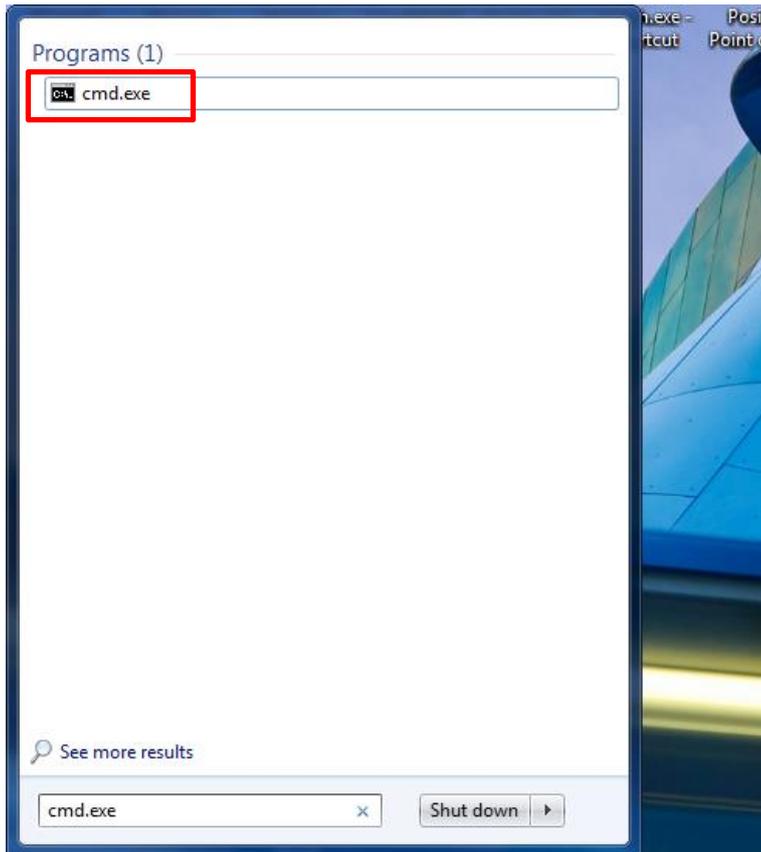
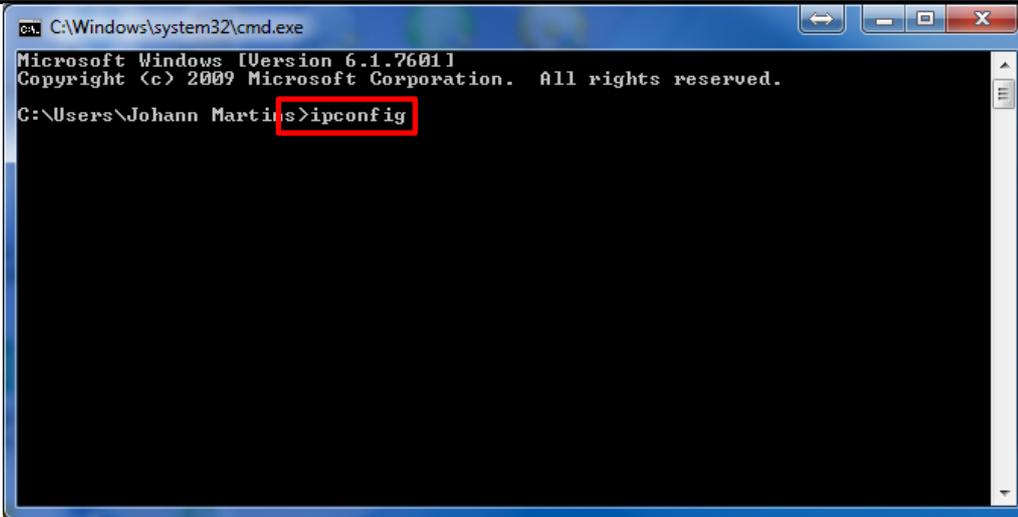


Connecting a 2nd POS device to your POSITIVE Point of Sale PC

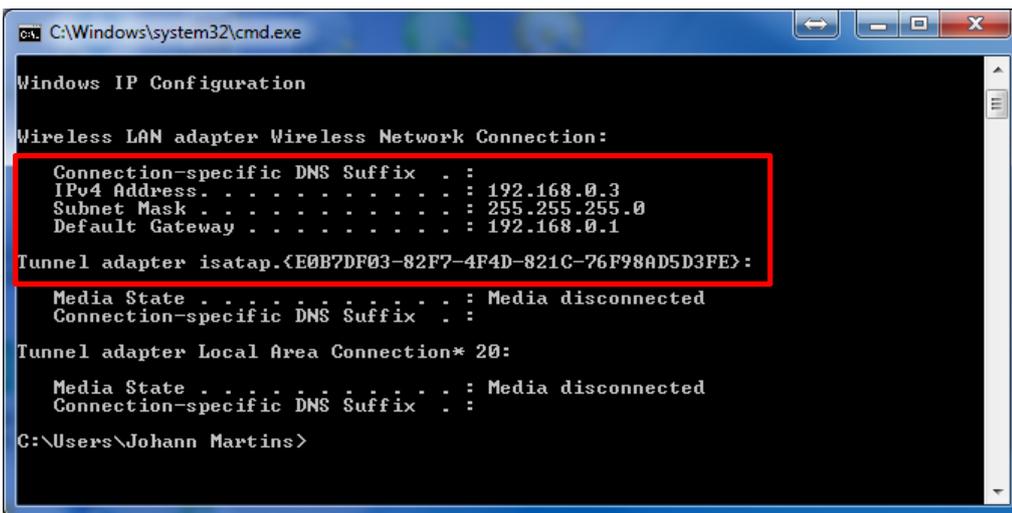
1. On your 2nd POS PC go to your Start menu.
2. Search for cmd.exe file.
3. Then open.



4. Then type 'ipconfig', see below.

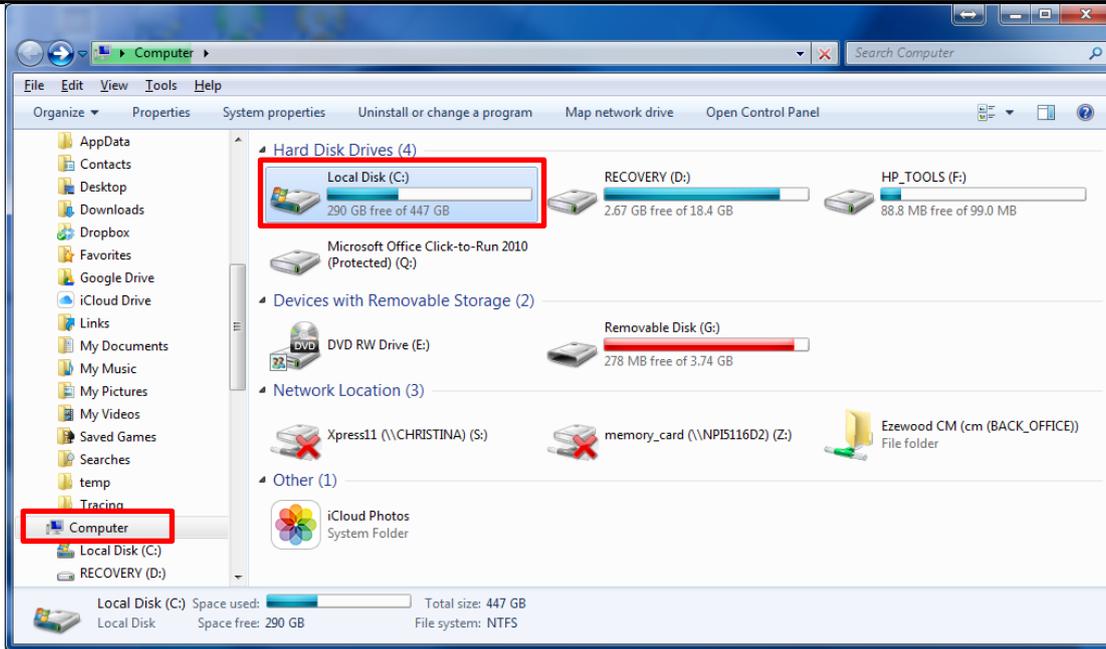


5. Search for the IP configuration where your main POS is connected to and write down the IP address.

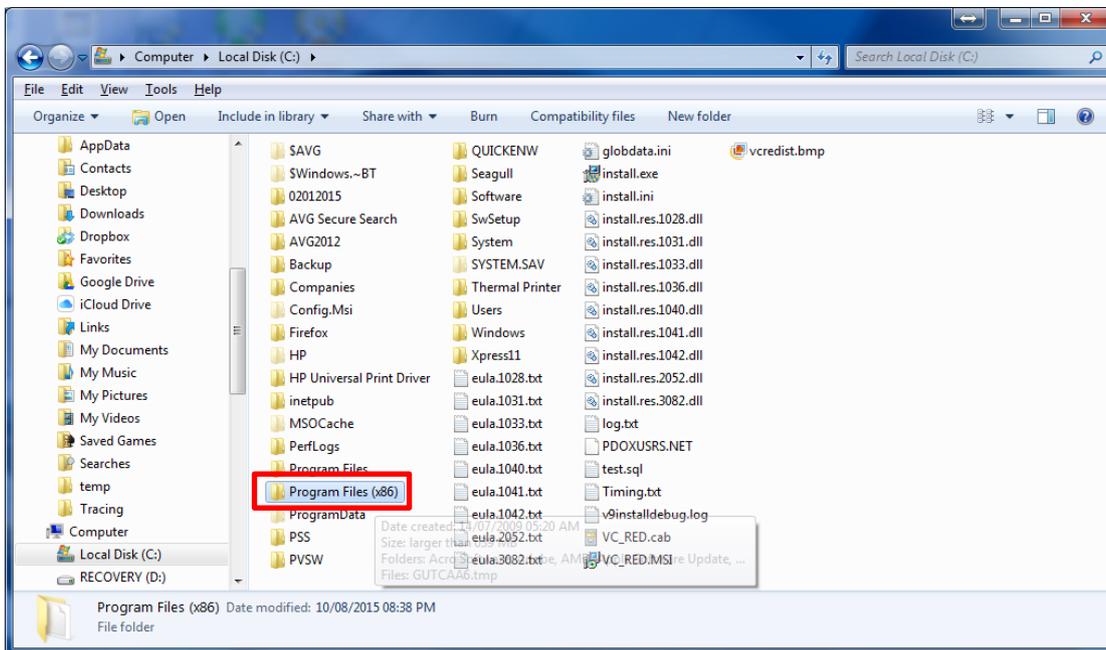


Do the same from your main POS PC and ping your 2nd POS PC from here. Nothing will work if you cannot ping the main POS PC from the 2nd POS PC. If it does not ping, please resolve.

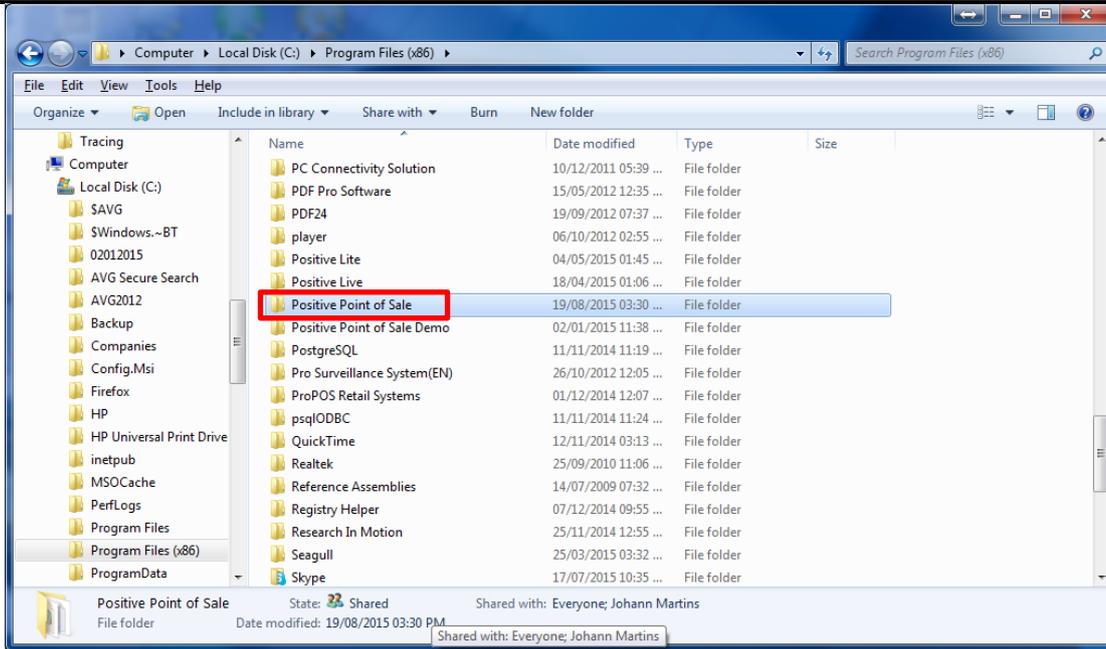
6. On the main POS PC go to My Computer.
7. Then go to C-Drive.



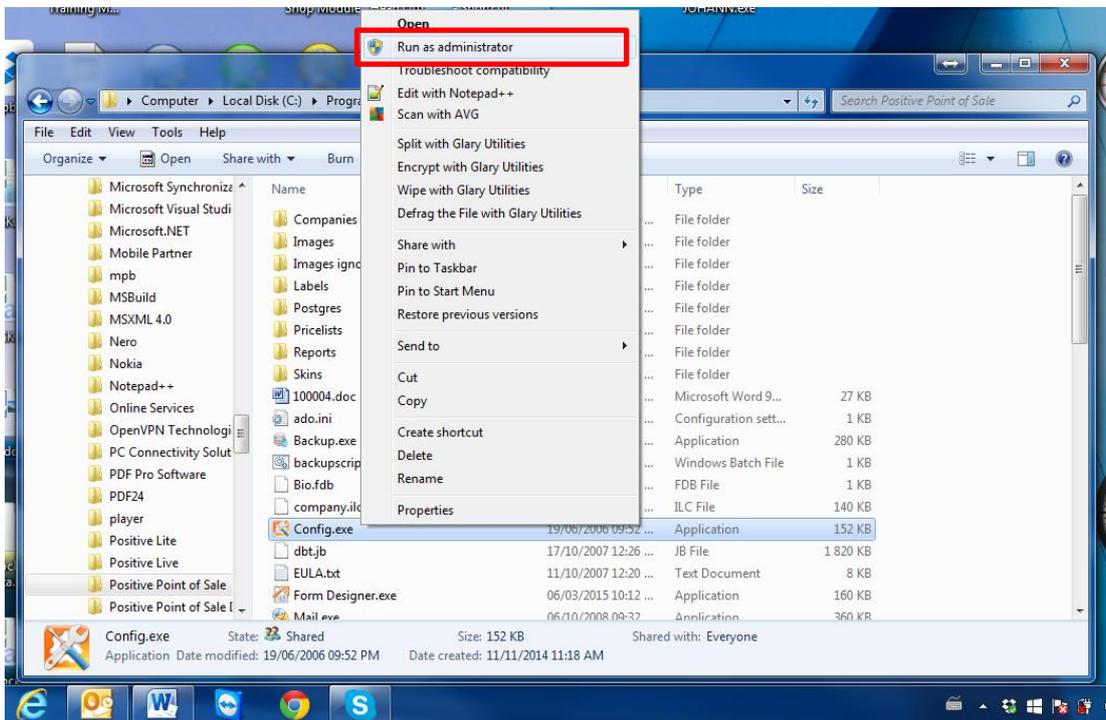
8. Go to Program Files (x86).



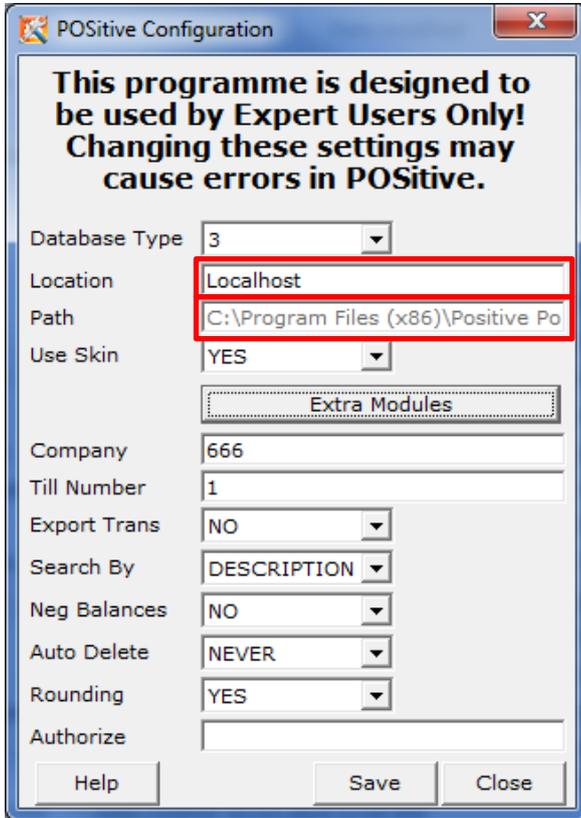
9. Go to Positive Point of Sale.



10. Go to Config.exe and right click, then click on – run as administrator.



11. Database Type should always be 3.



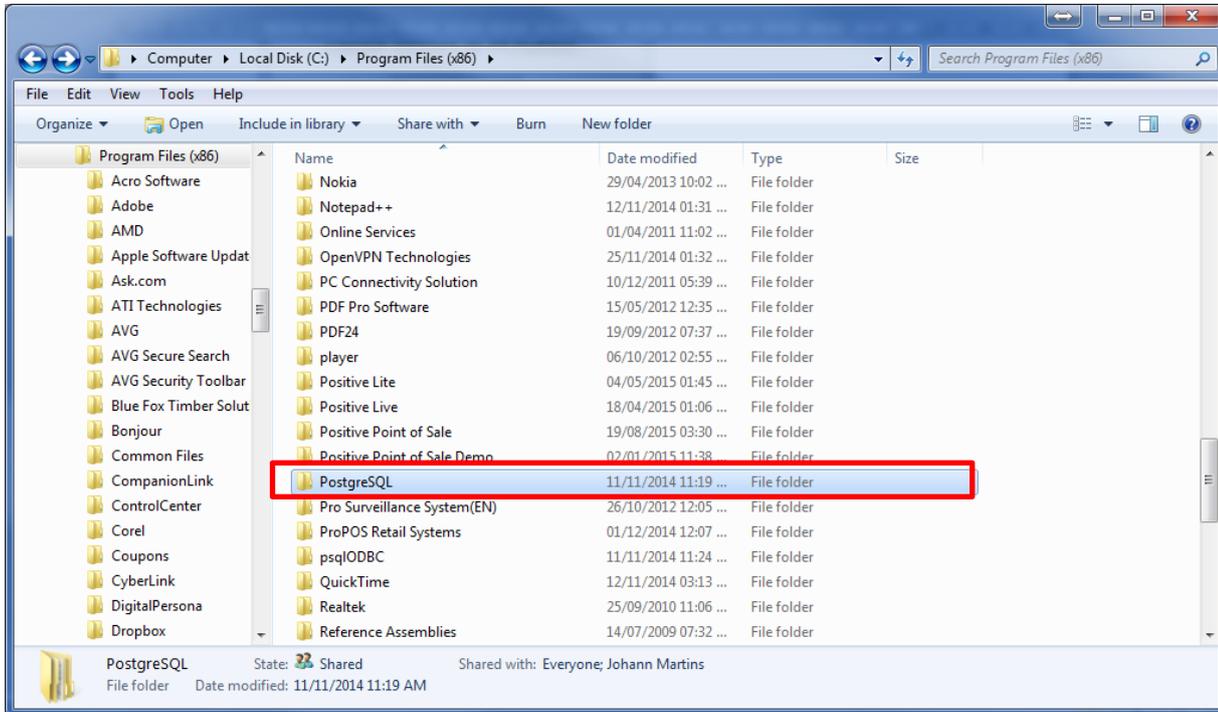
Location: Main POS PC: localhost
2nd POS PC: IP address of the main POS PC e.g. 10.0.0.3

Path: Main POS PC:
2nd POS PC: [\\main](#) POS PC ip address\Positive Point of Sale

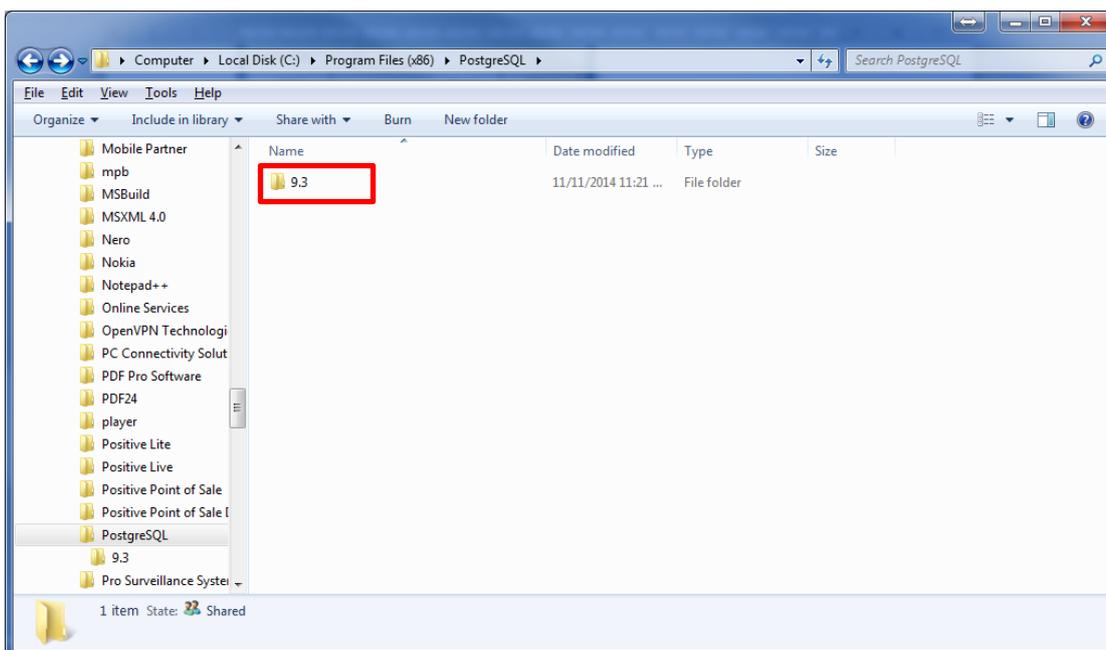
Company: Company number when you created your database e.g. 100

Till number: Till number for this PC, must be different for each PC e.g. 2

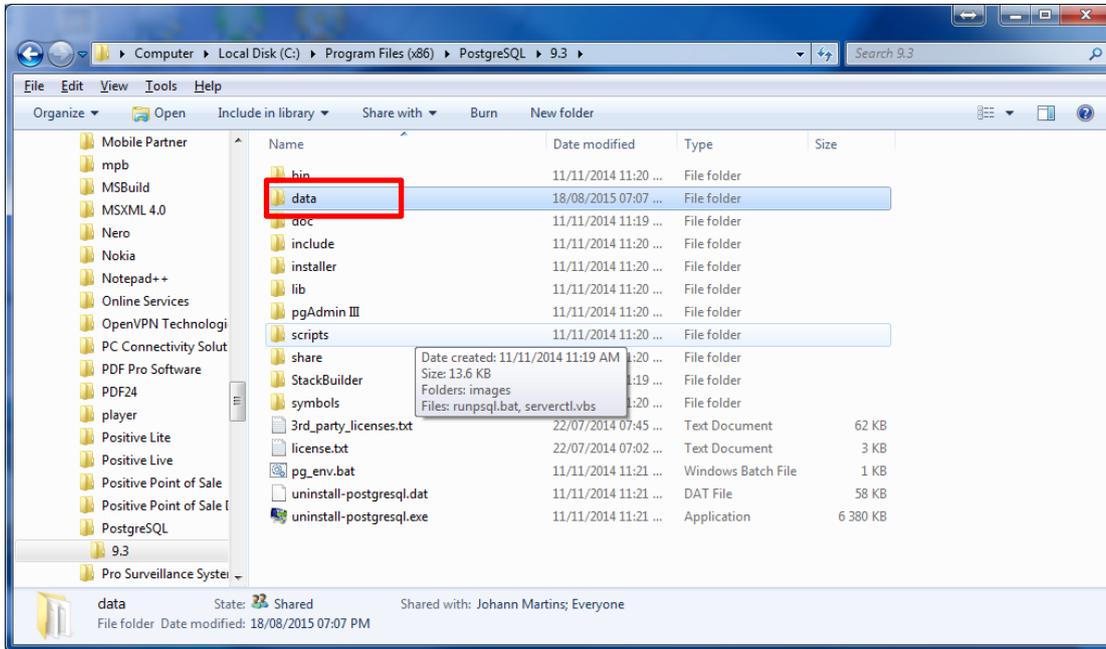
12. On the main POS PC go to My Computer, C-Drive and then PostgreSQL.



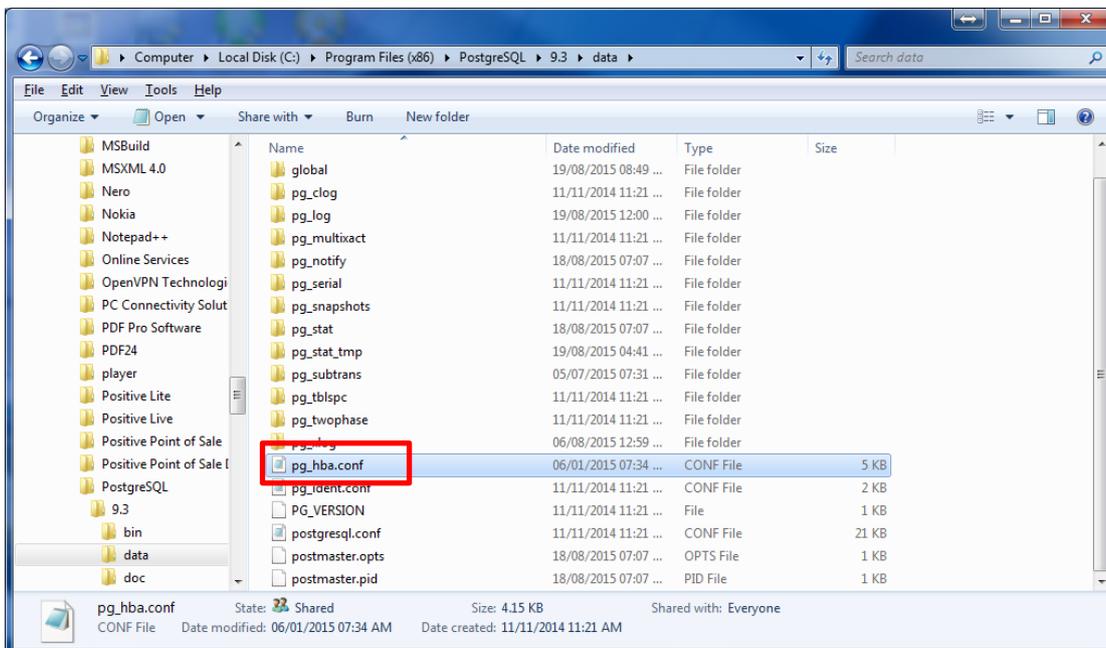
13. Click on 9.3.



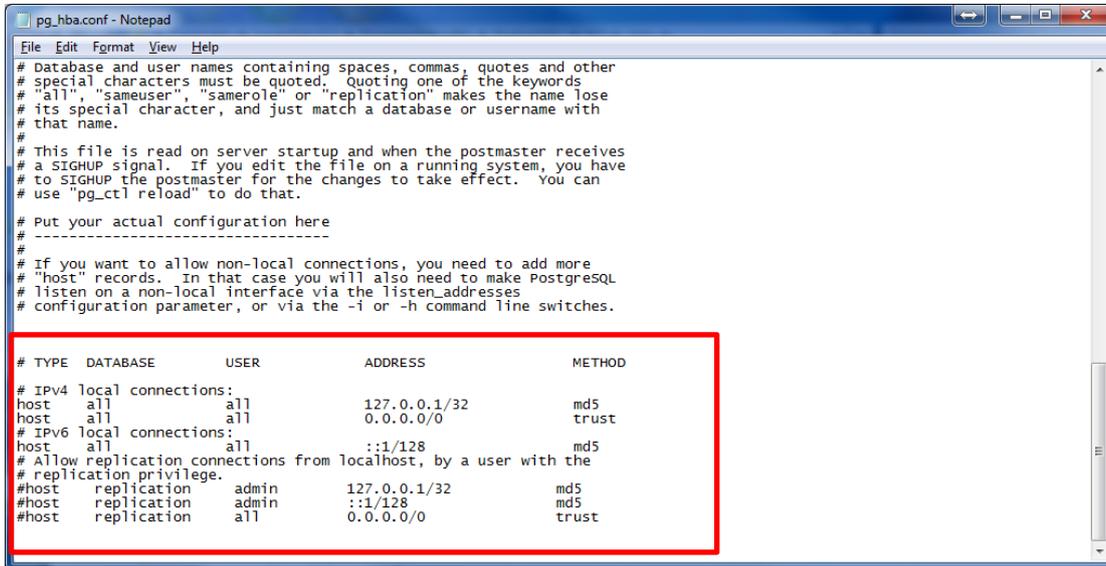
14. Click on data.



15. Click on pg_hba.conf.



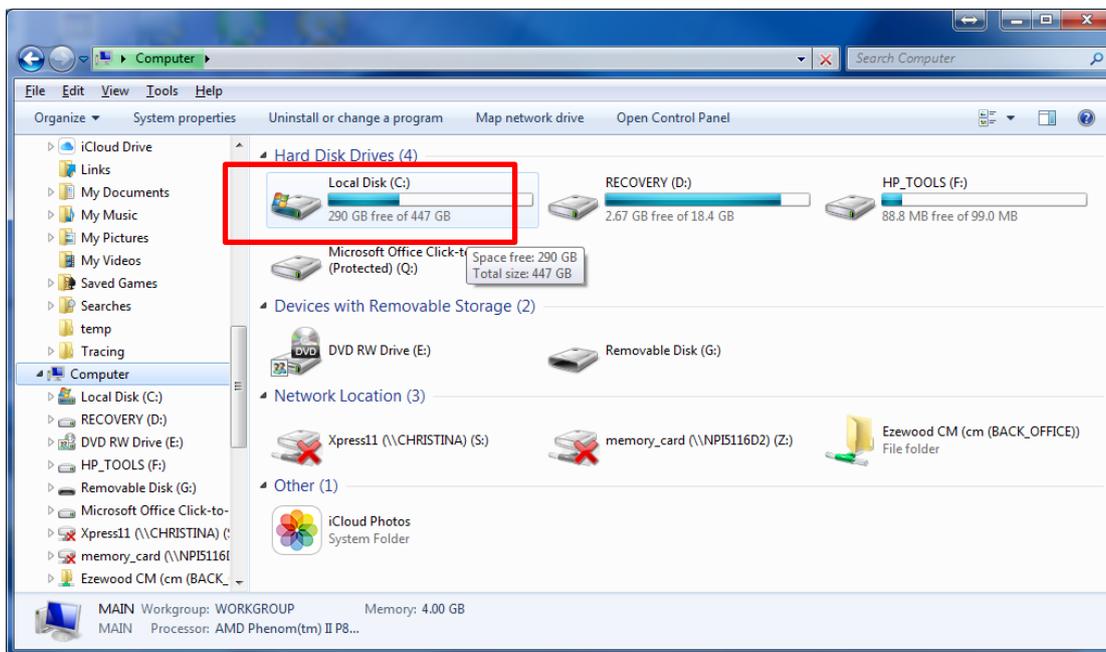
16. Change the setting like this below.



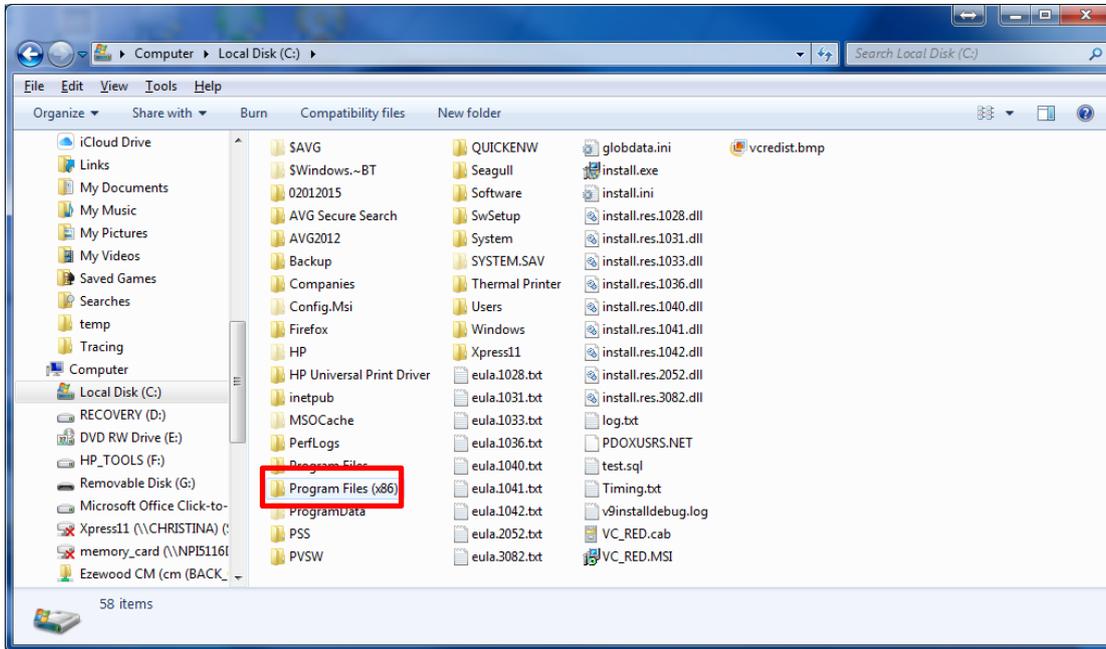
```
pg_hba.conf - Notepad
File Edit Format View Help
# Database and user names containing spaces, commas, quotes and other
# special characters must be quoted. Quoting one of the keywords
# "all", "sameuser", "samerole" or "replication" makes the name lose
# its special character, and just match a database or username with
# that name.
#
# This file is read on server startup and when the postmaster receives
# a SIGHUP signal. If you edit the file on a running system, you have
# to SIGHUP the postmaster for the changes to take effect. You can
# use "pg_ctl reload" to do that.
#
# Put your actual configuration here
#
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.
#
# TYPE DATABASE USER ADDRESS METHOD
# IPv4 local connections:
#host all all 127.0.0.1/32 md5
#host all all 0.0.0.0/0 trust
# IPv6 local connections:
#host all all ::1/128 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
#host replication admin 127.0.0.1/32 md5
#host replication admin ::1/128 md5
#host replication all 0.0.0.0/0 trust
```

SHARING YOUR MAIN POS PC WITH PERMISSIONS:

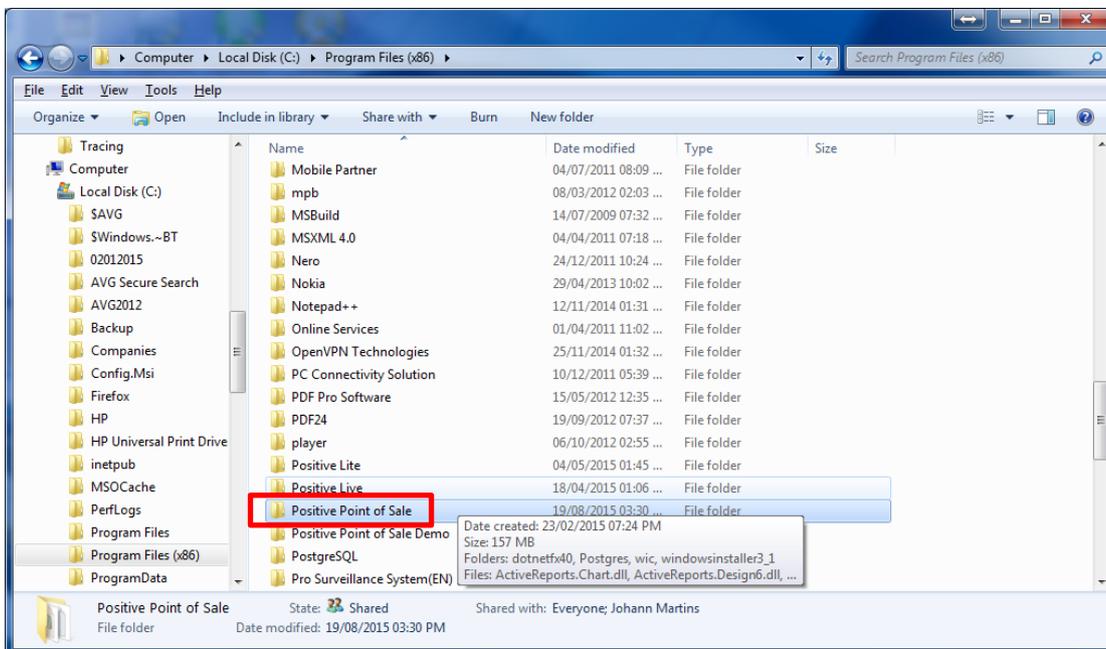
17. Go to your C-Drive on the main POS PC



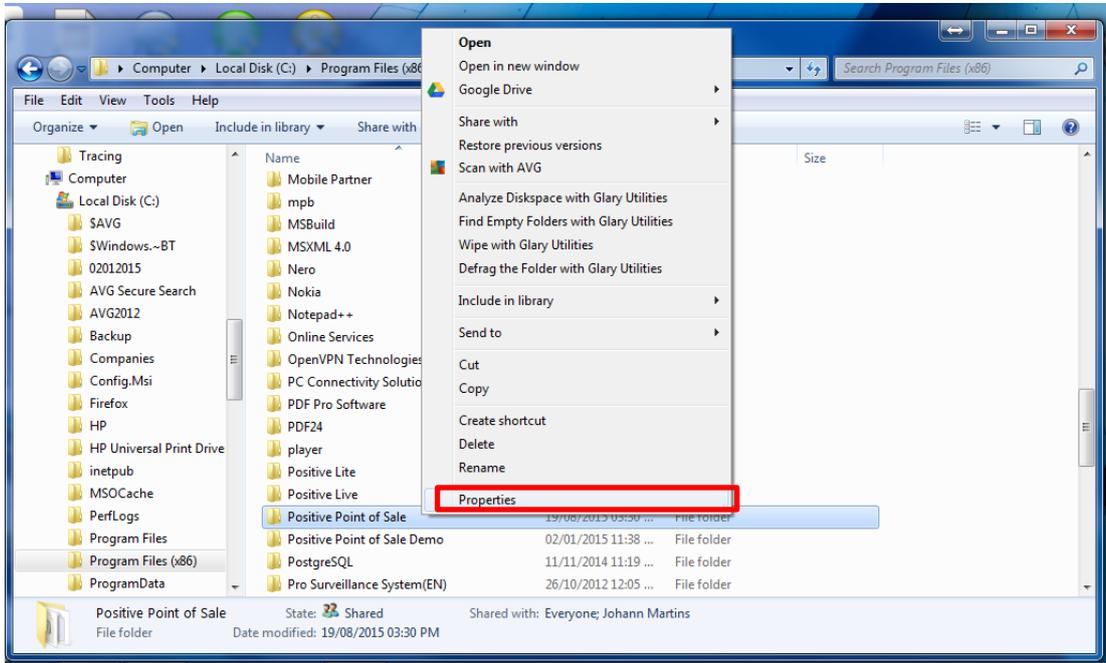
18. Go to Program Files (x86).



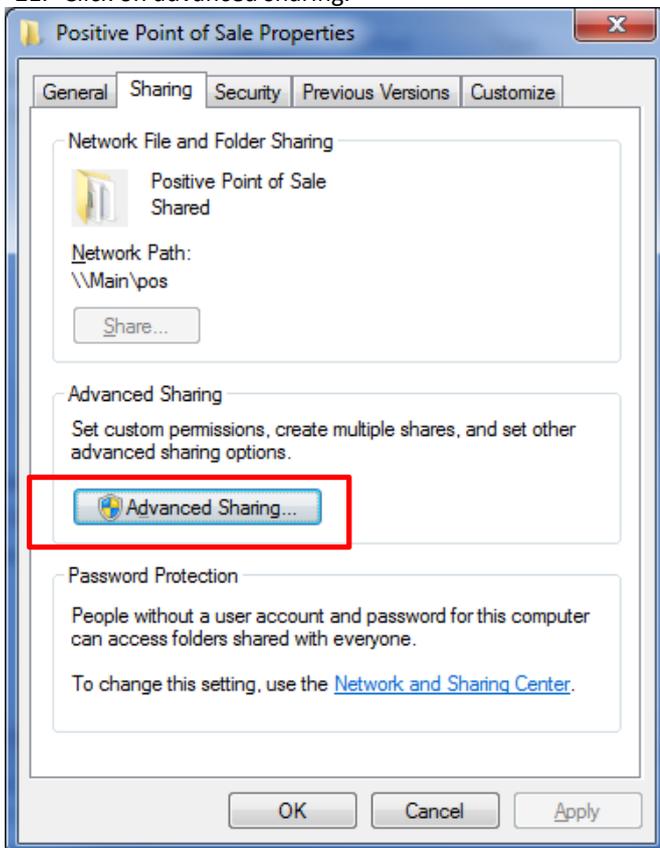
19. Go to Positive Point of Sale and right click.



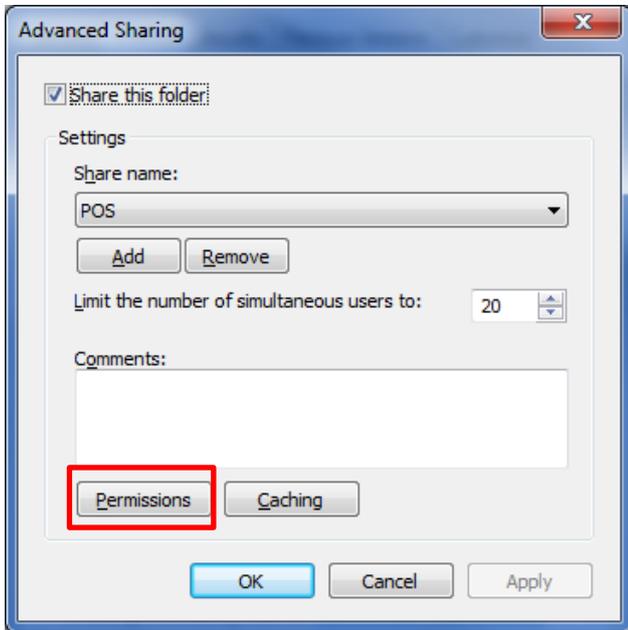
20. Click on properties.



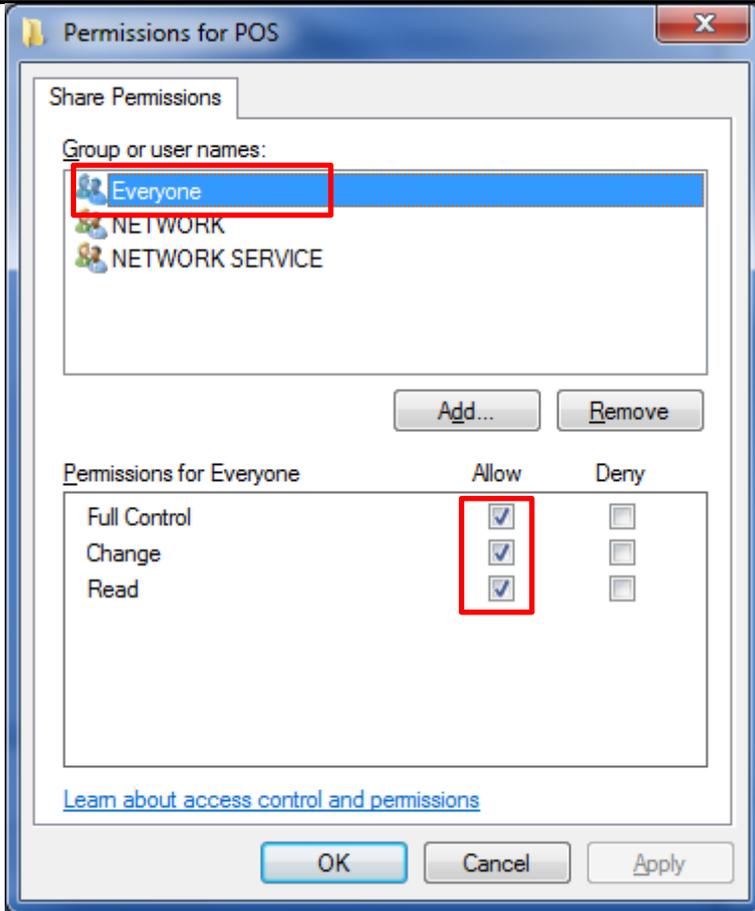
21. Click on advanced sharing.



22. Click "Share this folder" and ensure share name is "POSitive Point of Sale" else you will need to change the setting in 11 above. Click on permissions.



23. Choose everyone. And allow all permissions.

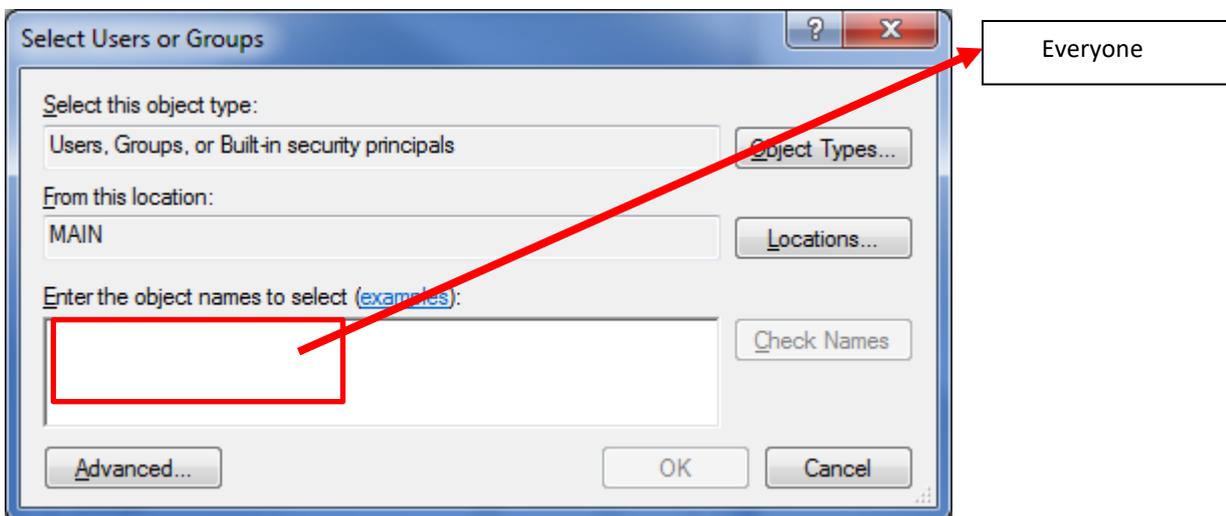


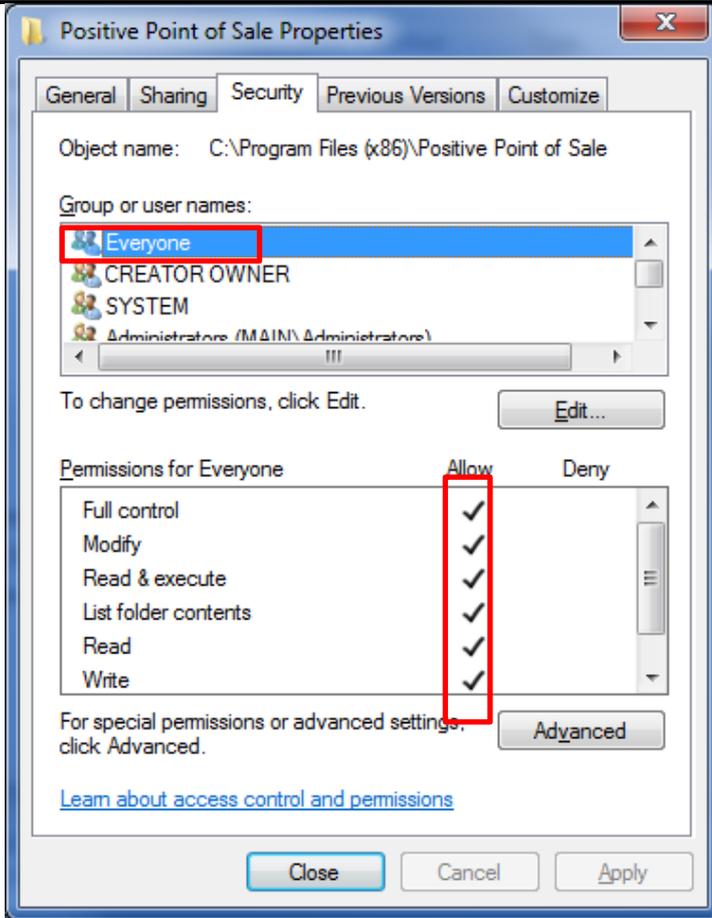
All the Permissions for Everyone should be ALLOW.

If there is not an everyone folder you should create one, see below how to do it.

Click Add:

Then add (Everyone)

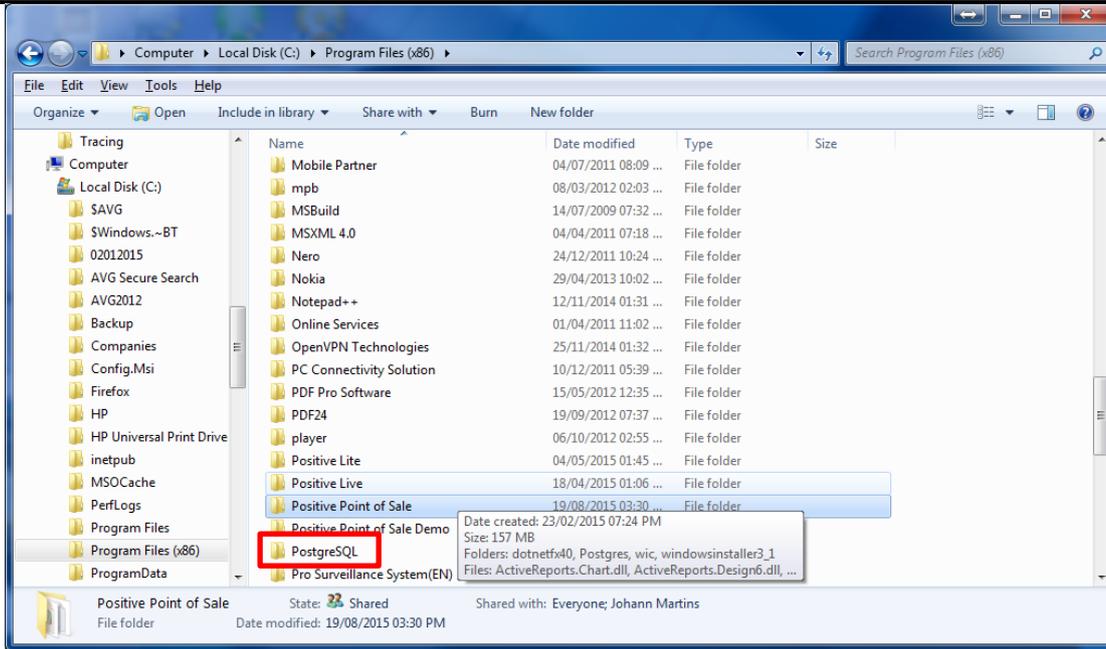




All the Permissions for Everyone should be ALLOW.

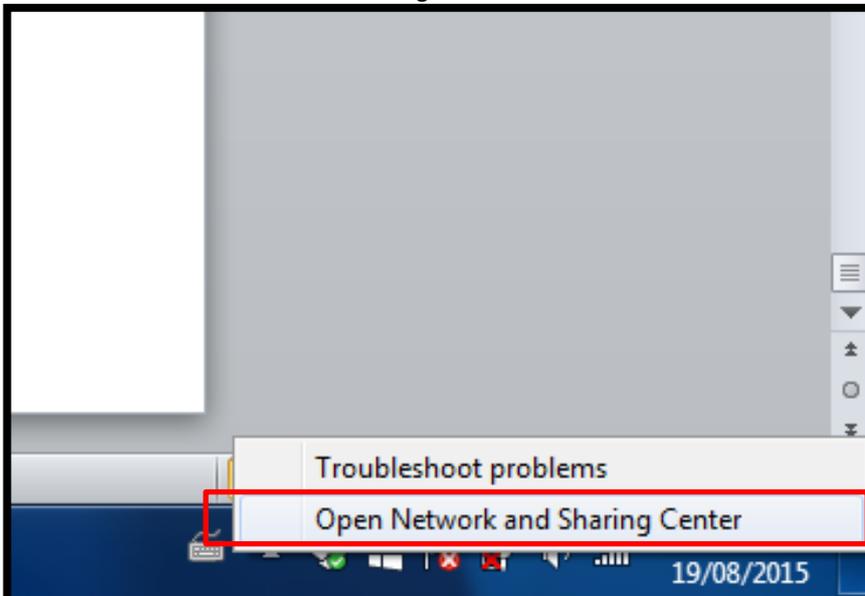
Do the same for permissions only on:

- PostgreSQL.

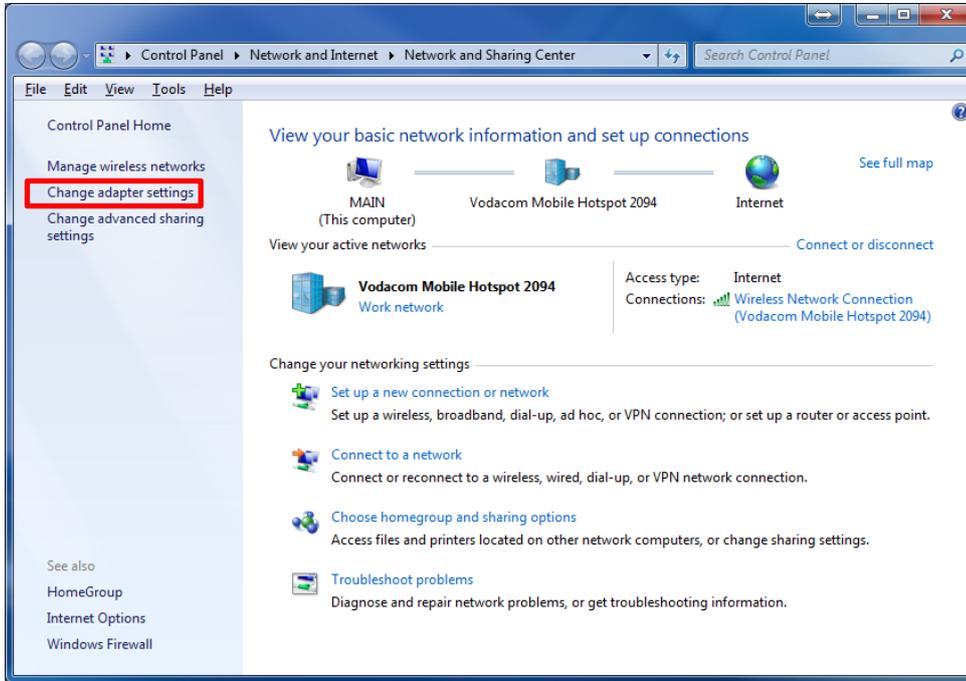


FIXED IP ADDRESS ON YOUR MAIN POS PC:

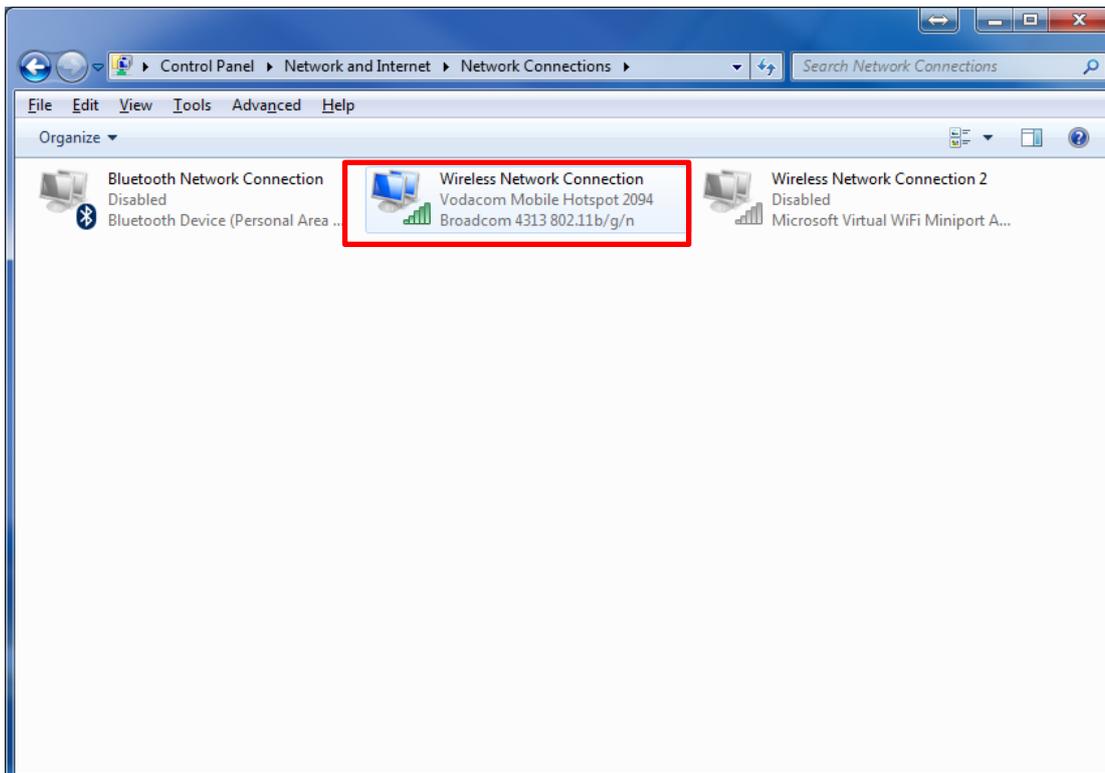
1. On the main POS PC, right click on network.
2. Then choose network and sharing.



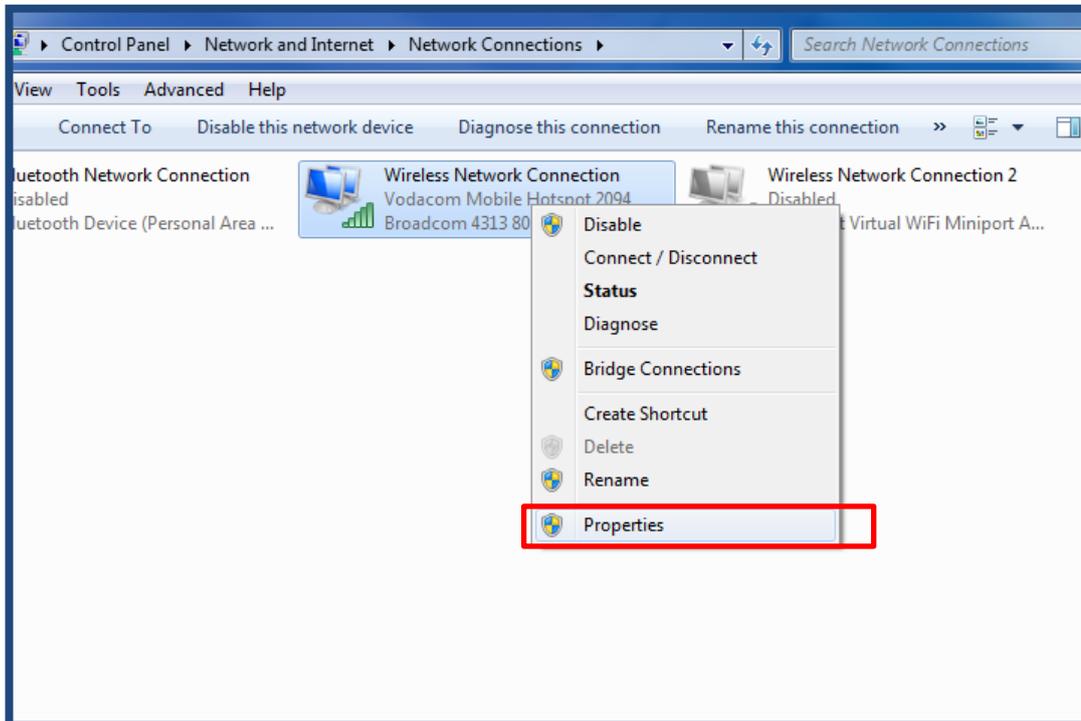
3. Click on change adapter settings.

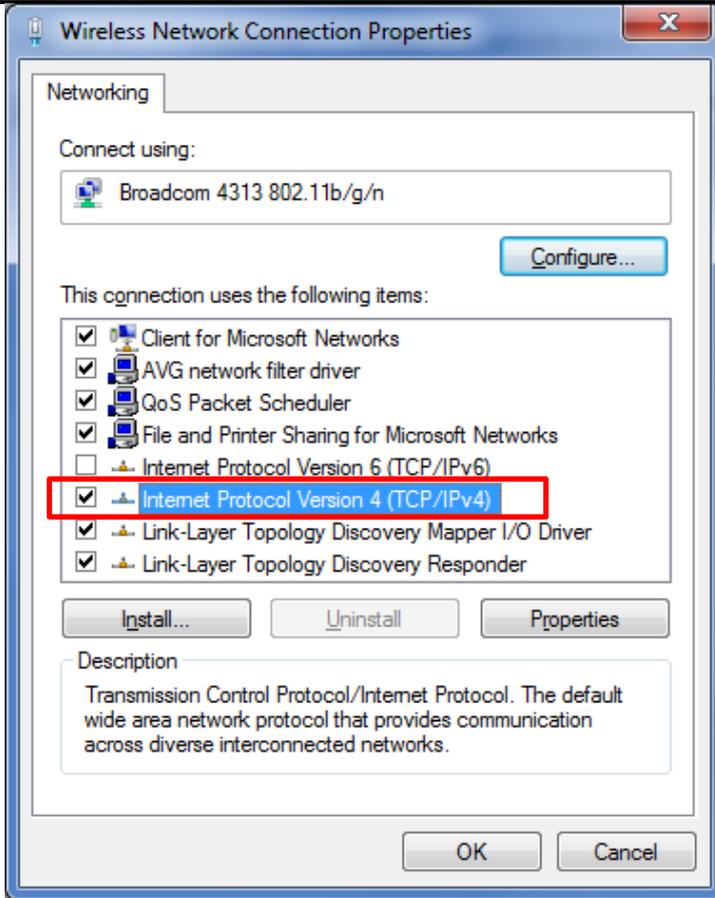


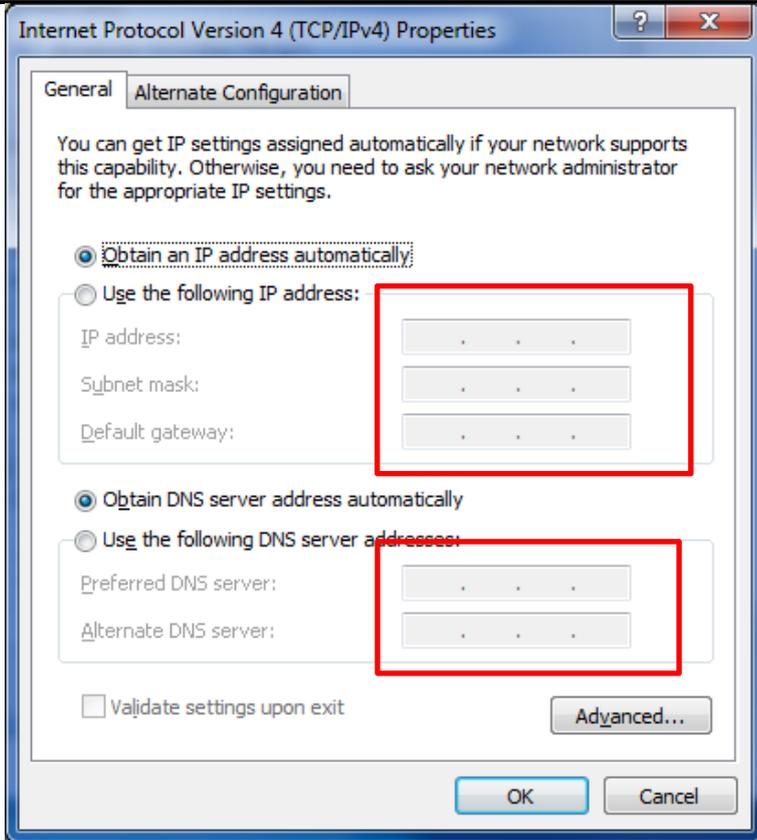
4. Right click on wireless network connection.



5. Click on properties.

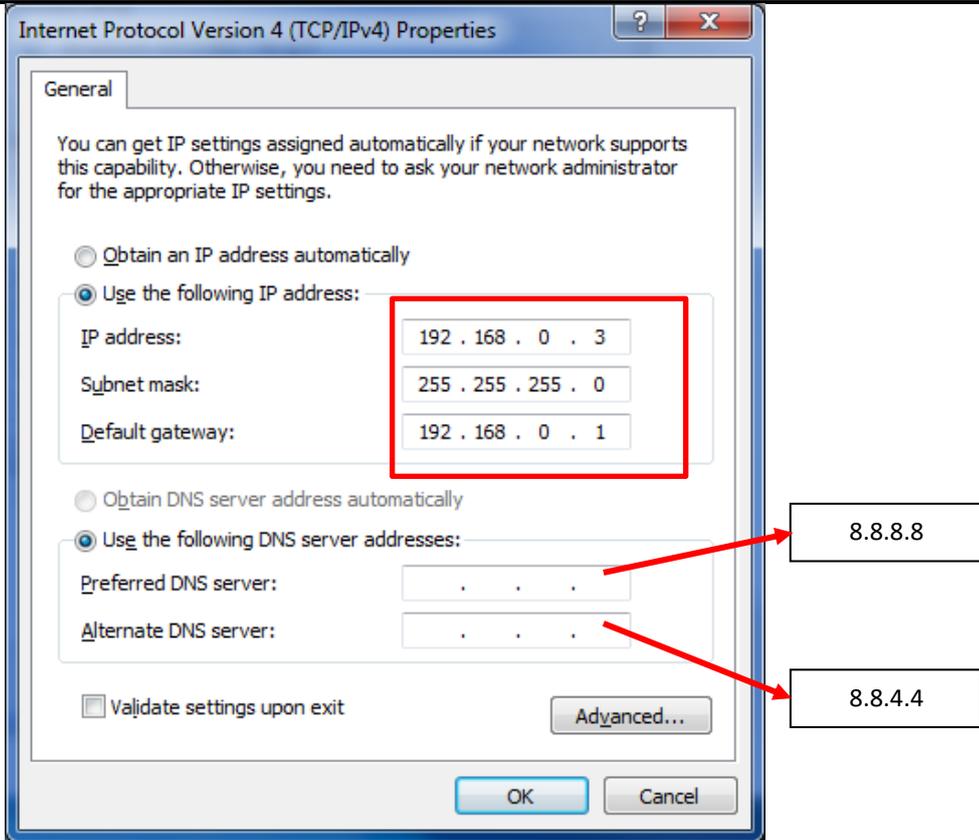






IP Address should be the same as the one in point 11 above.

Also Subnet mask should be as per your original ipconfig

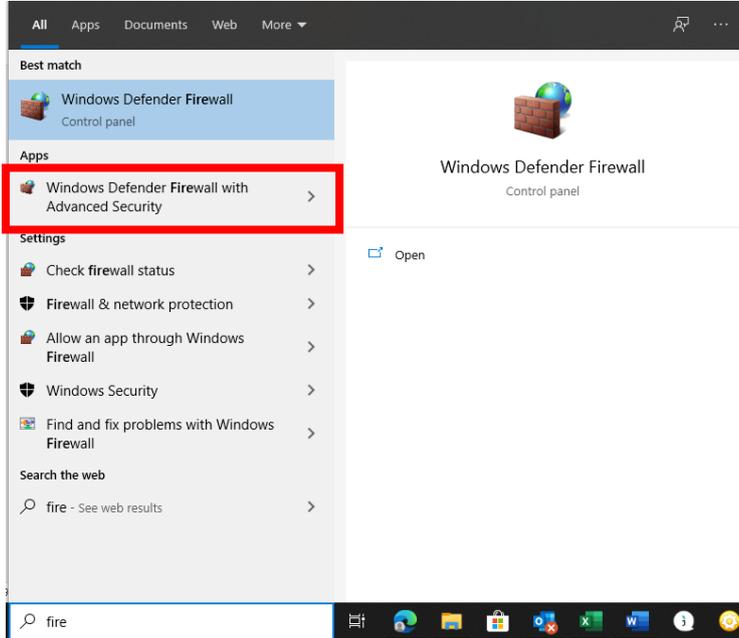


Your Subnet Mask as well your Default Gateway will be under your IP Address. (Wireless Connection)

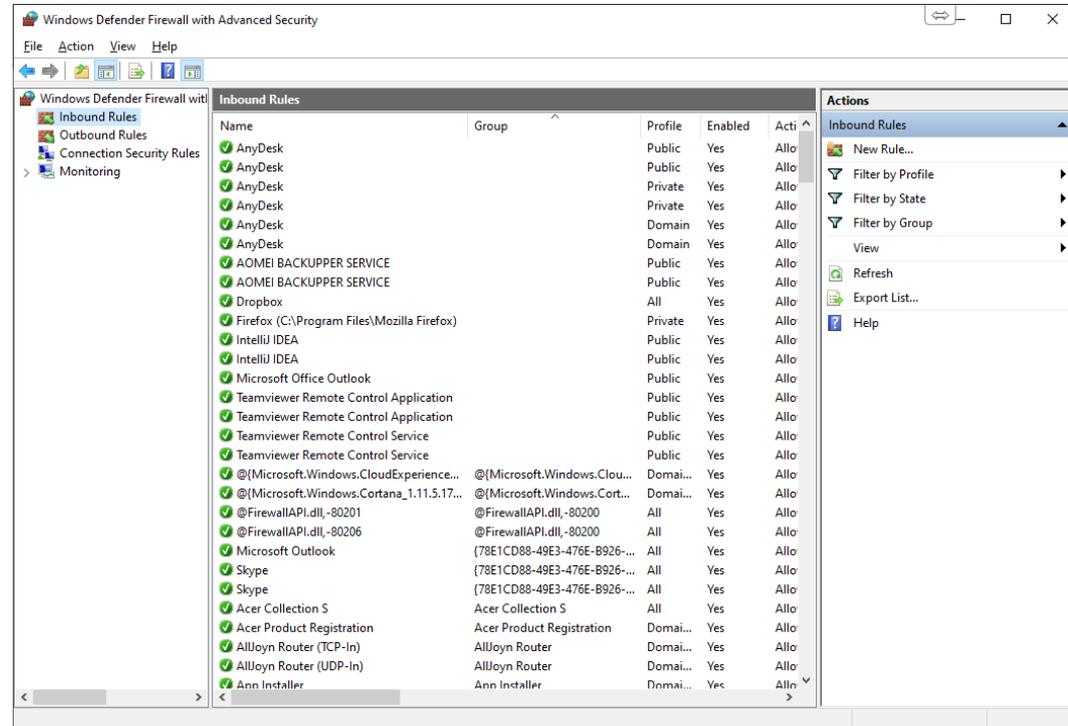
Please see video on how to do a connection - [Connection](#)

SETTING UP YOUR FIREWALL ON YOUR MAIN POS PC

Please go to Windows Defender.



Add an Inbound and outbound Rule.



New Rule according to screenshots below

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

Program
Rule that controls connections for a program.

Port
Rule that controls connections for a TCP or UDP port.

Predefined:
@FirewallAPI.dll,-80200
Rule that controls connections for a Windows experience.

Custom
Custom rule.

< Back Next > Cancel

New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

TCP

UDP

Does this rule apply to all local ports or specific local ports?

All local ports

Specific local ports:
Example: 80, 443, 5000-5010

< Back Next > Cancel

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- **Action**
- Profile
- Name

What action should be taken when a connection matches the specified conditions?

Allow the connection
This includes connections that are protected with IPsec as well as those are not.

Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

Block the connection

< Back Next > Cancel

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

When does this rule apply?

Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

< Back Next > Cancel

New Inbound Rule Wizard

Name

Specify the name and description of this rule.

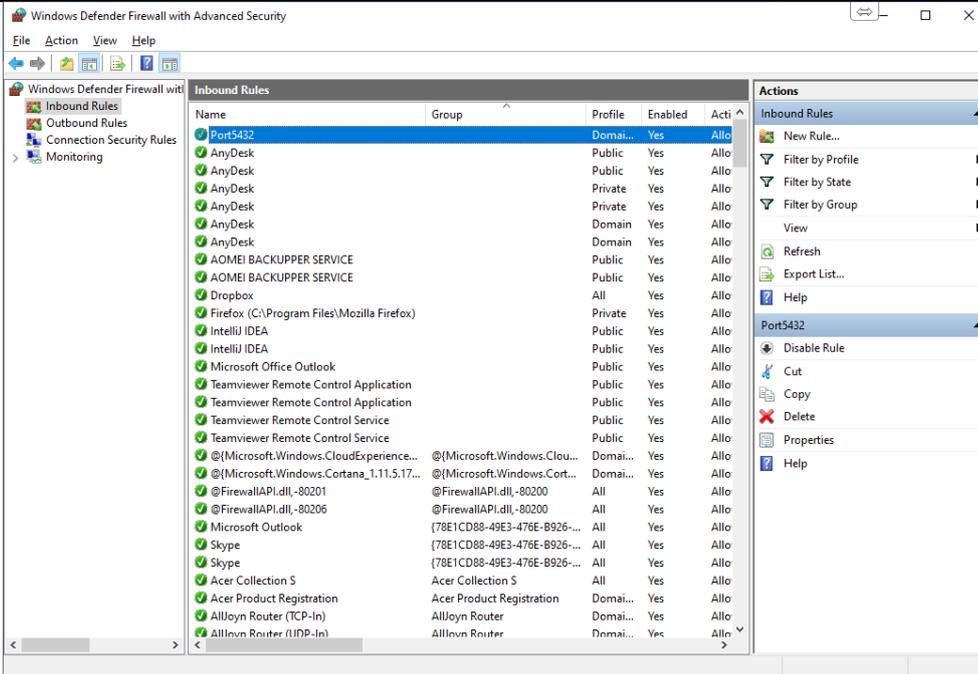
Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Name:

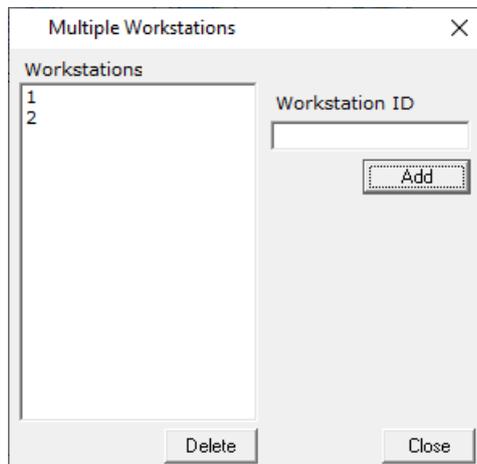
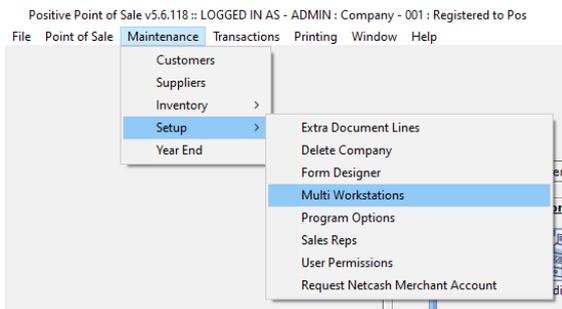
Description (optional):

< Back Finish Cancel



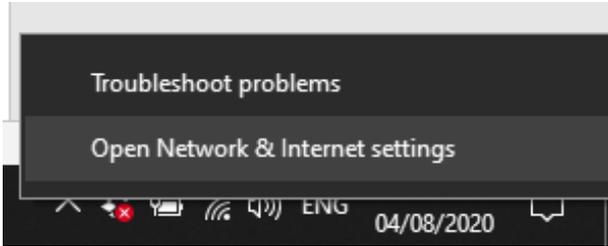
Do the same on the Outbound Rules.

1. Go to your main POS PC
2. Go to Maintenance – Setup – Multi Workstations

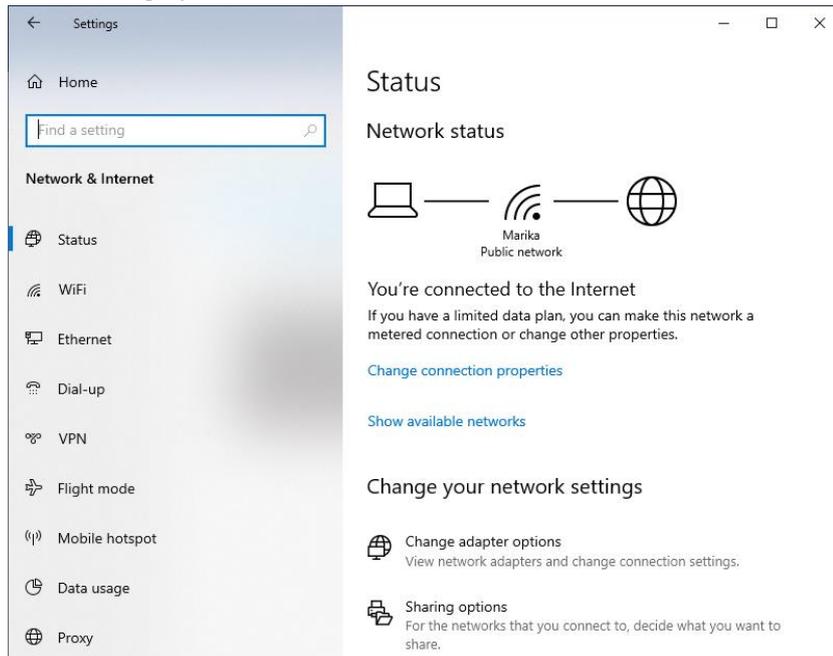


Add workstations as required and configured in 11 above

Go to Open Network & Internet Settings.



Go to Sharing Options.



Allow all.

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private ⬆

Network discovery ⬆

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

Turn on network discovery
 Turn on automatic setup of network-connected devices.
 Turn off network discovery

File and printer sharing ⬆

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

Turn on file and printer sharing
 Turn off file and printer sharing

Guest or Public (current profile) ⬇

All Networks ⬇

Turn off Password Sharing.

The screenshot shows the 'Advanced sharing settings' window in Windows. The breadcrumb trail is: Control Panel > Network and Internet > Network and Sharing Centre > Advanced sharing settings. The window title is 'Advanced sharing settings'. The settings are as follows:

- Private: (checked)
- Guest or Public (current profile): (checked)
- All Networks: (checked)
- Public folder sharing: Turn on sharing so that anyone with network access can read and write files in the Public folders. Turn off Public folder sharing (people logged on to this computer can still access these folders).
- Media streaming: (checked). Includes a link 'Choose media streaming options...'
- File sharing connections: Use 128-bit encryption to help protect file sharing connections (recommended). Enable file sharing for devices that use 40- or 56-bit encryption.
- Password-protected sharing: Turn on password-protected sharing. Turn off password-protected sharing.

At the bottom of the window, there are two buttons: 'Save changes' and 'Cancel'.