



Description: How to setup GENESIS components as services.

OS Requirement: Windows XP/2000/NT

General Requirement: GENESIS 7.0

GENESIS32 NT Services Support

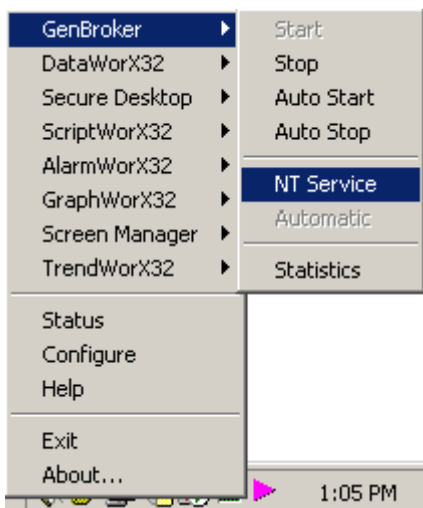
The key benefits of running a program as a service are that services start up automatically without the need for a user to log in. A good example of this is a web server; IIS on a Windows PC is a service so that no one must log in for it to start, this is especially critical in the case of a power failure.

Here is a list of GENESIS32 components that can be run as NT Services:

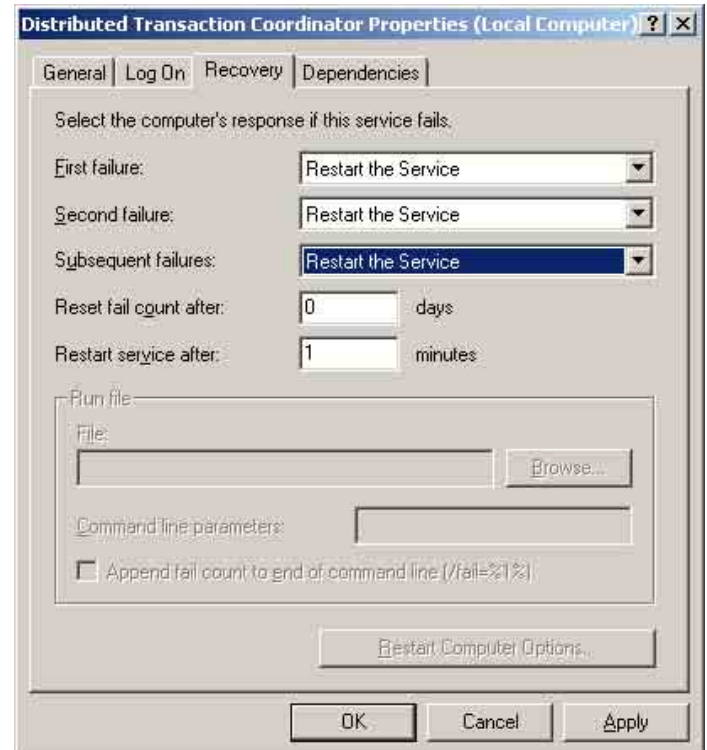
- **GenRegistrarServer** (Installed as a service by default)
- **GenBroker**
- **Secure Desktop**
- **AlarmWorX32 Server**
- **AlarmWorX32 Logger**
- **AlarmWorX32 Multimedia Server**
- **TrendWorX32 SQL Logging Server**
- **DataWorX32**

Every service has the capability of being started automatically (as in the case of IIS), or it can be started on demand (manually). If one wanted the AlarmWorX32 logger running as long as the PC was on for example, then one would elect to make the AlarmWorX32 logger an automatic service.

Turning one of the above listed components into a service and configuring it as either automatic or not is as simple as turning on GenTray and configuring them from there. All you have to do is select the component that you want to make a service (or stop being a service) from GenTray and select the option that says "NT Service".



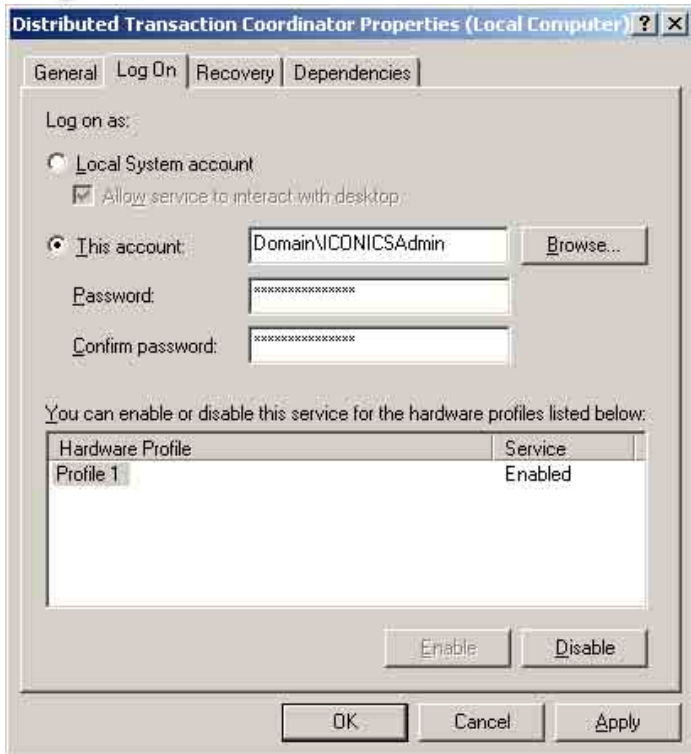
To make a service more fault tolerant, in Windows 2000 you can make a service restart itself on failure. You do this by going to Start -> Settings -> Control Panel -> Administrative Tools -> Services and then you double click on the service you want to edit. Once in the properties of the service, go to the "Recovery" tab and set the service to restart on failure.



NT Services Security Context

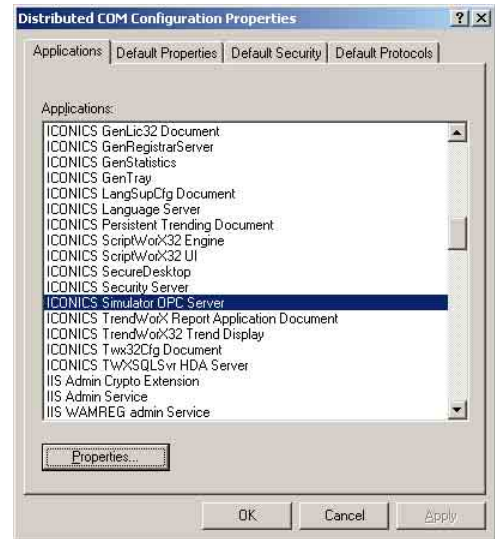
Please note that by default all services run under the security context of "System". If you need a service to run under a different security context you must go into the Services control and change who you want the service to run as. You may have to do this if you want to use the AlarmWorX32 Logger to log alarms from an AlarmWorX32 server somewhere else on the network. The logging computer's "System" account may not have permissions on a computer across the network to start the AlarmWorX32 server, so it must run under a security context that does have permission to start that server.

To change the security context of a service, you have to go Start -> Settings -> Control Panel -> Administrative Tools -> Services and then double click on the service you want to change. Once in the properties of the service, click on the "Log On" tab. In there you can specify a specific account for the Service to run under.

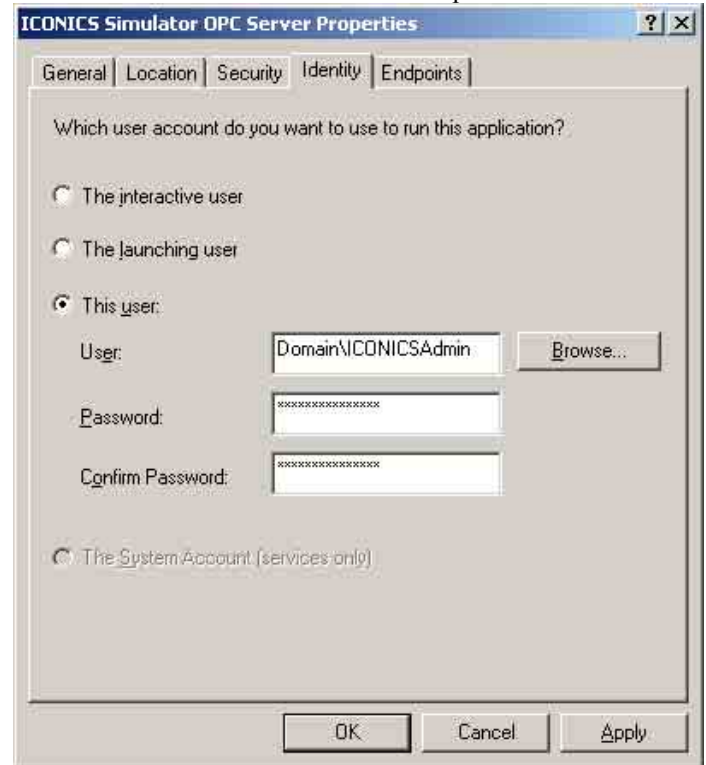


If you plan to do a lot of cross-network services it is advised that you create a network account that has permission to access and launch all necessary components and services. For example, one might create an account called "ICONICSAdmin" on their domain that has access and launch rights to all of their OPC servers and logging programs. Then in the service properties, one can specify them to run under the context of this user.

At this point you must also go to Start->Run and type DCOMCNFG [Note for DCOMCNFG on Windows XP or above, please see the AppNote entitled "GENESIS32 DCOM on Windows XP-2003 in a Domain"]. In here you must select your OPC servers from the list and go into their properties.



In the properties dialog, go to the "Identity" tab and select "This User" and fill in the information for the specific user.



By following the above steps, one can be sure that all of his servers and services have the ability to talk to one another.