



**Description:** Guide to making GENESIS32 work with Windows XP SP2.

**OS Requirement:** Windows XP Service Pack 2.

**General Requirement:** The ability to configure DCOM and the Windows Firewall in Windows XP Service Pack 2.

The goal of this Applications Note is to inform users on how to make GENESIS32 work in a networked environment with Windows XP Service Pack 2. One does not have to follow this document if GENESIS32 is going to be used in a standalone environment.

## What is the Win XP SP2 Firewall?

When one installs Service Pack 2 onto a Windows XP operating system many features are added and security enhancements made. One of these is the addition of the “**Windows Firewall**” which is installed and turned on during the installation by default.

The Windows Firewall allows traffic across the network interface when initiated locally, but by default stops any incoming “unsolicited” traffic. However, this firewall is “exception” based, meaning that we can specify applications that are exceptions to the rule and can 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 and the port and protocol level is where you can specify the firewall to allow or disallow traffic on a specific port for either TCP or UDP traffic. The importance here is that to make GENESIS32 (or any OPC client/server application) work, changes need to be made on both levels.

## Setting up the Windows Firewall

To use GENESIS32 over a network (either via OPC Direct or GenBroker) there are a set of steps you must follow in regards to the Windows Firewall. If you are using DCOM you need do some additional tasks in the DCOM configuration.

### STEP ONE:

Go to **Start → Settings → Control Panel → Windows Firewall** and you will see the dialog in **Fig.1**.



Fig. 1

We recommend that you turn on your firewall and then define your “exceptions” in the next step.

### STEP TWO:

Define your exceptions. These are just applications that you want to be able to respond to unsolicited requests from the network. The applications are all OPC servers and clients you have on your system.

Remote GENESIS32 clients first make requests to an application on the server called the GenAgent which lets the client know which OPC servers are available to it. Because of the critical “behind the scenes” role this application plays, it needs to be added as an exception. Here is a list of typical GENESIS32 applications one should add to the exceptions list:

AlarmWorX32	AWX32Svr.exe
DBOPCServerRuntime.exe	DWXRruntime.exe
GASEngine.exe	<b>GenAgent.exe</b>
GenRegistrarServer.exe	GenBroker.exe
GraphWorX32	LASEngine.exe
License Monitor	OPC Simulator
OPC DataSpy	ScriptWorX32
Tag Browser	TagVerify.exe
Microsoft Management Console	TrendWorX32 SQL Data Logger
TrendWorX32	VCRWorX.exe
Unified Data Configurator	



# GENESIS32 - With Windows XP Service Pack 2

## APPLICATIONS NOTE

August 2004



Note that you would need to add any OPC servers you are using and any other clients you may be using as well. The above list is merely a suggestion of what the typical user would need to add to their exceptions list. Microsoft Management Console was added because the DCOM configuration utility needs it.

You add applications to the exception list by going to the Exceptions tab of the Windows Firewall dialog and clicking on the **Add Program...** button

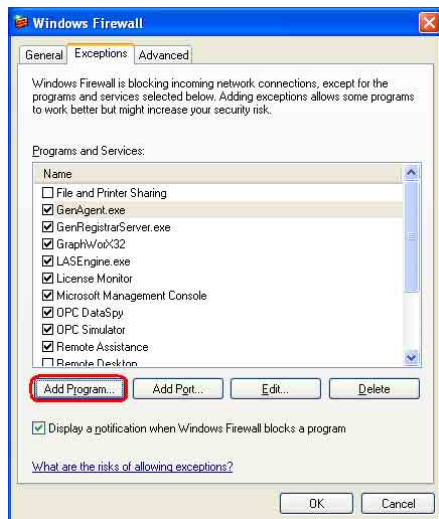


Fig. 2

In the **Add a Program** dialog, there is a listing of most applications on the machine, but note that not all of them show up on this list. Any of the applications listed in the previous table that end with .exe are applications that you need to browse for. GENESIS32 executables are located in the following directories:

```
\Program Files\ICONICS\GENESIS-32\bin
\Windows\System32
\Program Files\Common Files\ICONICS\
```

You need to add these applications one by one until you have them all.

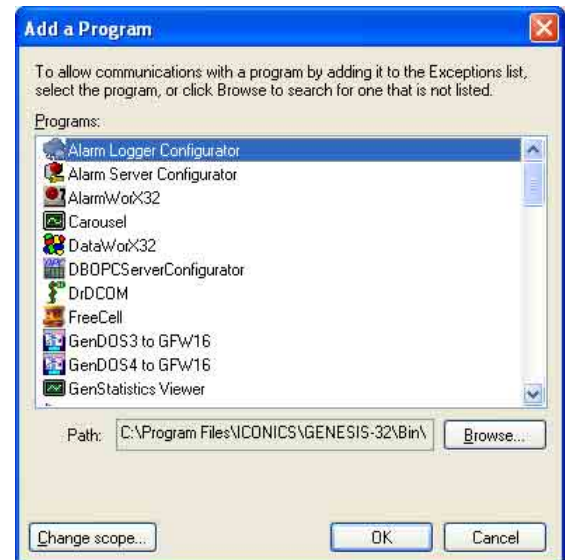


Fig. 3

### STEP THREE:

We now need to allow TCP communications on port 135 as it is needed to initiate DCOM communications, and allow for incoming echo requests. To do this you must:

1. In the **Exceptions** tab of the Windows Firewall, click on **Add Port...**

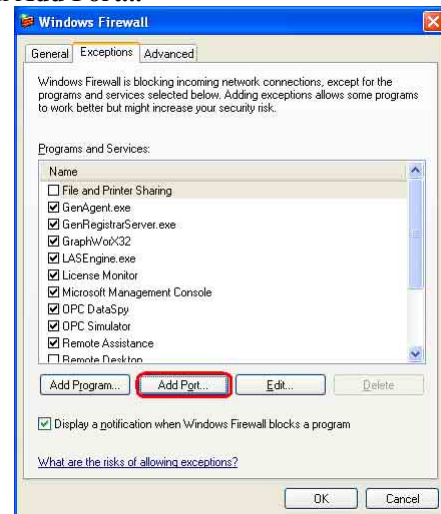


Fig. 4

2. In the **Add a Port** dialog, fill out the fields as follows:  
Name: DCOM  
Port number: 135  
Choose the TCP radio button



# GENESIS32 - With Windows XP Service Pack 2

## APPLICATIONS NOTE

August 2004

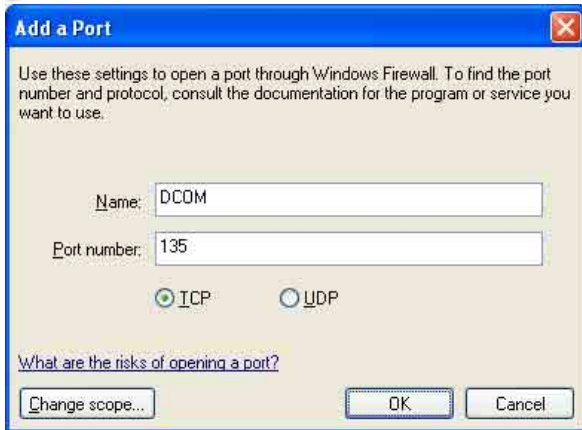


Fig. 5

3. Click on **OK** in the Add a Port dialog

### STEP FOUR:

Optionally, if you want to allow incoming ping requests (recommended), then you should do the following:

1. Click on **Settings...** under **ICMP** on the **Advanced** tab of the **Windows Firewall** dialog.

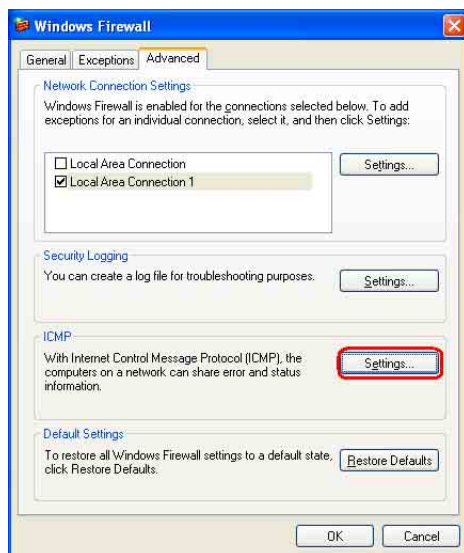


Fig. 6

2. Check the box marked **Allow incoming echo request** in the ICMP Settings dialog and click on **OK**

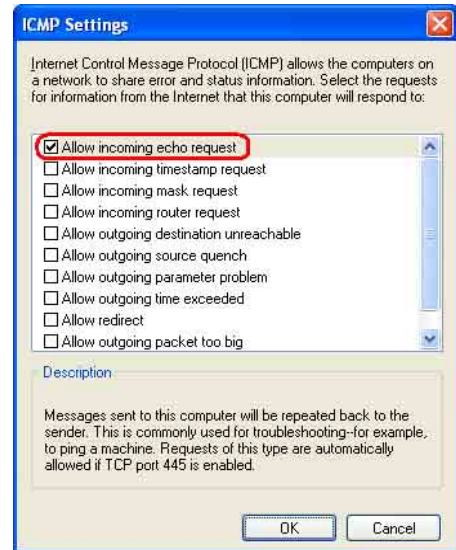


Fig. 7

Congratulations, you have now properly setup the Windows Firewall for use with GENESIS32.

## What is new with DCOM in SP2?

Service Pack 2 for Windows XP has also made some security enhancements to DCOM; two in particular need to be taken into consideration when using GENESIS32 on a network: First, the default Launch and Access permissions dialogs have been modified to allow the user to configure “limits” on the permissions given to applications using DCOM. Secondly, for each user now defined in the Launch and Access permissions, both local and remote access can be explicitly defined.

A brief background on default Launch and Access permissions in DCOM: Launch permissions define who can launch a COM based application (such as an OPC server) both over the network or locally. Access permissions define who can access that application once it has been launched. Applications can get their Launch and Access permissions from one of three places: they can use explicitly defined setting for their application, they can use the default permissions or they can set their own permissions programmatically. Because an application could set its own permissions programmatically, the explicitly defined or default settings, although set properly, may not be used and therefore the user is not able to explicitly have control over these settings.

To overcome this security flaw, Microsoft has added “limits” to the DCOM security settings from Launch and Access to limit the permissions that an application can use. This limit prevents the application from using permissions beyond what is specified in the DCOM configuration settings. By default the limits set by Service Pack 2 will not allow for OPC communications over the network.





In addition to the new permissions limits, one must now specify if the user or group specified has permissions locally or remotely (or both). In order for GENESIS32 to work over the network with DCOM one must set the permissions such that remote users can launch and/or access the OPC servers and clients on the machine.

## Setting up DCOM in Win XP SP2

This section will step you through the changes that must be made to DCOM in order to use OPC Direct communications over a network. *If you are using GenBroker over TCP, you do not have to make these changes.*

1. Go to **Start → Run** and type **DCOMCnfg** and click on **OK**.



Fig. 8

2. Click on **Component Services** under the **Console Root** to expand it.
3. Click on **Computers** under **Component Services** to expand it.
4. Right-click on **My Computer** in the pane on the right and select **Properties**.

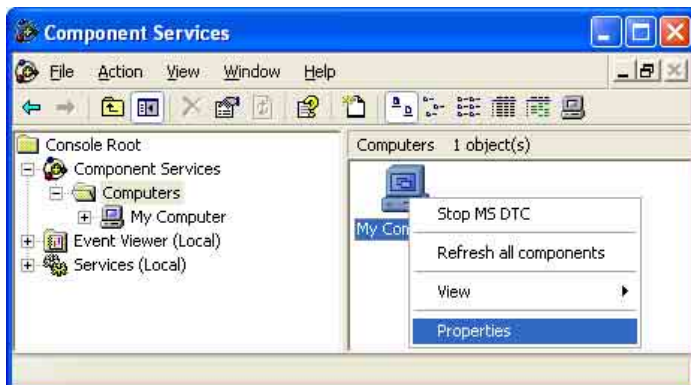


Fig. 9

5. Go to the **COM Security** tab and note these are the four permission configurations that we will have to edit, as shown in **Fig. 10**.

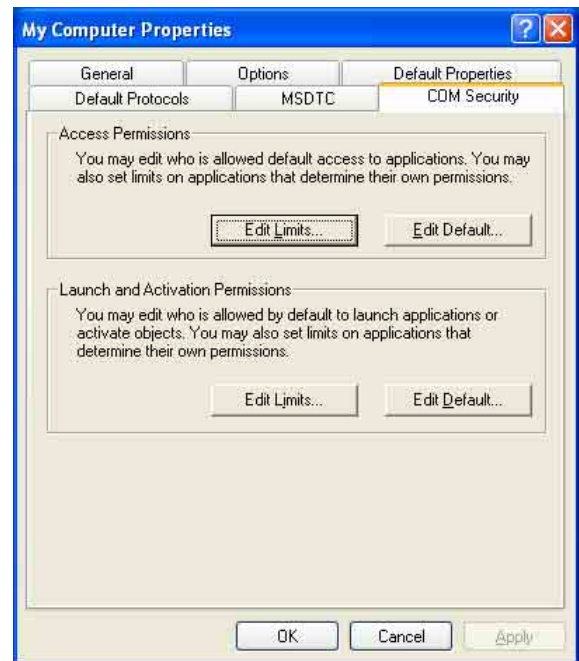


Fig. 10

6. Edit the Limits for Access and Launch
  - a. **Access Permissions – Edit Limits...**  
The default settings for this will work fine; you do not need to edit these.
  - b. **Launch and Activation Permissions – Edit Limits...**  
You need to check the remote boxes for the user labeled **Everyone** in this dialog.

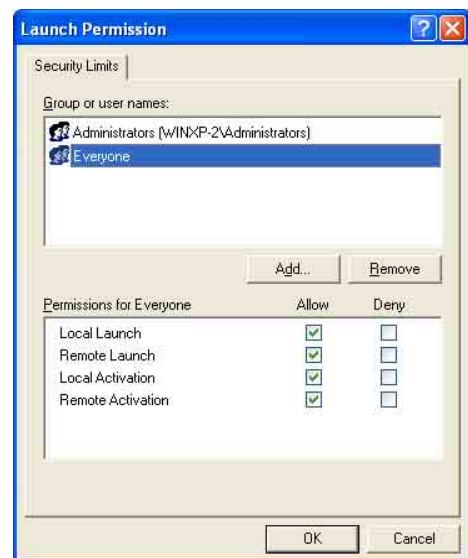


Fig. 11



7. Edit Default Permissions for Access and Launch. To do this, please setup these permissions as stated in the ICONICS Applications Note titled **GENESIS32 DCOM** for your particular Operating system.
8. Once you have the correct users specified for both launch and access permissions, make sure that both the **Local Allow** and **Remote Allow** checkboxes are both checked for all users.

Access Permissions per user:

Permissions for Everyone	Allow	Deny
Local Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig. 12

Launch and Activation permissions per user:

Permissions for Everyone	Allow	Deny
Local Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Local Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Fig. 13

Congratulations, at this point both the Windows Firewall and DCOM should be setup such that you can use GENESIS32 on your Windows XP Service Pack 2 computer with networked communications.