Firewall Configuration

Firewall software is an integral part of most business environments these days. Unfortunately, the default settings for most of these products disable/block the communication of the ASTRA software with Wyatt Technology instruments (DAWN HELEOS/TREOS, ViscoStar & Optilab rEX) via a TCP/IP network

If the client computer running ASTRA has an enabled firewall, a few specific TCP ports must be opened for instrument communication. The ASTRA installer will add any necessary Windows Firewall exceptions during the install. If a firewall other then the Windows Firewall is used, you must enable the following firewall exceptions:

TCP Port Exceptions required by ASTRA:

- 135 (Wyatt Instrument Communication)

Application Exceptions

- astra.exe
- isiu.exe
- wsisu.exe
- diagnosticmanager.exe

Note: The default application installation path for these files is “C:\Program Files\WTC\ASTRA 5.x”, where x corresponds to the minor version of the installed software.

Optional: TCP Port Exceptions (non-ASTRA related Wyatt Technology software)

- 9001 (HELEOS/TREOS Instrument Communication)
- 9002 (ViscoStar Instrument Communication)
- 9003 (QELS Instrument Communication)

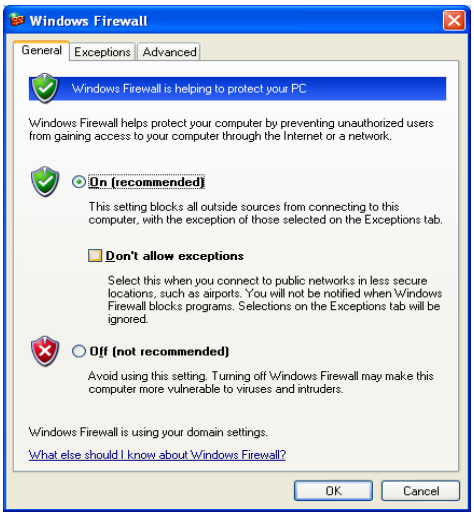
Note: The DAWN HELEOS/TREOS instrument has an embedded QELS option. The QELS option requires TCP Port 9003.

This document contains configuration instructions for the Windows Firewall in Windows XP, and ZoneAlarm by ZoneLabs.

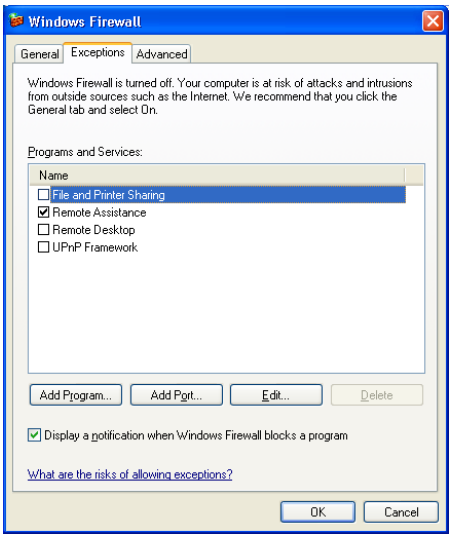
Windows XP Firewall

Configuring the Windows Firewall

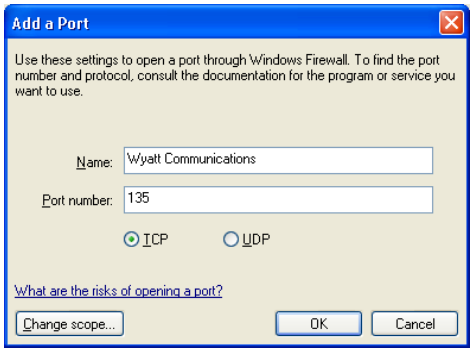
1. From the Start menu, choose “Control Panel”.
2. In the control panel, open the “Windows Firewall”
3. If the Windows Firewall is “Off” and will never be used, you can skip these instruction. Many corporate networks have a firewall for the entire site and disable the firewall on individual client machines.
4. If the Windows Firewall will be used, ensure that it is “On”, in the Windows Firewall dialog, and verify that the “Don’t allow exceptions” check box is NOT set.



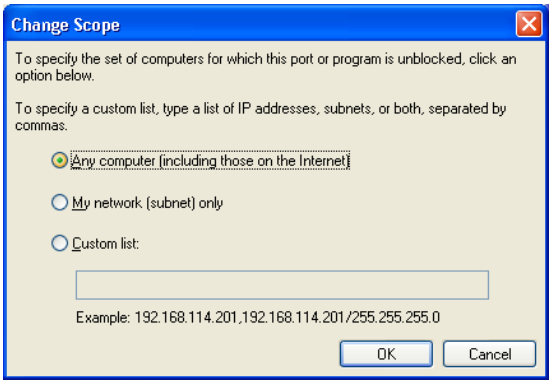
5. Select the “Exceptions” tab. You will need to add a Port and four programs to the “Programs and Services” exception list. Press the “Add Port” button.



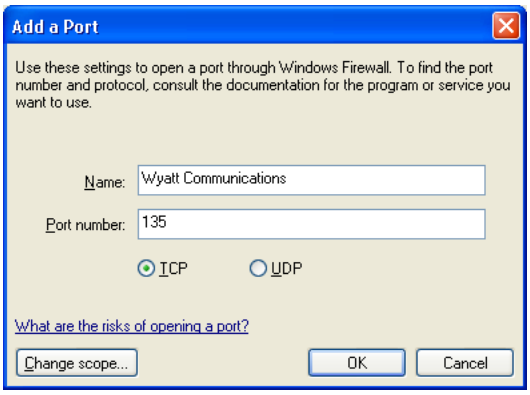
6. Configure the port settings:
   a. Enter “Wyatt Communications” in the “Name” field.
   b. Enter “135” in the “Port number” field.
   c. Select the TCP radio button.
   d. Press the ‘Change Scope’ button.



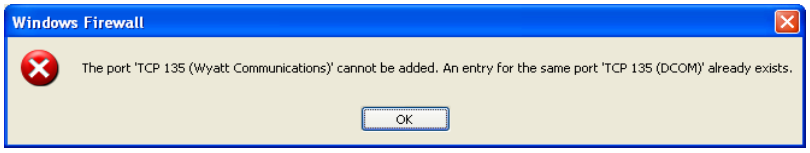
7. Confirm that the “Any computer (including those on the internet)” option is selected. Press OK to return to the “Add a Port” dialog.



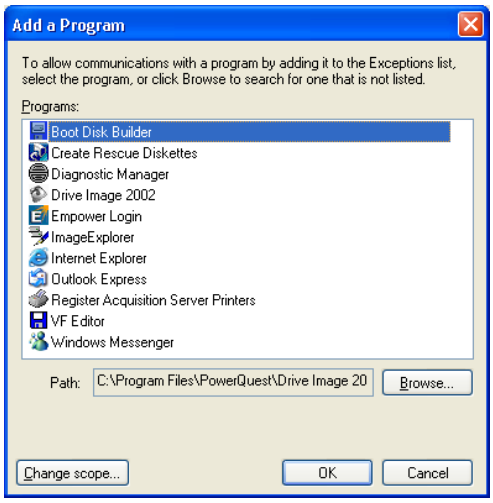
8. Press OK to complete the “Add a Port” process.



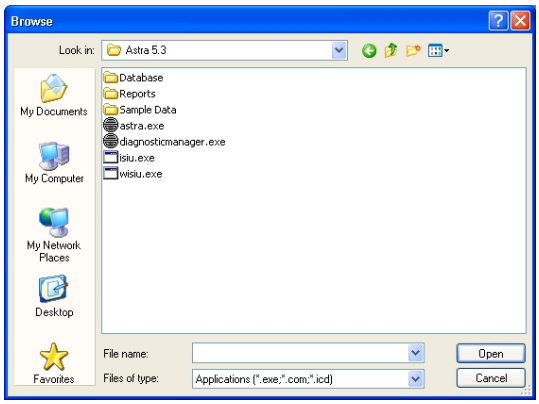
9. **Note:** You can safely ignore any error message indicating that the port “cannot be added. An entry for the same port already exists.” This error just means another application required TCP Port 135, and has already configured your system appropriately. Go on to the next step.



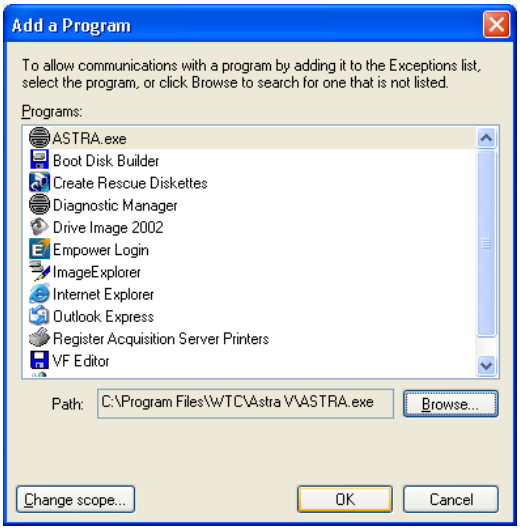
10. Press the ‘Add Program’ button. Press the ‘Browse’ button.



11. Navigate to the ASTRA install location (usually at **"C:\Program Files\WTC\ASTRA 5.x",** where x is the minor version number).
    a. Select ASTRA.exe
    b. Press the 'Open' button.

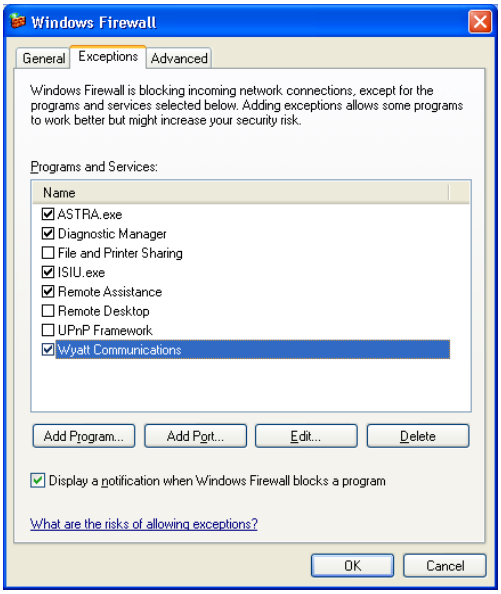


12. The 'Add a program' dialog will now include the 'ASTRA.exe' program in its list. Click the OK button.

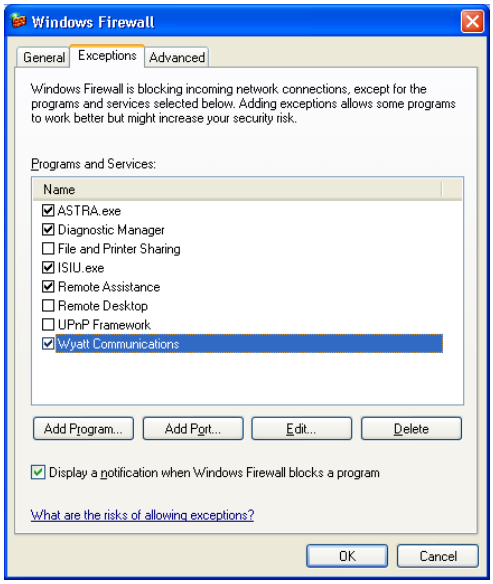


13. Repeat steps 8-10 for the diagnosticmanager.exe, isiu.exe and wisiu.exe programs (located in the same directory as astra.exe).

14. When finished, the Windows Firewall 'Exceptions' page should look similar to the image below, and should contain the following entries:
    a. ASTRA.exe
    b. Diagnostic Manager
    c. ISIU.exe
    d. WISIU.exe
    e. Wyatt Communications



15. **Note:** If you received an error on Step 7 (indicating Port 135 was already in use), you will not see “Wyatt Communications” in the list at right. You can safely ignore this and continue with the rest of the configuration.



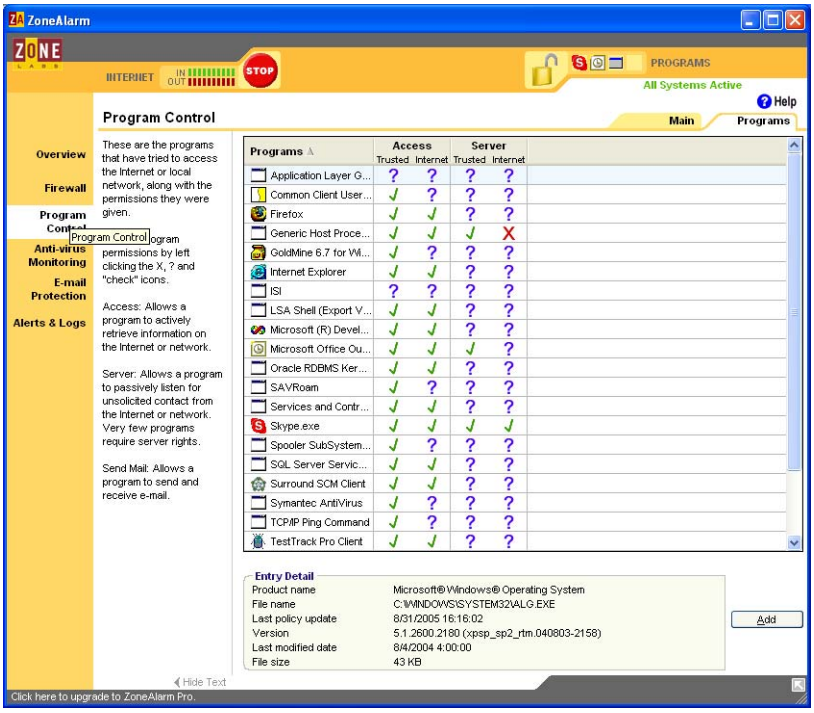
16. Press OK to save all settings and close the Windows Firewall

ZoneLabs Firewall

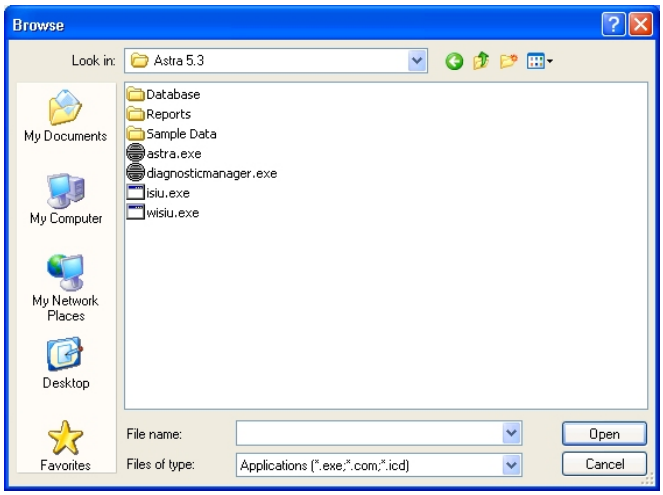
Configuring ZoneAlarm

1. When ZoneAlarm is running, a tray icon will be shown. Right-click on this icon (which usually shows up as a “ZA” icon), and select “Restore ZoneAlarm Control Center.”

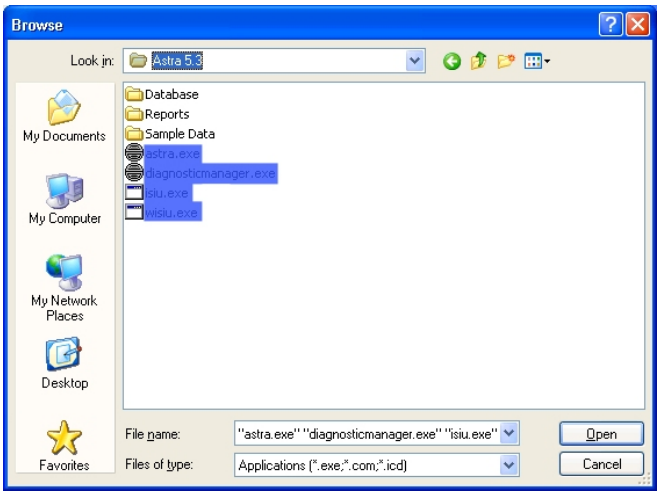
2. Select the “Program Control” option, and the “Program” tab.



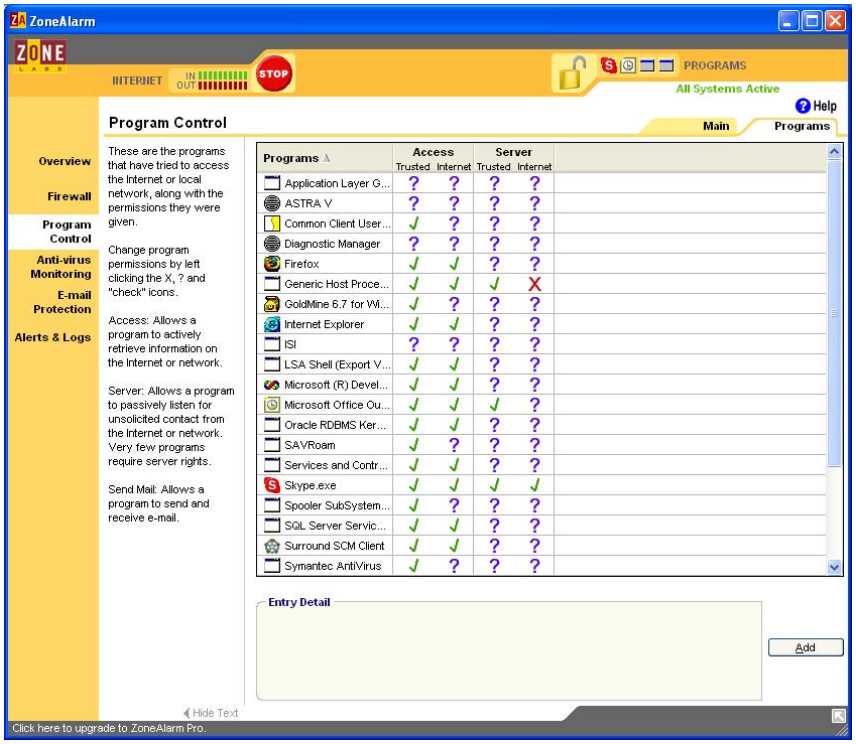
3. We will need to add three programs to ZoneAlarm’s list, ASTRA.exe, ISI.exe, and DiagnosticManager.exe. Click the “Add” button, then navigate to the installation path for the ASTRA software. This is typically “C:\Program Files\WTC\Astra 5.x”



4. Select astra.exe, diagnosticmanager.exe, isiu.exe and wisiu.exe files and press Open:

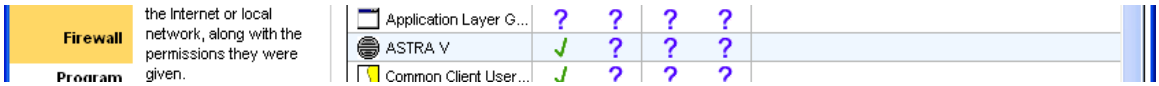


5. All three of these programs must be configured to allowed to access the network, and to function as servers. The "Program Control" screen allows you to configure "Access" and "Server" settings for each program. By default, the programs are configured to ask the user each time a program attempts to access the network, or to function as a server. This is signified in the user interface by displaying a "?" for each column).



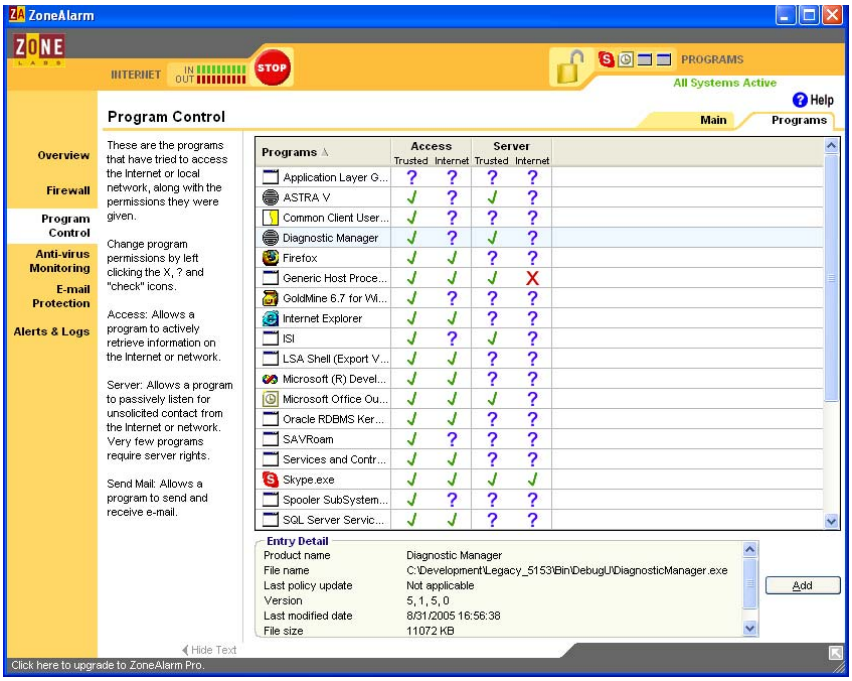
6. At this point, you must decide how secure your firewall needs to be. If you feel confident in the security of your network, you can configure the software to allow "Access" and "Server" support for the "Internet" setting, avoiding the need for further configuration. A more secure configuration is to leave the "Internet" columns at the default "?" (ask) setting, configure the "Trusted" columns to permit access, then add each Wyatt instrument to the list of known (trusted) systems.

7. To allow network access to the trusted zone of your network, click on the question mark for one of the programs (e.g., the "ASTRA V" program) under the "Access" column, "Trusted" field, and select "allow". The question mark will change to a green check-mark.

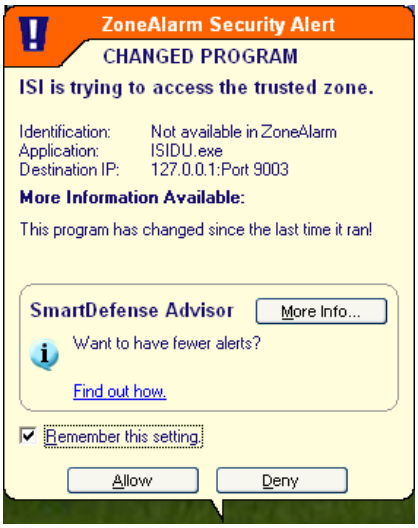


8. Repeat this step for the “Server” column, “Trusted” field.

9. Repeat steps 7 and 8 for each of the programs (“ASTRA V”, “Diagnostic Manager”, and “ISI”).

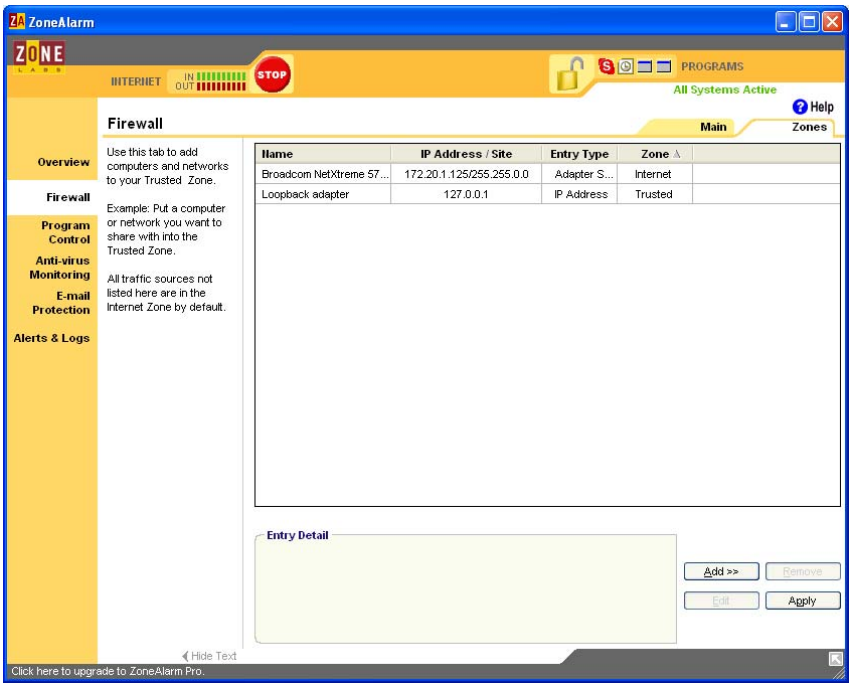


10. Another way to make these changes is to respond to any “ZoneAlarm Security Alert” pop-pup windows for ASTRA, Diagnostic Manager, or ISI and select the “Remember this setting” box, and select the “Allow” button. This will



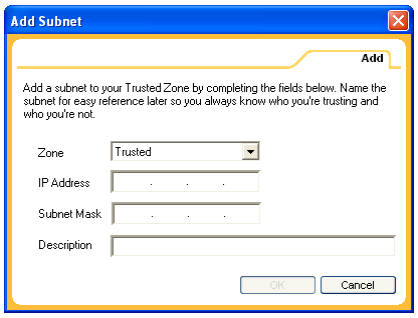
11. Most corporate environments use DHCP to assign IP addresses to computers on the network. In most cases, your Wyatt instrument will be assigned an IP address via DHCP. Consequently, you should specify a valid range of IP addresses as your “Trusted” zone so that any reassignment of IP addresses does not prevent data collection.

    a. If you wish to add each instrument individually, go to Step 12.
    Otherwise, select the “Firewall” tab on the ZoneAlarm control screen:

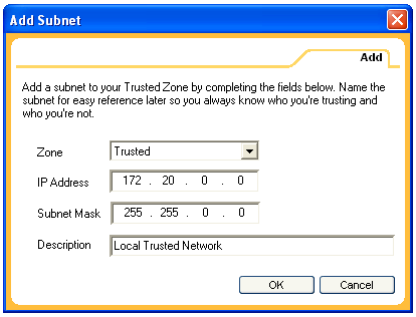


    b. Click on the “Add >>” button. This will pop up a menu asking you to choose between “Host/Site”, “IP Address”, “IP Range”, or “subnet”. Select the “subnet” range.

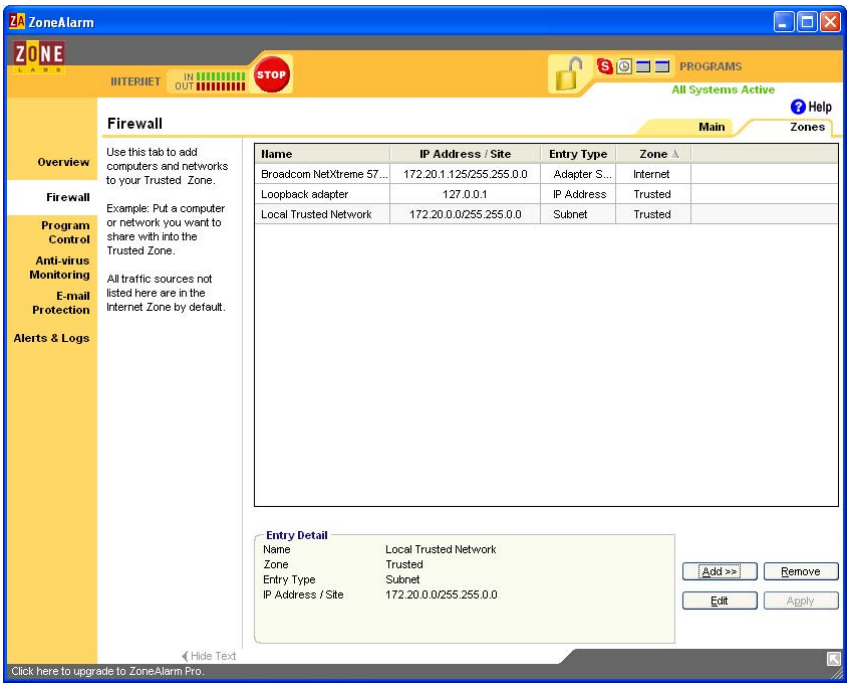
    c. A dialog will be presented allowing you to specify the IP address and subnet mask.



    d. Fill in the starting IP address range and subnet mask, which you can get from your system administrator. Press the OK button to add the subnet.



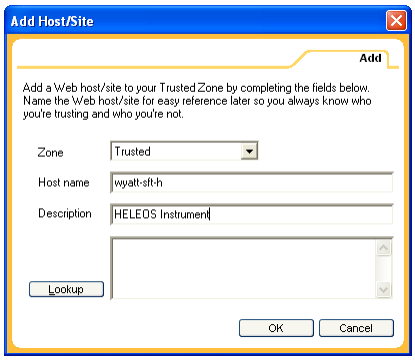
e. Press the “Apply” button to update your settings:



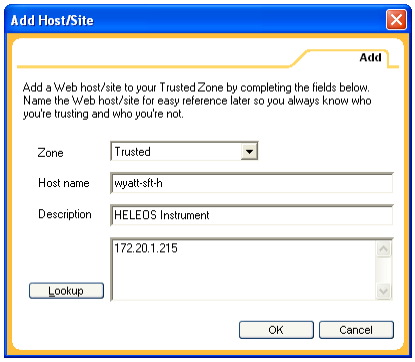
f. You are done. You should be able to access these instruments from ASTRA and the Diagnostic Manager without further problems.

12. To add an instrument, click on the “Add >>” button. This will pop up a menu asking you to choose between “Host/Site”, “IP Address”, “IP Range”, or “subnet”. In most cases, the best approach is to add the Wyatt instrument name using the “Host/Site” option. If you select the “IP Address” option, you may need to change the IP Address if the instrument receives a new IP Address via the DHCP server. So, select the “Host/Site” option.

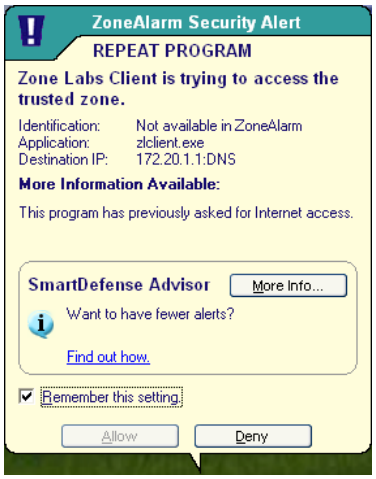
13. A dialog will be presented allowing you to add the instrument (or instruments) you need:



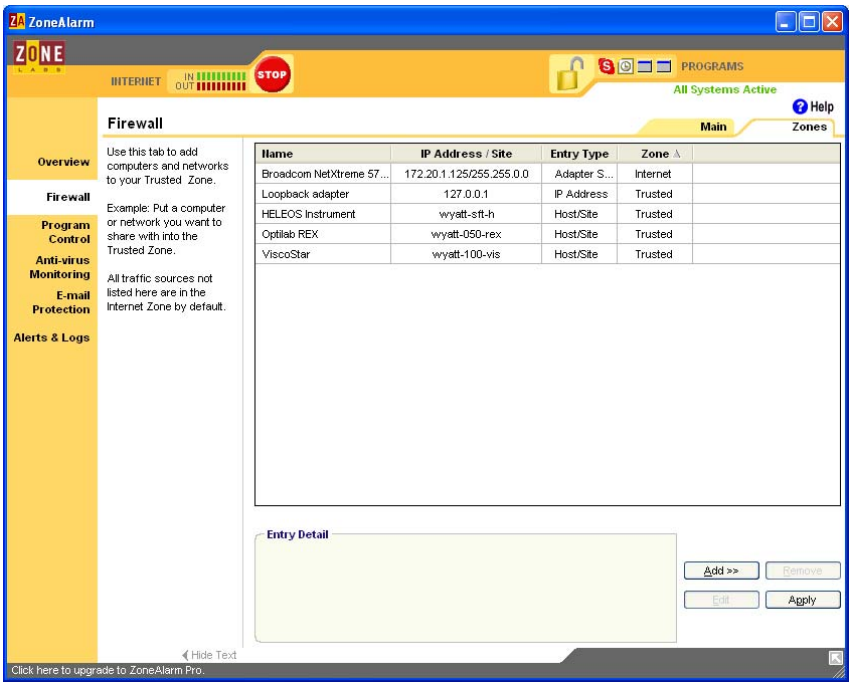
14. Press the “Lookup” button to get the current IP address for the instrument, the press the OK button.



15. Note: If ZoneAlarm requests permission to access the trusted network, select “Remember this setting” and click the “Allow” button:



16. Repeat steps 12-15 for each instrument you wish to monitor or control from this workstation.



17. Now push the “Apply” button so that these changes take effect.

18. You are done. You should be able to access these instruments from ASTRA and the Diagnostic Manager without further problems.