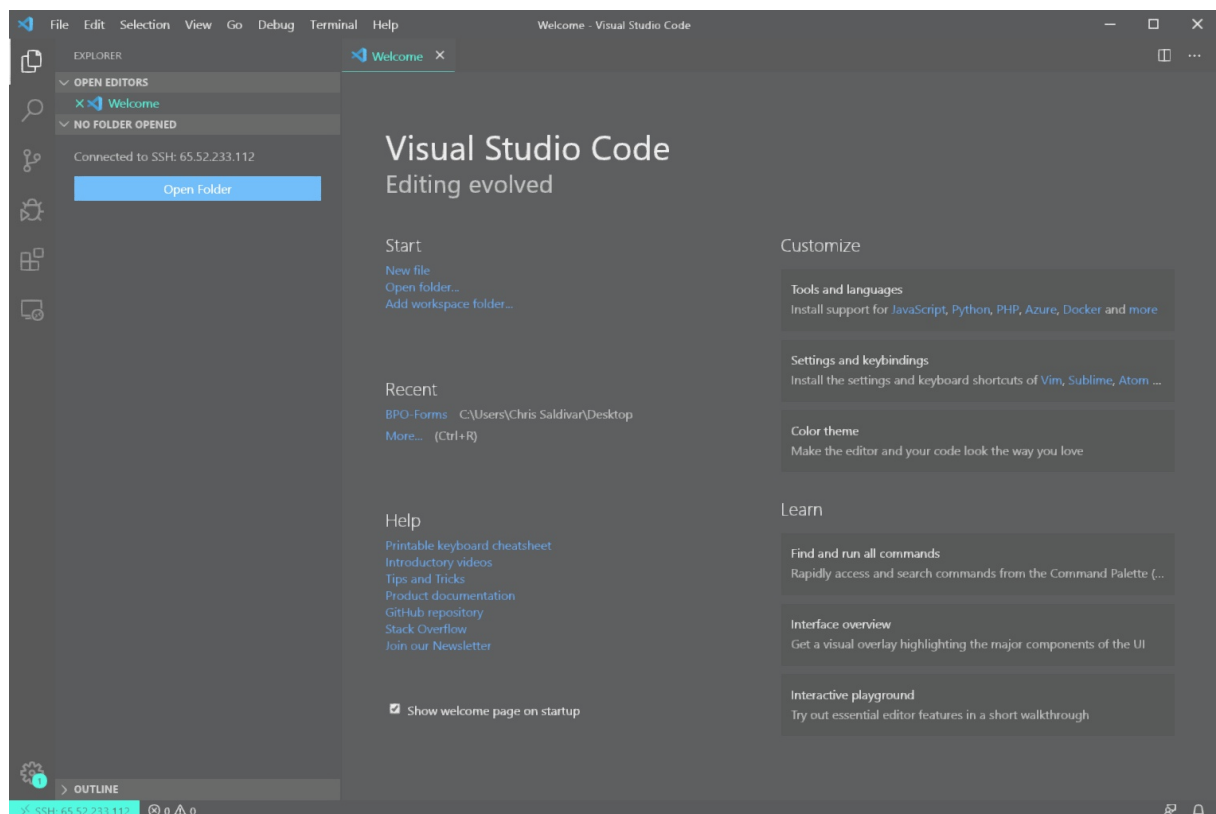


This is asking if you trust the IP's fingerprint. Verify the IP is correct and then click continue. Checking the IP alone is actually sufficient to trust it; if this concerns you then skip to instructions at the very end to learn how to check the fingerprint.

Give it a second to connect to your VM. Once it's done it should say "SSH: <you VM's public IP>" in the lower left corner. Like the image below.

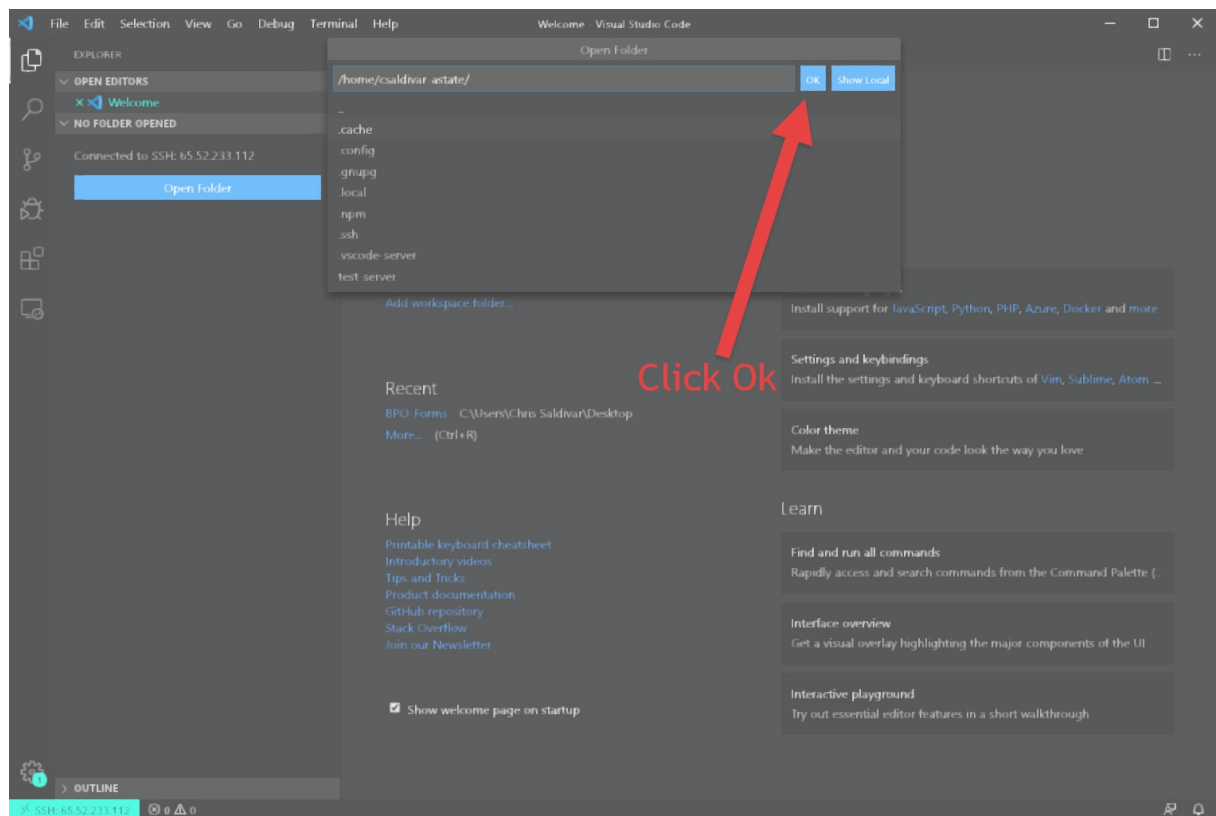


Once it's connected you can open your folder remotely. Click the “explorer” icon (icon at the top left; above the magnifying glass) to open the **Explorer** tab. You should see something similar to the image below:



Click the **Open Folder** button and you'll get a dialog box asking which folder you want to open. Just click

OK and you'll open your home directory in your VM.



Give it a second to load everything and you should see your files and folders from your VM on the left panel. Now you can edit and save them directly without having to mess with MobaXterm or SFTP and if you open the terminal from within VS Code it will automatically open an SSH session with the VM.

You can open the terminal with this command:

```
ctrl+`
```

That's a **back-tick** it's the key in the upper left corner of your keyboard: it also has the tilde (~) on it. This command works on both Windows and MacOS.

Checking the SSH fingerprint

The fingerprint that you're shown when you connect via SSH is a SHA256 hash of your VM's public key. This is essentially asking if you recognize the hash. If you don't then someone has gained control of your VM and changed the public/private key pair. (This is extremely unlikely however since we don't have much of an attack surface on our VMs right now) However, if it really concerns you then you can get your server's fingerprint like this:

Unfortunately the only way to get the fingerprint is to connect to the server via SSH and the only way to connect to the server via SSH is to trust the fingerprint it gives you. This is OK since when you initially set up the server it should be clean (since you've just created it). So you would trust it by default (at least at

first). So when you connect for the first time you can run the following command from the terminal:

```
ssh-keygen -lf /etc/ssh/ssh_host_rsa_key.pub
```

This will output the SHA256 hash of your public key (with some other info). You could make a note of it and then reference the note whenever you need to verify it. However, you don't need to bother with this.

When you connect for the first time you and you accept the fingerprint is correct it will be automatically added to your **known hosts** file. Whenever you SSH into the server this file will be automatically checked and if the fingerprint is in your **known hosts** the process will continue without asking you to verify.

If someone gets control of your VM and swaps out the public/private key pair then when you connect the fingerprint will be different. This new fingerprint won't be in your **known hosts** and you'll be asked to verify it. This should be a signal that something's up.