GENESIS32 – Running on Windows XP Service Pack 2

APPLICATIONS NOTE

December 2007

Description: Guide to making GENESIS32 work on Windows XP SP2.
OS Requirement: Win XP Pro Service Pack 2
General Requirement: The ability to configure DCOM and Windows Firewall in Windows XP Service Pack 2, GENESIS32 pre-version 8.o or earlier.

Introduction

Windows XP Service Pack 2 contains many new features. One of these features is the addition of Windows Firewall, which is installed and turned on during the installation by default.

By default, Windows Firewall stops any "unsolicited" incoming traffic, but we can allow exceptions. We can specify applications or ports as exceptions to he rules, which will then allow the applications or ports to respond to unsolicited requests.

The firewall has two main levels: the application level and the port and protocol level. The application level is where you specify which applications are able to respond to unsolicited requests. On the port and protocol level you can specify the firewall to allow or block a specific port for either TCP or UDP traffic.

In order to make GENESIS32 work, we need to make changes on both levels. This document will detail the steps necessary to make GENESIS32 work in a network environment. If GENESIS32 is going to be used in a standalone environment, you do not need to go any further.

Manually Setting up the Windows Firewall

1. Go to Start → Settings → Control Panel → Windows Firewall and you will see the Windows firewall window as show in Figure 1.

Figure 1 - Windows Firewall

2. Click on the Exceptions tab and click on the "Add Programs…" button.

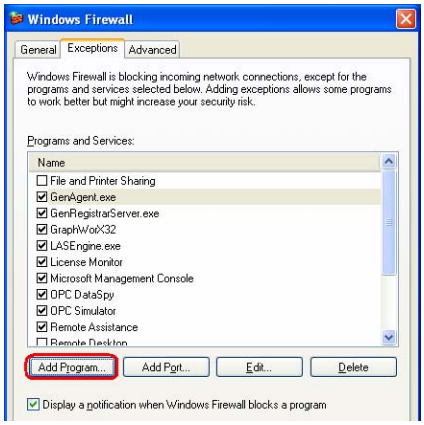

Figure 2 - Windows Firewall Exceptions

3. The Add a Program dialog will appear, you can select the programs you want to respond to unsolicited request here. Select the Microsoft Management Console, and click "OK"

Figure 3 - Add a Program to Allow Unsolicited Request Response

NOTE: Most applications on the machine would be in this list, but not all of them. In this case, you will need to browse for the executable file to add it.

4. You should see the file that you have just added in the Windows Firewall exception list. Make sure that it is also checked.
5. Repeat steps 2-4 for any applications that you want allow unsolicited response. Here is a suggested list of applications.

Table 1 - Suggested List of Applications

Name	File Path
AlarmWorX32	
AWX32Svr.exe	C:\Program Files\ICONICS\GENESIS32\Bin
DBOPCServerRuntime.exe	C:\Program Files\Common Files\ICONICS
DWXRuntime.exe	C:\Program Files\ICONICS\GENESIS32\Bin
GASEngine.exe	C:\Program Files\Common Files\ICONICS
GenAgent.exe	C:\WINDOWS\system32
GenRegistrarServer.exe	C:\Program Files\Common Files\ICONICS
GenBroker.exe	C:\Program Files\Common Files\ICONICS
GraphWorX32	
LASEngine.exe	C:\Program Files\Common Files\ICONICS

License Monitor	
OPC Simulator	
OPC DataSpy	
ScriptWorX32	
Tag Browser	
TagVerify.exe	C:\Program Files\ICONICS\GENESIS32\Bin
Microsoft Management Console	
TrendWorX32 SQL Data Logger	
TrendWorX32	
VCRWorX.exe	C:\Program Files\ICONICS\GENESIS32\Bin
Unified Data Manager	
MonitorWorX	

NOTE: If there is no file path for an application, this means that you should be able to select it directly from the application list and the name of the application as it appears in the list is given instead of the executable file name.

NOTE: You would also need to add any OPC servers and other clients that you may be using. Table 1 contains only a suggested list of applications.

6. Click on the "Add Port…" button to add the TCP port 135 that initiates DCOM communications.

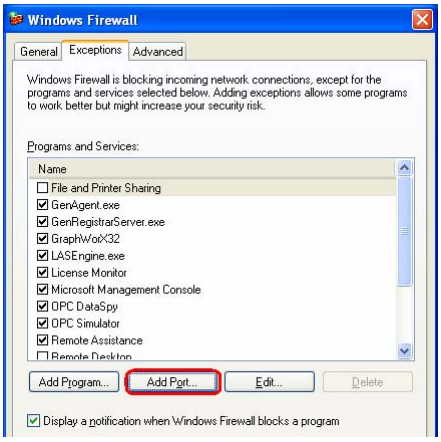

Figure 4 - Windows Firewall Add Port

7. The Add a Port dialog will appear and give port Name DCOM and the port number 135. Select TCP IP as the port type and click "OK".

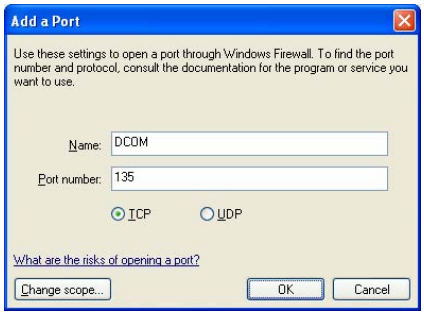

Figure 5 - Add Port 135

8. We will now add the ability to receive ping requests by going to the Advnaced tab.
9. In the ICMP section, click on the "Settings…" button.

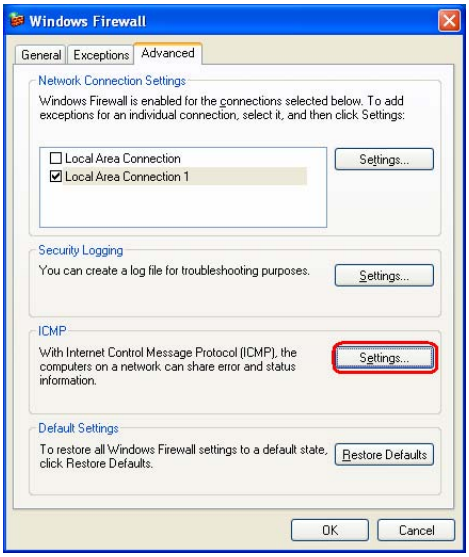

Figure 6 - Windows Firewall ICMP Settings

10. In the ICMP Settings window, check "Allow incoming echo request" and click "OK".

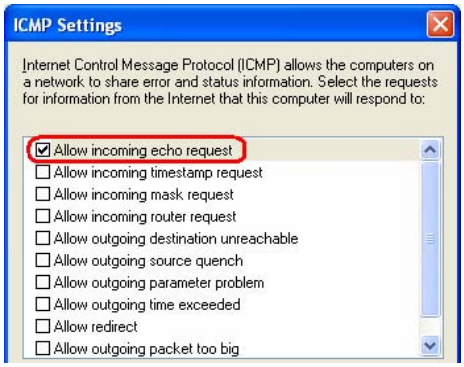

Figure 7 - ICMP Settings

11. Once you are done, you can close the Windows Firewall window.

Windows XP SP2 DCOM

In order for GENESIS32 to work over the network with DCOM, you must set permissions such that remote users can launch and/or access the OPC servers and clients on the machine. Please refer to the application note entitled *GENESIS32 - DCOM on Windows XP and Server 2003 in a Workgroup* or *GENESIS32 - DCOM on Windows XP and Server 2003 in a Domain* to setup DCOM on your computer.