

Description: Guide to set up GENESIS32 components as services

OS Requirement: Win 2000 Pro/Server, XP Pro, Server 2003

General Requirement: installation of GENESIS32 v9.x

Introduction

You can run some of the ICONICS applications as Services. A key benefit of running programs as services is 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 runs as a service where no one logs in to start it. This is especially useful in cases of a power failure.

Below is a list of GENESIS32 applications that you can run as an NT Service:

- GenRegistrarServer (Installed as a service by default)
- GenBroker
- Secure Desktop
- AlarmWorX32 Server
- AlarmWorX32 Logger
- AlarmWorX32 Multimedia Server
- TrendWorX32 SQL Logging Server
- DataWorX32
- ScriptWorX2006

Every service has the capability of being started automatically or manually. If you want the AlarmWorX32 logger to run as long as the PC is on, then you would make the AlarmWorX32 Logger run as an automatic service.

Setting Application to Run as a Service

1. Start GenTray by going to Start → Programs → ICONICS Tools → GENESIS32 Tray
2. Once GenTray Starts, you would see a pink triangle in your system tray near your clock
3. Click on the pink triangle, select the application that you would like to run as services and select NT Service.
4. Once you have selected the particular application to run as a service, the Automatic option becomes available. You can select this as well if you would like the service to start automatically at system startup.

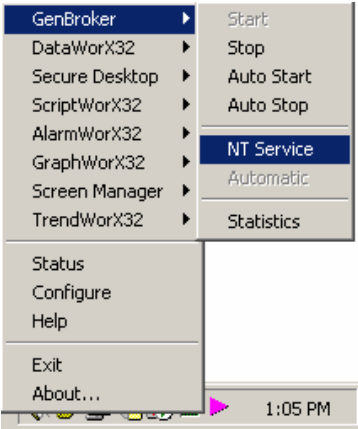


Figure 1 - NT Service from GenTray

5. To make a service more fault-tolerant, in Windows 2000, you can make a service restart itself on failure. Go to Start → Settings → Control Panel → Administrative Tools → Services
6. Double-click on the service you want to edit.
7. Once in the properties of the service, go to the Recovery tab and set the service to restart on failure.

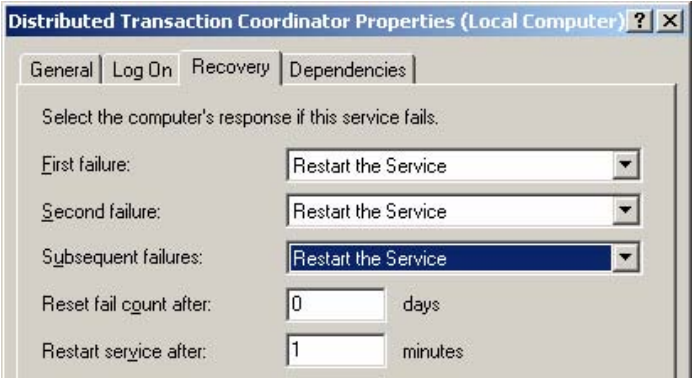


Figure 2 - Recovery Tab

NT Services Security Context

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 Panel and change who you want the service to run as. You may have to do this if you want to use 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 remote computer to start the AlarmWorX32 server. Therefore, the logger must be running under a security context that has permission to start the server.

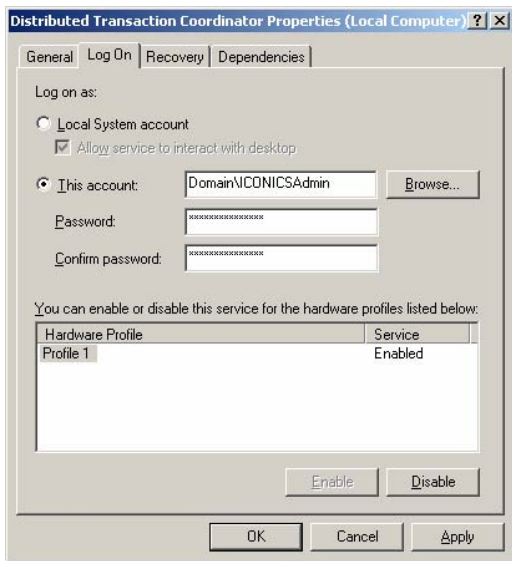


Figure 3 - Log on Tab

If you plan to do a lot of cross-network services, we advise 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 in “dcomcnfg”. In here, you must select your OPC servers from the list and go into their properties.

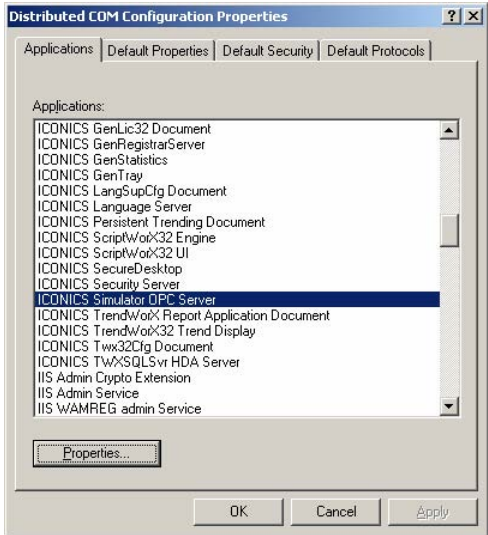


Figure 4 - DCOM Configuration

In the properties dialog, go to the Identity tab and select “This User” and fill in the information for the specific user. Once you are done editing DCOM, you should, as always, restart your computer.