GENESIS32 – Running Applications in an Unattended Environment

APPLICATIONS NOTE

October 2013

Description: Guide to setting up ICONICS Applications to run in an unattended environment (running as services).
OS Requirement: Win 2000, XP Pro, Server 2003, Vista, Server 2008, Windows 7
General Requirement: Familiarity with how to create a user in windows, windows services, and DCOM

Introduction

As the IT department gets more involved with plant floor operations, they sometimes require the servers that monitor plant operations sit in a locked server room. These servers must then be able to run all applications as required on system restart without console login.

One way of doing this is to run your 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 or the situation mentioned above.

Below is a list of GENESIS32 applications that you can run as an NT Service in version 9:

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

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

This document will walk you through the general steps on how to set your ICONICS applications to run as a service.

The ICONICS Application Setup Utility

Because we understand the need to run applications as services, we have created the Application Setup Utility, which runs by default during installation.

The first time the utility runs, it will try to create a user called the **ICONICS_User** in the Administrators group of the local machine. You can change the name of the user or the group that it belongs to in the dialog. You will also have to give this user a password. In order to run ICONICS applications as a service with this user, the user must have a password. Once you are done setting up the user and its password, simply click on OK to let the utility run.

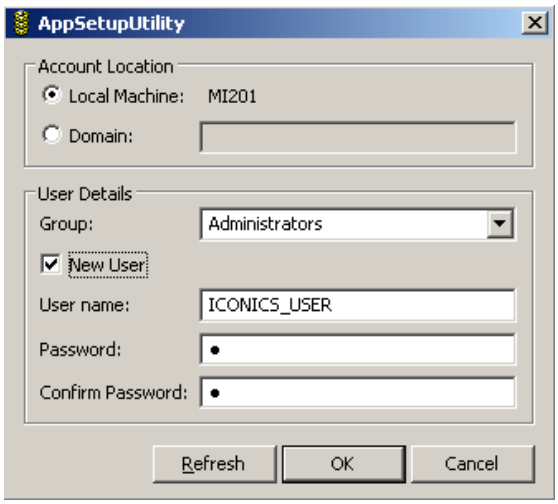

Figure 1 - Application Setup Utility

This utility will take care of setting up DCOM permissions and make the available ICONICS applications run as a service. Since it is changing DCOM settings, you will have to restart the machine after you run it.

If at any point, you need to change the password of the user or change the user altogether, you can use this utility to reset all DCOM and service settings for you.

Once you run the utility, you should go into your windows services manager and turn those services that you want to start up when the computer starts to run as an automatic service.

> **NOTE:** After you run the utility and reboot machine, some applications in the above list may not show up in your windows services manager. You can setup those services by following the below steps.

Creating an Account to Run Services

In the event that you do not want to use our Application Setup Utility, you can follow the procedure below to set up your application and services manually.

First, you will need to create/use an administrative user to run the services. By having the same user running all ICONICS applications, it will minimize the amount of DCOM issue, which may render the system in a non-working state after

changing the applications to run as a service. This will also make it simpler in maintaining your system as well as users.

1. On your Desktop, you can right-click on the "My Computer" icon and select Manage.
2. In the Computer Management Console, expand System Tools → Local Users and Groups → Users.
3. Right-click on Users and select New User.
4. Create a user called IconicsApp and give it a password. Set the expatriation date of the password to be never.

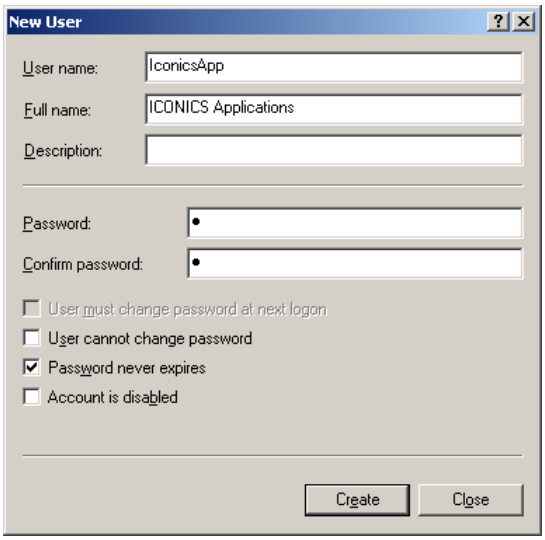

Figure 2 - New User Dialog

5. Click on the "Create" button and click on the "Close" button to exit the dialog.
6. In the Computer Management console, you should find the IconicsApp user. Double-click on the user to bring up its properties.
7. Select the "Members Of" tab and remove the "Users" group already listed for the user.
8. Click on the add button and add the "Administrators" Group. This will include administrative privilege for the IconicsApp user.

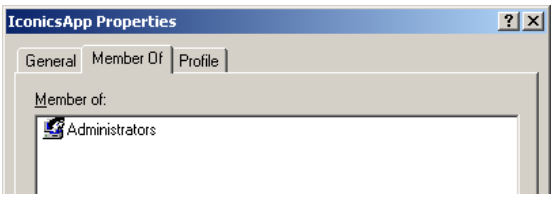

Figure 3 - IconicsApp User Properties Dialog

9. Click "OK" to save the changes and exit the Computer Management Console.

Setting Applications 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.

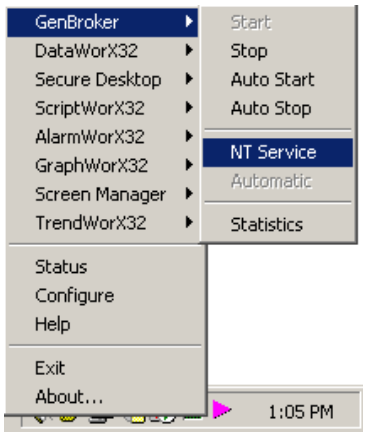

Figure 4 - NT Service from GenTray

5. To make a service more fault-tolerant, 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.

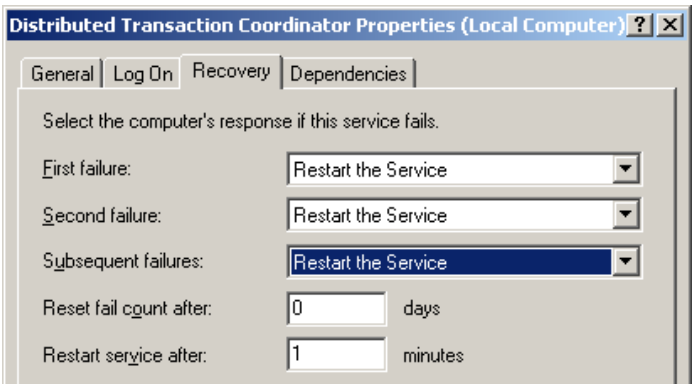

Figure 5 - Recovery Tab

NT Services Security Context

By default, all services run under the security context of "System". You may have to do this if, for example, you want to use AlarmWorx32 Logger to log alarms from a remote AlarmWorX32 server 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/access the server.

This is true even for applications on the same system. If, for example, your alarm server is running as UserA and your alarm logger is running as UserB, you may not be able to log alarms if the alarm server does not allow UserB to communicate to it to get information.

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, you may create a user called "ICONICSAdmin" on your domain that has access and launch rights to all of your OPC servers and logging programs. Then, in the service properties, specify the services to run under the context of this domain user.

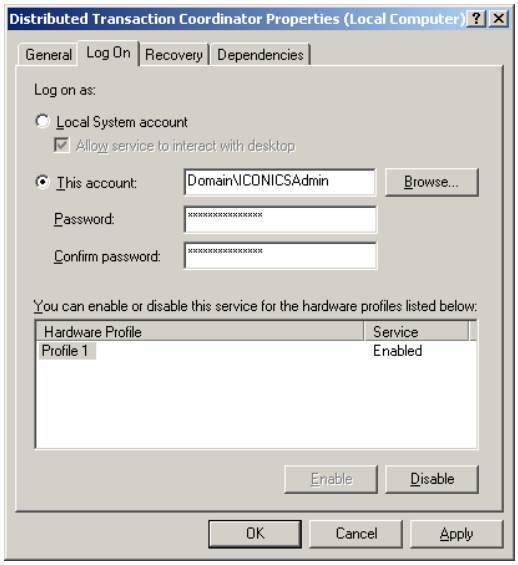

Figure 6 - Log on Tab

In this section, we will set the IconicsApp user that we've created earlier to run the ICONICS applications that you are interested. If you want to use a domain user, you can follow the same steps; simply browse for the domain user instead of the local user we've created in the previous section.

1. Go t o Start → Settings → Control Panel → Administrative Tools → Services to open the Services Manager
2. Scroll down the list to find the ICONICS services. Select the first service (ICONICS AlarmWorX32 Logger) and double-click on it to bring up its properties.

   NOTE: Since we will need to run each application that you plan on using as a service, you can pick which application you want to start with. You may use the list in the Introduction section as guide.

3. Select the "Log On" tab and choose "This account" in the radio buttons.
4. Click on the "Browse" button and select the user you would like to run the ICONICS applications. If you are using our example, the user would be IconicsApp.
5. Type in the password for the user and click on "Apply" to save the settings.

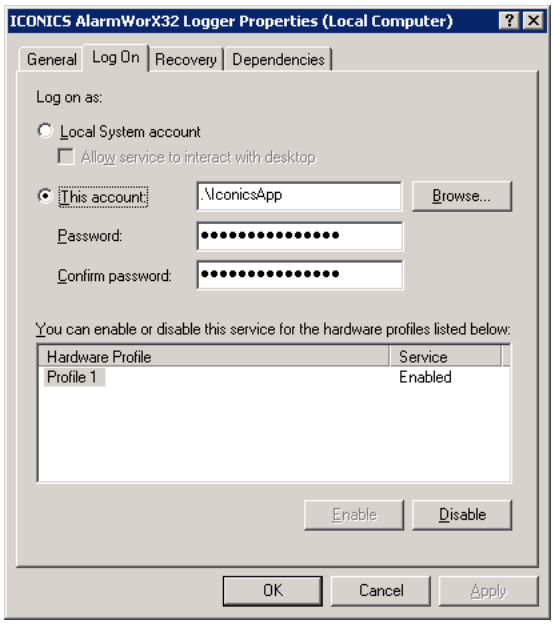

Figure 7 - Services Properties: Log On Tab

6. Repeat the above steps for all other ICONICS services in the Services Manager.

   NOTE: Since the License Server was installed as a service to run as the system account, the permissions has been set for this service to work with most users on the computer; we advice that you leave the user to run this service as the Local System User.

Configuring DCOM

We published many applications notes in an effort to help you configure DCOM on different systems and different networks, if you are unfamiliar with DCOM, please read those applications notes first and setup your computer as recommended by those documents. We will not go through DCOM here as detailed as those documents have described. If you find yourself lost, please

refer to the specific DCOM application note that applies to your environment.

1. Add the user you have created previously (IconicsApp) into the Default COM Security. If you are using a Domain User, you should add the Domain User. Depending on the version of Windows, you may also have to add the user in "Edit Limits"
2. Your finished configuration should look similar to Figure 8.

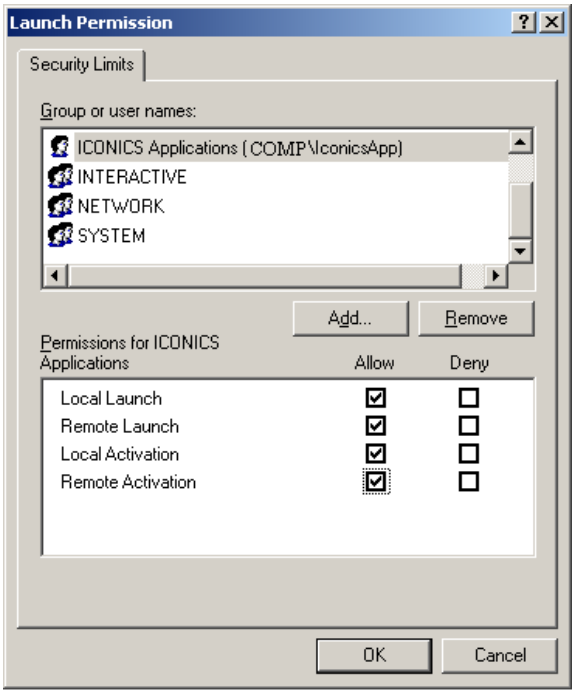

Figure 8 - Default Launch Limit Access

NOTE: You may not need all of the users listed here or in the DCOM application note. However, we advice that during development that you open your security to get the programs working. From this point, you can tighten security as needed for production.

3. Drill down to the specific application's DCOM setting. We will need to add the user running the services to a few ICONICS applications and your OPC servers. Below is a list of applications that we will need to go through.

   - ICONICS DBOPCServer
   - ICONICS MonitorWorX
   - ICONICS Security Server
   - ICONICS Simulator OPC Server
   - ICONICS GenRegistrarServer

NOTE: These DCOM settings should be considered also for any other OPC server that is being used by the project. Setting the Identity to "This user" in Step 6 makes sure the OPC server can be run when no interactive user is logged in (unattended environment) and prevents from launching multiple instances of the same OPC server.

4. In the Properties for each of the applications, select the "Security" tab, select "Use Default" for both the Launch and Activation Permissions and Access Permissions.

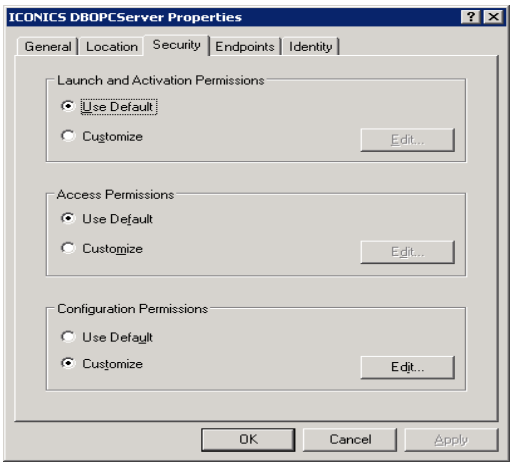

Figure 9 - Individual Applications DCOM Properties: Security Tab

NOTE: If the applications weren't already set to use Default, you may want to take a look at the users that were in the Custom Security and make a note of the users that are not included by setting it to run with Default permission. If you find permission to be too restrictive after setting this, you may want to include the omitted users in the Default security section.

5. For each of the applications that you have set to run as the specific user, go into the DCOM setting for that service and select the "Identity" Tab.
6. Walk through the same procedure as we did before, setting each identity to be the Specific user.

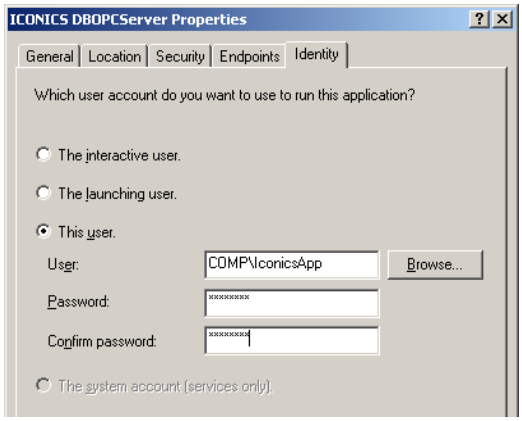

Figure 10 - Individual Applications DCOM Properties: Identity Tab

7. Since we changed DCOM settings, we now must restart the computer.
8. Once the computer starts, check that all your services are running OK and things are working as normal. You are now ready to lock the system in a server room.