



Security Software Configuration

Windows XP:

By Jon Ellender

The following documentation has been to assist in configuration of windows firewall, as well as provide a resource to identify the required services, ports, programs, and file groups to configure 3rd party Firewalls, A/V (Antivirus) and A/M (Antimalware) programs.

A. Firewalls

Please consult your I.T. Consultant for the best possible solution for your firewall needs. There are 2 main options. One is Windows Firewall and secondly is a 3rd party firewall.

Note: These steps are general overview of how to add ONLY E-woo software. Information on configuring any other applications or ports, please visit Microsoft.com for more information.

A-1. Navigating to Windows firewall and turning on the service.

1. Click start

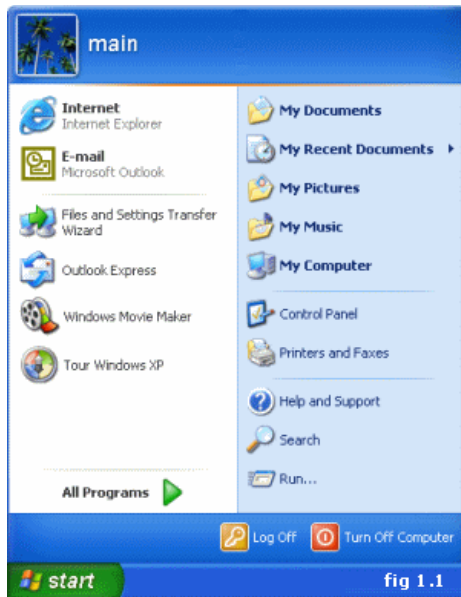
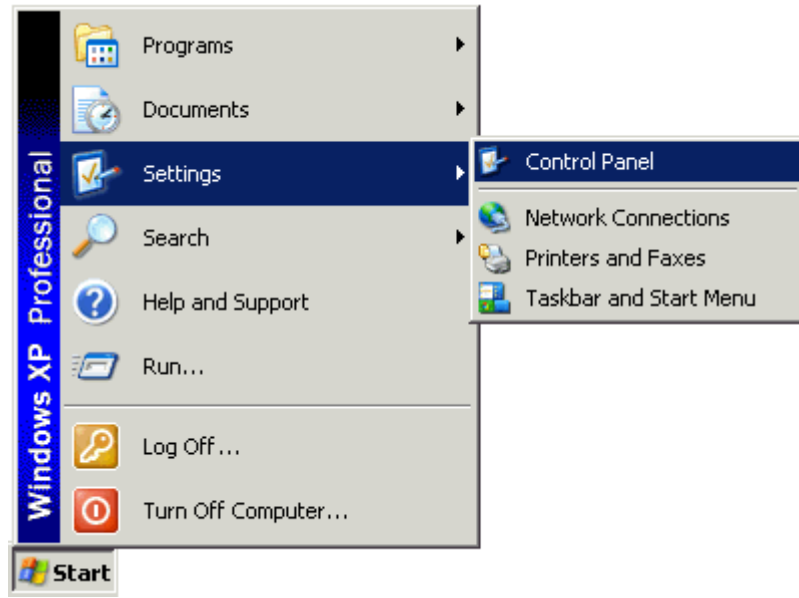


fig 1.1

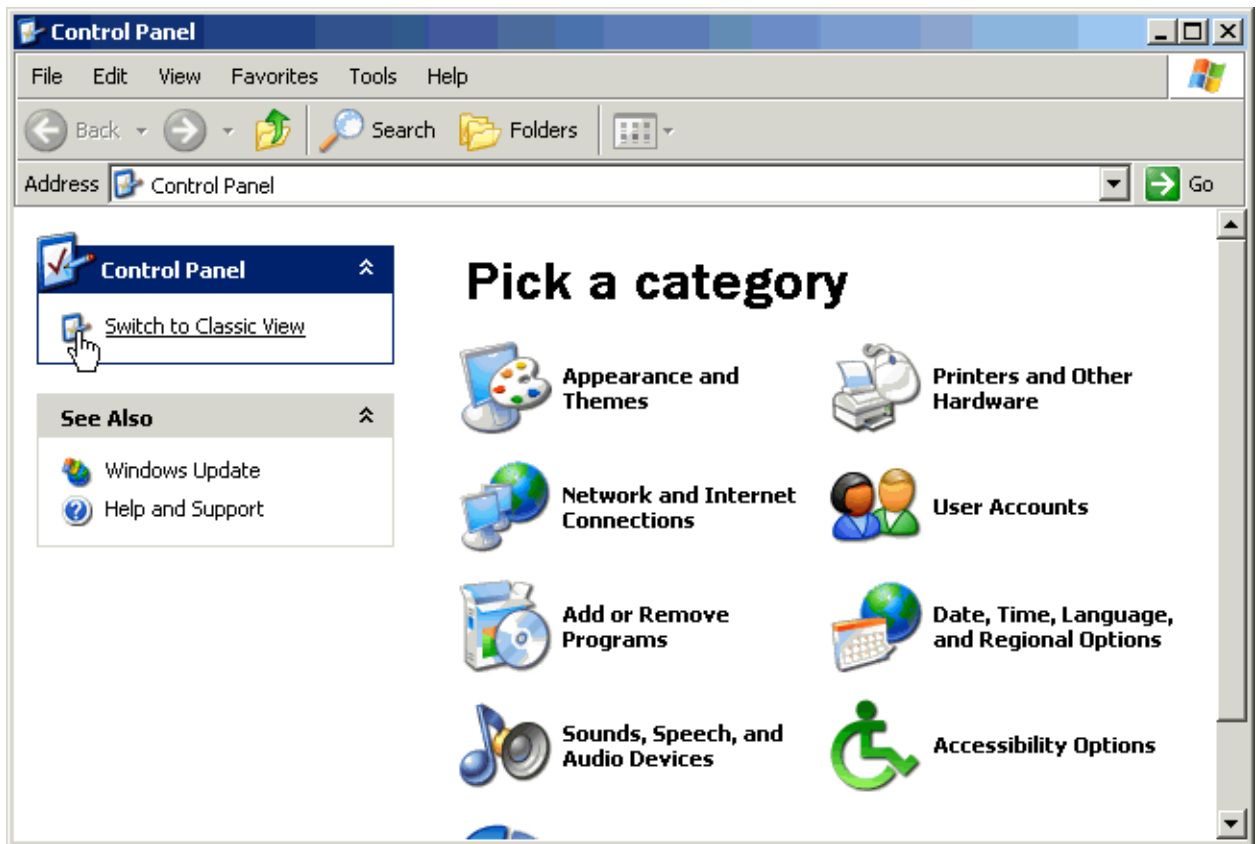
2. Click Control panel (If "Control Panel is not listed see next line)



Click Settings (advanced display mode only)



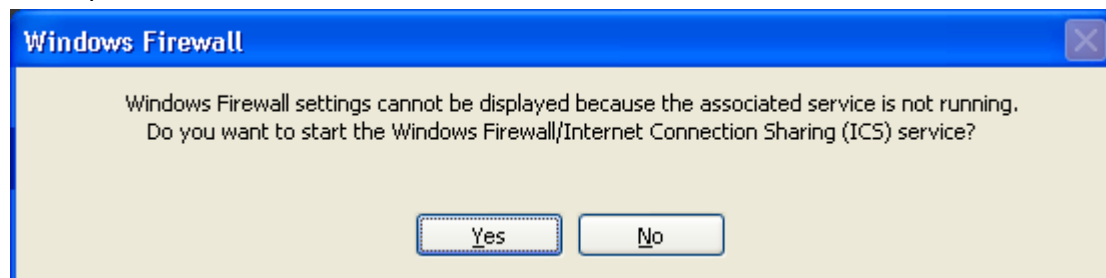
3. In the left hand Column, Please click "Classic View"



4. Open "Windows Firewall" (SP2 or higher only on XP)
 (On XP SP1 or earlier please choose network connections, right click, click properties, click windows ICF tab Click "Configure" if you do not see "Windows Firewall Icon" in the control panel.)



5. Click Yes- If windows firewall warning appears "Firewall unable to start because the Windows Internet connection firewall is disabled If error does not appear continue to next step.



6. Verify the Firewall is "On" by checking the bullet point "On-Recommended"



7. Do NOT check the “Do not allow Exceptions” as this will override any exceptions you create or add.
8. Click “Apply” to enable the settings changed.

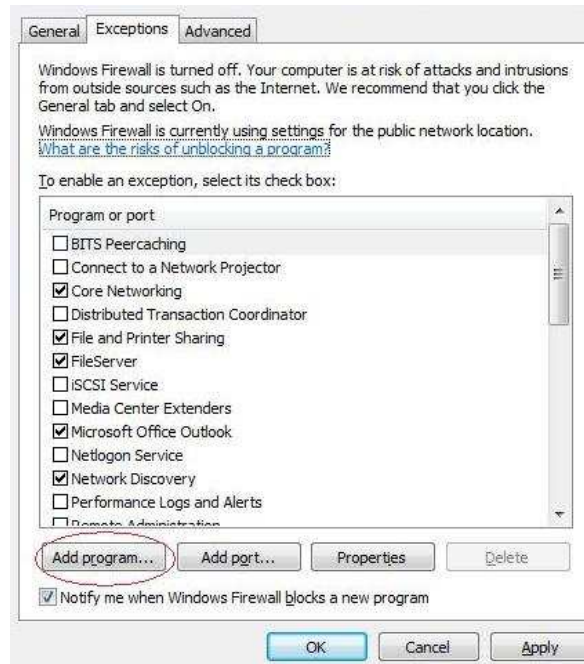
A-2 Allowing specific programs to Windows Firewall exclusion list.

To add programs to the exclusion list in Windows firewall please follow the following steps.

1. Click “Exceptions” tab



2. Click “Add Program”

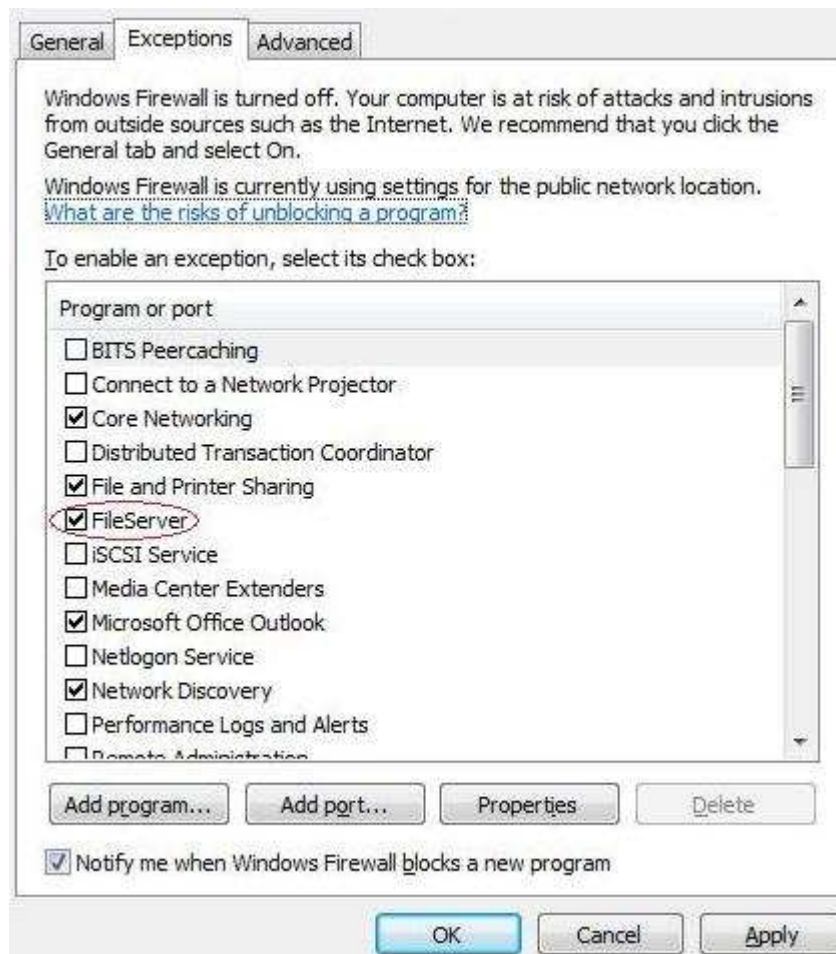


3. Choose the program desired (please see section E. for more information on which programs are required)

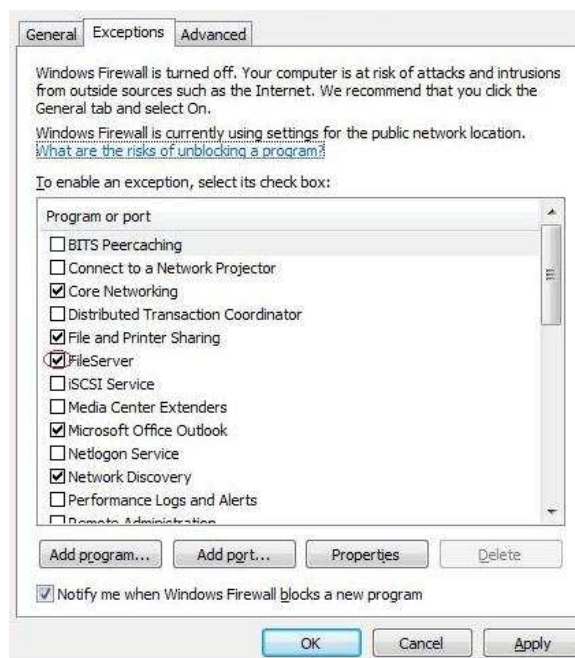


4. Click “Ok”

5. Once added to the list, verify the program is listed, and the box is checked



6. To enable the exclusion check the box.

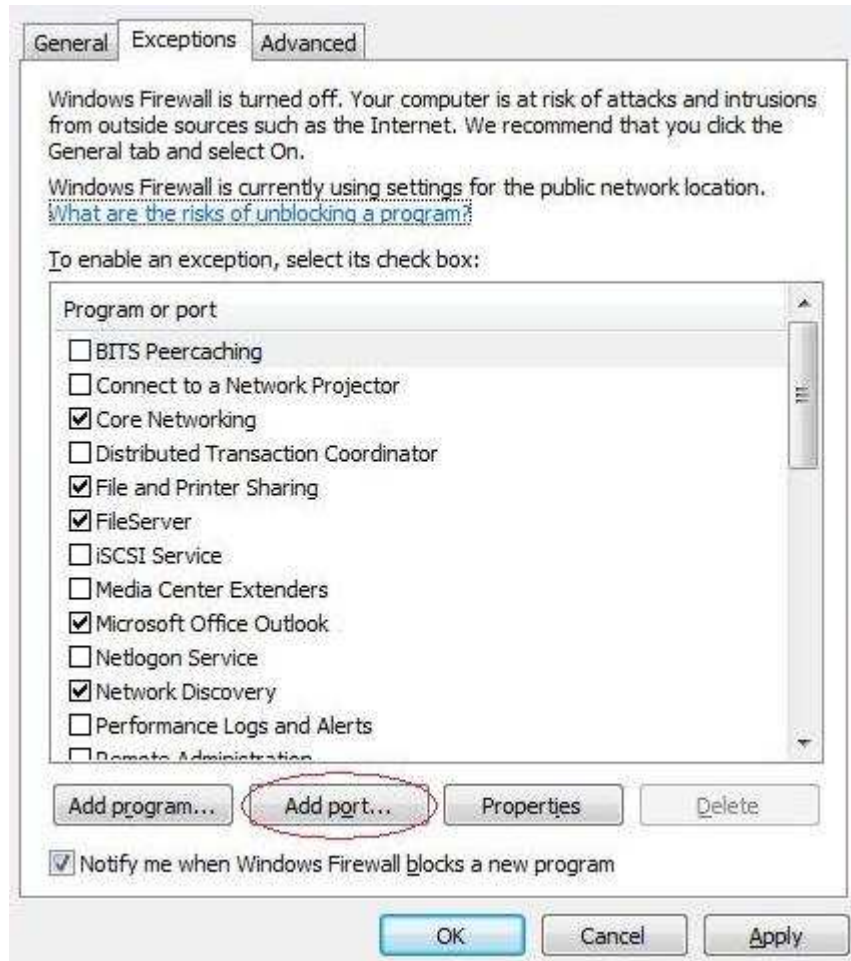


7. To remove the exclusion, uncheck the box.
8. Repeat steps 1-5 to add more programs.

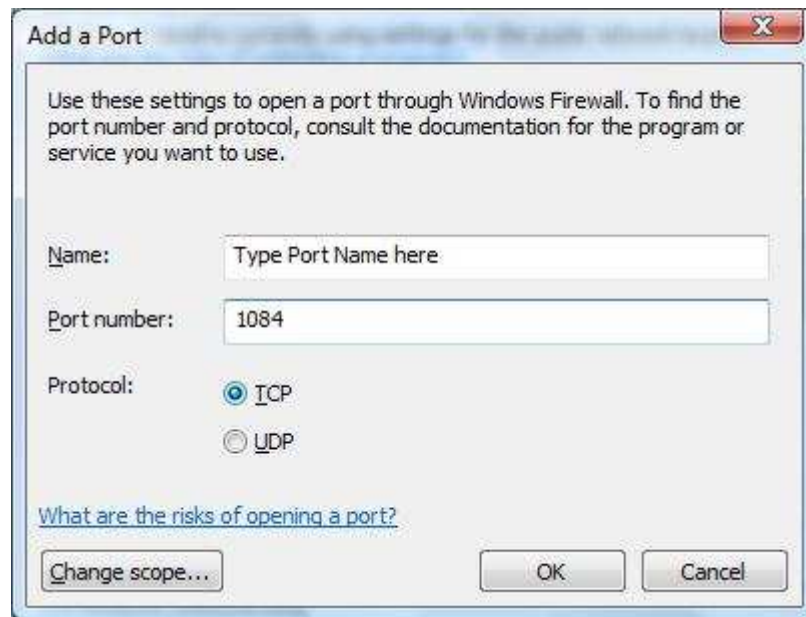
A-3 Add a specific port to Windows Firewall exclusion list.

To add a specific port to Windows firewall, please follow the following steps.

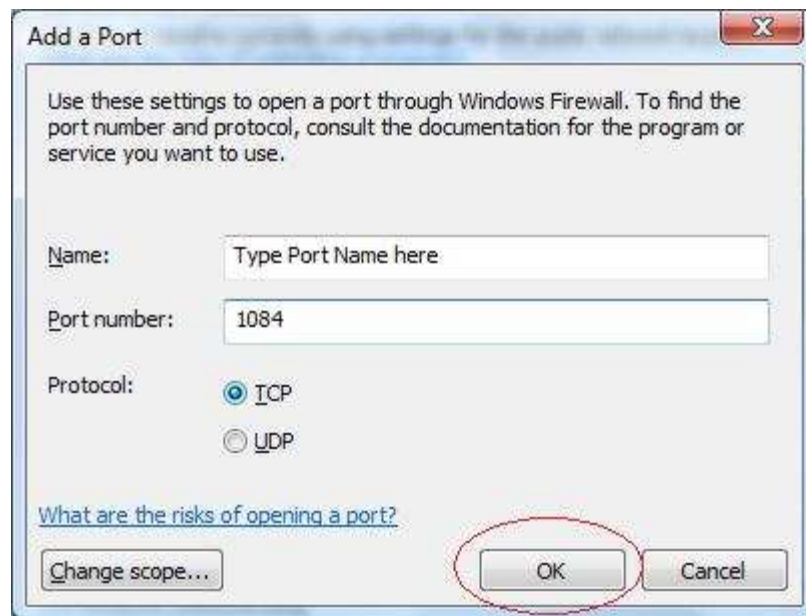
1. Click “Add port”



2. Name the port in the “Name:” box
3. Type the port number in “Port number:” box
4. Select rather this is a TCP port or a UDP port.



5. Click ok.



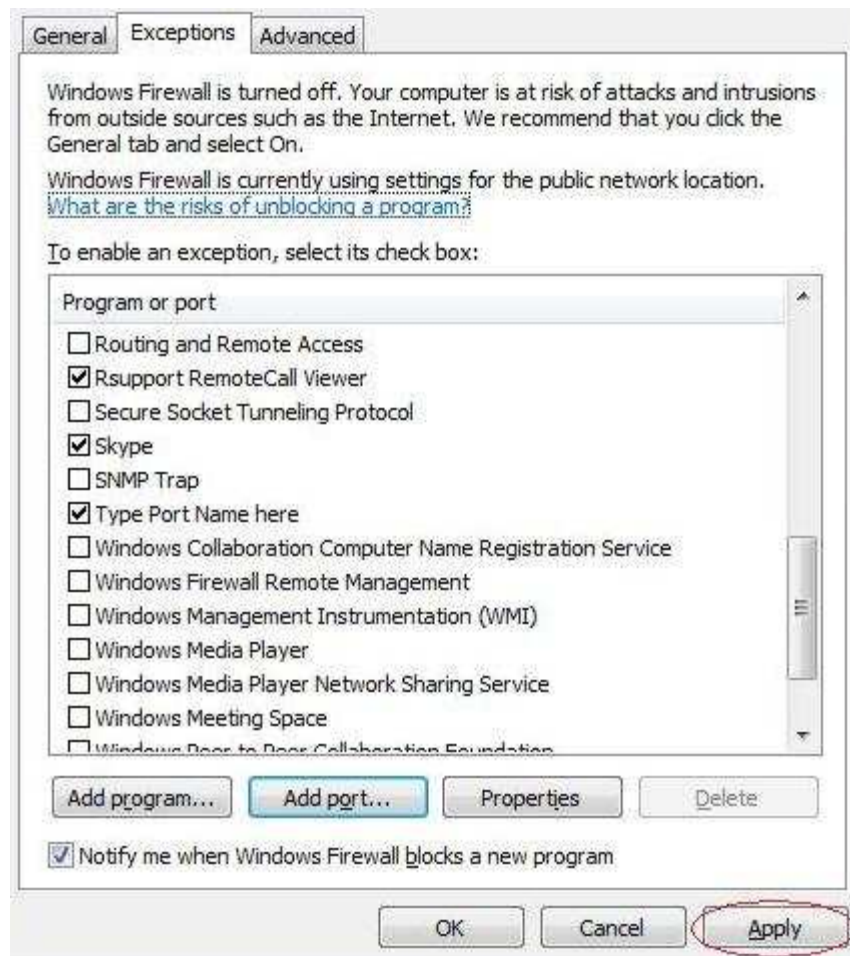
6. Verify the added port is listed.



7. To add the port to the exclusion list, check the box.



8. Click “Apply ” to save settings.



9. To remove the port from the exclusion list uncheck the box.

10. To add more ports to the exclusion list, follow steps 1-7 for each port desired.

A-4. 3rd party Firewalls

It is recommended that you first consult an I.T. Consultant before choosing, or installing any 3rd party Firewall on your system.

Please have an I.T. consultant administrate your program, and Port exclusion lists for 3rd party firewalls.

Note: E-woo is unable to provide specific instructions for 3rd party firewall software as those settings, steps, and procedures vary firewall to firewall.

B. Services, Ports, Dynamic Ports, File Groups.

Recourse: This section identifies the specific Services, Ports, virtual ports, file groups.

B-1. Main Services

1. Nhservice
2. Hasp
3. Sqlight
4. Sql
5. Fileserv
6. Ezdent
7. Ezimplant

B-2. AnySensor (All Makes)

1. AnySensor.exe
2. Ezx.exe
3. Vakap.exe

B-3. Ports

1. 475 UDP
2. 1947 TCP
3. 3306 TCP
4. 1433 TCP

5. 19092 TCP
6. 1433 TCP
7. 19091 TCP
8. 80 TCP

B-4 Dynamic Ports

Note: We DO NOT recommend anyone blocking any virtual ports. Virtual ports should only be modified by Trained and Certified I.T. Consultants. Please do not attempt. Port

1. Range 52000-53000

B-5 Program Directories

B-5 A. EazyDent

1. %SystemRoot%\Eazydent4
2. %SystemRoot%\Eazydent

B-2. AnySensor & EzSensors (All Makes)

4. AnySensor.exe
5. EzSensor.exe
6. Ezx.exe
7. Vakap.exe

B-3. Ports

9. 475 UDP
10. 1947 TCP
11. 3306 TCP
12. 1433 TCP
13. 19092 TCP
14. 1433 TCP
15. 19091 TCP
16. 80 TCP

B-4 Dynamic Ports

Note: We DO NOT recommend anyone blocking any virtual ports. Virtual ports should only be modified by Trained and Certified I.T. Consultants. Please do not attempt. Port

1.Range 52000-53000

B-5 Program Directories

B-5 A. EasyDent4

3. %SystemRoot%\Easydent4
4. %SystemRoot%\Easydent

B-5 B. AnySensor & EzSensor

5. %SystemRoot%\AnySensor150
6. %SystemRoot%\AnySensor150N
7. %SystemRoot%\AnySensor100
8. %SystemRoot%\AnySensor100N
9. %SystemRoot%\EzSensor100
10. %SystemRoot%\EzSensor150
11. %SystemRoot%\EzSensor200

B-5 C. EzImplant

1. %SystemRoot%\Ezimplant

B-5 D. Ez3D2009

1. %SystemRoot%\Ez3D2009

B-6 E. Hasp

1. %SystemRoot%\ProgramData\Microsoft\Windows\Start Menu\Programs\Hasp License Manager

C. A/V & A/M Security Software (3rd Party)

C-1. Recommended Software

Not: E-woo recommends the following A/V (Antivirus) software as it has been tested to not interfere with our software.

Avast Free/Pro [Http://www.avast.com/](http://www.avast.com/)

Malwarebytes [Http://www.malwarebytes.org/](http://www.malwarebytes.org/)

C-2. 3rd Party Software

1. *Please use section B for advanced or custom exclusion policies for 3rd party A/V and A/M Software by adding custom exclusions and permissions for “Full access” or “Full control”.*

Important Notice: It is recommended for even those software's that normally do not interfere with any given program, caution should be used when using software, inspect files that are claimed to be 'infected' and verify what file it is and determine if it could be a false positive.

While we recommend certain program's for Anti-Virus/Anti-Malware (Spyware) we recommend them on the basis that they are tested to normally not interfere with our software. Detection rates are those of the respected companies and with any software Supplemental scanning should be used with any system alike, manually by an I.T. Consultant.