

Partnership Courtyard, The Ramparts,

Dundalk, Ireland

Version 6.4.1.2

March 31, 2017

www.measuresoft.com

+353 42 933 2399

This document is the copyright of Measuresoft and may not be modified, copied or distributed in any form whatsoever without the prior permission of Measuresoft.

*System Integrator Guide*

1. PRODUCT RENAME 5

2. MAIN MENU BITMAP 8

3. NETSENTINEL INSTALLATION 10

4. NETWORK DDE 12

5. MASKING USING SECURITY 15

5.1. GWFR1 Rig-Specific Directory. 15

6. MASKING USING ENVIRONMENT VARIABLES 19

7. REMOTE ALARM PRINTER 21

8. SERVER NOT APPEARING IN NETWORK BROWSER 21

9. TRENDS COMMAND LINE PARAMETERS 22

10. PRINTING MONITORS/TRENDS FROM COMMAND LINE 23

11. EMAIL ON ALARM 24

12. ALARM SYSTEM MODIFICATIONS 26

12.1. Suppression of Alarm and Warning Reporting 26

12.2. Warnings as Alarms 26

12.3. Driving a Digital for Active Alarms 26

12.4. Driving a Digital for Active Unacknowledged Alarms 28

13. RESTRICTING WINDOWS NT 4.0 UI 29

14. ENABLE NETWORK BROWSER WITH AN EDIT BOX 31

15. WRITING TO CHANNELS FROM EXCEL MACROS 32

16. TRENDS RENAMING LOG FILES 33

17. Main menu command line parameters 34

18. Client logger enable Registry Key. 35

19. Detecting Time Change 36

20. Modbus System Modifications 37

20.1. Modbus Register Fragmentation 37

20.2. Modbus MAX Registers Setting 37

20.3. Modbus Transmit Delay Setting 37

20.4. Modbus Tries Setting 38

20.5. Modbus StopBits Setting 38

20.6. Switching Debugging On 38

20.7. Selecting the Debug Type 38

20.8. Switching On the Debug Counts 39

20.9. Adding Multiple Modbus slave Devices 40

21. Communication resources sharing between annunciators and RAS (RRAS) 41

22. Disabling Monitor Locking in Configurable Monitor 45

23. Disabling Value Entry Handles 45

24. Disabling Prompt to Save on exit 45

25. Log by Tag 45

26. Alarm Annunciator Debugging 45

27. Data Exchange Options 45

28. Datascan Timeout 46

29. Default WITS External Driver 46

30. Auto Open Configuration When Service Starts 46

31. Multiple Calculators 46

32. Data Export Strings 46

33. Running Processors from Desktop/Using Network DDE in Data Exchange 47

34. Rainbow Sentinel Driver Error Codes 48

35. Adding SCADA Product OPC Tags to InTouch 50

35.1. Prerequisites 50

35.2. Procedure 50

35.3. Configure the OPCLink Application. 51

35.4. Configure a new InTouch Access Name 51

35.5. Configure a new InTouch Tag: 52

35.6. Configure a window that uses the InTouch Tag: 54

36. Configuring Excel RTD Network Settings 57

37. Running Clients on Windows 2000 Workgroups 67

38. Configuring an SQL Server to Publish Logged Data 67

39. Configuring an SQL Server to Subscribe to a Published Database 74

40. Configuring a Logger to Replicate Data 79

41. Logging to a Remote Database over HTTP 83

42. Exposing SQL Server Logged data to Web Pages via XML 88

43. Select First Available Server 89

44. Disabling Purge of Configuration Sub Directories 89

45. Enabling Debug for the PID Controller 89

45.1. Switching Debugging On 89

45.2. Selecting the Debug Type 89

46. Adding directories on a Save 90

47. Adding registry entries on a setup 90

48. Storing Digital States as Text in Database Logs 90

49. Storing DATATIME in UTC format in Database Logs 90

# PRODUCT RENAME

NOTE: THE NEW PRODUCT NAME MUST BE 12 CHARACTERS OR LESS INCLUDING SPACES WHICH ARE PERMITTED.

If the SCADA product has not already been been installed.

* Edit the product.ini file on disk1 of the Server and/or client disk set and set the entry

[General]

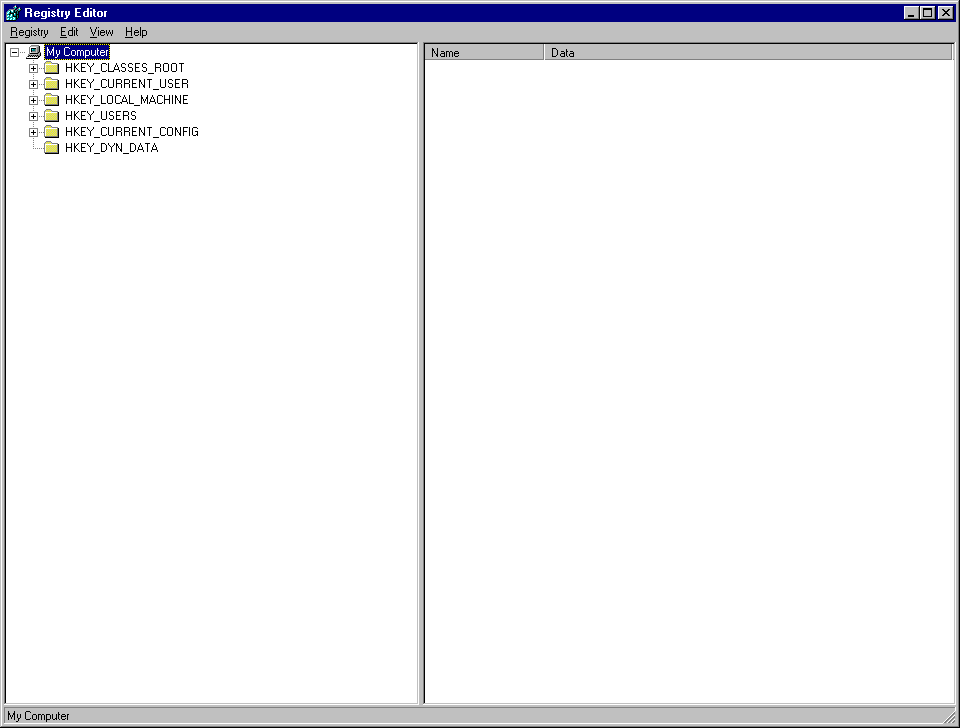
PRODUCT\_NAME=

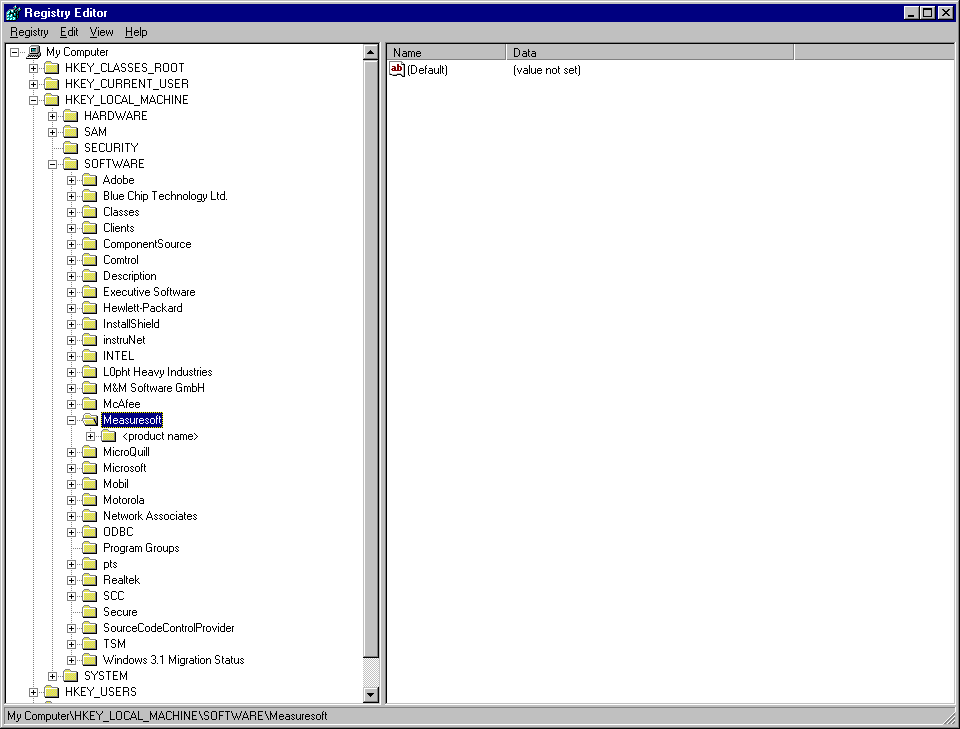
to

[General]

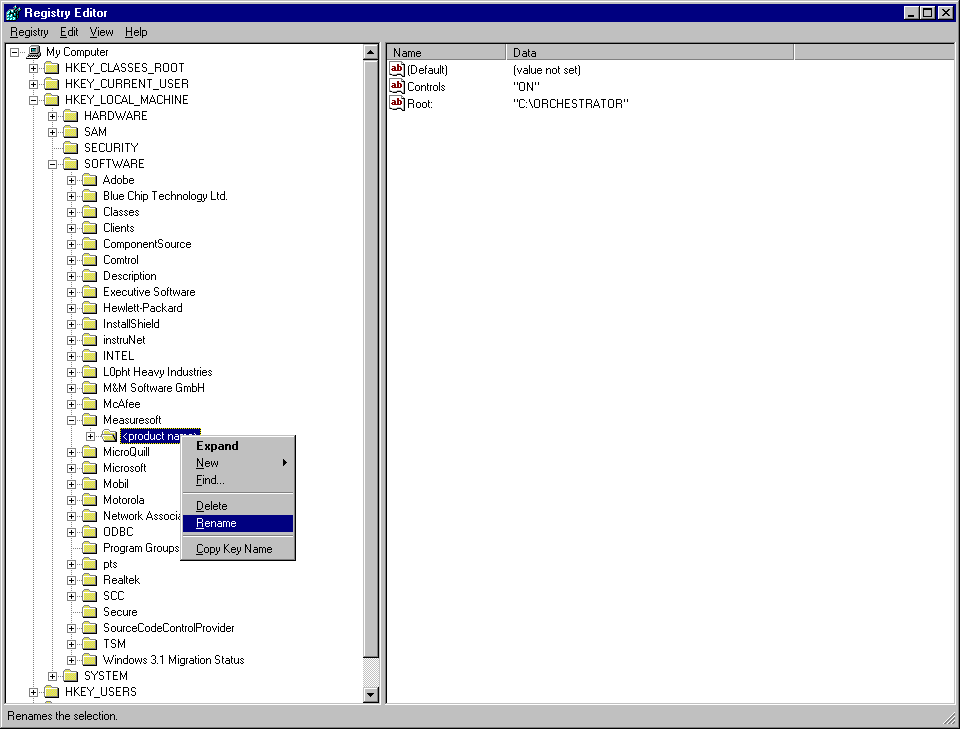
PRODUCT\_NAME=<product name>

If the SCADA product has already been installed.

* Click on the “Start” button and select the “Run…” option.
* In the “Run” dialog that appears, type “regedit” into the “Open” field and click “OK”
* The Registry Editor will appear on screen and will look something like the following:
* Expand the HKEY\_LOCAL\_MACHINE branch (by clicking on the small plus (+) sign beside the text. From the new branch, expand the SOFTWARE branch and then expand the MEASURESOFT branch.
* Select the MEASURESOFT branch (by clicking on the text). The keys associated with this branch will appear in the right hand pane of the window. It should appear something like the following:



* Click the right mouse button on a blank portion of the right hand pane. A menu will appear.



* Select New from the menu and then String Value from the subsequent menu which appears.
* Replace the text “New Value #1” which appears by default with the text “ProductName” and then hit the enter key.
* Hit the Enter key a second time and an “Edit String” dialog will appear.
* In the “Value data” field, type the text which represents the name you want the product to appear as and click “OK”
* Select the <product name> branch (by clicking on the text) with the right mouse button and select rename
* Select the <product name> branch (by clicking on the text) with the right mouse button and select rename
* Rename the <product name> branch to the desired name
* You may also wish to rename program groups and shortcuts.

# MAIN MENU BITMAP

If the product has not been installed:

Name the bitmap you wish to use Product.bmp and place it into Disk 1 of the installation series. This automatically creates a system environment variable Orc\_Bitmap with the correct path to the bitmap.

Upon restart at the end of the installation, the bitmap will be displayed correctly.

If the Scada product has already been installed:

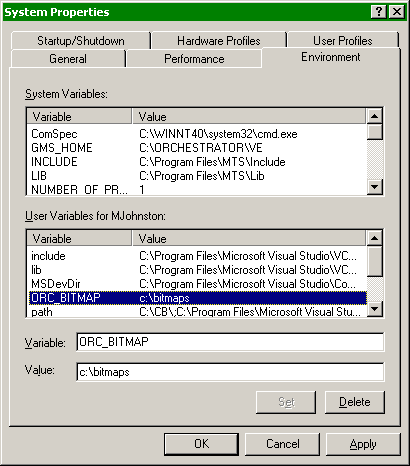
Two options;

1. Define an ORC\_BITMAP environment variable.

Rename the bitmap you wish to use to Product.bmp

Then go to start menu\setting\control panel\system and selecting the environment tab.

Once there enter the following string into the variable Name ORC\_BITMAP, and in the path name enter the location of the Product.bmp



1. Implant a bitmap into the Scada bin directory

.

Name the bitmap you intend to use to Orchest.bmp and place it into the bin directory of your scada product.

# NETSENTINEL INSTALLATION

The following procedures assume that your network is set up using NetBEUI and/or TCP/IP protocols and is functioning properly.

The Security Server is the machine which has the Net Sentinel key installed in its parallel port and is running the Net Sentinel service. Installation procedures for both follow.

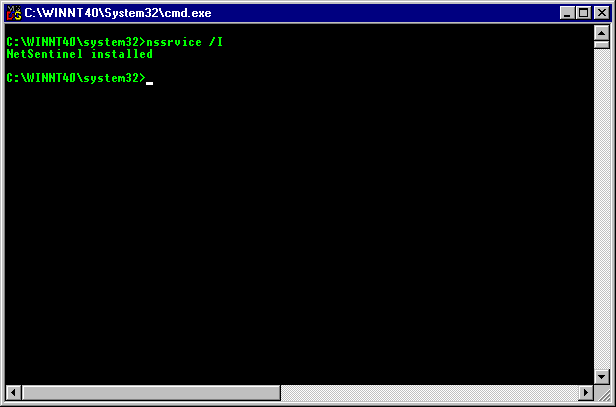
**Installation procedure for Net Sentinel Key and Drivers**

**Net Sentinel-C Key**

The machine to be the security server must have an Net Sentinel-C key installed in one of its parallel ports. If this machine is also to act as an RTE Server, then a Sentinel SuperPro key must also be installed. In this case, it is recommended to insert the Net Sentinel-C key directly into the machine’s parallel port, and the Sentinel SuperPro key into the back of the Net Sentinel-C key. The Security Server machine must be running Windows NT v3.51 or later.

**Net Sentinel Drivers (Server only)**

To install the software insert the Rainbow Sentinel Drivers Disk into drive A: on the machine to act as the security server and then run A:\SETUP.exe. This runs the Sentinel Drivers Setup program. Click on the Functions menu and then on Install Sentinel Driver. Click OK on the following dialog box (the default path to the drivers should work). Once completed, the message “Drivers Installed, Restart your system” will appear. Before restarting your system, a file called nssrvice.exe must be manually copied from the Rainbow Sentinel Drivers Disk to the Windows System32 directory. When this is done, open an MS-DOS command window. Change to the Windows System32 directory and type the following:



NSSRVICE /I

If the command is successful, you will get the message “NetSentinel Installed”.

Once this is done, you must shut down and restart your computer. The NetSentinel drivers and service are now installed on your machine and it is ready to act as the Client Security Server.

**On each client machine including the following registry string value must be set to ON. HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<ProductName>\CheckNetSentinel**

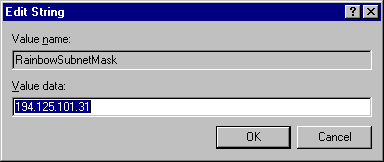
**NetSentinel Support for RAS**

There are up to 4 computers that can participate in a client connection to a server using RAS and NetSentinel. They are

1. The client computer which can be Windows 95, Windows NT 3.51 with Service Pack 5 or Windows NT 4.0 with Service Pack 3. Netbeui and TCP/IP must be installed and enabled on the RAS connection.
2. The RAS server which can be Windows NT 3.51 with Service Pack 5 or Windows NT 4.0 with Service Pack 3. Netbeui and TCP/IP must be installed and enabled on the RAS connection.
3. The Netsentinel Security server which can be Windows NT 3.51 with Service Pack 5 or Windows NT 4.0 with Service Pack 3. Netbeui and TCP/IP must be installed.
4. The Orchestrator server which can be Windows NT 3.51 without service packs or Windows NT 4.0 without service packs.

Windows NT will not allow the remote RAS client to interrogate each computer on the network to see if it is a NetSentinel security server. Therefore the RAS client must be configured to identify the TCP/IP address of the NetSentinel server. If the RAS server and the NetSentinel Security server are the same machine, the RAS server must be configured to assign remote TCP/IP client addresses from a static pool. The address of the NetSentinel Security server is the first address in this pool. If the RAS server and the NetSentinel Security server are not the same machine, the address of the NetSentinel Security server is the TCP/IP address of the primary network card in the NetSentinel server.

When the TCP/IP address of the NetSentinel Security server has been determined, the REG\_SZ registry key HKEY\_LOCAL\_MACHINE\Software\Measuresoft\Orchestrator\RainbowSubnetMask must be configured on the client computer with the TCP-IP address of the NetSentinel security server e.g.



# NETWORK DDE

In order for to act as a Server for Network DDE from other machines, DDE Shares must be setup in the context of the service

***To Setup Network DDE for Orchestrator***

1. The ***Network DDE and Network DSDM*** services (in the Control Panel) should be configured as follows :

Start-up Type : Automatic

Log On As : Allow Service to Interact with Desktop

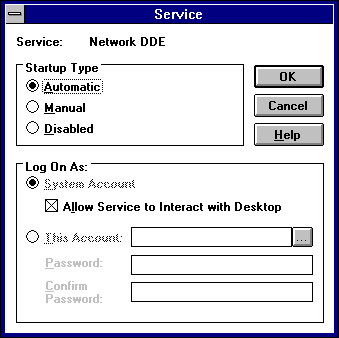
To do this : Choose Control Panel. The following appears :



Choose Services and the next dialog appears :



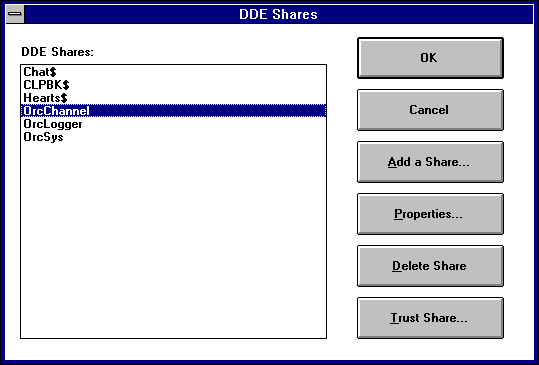
Double Click on each of the 2 services highlighted above and the following dialog appears :



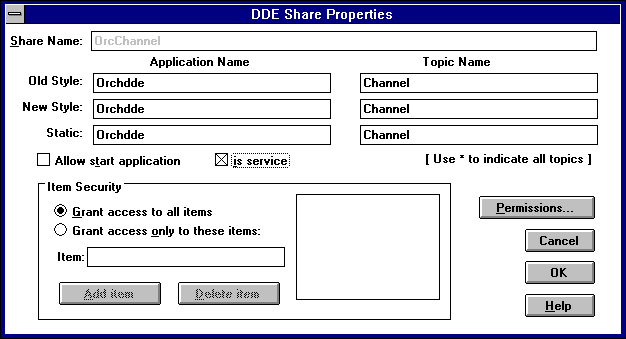
2. Run **<drive>\WINNT\SYSTEM32\DDESHARE.EXE**.

Select the ***DDE Shares...*** command from the ***Shares*** menu.

The following appears :



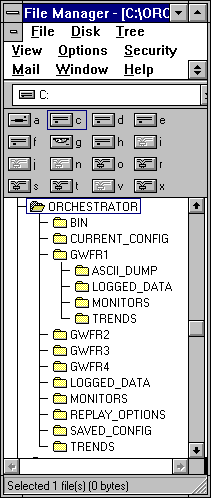
Select the required topic(s) and select the Properties button.



In this Share Properties dialog click on ***“is a service”.*** Then select OK

Network DDE is ready to operate

# MASKING USING SECURITY



**Rig-Specific Directory Structure .**

**(using GWFR1 as an example)**

Executables Directory.

Current Configuration Directory Structure.

GWFR1 Rig-Specific Directory.

GWFR1 Default Data Export Directory.

GWFR1 Default Loggers Directory.

GWFR1 Default Monitors Directory.

GWFR1 Default Trends Directory.

## 5.1. GWFR1 Rig-Specific Directory.

1. **GWFR1 Default Data Export Output Directory.**

This directory was created as a temporary solution as BP ultimately want to export directly to their UNIX servers.This is a Macintosh mountable volume on the server which is set up as the users home directory in User Manager for Domains. The very first time the Data Export utility is run the users home directory is saved along with other configuration options in the **Orchestrator\Replay\_Options** directory on the client machine. To change were Data Export defaults its output files to you must you must delete the user configuration file **GWFR1\_dataexport** in this directory and then change the users home directory. The home directory for a GWFR1 user is : \\XTP4242\ORCHESTRATOR\GWFR1\ASCII\_DUMP

1. **GWFR1 Default Loggers Directory.**

This is the parent directory of all GWFR1 loggers. This will contain sub-directories pertaining to each logger name.

1. **GWFR1 Default Monitors Directory.**

All GWFR1 Configurable Monitor documents (.orm) are stored here.

1. **GWFR1 Default Trends Directory.**

All GWFR1 Trends documents (.ort) are stored here.

The Orchestrator clients navigate to all these directories using the following environment variables :

**ORC\_LOGGED\_DATA** = \\XTP4242\ORCHESTRATOR\GWFR1\LOGGED\_DATA

**ORC\_CMONITORS** = \\XTP4242\ORCHESTRATOR\GWFR1\CMONITORS

**ORC\_TRENDS** = \\XTP4242\ORCHESTRATOR\GWFR1\TRENDS

These environment variables are set using the System icon in the Control Panel. These are then saved off into a Mandatory User Profile using the User Profile Editor. The User Manager for Domains is then used to assign the profile to a user.

The following Mandatory User Profile files have been set up on the Orchestrator server, the Primary Domain Controller and the Backup Domain Controller in the <drive>\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS directory :

GWFR1.MAN

GWFR2.MAN

GWFR3.MAN

GWFR4.MAN

Rig masking permissions are directory based and are as follows :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **GWFR1** | **GWFR2** | **GWFR3** | **GWFR4** | **GASM** | **Administrator** |
| **ALARM** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **CALC** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **CALC2** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **CALC3** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **CALC4** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **CALC5** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **DATASCAN\_1** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **DATASCAN\_2** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **DATASCAN\_3** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **DATASCAN\_4** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **HISTORY** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **LOGGERS** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **NOVO\_1** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **NOVO\_2** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **NOVO\_3** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **NOVO\_4** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **USERA** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **USERD** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **GWFR1** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **GWFR2** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **GWFR3** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **GWFR4** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **LOGGED\_DATA** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **MONITORS** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **REPLAY\_OPTIONS** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **SAVED\_CONFIG** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **SAVED\_VALUES** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |
| **TRENDS** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** | **ALL** |

**R** = Read

**All** = Full Control

Logger permissions are set in the directory **Orchestrator\current\_config\loggers** are file based rather than directory based and are as follows :

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **GWFR1** | **GWFR2** | **GWFR3** | **GWFR4** | **GASM** | **Administrator** |
| **standard\_1** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_2** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_3** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_4** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_5** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_6** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_7** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_8** | **ALL** | **R** | **R** | **R** | **ALL** | **ALL** |
| **standard\_9** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_10** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_11** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_12** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_13** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_14** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_15** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_16** | **R** | **ALL** | **R** | **R** | **ALL** | **ALL** |
| **standard\_17** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_18** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_19** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_20** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_21** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_22** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_23** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_24** | **R** | **R** | **ALL** | **R** | **ALL** | **ALL** |
| **standard\_25** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_26** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_27** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_28** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_29** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_30** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_31** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |
| **standard\_32** | **R** | **R** | **R** | **ALL** | **ALL** | **ALL** |

**R** = Read

**All** = Full Control

# MASKING USING ENVIRONMENT VARIABLES

Orchestrator uses environment variables to navigate/browse to logger directories, trend files and monitor files. To achive the type of rig masking that BP wanted we had to create rig-specific directories for loggers, monitors, trends and data export. As you know there are 4 rigs in use. The directory structure for rig 1 is explained in the document entitled “**Orchestrator Rig-Specific Directory Structure**”. The settings would be the same for the other 3 rigs except for the rig number.

In order to ensure that these settings would be the same for all users we had to create Global User Groups and assign user profiles (with the above environment variables set) to each user. The user groups are as follows:

GWFR1 - Rig 1 user group.

GWFR2 - Rig 2 users group.

GWFR3 - Rig 3 users group.

GWFR4 - Rig 4 users group.

There is also an Orchestrator Administrators group - I think its called ORCADMINS.

4 users were then set up :

GWFR1 - Rig 1 user - member of GWFR1 user group.

GWFR2 - Rig 2 user - member of GWFR2 user group.

GWFR3 - Rig 3 user - member of GWFR3 user group.

GWFR4 - Rig 4 user - member of GWFR4 user group.

To create the user profiles do the following:

Log onto the Orchestrator server as an administrator (but not the built-in Adminstrator account). Set up the following User Environment Variables in the Control Panel - System applet:

**ORC\_LOGGED\_DATA**  = \\XTP4242\ORCHESTRATOR\GWFR1\LOGGED\_DATA

**ORC\_CMONITORS** = \\XTP4242\ORCHESTRATOR\GWFR1\CMONITORS

**ORC\_TRENDS** = \\XTP4242\ORCHESTRATOR\GWFR1\TRENDS

**ORC\_MONITORS** =CONFIGURABLE MONITOR;ALARM MONOITOR

**ORC\_REPLAYS** =TRENDS;DATA EXPORT

Start the User Profile Editor. Click on the button to the right of the “Permitted To Use Profile:” edit box and select the Glonal User Group - GWFR1. Click on the Add button, to return click OK. Select the Save As File... menu option and save the file as:

<drive>\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS\GWFR1.MAN

This save it as a mandatory user profile.

Repeat the above for Rig2, Rig3 and Rig 4 replacing Rig numbers where appropriate.

These files should be replicated on the Primary Domain Controller and the Backup Domain Controller. Ask Minesh Lad of SEMA (or John Rousse) for help on this. Minesh knows how to do this as he was with me when I set it up the last time.

On each client machine and the server delete all files in the ORCHESTRATOR\REPLAY\_OPTIONS directory.

Go into the User Manager for Domains.

Double click on User GWFR1 and the click on the Profile button. Set the User Path to be

\\NETLOGON\GWFR1.MAN

NETLOGON should be a system share already set up for <drive>\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS\

Set the Home Path to be

\\XTP4242\ORCHESTRATOR\GWFR1\ASCII\_DUMP

Click on OK.

Repeat the above for Rig2, Rig3 and Rig 4 replacing Rig numbers where appropriate.

That should sort out all Windows NT clients.

Unfortunately Windows 95 does not support user profiles in the same way as NT does.

You have to use logon scripts whichg are run every time the user logs on.

All we need to do is to set some environment variables. Normally the **SET** command would work. however this is not persistent. There is a utility called **WINSET** which is on the Windows 95 CD Rom. It is not normally installed on the Windows 95 machine itself. It can be found (with a ReadMe file) on the CD Rom in the directory ADMIN\APPTOOLS\ENVVARS. You’ll have to copy it on to all the Orchestrator machines.

On the server create a batch file called GWFR1.BAT

Enter the following lines

**WINSET ORC\_LOGGED\_DATA**  = \\XTP4242\ORCHESTRATOR\GWFR1\LOGGED\_DATA

**WINSET ORC\_CMONITORS** = \\XTP4242\ORCHESTRATOR\GWFR1\CMONITORS

**WINSET ORC\_TRENDS** = \\XTP4242\ORCHESTRATOR\GWFR1\TRENDS

Save as <drive>\WINNT35\SYSTEM32\REPL\IMPORT\SCRIPTS\GWFR1.MAN and replicate on to the domian cotrollers as above.

Go into the User Manager for Domains.

Double click on User GWFR1 and the click on the Profile button. Set the Logon Script Name to be

\\NETLOGON\GWFR1.BAT

Repeat the above for Rig2, Rig3 and Rig 4 replacing Rig numbers where appropriate.

You might have to put some sort of a condition into the batch files if WINSET does not run on NT.

Eg.

if %OS% == “Windows 95” goto WIN95

:WIN95

WINSET bla bla

:end

# REMOTE ALARM PRINTER

The alarm printer can be a remote printer in another Windows-NT machine.

To install the alarm printer on the server

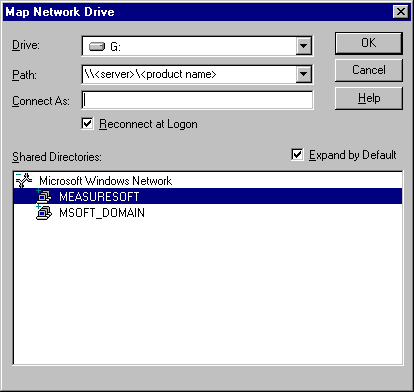
<drive>\<product name>\BIN\alrmprnt -install

To remove the alarm printer on the server

<drive>\<product name>\BIN\alrmprnt –remove

# SERVER NOT APPEARING IN NETWORK BROWSER

Make sure that you can map to the product network drive using Map Network Drive in Explorer



The create a shortcut or run a command line as follows

<drive>\<product name>\BIN\mainmenu /s <server>

The server can be a UNC server name or an IP address.

# TRENDS COMMAND LINE PARAMETERS

To select a trend without selecting a log file

***<drive>\<product name>\BIN\trend\_nt <path to trend file>***

To select a trend and a log file

***<drive>\<product name>\BIN\trend\_nt <path to log file> <path to trend file>***

To select a trend and the most recent file in a logger directory log file

***<drive>\<product name>\BIN\trend\_nt <path to logger directory><path to trend file>***

To select last trend layout

***<drive>\<product name>\BIN\trend\_nt***

To run trends in configure mode

***<drive>\<product name>\BIN\trend\_nt /S <server name>***

To run trends and export and image

***<drive>\<product name>\BIN\trend\_nt <log file> <trend file> /x:<bitmap file>***

To run trends and export an image and exit

***<drive>\<product name>\BIN\trend\_nt <log file> <trend file> /X:<bitmap file>***

To run trends and and zoom to a time

***<drive>\<product name>\BIN\trend\_nt <log file> <trend file> /z:”YYYY/MM/DD HH:MM:SS YYYY/MM/DD HH:MM:SS”***

To run trends and zoom to a time and append period name in subsequent export image

***<drive>\<product name>\BIN\trend\_nt <log file> <trend file> /Z:”YYYY/MM/DD HH:MM:SS YYYY/MM/DD HH:MM:SS”***

# PRINTING MONITORS/TRENDS FROM COMMAND LINE

Printing from command line can be used to schedule print either at end of a log cycle or using the Windows NT scheduler.

To print a trend without selecting a log file

***<drive>\<product name>\BIN\trend\_nt /p <path to trend file>***

To print a trend and select a log file

***<drive>\<product name>\BIN\trend\_nt /p <path to log file> <path to trend file>***

To print a trend and select the most recent file in a logger directory log file

***<drive>\<product name>\BIN\trend\_nt /p <path to logger directory> <path to trend file>***

To print a channel monitor file

***<drive>\<product name>\BIN\mon\_nt /p <path to channel monitor file>***

To print an alarm monitor file

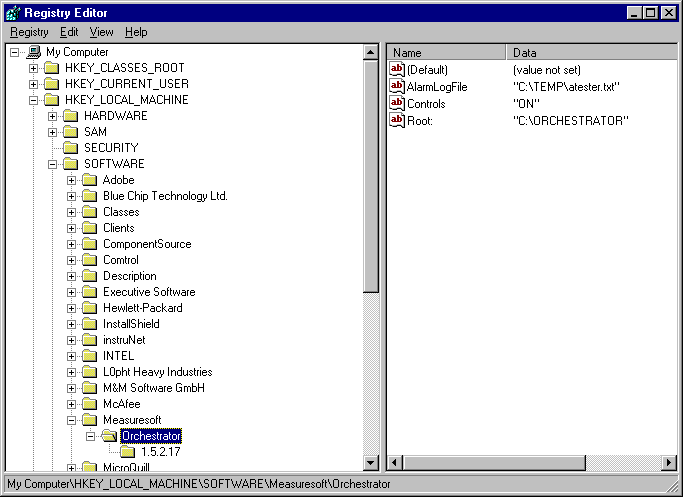
***<drive>\<product name>\BIN\almon\_nt /p <path to alarm monitor file>***

To print an configurable monitor file

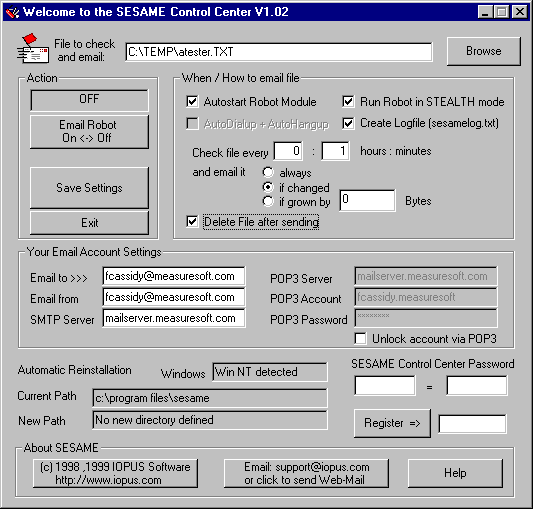
***<drive>\<product name>\BIN\cfmon\_nt /p <path to configurable monitor file>***

# EMAIL ON ALARM

1. Specify the key HKEY\_LOCAL\_MACHINE\Software\Measuresoft\Orchestrator to be the name of a supplementary log file as follows:



1. Download the Sesame emailer from [www.iopus.com](http://www.iopus.com) and use the following settings.



# ALARM SYSTEM MODIFICATIONS

A number of changes have been implemented for the Alarm System of the DataScan Driver. These changes can be enabled through registry settings as follows

## Suppression of Alarm and Warning Reporting

Alarm and Warning reporting can be suppressed by creating the following *String Value* in the registry and setting its value to “ON”

HKEY\_LOCAL\_MACHINE\SOFTWARE\MEASURESOFT\<ProductName>\<Device Dir>\_SuppressAlarms

When this feature is enabled the Alarm and Warning Flags will appear in Channel Monitor but will not be reported by the Alarm System.

This feature can be disabled by either removing the *String Value* or by setting the *String Value* value to “OFF”.

## Warnings as Alarms

Warnings will be treated as alarms if the following *String Value* appears in the registry with a valid value

HKEY\_LOCAL\_MACHINE\SOFTWARE\MEASURESOFT\<ProductName>\<Device Dir>\_ WarningAlarmAdj

This *String Value* holds the value to adjust the alarm priority by for reporting warnings. i.e. If the High Alarm Priority is 10 and this *String Value* holds a value of 2 then warnings will be reported as alarms with a value of 12. If the *String Value* holds a value of –2 then the High Warning will be reported as alarms with a value of 8. The same is true for Low Warnings and Alarms.

The adjustment value can only be in the range –255 to 255.

If the adjustment value plus the priority is less then 0 the priority will be set to 0 and if greater than 255 the priority will be set to 255.

## Driving a Digital for Active Alarms

A digital channel can be specified that will be set high if there are any active alarms in the system or set low if there are no active alarms in the system. This can be enabled by creating the follwing *String Value* in the registry

**HKEY\_LOCAL\_MACHINE\SOFTWARE\MEASURESOFT\<ProductName>\<Device Dir>\_ AlarmActiveChannel**

This *String Value* holds the **<prefix><channel number>** string for the digital channel that is to be driven by the active alarms.

## Driving a Digital for Active Unacknowledged Alarms

A digital channel can be specified that will be set high if there are any active unacknowledged datascan channels in alarm or set low if there are no active unacknowledged datascan channels in alarm. This can be enabled by creating the following *String Value* in the registry

**HKEY\_LOCAL\_MACHINE\SOFTWARE\MEASURESOFT\<ProductName>\<Device Dir>\_ AlarmUnackChannel**

This *String Value* holds the **<prefix><channel number>** string for the digital channel that is to be driven by the active unacknowleged alarms.

# RESTRICTING WINDOWS NT 4.0 UI

For certain industrial applications is it required that the operator is not able to modify anything in the windows NT environment. This application note gives some additional help in this area.

Prior Knowledge:

* Working with the Windows Registries
* Adding Users to the Windows NT Environment

Software Requirements:

* Windows NT 4.0 SP4

Restricting Windows NT functionality

Most of the functionality of Windows NT can be limited in the registry editor. However the user account that needs to be limited is usually not the user account that is able to make changes to the registry, therefore follow the following steps:

1. Log on the system using an administrator account
2. Start the Windows NT User Manager
3. Select User | New Local Group to create a new local group, give this group the name Operators and press OK to save the group settings
4. Select User | New User to create a new user, enter an user name
5. Uncheck “User Must Change Password At Next Logon”, check “User Cannot Change Password” and “Password Never Expires”
6. Click on “Groups”
7. Remove the “Users” group and add the “Operators” group to the user
8. Close the User Manager application
9. Select Start | Shutdown
10. Choose “Close All Programs And Log On As A Different User”
11. Log on as the new user, this will force Windows NT to create a directory with the default settings for this new user
12. Choose “Close All Programs And Log On As A Different User”
13. Log on the system using an administrator account
14. Select Start | Run
15. Enter “Regedt32” and press OK
16. Open the “HKEY\_USERS on Local Machine” window from the window list
17. Select “HKEY\_USERS”
18. Select Registry | Load Hive from the menu
19. Select the file “NTUSER.DAT” from the profile directory of the newly created user.
20. Enter as hive name “NTUSER”
21. Open the “NTUSER” folder
22. Open the “Software” folder
23. Open the “Microsoft” folder
24. Open the “Windows” folder
25. Open the “CurrentVersion” folder
26. Open the “Policies” folder
27. Open the “Explorer” folder
28. Select Edit | Add Value from the menu and add one or more of the following items to disable or enable specific functionality. All entries use the datatype REG\_DWORD and should have a value of 1 (one):
29. To disable the shutdown button  
    Name: NoClose
30. To disable the desktop icons  
    Name: NoDesktop
31. To disable the Find menu  
    Name: NoFind
32. To disable the logoff button on the Windows NT Security Dialog:  
    Name: NoLogoff
33. To disable the RUN menu:  
    Name: NoRun
34. To disable the control panel:  
    Name: NoSetFolders
35. To disable the taskbar   
    Name: NoSetTaskbar
36. To disable the tray context menu   
    Name: NoTrayContextMenu
37. To disable the window context menu   
    Name: NoViewContextMenu
38. Once all settings are entered or modified as desired select the ‘NTUSER’ folder.
39. Select Registry | Unload Hive from the menu
40. Select Registry | Exit from the menu to exit REGEDT32
41. Select Start | Shutdown to logoff as administrative user
42. Logon as the new user with disabled functions

# ENABLE NETWORK BROWSER WITH AN EDIT BOX

We have added this facility as a late release to version 2.0. It will not be supported as standard product but can be enabled by adding the following string value to the system registery after installation:

In the following registry key:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<*ProductName>***

Add the following string value:

***AdvancedServerBrowsing ON***

This will enable an edit box in the network browser dialogs allowing you to type the name of the server (including an IP address).

# WRITING TO CHANNELS FROM EXCEL MACROS

This a solution to writing to channels from Excel. You need to install the Visual C/Visual Basic Library.

The following example write the value of A1 into P2.

Option Explicit

Private Declare Function orc\_write\_an Lib <install dir>\VB\orc\_user.dll" (ByVal prefix As String, ByVal from\_channel As Long, ByVal tochannel As Long, ByRef val As Single) As Long

Sub ss()

Dim Value As Single

Dim ret As Long

Value = Worksheets("Sheet1").Range("A1").Value

ret = orc\_write\_an("P", 2, 2, Value)

MsgBox Value

End Sub

# TRENDS RENAMING LOG FILES

Version 2.0 provided the feature for Trends to rename open log files when they are closed. This caused problems with other processes using the origional open file name. Problems were also seen with remote Trends clients that had different times than the server.

To stop Trends renaming log files in Version 2.0 and 2.1 set the following registry entry:

***HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product Name>\RenameLogs***

Value: ***OFF***

In version 2.2 the logic of Trends was changed so that you now have to explicitly set the above value to ON for the renaming of log files to work.

To set Trends to rename log files in Version 2.2 (and greater) set the following registry entry:

***HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product Name>\RenameLogs***

Value: ***ON***

# Main menu command line parameters

To launch server browser specify /A in command line.

Example:

*mainmenu.exe /A*

To preselect a server specify /S and server name in command line.

Example:

*mainmenu.exe /S <server name or IP address>*

To preselect a local server specify /S and . name in command line.

Example:

*mainmenu.exe /S .*

# Client logger enable Registry Key.

If the ClientLogger registry option is set to “On”, client logger capabilities are enabled in Configurable monitor application independently of current server settings. If this registry options is undefined or not “On” client logger is only enabled if remote server selected.

To enable Client Logger capabilities in Configurable monitor Version 2.3 and higher - set the following registry entry:

***HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product Name>\ClientLogger***

Value: ***On***

***HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product Name>\***ConfigurableMonitorClientLoggerConfig

Name of configuration file defaults to Default.clc

# Detecting Time Change

If the DetectTime registry option is set to “On”, the system will detect time changes. This is necessary if daylight savings time is enabled or if the system is regularly synchronizing time with other systems. When a time change is detected all loggers are stopped and restarted. When using Windows NT ensure that Service Pack 6 or greater is installed.

To enable detection of time change in Version 2.3 and higher - set the following registry entry:

***HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product Name>\DetectTimeChange***

Value: ***On***

# Modbus System Modifications

## Modbus Register Fragmentation

The Modbus Driver can facilitate the fragmentation of command blocks with the following **Registry Entry.**

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\EnableBlockFrag***

The above key must be a **DWORD**.

* Setting the value to **“1” :** will cause command blocks to be fragmented if there is a gap of one register in the configured range.

i.e. IF channels 1,2,3,4 and 7 are configured, the command block will fragment to issue commands for channels 1-4 and channel 7.

* Setting the value to **“0” :** will not cause fragmentation of the command block.

**i.e.** If channels 1,2,3,4 and 7 are configured, there will be only one command block issued for all channels.

The Modbus driver contains a debug facility which allows it to be debugged at run-time should an error occur. To enable this facility a number of **Registry Entries** must be set:

## Modbus MAX Registers Setting

The Modbus Driver can facilitate the setting of the maximum registers read in per block read

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\ModbusMaxBlockSize***

The above key must be a **DWORD**.

E.G.

Setting the value to **“32”** will cause 32 Anaolg values or 512 Digital values be read per block.

Setting the value to **“120”** will cause 120 Anaolg values or 1920 Digital values be read per block.

This value must not be set to **“0”.** If this facility is not required then it should not be entered in the registry.

If this registry key is not set the ModbusMaxBlockSize defaults to 32.

## Modbus Transmit Delay Setting

The Modbus Driver can facilitate a delay on each transmission to allow for some idle time on a 485 network.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\Modbu\_<dev number>\_TransmitDelay***

The above key must be a **DWORD**.

E.G.

Setting the value to **“1”** will cause a 1 millisecond

If this registry key is not set the TranmitDelay defaults to 0

## Modbus Tries Setting

The Modbus Driver can facilitate retrying of a failed Modbus read or write transaction .

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\Modbu\_<dev number>\_Tries***

The above key must be a **DWORD**.

E.G.

Setting the value to **“2”** will cause a second retry on failed transactions.

If this registry key is not set the TranmitDelay defaults to 1

## Modbus StopBits Setting

The Modbus Driver defaults to one stop bit if parity or two stops bits if no parity.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\Modbu\_<dev number>\_StopBits***

The above key must be a **DWORD**.

## Switching Debugging On

To switch debugging on for modbus master simply add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_Debug*** and set its value to “**ON”.**

To switch debugging on for modbus slave simply add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBL\_Debug*** and set its value to “**ON”.**

## Selecting the Debug Type

The Modbus Driver allows you to output the debug information to a Console Window, Text File or as a Trace Statement which can be displayed by applications such as DBWIN32.EXE.

To enable these facilities for modbus master add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugType***

To enable these facilities for modbus slave add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBL\_DebugType***

The values of this key can be as follows:

**“CON”** to send output to a console window

**“FILE”** to send the output to a text file or

**“TRACE”** to send the output as a trace statement.

These can be concatenated to send the output to multiple types by using the **|** symbol.

e.g. “**FILE|CON”** would send the output to both File and Console Window.

When sending output to the **FILE** type you must specify the file.

To do this for modbus master add the following registry entry

**Note:** Console (CON) is not supported on Windows Vista. Instead set the output mode to TRACE, and to view the debug data you must use SysInternals Debug Viewer. This can be downloaded from <http://www.microsoft.com/technet/sysinternals/Utilities/DebugView.mspx>

In order for Console mode to work on Windows XP the service must be configured to logon as the System Account with Interact with Desktop enabled

HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugFile

To do this for modbus slave add the following registry entry

HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBL\_DebugFile

Its value should contain the name of the file you wish to output debug information too.

**e.g.** C:\MyDocuments\Modbusdebug.txt

## Switching On the Debug Counts

The Modbus Driver allows you to count the number of bytes received and transmitted.

To enable these facilities for modbus master add the following registry keys

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugRxCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugTxCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugRxTimeoutCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugTxTimeoutCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugRxCommErrorCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugTxCommErrorCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugRxCRCErrorCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugTxCRCErrorCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugRxGoodPacketCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBU\_<dev\_number>\_DebugTxGoodPacketCount***

To enable these facilities for modbus slave add the following registry keys

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBL\_DebugRxCount***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\MODBL\_DebugTxCount***

The values of these key specify a channel used to store the count e.g. P1

The channel used must be configured. To reset the counts, use a calculation function.

Note: Debugging must be switched ON

## Adding Multiple Modbus slave Devices

Modify datproc.txt as follows

modbl,MODBUS SLAVE 1,,run

modbm,MODBUS SLAVE 2,,run

modbn,MODBUS SLAVE 3,,run

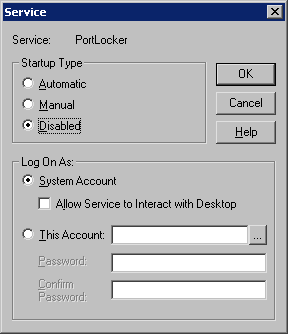
modbo,MODBUS SLAVE 4,,run

# Communication resources sharing between annunciators and RAS (RRAS)

New component has been added to Alarm System. PortLocker.exe is a COM service, which is responsible for COM ports sharing between Pager, SMS and Vodafone annunciators from one side and Remote Access Server (Remote Access and Routing Server) from other side. If RAS is configured to use the same ports as alarm annunciators, PortLocker will stop RAS service before sending messages to pagers or mobiles and start it after messages will be sent. If RAS and alarm annunciators use different ports, nothing will occur.

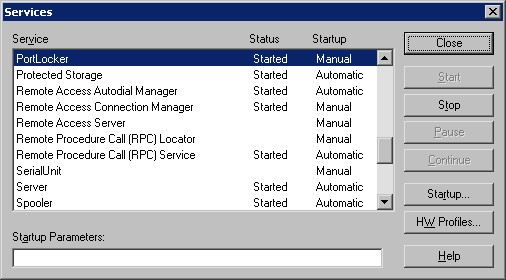
To prevent stoping RAS service user can disable PortLocker from Contol Panel by Services applet.

Select “PortLocker” in list of services, press “Startup” button, switch “Startup Type” to “Disabled” and press “Ok” button to finish.



If PortLocker is installed and not disabled but system cannot send messages because of locked communication resourses, check next issues:

1) if PortLocker is running go to Control Panel, start Services applet and find “PortLocker” in list of services

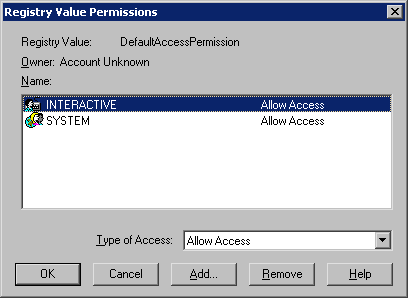


If status of PortLocker is not “Started”, try start it manually. If error occur, it means that component isn’t installed properly and it requires reinstall.

If status of PortLocker is “Started” but system still cannot send messages check security settings:

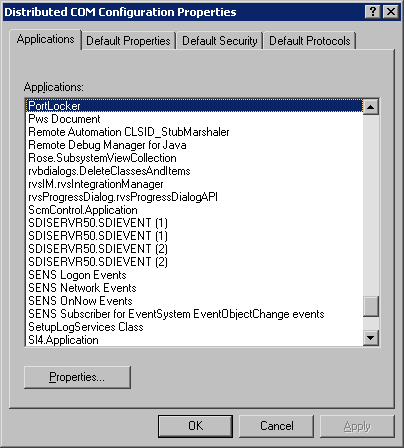
2) start Distributed COMConfiguration Properties – dcomcnfg.exe, select “Default Security” tab and

check “Default Access Permission” and “Default Launch Permissions”. They should contain at least SYSTEM and INTERACTIVE names.

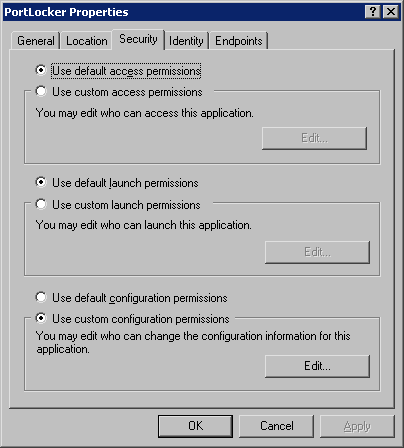


If not, add them to list with “Allow Access” rights. Then return to Applications tab,

find PortLocker component in application list and press “Properties” button.



Switch to “Security” tab and make sure that “Use default access permissions” and “Use default launch permissions” are selected.



Restart system and check how it will work after reconfiguration.

# Disabling Monitor Locking in Configurable Monitor

By default when you launch an \*.orm from the command line or via the navigation buttons in configurable monitor the monitor that is opened will be set to value entry and locked. However, there are situations where the user may not wish the monitor to be locked. To prevent this from happening simply add and set the following registry entry to **“ON”**.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\*** ***DisableMonitorLock***

# Disabling Value Entry Handles

In some cases a user may wish to disable the handles surrounding selected objects in value entry mode. To do this simply add the following registry entry with a value of **“OFF”.**

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\ValueEntryHandles***

# Disabling Prompt to Save on exit

In some cases a user may wish to disable the prompt to SAVE when exiting from mainmenu. To do this simply add the following registry entry with a value of **“OFF”.**

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\PromptToSave***

# Log by Tag

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\LogByTag***

Set to ON

# Alarm Annunciator Debugging

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***Alarm\_Debug ON

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***Alarm\_DebugType CON or FILE

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***Alarm\_DebugFile

**Note:** Console (CON) is not supported on Windows Vista. Instead set the output mode to TRACE, and to view the debug data you must use SysInternals Debug Viewer. This can be downloaded from <http://www.microsoft.com/technet/sysinternals/Utilities/DebugView.mspx>

In order for Console mode to work on Windows XP the service must be configured to logon as the System Account with Interact with Desktop enabled

# Data Exchange Options

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\DataExchange\***Debug ON

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\DataExchange\*OPC Options\**TagReferenced ON

# Datascan Timeout

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***DatascanScanTimeout REG\_DWORD set in milliseconds.

Defaults to 5 seconds for continuous measurement

Defaults to 30 seconds for single shot measurement

# Default WITS External Driver

Delete headers.bin in <product name>\CURRENT\_CONFIG\EXTERN\_<n>

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***DefaultWits ON

Run the advanced configuration and save configuration.

# Auto Open Configuration When Service Starts

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***AutoOpenConfig ON

The name of the file to open is the last saved file in the main menu which is stored in

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\****Root:*

The directory used is determined by ORC\_SAVED\_CONFIG system environment variable which can be set using Control Panel/System/Advanced or using the following registry entry

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment**\ORC\_SAVED\_CONFIG

This registry entry can reference other registry entries instead of fixed directory names using % at start and end e.g.

%\\LocalMachine\\Software\\KOPL\\Configuration\\Configuration Directory%

# Multiple Calculators

Up to 3 calculator processors can be installed,

Change the entry CALCULATORS=1 to CALCULATORS=n in the Server\product.ini file.

# Data Export Strings

Channels in error are normally displayed as ERROR. This string can be changed by specifying

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\****DataExportErrorString*

Sometimes it is necessary to format the date and time column in a specific manner before export. This has the same formatting effect on time/dates as the **STRFTIME** function. To format the Time or Date you must enter the following strings:

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\DataExportTimeFormat***

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\DataExportDateFormat***

The value field can contain formatting codes as per the strftime formatting codes.

e.g. %H:%M:%S

where %H = Hour in 24-hour format (00 – 23)

%M = Minute as decimal number (00 – 59)

%S = Second as decimal number (00 – 59)

# Running Processors from Desktop/Using Network DDE in Data Exchange

Sometimes it is necessary for background processor tasks to run from the desktop. This is necessary if Data Exchange is configured with Network DDE links.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***Processor Name From Desktop ON

e.g

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\***Data Exchange From Desktop ON

This will cause the processor to run from the desktop of the currently logged on user. If the user logs off, the processor task will stop. The user may be warned about quitting on a log off.

# Rainbow Sentinel Driver Error Codes

|  |
| --- |
| 1. Success – The call completed successfully |
| 1. **Invalid Function Code** – You specified an invalid function code. See your language’s include file (e.g., SUPRPRO.H) for valid API function codes. Generally, this error should not occur if you are using a Rainbow – provided interface to communicate with the driver. |
| 1. **Invalid Packet** – A checksum error was detected in the command packet, indicating an internal inconsistency. The packet record or UNITINFO structure has not been initialised or may have been tampered with. Generally, this error should not occur if you are using a Rainbow – provided interface to communicate with the driver. |
| 1. **Unit not found** – Either sproFindFirstUnit() or sproFindNextUnit() could not find the specified SentinelSuperPro Key. Make sure you are sending the correct developer ID. This error is returned by oter functions if the key has disappeared (that is, has been unplugged). |
| 1. **Access denied** – Your attempted to perform an illegal action on a word. For example you may have tried to read an algorithm/hidden word, write to a locked work, or decrement a word that is not a data or counter word. |
| 1. **Invalid memory address** – You specified an invalid SentinelSuperPro memory address. Valid addresses are 0-63 decimal (0-3F hex). Cells 0-7 are invalid for man operations. Algorithm descriptors must be referenced by the first (even) address |
| 1. **Invalid access code** – You specified an invalid access code. The access code must be 0 (read/write data), 1 (read-only data), 2 (counter), or 3 (algorithm/hidden). |
| 1. **Port is busy** – The requested operation could not be completed because the port is busy. This can happen if there is considerable printer activity or if a unit on the port is performing a write operation and is blocking the port. Try the function again. |
| 1. **Write not ready** – The write or decrement could not be performed due to a momentary lack of sufficient power. Try the operation again. |
| 1. **No port installed** – No parallel ports could be found on the workstation. |
| 1. **Already zero** – You tried to decrement a counter or data word that already contains the value 0. If you are using the counter to control demo program executions, this condition may occur after the corresponding algorithm descriptor has been reactivated with its activation password |
| 1. **Driver not installed** – The system device driver is having problems communicating with the unit. Verify that the device driver is properly installed. |
| 1. **Communications error** – The system device driver is having problems communicating with the unit. Verify that the device driver is properly installed |
| 1. **Version not supported** – The current system device driver si outdated. Update the driver. |
| 1. **OS environment not supported** – The operating system or environment is not supported by the client library. Contact Technical Support. |
| 1. **Query too long** – You sent a query string longer than 56 characters. Send a shorter string. |
| 1. **Driver is busy** – The system driver is busy. Try the operation again. |
| 1. **Port allocation failure** – Failure to allocate a parallel port through the operating system’s parallel port contention handler. |
| 1. **Port release failure** – Failure to release a previously allocated parallel port through the operating system’s parallel prot contention handler. |
| 1. **Acquire port timeout** – Failure to acquire access to a parallel prot within the defined time-out |
| 1. **Signal not supported** – The particular machine does not support a signal line. For example, an attempt may have been made to use the ACK line on a NEC 9800 computer |
| 1. **Init not called** – The key is not initialised. Call the sproInitialize() function before calling the function that generated this error. |
| 1. **Driver type not supported** – The type of driver access, either direct I/O or system driver, is not supported for the defined operating system and client library. |
| 1. **Fail on driver comm**. – The client library failed on communicating with the Rainbow system driver |
| 1. **API status unavailable** – The extended API status function is unavailable. |
| 1. **Invalid status** – An invalid status code was returned |

# Adding SCADA Product OPC Tags to InTouch

This procedure outlines how to configure Wonderware InTouch to display OPC Tags from the SCADA product.

## Prerequisites

The following software should be installed on the PC.

**Note:** While it is possible to get OPCLink to work with remote data, we have been unable to get it to work with remote data when configured as a service.

* SCADA Server 2.0 or later

Make sure to configure some tags.

* SCADA OPC Server 2.0 or later

We **recommend** that the following Registry settings be configured for the SCADA product OPC Browser settings:

* + HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\OPCServer\DisplayOption
    - ChannelIdentifier ON
    - Description OFF
    - Tag OFF

This will make it easier to track the tags in InTouch.

* Wonderware InTouch 7.1 or later
* Wonderware OPCLink I/O Server 7.1 or later

## Procedure

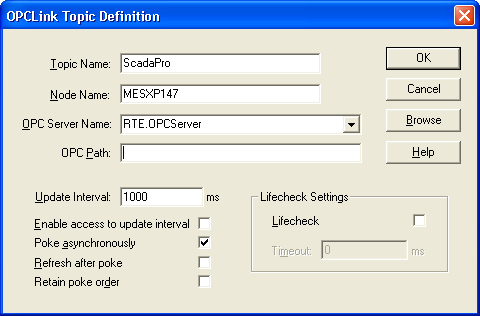
Configuring OPC tags in Wonderware is complex and involves the following:

* Configuring the OPCLink OPC Client application to create a Topic Definition
* Configuring an Access Name in Window Maker. The Access Name uses the Topic Definition.
* Configuring an Tag in Window Maker. This is where you specify which OPC Item you want to use from the Access Name/Topic Definition.
* Configuring a Window item such as a Meter to use the Tag in Window Maker
* Running the Window in Window Viewer
* Verify that OPCLink is getting the data.

**Note:** This procedure assumes that DCOM settings have been configured correctly.

## Configure the OPCLink Application.

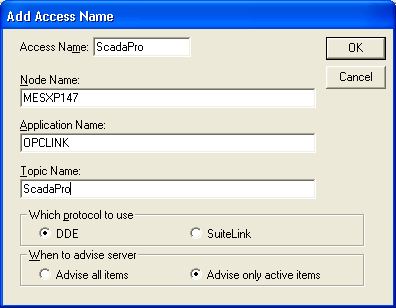
1. Run the OPCLink application.
2. Configure a new Topic Definition as follows:
   1. From the **Configure** menu select **Topic Definition…** The Topic Definition dialog box will appear.
   2. Click on the **New…** button to create a new topic definition. The OPCLink Topic Definition dialog box appears.
      1. Enter **SCADA** in the **Topic Name** field.
      2. Enter the ***machine name*** where SCADA resides in the **Node Name** field. This should be the local machine name.
      3. Select **RTE.OPCServer** from the **OPC Server Name** field. You can click on the **Browse** button to test the connection to the OPC Server.
      4. Leave the **OPC Path** field **blank**. Leave the other settings at their defaults.



* 1. Click **OK** and select the **File | Save** command. Save the configuration file E.g. SCADA.cfg. Click **Done**. You will not see any data in the OPCLink window at this stage. Leave OPCLink running.

## Configure a new InTouch Access Name

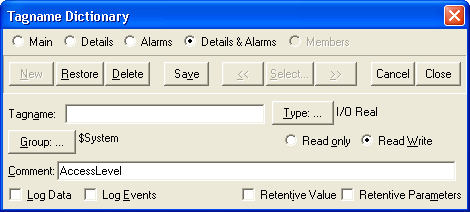
1. Run InTouch and create a new application or open an existing application in Window Maker.
   1. From the **Special** menu select **Access Names…**
   2. Click on the **Add…** button.
   3. In the **Access** **Name** field type **ScadaPro**.
   4. In the **Node Name** filed enter the **name of the machine** where OPCLink is running. This should be the local machine name.
   5. In the **Application Name** field type **OPCLINK**.
   6. In the **Topic Name** field type SCADA.
   7. Leave the other settings at their defaults.



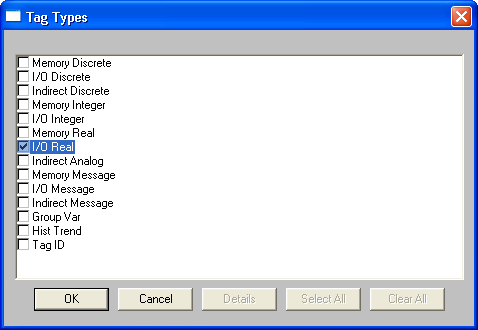
* 1. Click on the **OK** button.
  2. Click on the **Close** button.

## Configure a new InTouch Tag:

1. Run InTouch Window Maker with the last application
   1. From the **Special** menu select **Tagname Dictionary…**
   2. Select the **Details & Alarms** radio button on.
   3. Click on the **New** button.

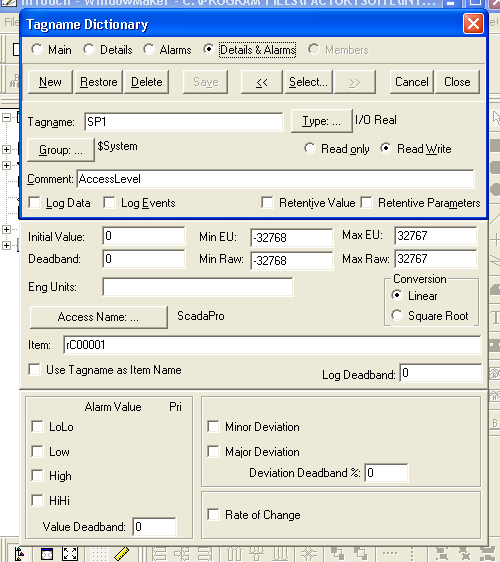


* 1. Click on the **Type…** button and select the I/O Real type as follows:



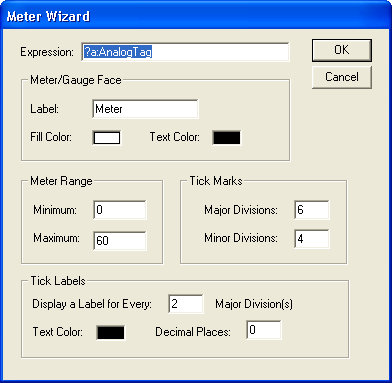
* 1. Click **OK** and enter in the name of the new tag in the **Tagname** field. Type ***SP1*** as the tag name.
  2. Click on the **Access Name**… button to assign the tag an access name. The dialog will list all the access names in the system. Select the SCADA access name and click on the **Close** button.
  3. In the **Item:** field below the **Access Name** field you must enter the name of the ScadaPro item name that you want.

**Note:** InTouch expects you to prefix the item name with a letter indicating the type of the data item. All OPC items in SCADA are Reals so for SCADA Calculator Channel C00001 you would enter **rC00001**.

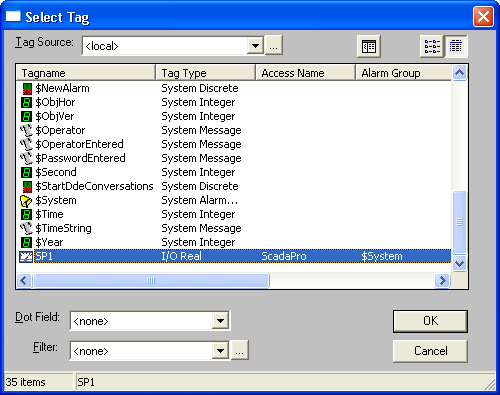


## Configure a window that uses the InTouch Tag:

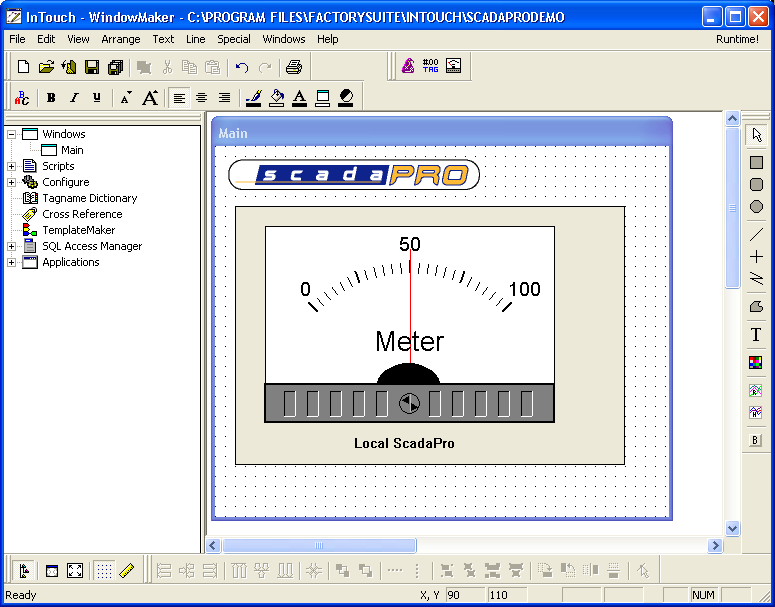
1. Run InTouch Window Maker with the last application
   1. Create a new window in File Maker.
   2. Using the **Wizards** **toolbar** button add a **panel meter** to the toolbar.
   3. Drag the panel meter object on to the window.
   4. Right click on the meter and select **Properties…**
   5. Delete the values in the **Expression** field and double click the field to select a tagname



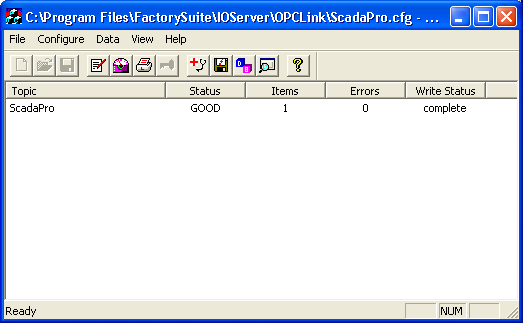
* 1. Select the **SP1** tag and click **OK**.



* 1. Configure the range of the meter to suit the tag values.
  2. Save the window and open in Window Viewer.



* 1. When Window Viewer opens you should see the following in the OPCLink window:

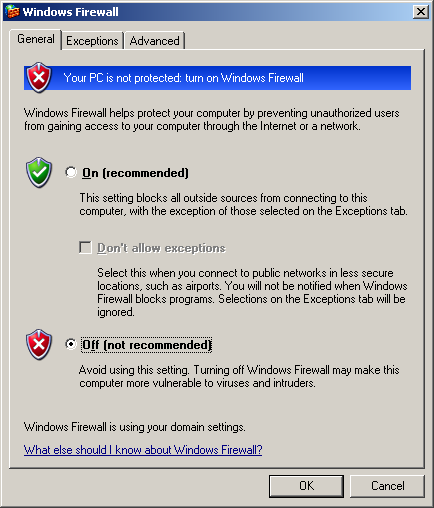


* 1. You can check the Wonderware Logger application to trouble shoot any problems.

# Configuring Excel RTD Network Settings

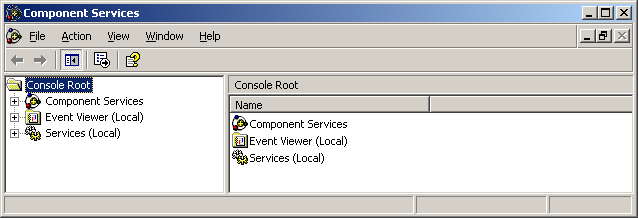
1) Switch off Windows firewall on **both server and client**

Start/Programs/Control Panel/Network Connection/Local Area Connection/Properties/Advanced/Settings

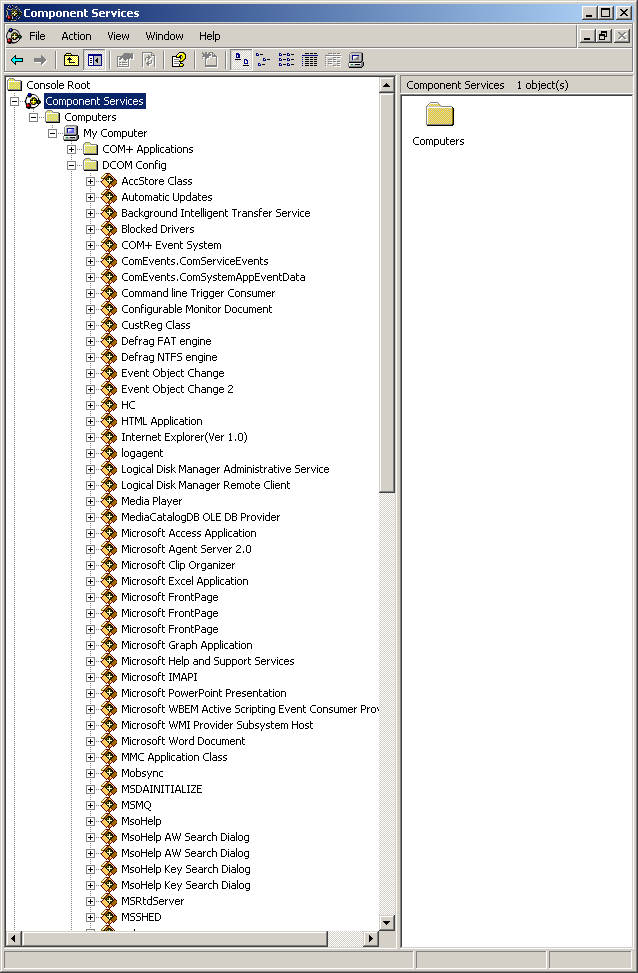


2) Configure DCOM on the server

Start/Control Panel/Administrative Tools/Component Services



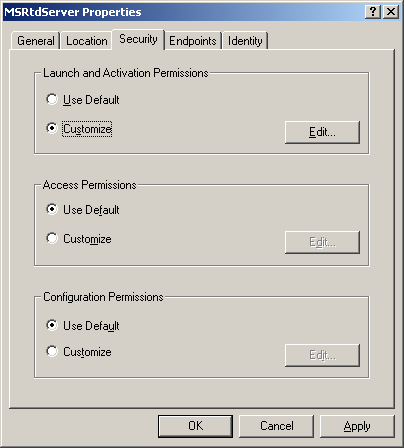
Expand Component Services/Computers/My Computer/DCOM Config



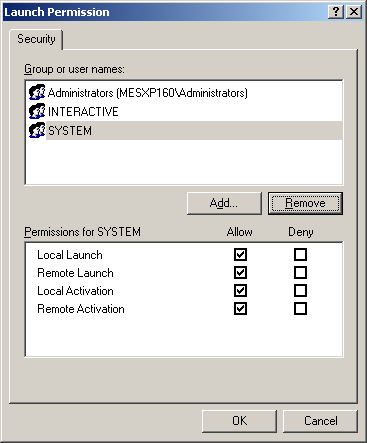
Right click MRtdServer and select properties

Select Security Tab

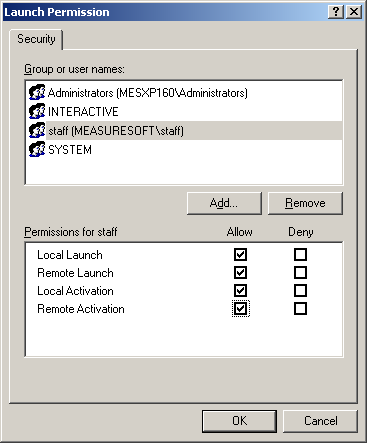
Set Launch and Activation Permissions to Customise



Edit Launch and Activation Permissions

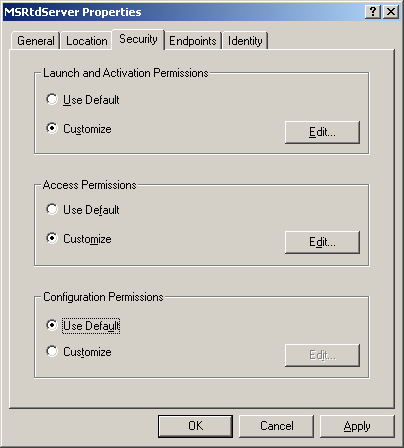


Add the users who will access the local RTD server remotely.

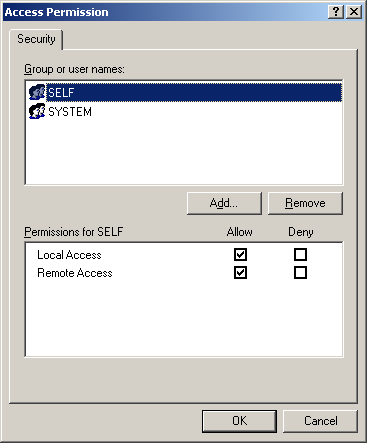


Click OK

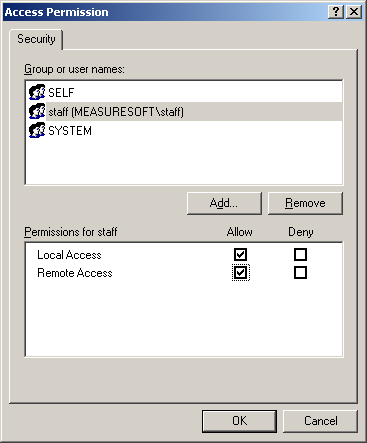
Set Access Permissions to Customise



Edit Access Permissions



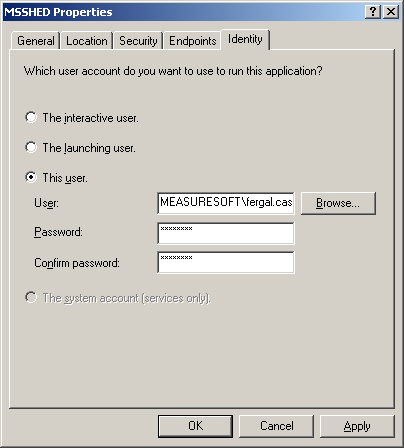
Add the users who will access the local RTD server remotely.



Click OK

Select the Identity Tab

Select an appropriate account to run the rtd server. The account should be an administrator.



Close Component Services and re-boot the server.

3) Configure the client

If the client is not a product server system, copy the MSRtdServer.exe program from the <server>\<product>\BIN folder to the client and ensure the registry key HKEY\_LOCAL\_MACHINE\Software\Measuresoft\Product Name is set to the value as the key on the server and then run “MSRTDServer –RegServer”

# Running Clients on Windows 2000 Workgroups

For a Client to run on a Windows 2000 Workgroup the same user account must exist on both the server and the client computer. This account must have the same password on both computers.

The registry on the server computer must also be edited so that the client PC can access the servers registry. Follow these steps:

* Click Start & Run
* Type in regedt32 and click Ok
* From the Windows Menu select HKEY\_LOCAL\_MACHINE
* Browse System\CurrentControlSet\Control\SecurePipeServers\winreg
* From the Security menu give the Guest account and the Guests group full control of this group.

Restart the Server PC for these changes to take effect.

# Configuring an SQL Server to Publish Logged Data

It is possible to configure SQL Server to make Logged Data available to another SQL Server. The server where the data is resident and becomes a publisher. The remote server becomes a subscriber.

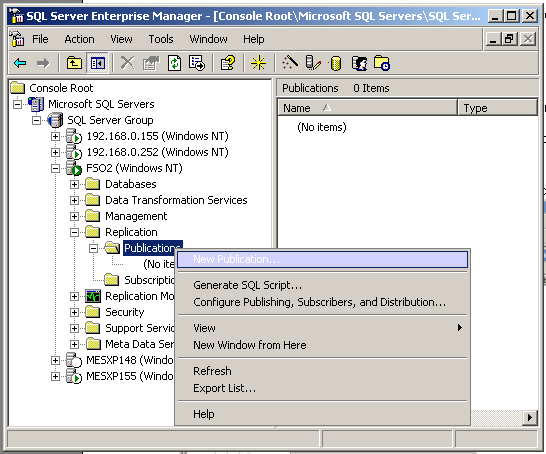
When creating a publication, you can choose the tables, filtered partitions of data, and database objects that you want to publish.

**To create publications**

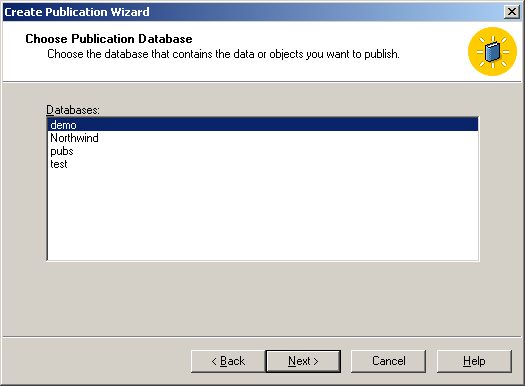
1. At the Publisher, open SQL Server Enterprise Manager, expand a server group, expand the **Replication** folder, right-click the Publications folder, and then click **New Publication**.
2. On the Welcome to the Create Publication Wizard page, select **Show advanced options in this wizard** to enable updatable subscriptions or transformable subscriptions (options available with snapshot replication or transactional replication).
3. The wizard guides you through:
   * Choosing a publication database - demo
   * Using a publication template.
   * Selecting the type of publication - merge
   * Selecting updatable subscriptions or transformable subscriptions (snapshot replication or transactional replication).
   * Specifying Subscriber types.
   * Specifying data and database object articles to publish – test data table
   * Selecting a publication name and description. Publication names cannot contain these characters: / \ < >.
   * Customizing the properties of the publication including filtering columns, filtering rows, enabling dynamic filters, validating subscription information, optimizing synchronization, allowing anonymous subscriptions, and setting the snapshot agent schedule.

From Enterprise Manager expand the replication group, right click on Publications and select

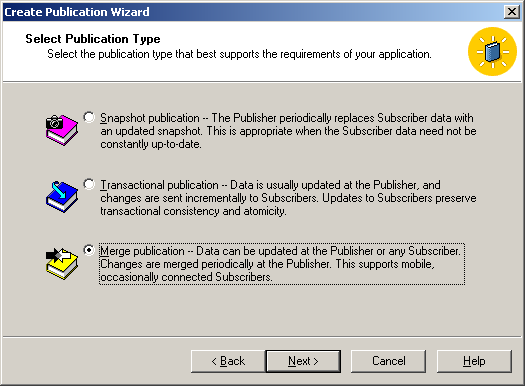
New Publication



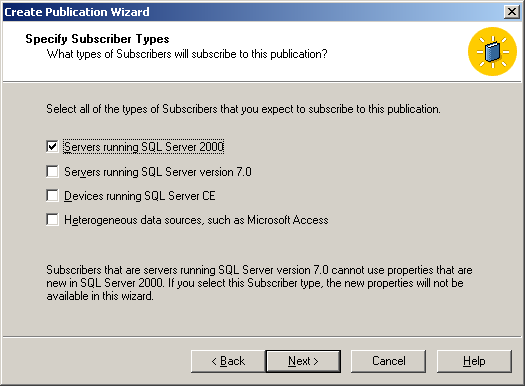
Click Next and Select the database to be used with the logger. The database must already exisit.

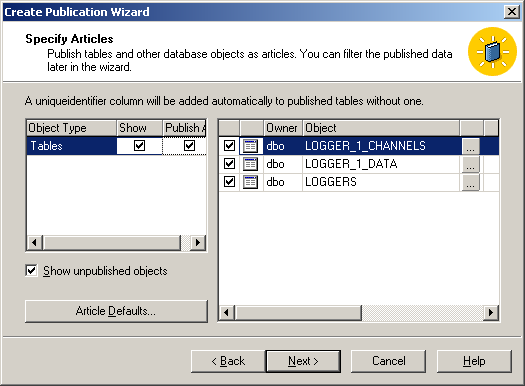


Select a merge publication and click next.

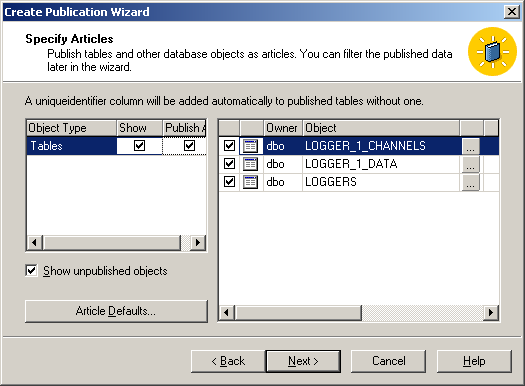


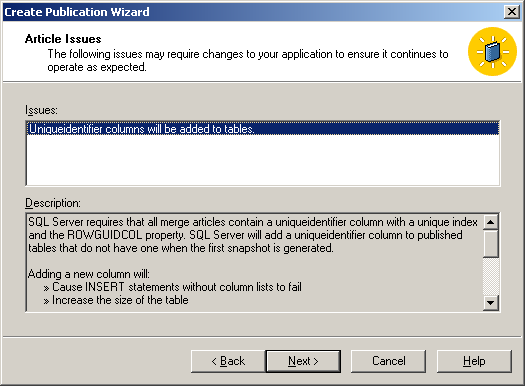
Select the appropriate version of SQL Server and click next.



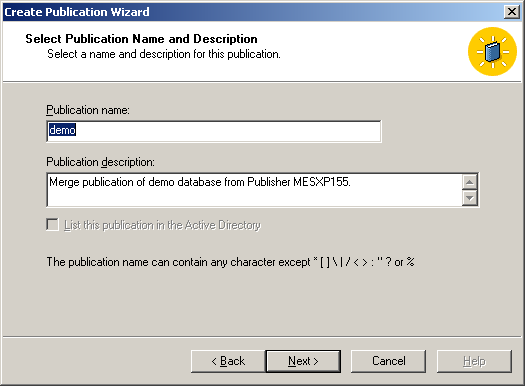


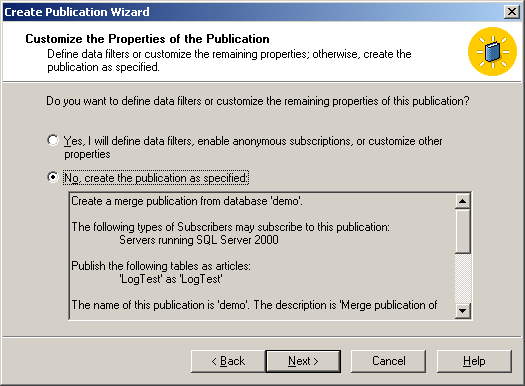
Select the tables from the database that you wish to make available for publication.





Give your publication a name and description and click next.





Click the finish button.



Adding a publication of a database logger tables cannot be performed when the database is being accessed by the logger.

# Configuring an SQL Server to Subscribe to a Published Database

A subscription is the request for data or database objects to be published to a specific Subscriber. A Subscriber can have several subscriptions to different publications.

A subscription defines what publication will be replicated, where and when. A subscription can be created either at the Publisher (a push subscription) or at the Subscriber (a pull subscription). Push subscriptions are then created and synchronized at the Publisher/Distributor and the synchronizing agent (Distribution Agent or Merge Agent) is typically run at the Distributor. Pull subscriptions and anonymous subscriptions are created and synchronized at the Subscriber and the synchronizing agent is typically run at the Subscriber.

Push subscription is used when

* Data will typically be synchronized on demand or on a frequently recurring schedule – in this case data will be synchronised as new records are added to the production and test logging tables.
* Publications require near real-time movement of data without polling.
* The higher processor overhead at a Publisher using a local Distributor does not affect performance.
* You need easier administration from a centralized location (the Distributor).
* The centralized Distributor will establish the schedule on which connections will be made with remote, occasionally connected Subscribers

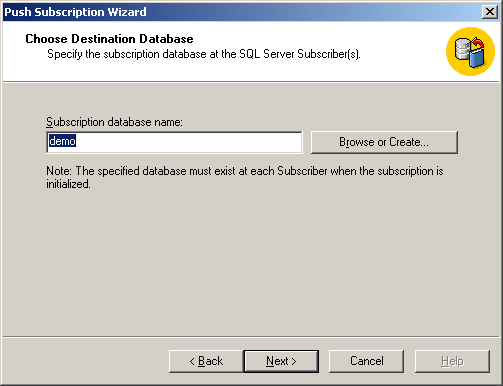
In the replication group right click on the Publication you have just made and select New Push Subscription. Click next.



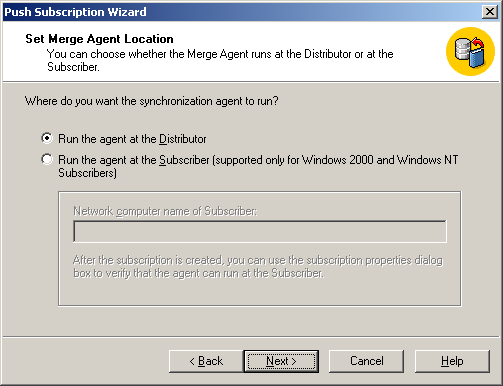
From the list of servers select the server you wish to publish to and click next.

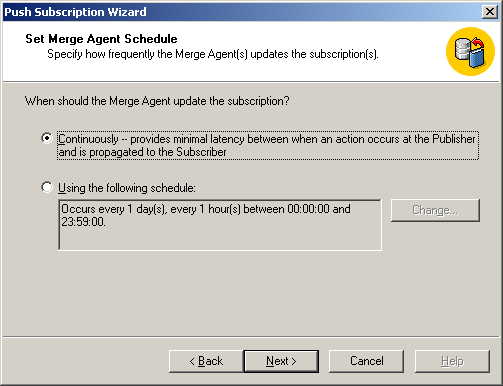


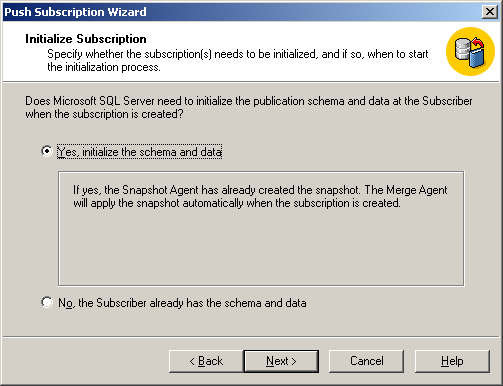
Browse or create the SQL Server database where the published data will reside. Click next

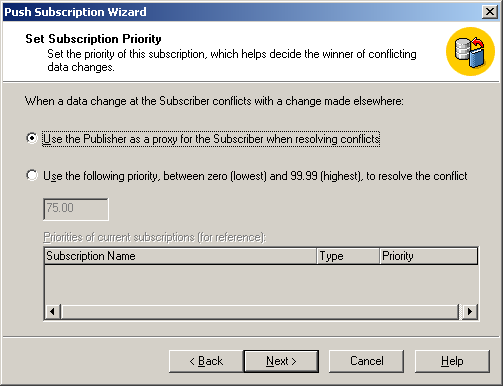


Select whether you want the Publication Agent to run at the Distributor or the Subscriber. In cases where the Distributor is low on system resources it may be advisable to run the agent at the subscriber, otherwise it can be run at the distributor.

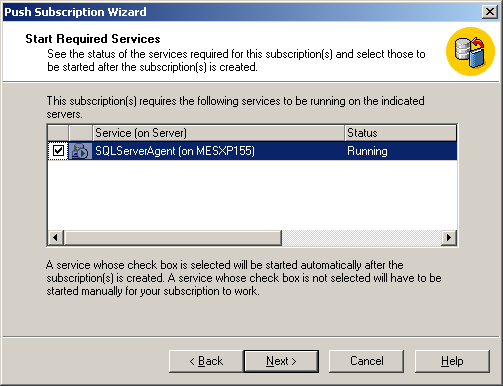








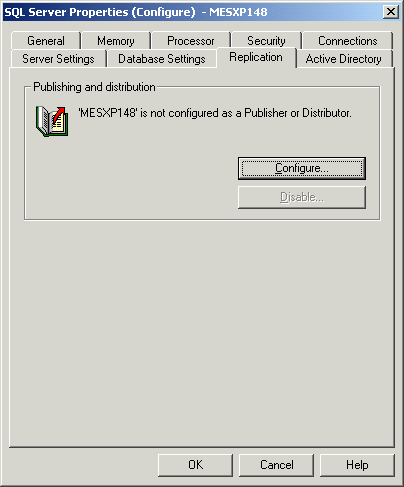
Click next the start the required services.



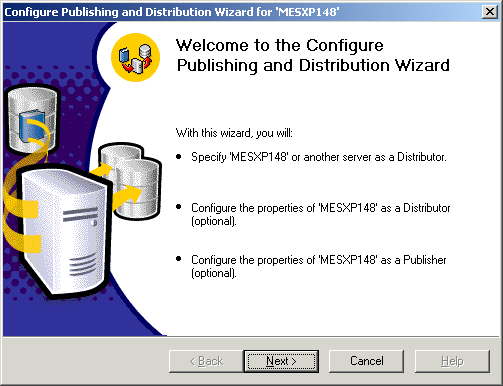
# Configuring a Logger to Replicate Data

It is possible to have a Logger replicate data to a second database, this database can be on the same SQL server or on a remote SQL Server. In order to make this work replication must be enabled on the SQL Server.

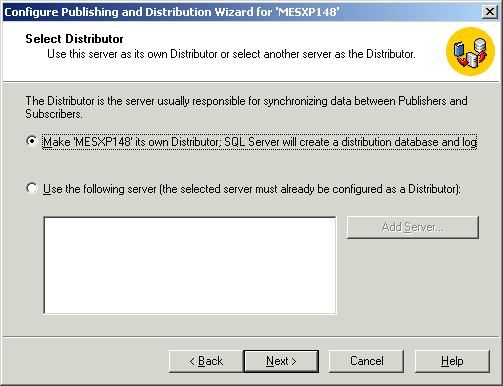
* Right click on the SQL Server registration and select properties
* Click on the Replication Tab

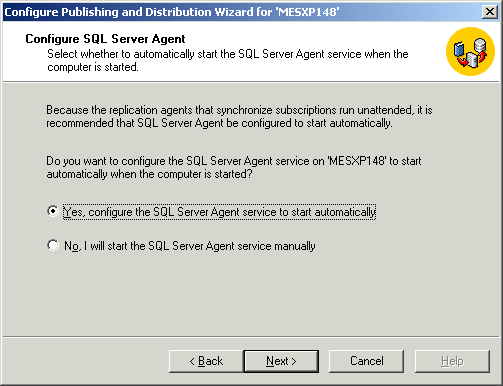


* Click Configure

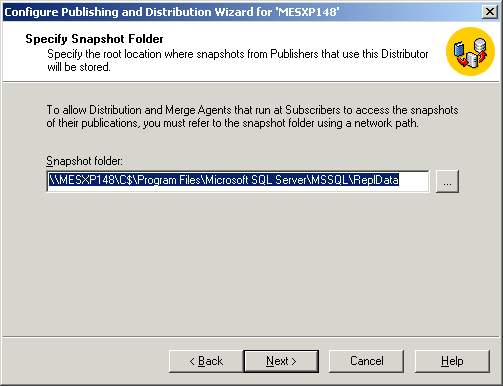


* Click Next

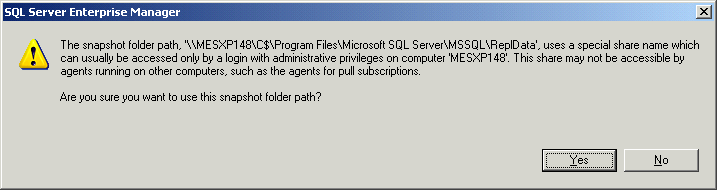




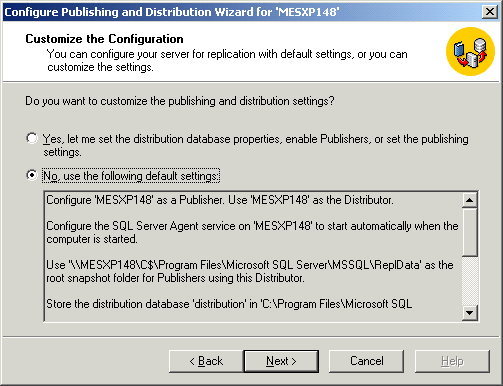
* Select Yes to allow the SQL Server Agent to start automatically.



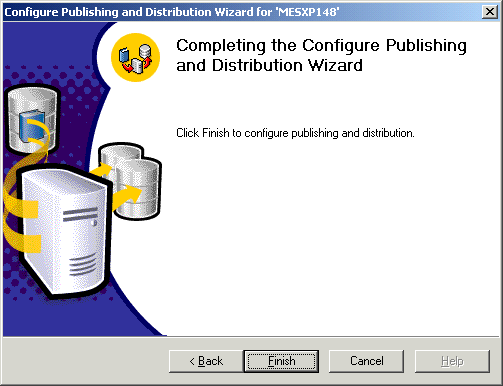
* Accept the default snapshot folder.



* Select Yes.



* Click Next



* Click Finish.

**Note:** Each time a logger cycles and a new table is created the new table is added to the publication. This could lead to a situation where many tables are being replicated even though only the most recent table needs to be replicated. It is possible to have the logger remove old tables from the publication by assigning the following registry key the value ON.

Hive: HKEY\_LOCAL\_MACHINE\Software\Measuresoft\<Product\_Name>\

Key: DropReplicationOnCreate

This key should be created as a String Value.

**Note:** A problem has been encountered where the Logger fails to create the SQL Server Publication. To resolve this problem it was necessary to create a publication manually on the server. Instructions for creating the Publication manually are found in section 37 (Configuring an SQL Server to Publish Logged Data) of this manual.

# Logging to a Remote Database over HTTP

It is possible to log data directly to a remote SQL Server/Access Database over the Internet/Intranet via the HTTP protocol. For this to work the RDS Service, Internet Information Server and SQL Server or the Access Database must all be located on the same machine. MSADC and RDS is configured differently for Windows XP & 2003 Server and Windows 2000 server, the separate instructions are detailed below.

Windows XP & 2003 Server

**Create a Virtual Directory**

* Click Start, click Run, type inetmgr, and then click OK. The Internet Information Services (IIS) Manager window appears.
* In the left pane, locate, and then right-click the Default Web Site node.
* In the left pane, locate, and then right-click the Default Web Site node.
* Point to New, and then click Virtual Directory. The Virtual Directory Creation Wizard appears.
* Click Next.
* Type MSADC in the Alias box, and then click next.
* Type *System Drive Letter*:\Program Files\Common Files\System\msadc in the Path box.  
    
  **Note** *System Drive Letter* is the placeholder for the letter that is assigned to your system drive where the operating system is installed.
* Click Next.
* If the following check boxes are not selected, click to select them: Read, Run scripts (such as ASP) & Execute (such as ISAPI application or CGI)
* Click Next.
* Click Finish.

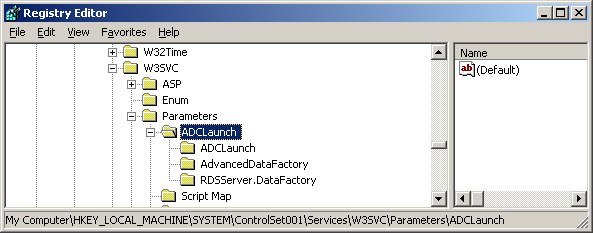
**Add a Web service extension (Windows Server 2003 Only)**

* From the Start Menu, click Control Panel, double click administrative tools, and launch Internet Information Services (IIS).
* In the left pane of the Internet Information Services (IIS) Manager window, locate, and then right-click Web Service Extensions.
* Click Add a new Web Service Extension. The New Web Service Extension dialog box appears.
* Type RDS in the Extension name box, and then click Add. The Add file dialog box appears.
* Type *System Drive Letter*:\Program Files\Common Files\System\msadc\msadcs.dll in the Path to file box, and then click OK.  
    
  **Note** *System Drive Letter* is the placeholder for the letter that is assigned to your system drive where the operating system is installed.
* Click OK.

**Create keys in the registry**

**Note** If the following registry keys are already present in the registry database, do not create them again.

* Click Start, click Run, type regedit, and then click OK.
* In the left pane of Registry Editor, locate, and then right-click the following subkey:HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\W3SVC\Parameters\ADCLaunch. If the ADCLaunch Subkey does not exist create the Key.
* Click New, and then click Key. A new subkey is created under the ADCLaunch subkey. Rename this key AdvancedDataFactory
* Repeat the previous step and create the keys: ADCLaunch and RDSServer.Datafactory as shown below.



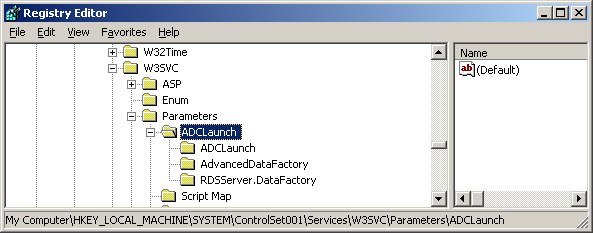
Windows 2000 Server

NOTE: Ensure that the virtual directory created by default in IIS for the MSADC directory has Read, Run scripts (such as ASP) & Execute (such as ISAPI application or CGI) permissions.

**Create keys in the registry**

**Note** If the following registry keys are already present in the registry database, do not create them again.

* Click Start, click Run, type regedit, and then click OK.
* In the left pane of Registry Editor, locate, and then right-click the following subkey:HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\W3SVC\Parameters\ADCLaunch. If the ADCLaunch Subkey does not exist create the Key.
* Click New, and then click Key. A new subkey is created under the ADCLaunch subkey. Rename this key AdvancedDataFactory
* Repeat the previous step and create the keys: ADCLaunch and RDSServer.Datafactory as shown below.



Windows XP & 2003 Server and Windows 2000 Server

**Check Msdfmap.ini Configuration for SQL Server and Microsoft Access**

Open <Windows>\msdfmap.ini file and edit default connection access rights and default SQL substitution. Shown below are the possible settings for SQL Server and Microsoft Access Databases.

**Msdfmap.ini Configuration for SQL Server**

Check that the connect default and the SQL default sections appear as shown below:

[connect default]

Access=NoAccess

[sql default]

invalid query.

;Sql=" "

[connect (local)]

Access=ReadWrite

**Msdfmap.ini Configuration for Microsoft Access**

Check that the connect default and the SQL default sections appear as shown below:

[connect default]

Access=ReadWrite

[sql default]

;Sql=" "

**Microsoft Access Database Permissions**

It is necessary to configure the Security permissions on the access database. In Windows Explorer browse to the location of the Access Database. Right click on the Database and select properties. Click the security tab and add button. Since the connection will be made over http IIS anonymous users must be given access to the database. These accounts are: IUSR\_*MachineName* and IWAM\_*MachineName.*  Replace the machine name with the computer name of the server.

**Run the Web server in an unsafe mode**

To use RDS, you must run the Microsoft Internet Information Services (IIS) server in an unsafe mode. To make the IIS server run in an unsafe mode, you must run the Handunsf.reg file that is installed together with the Microsoft Data Access Components (MSDAC).

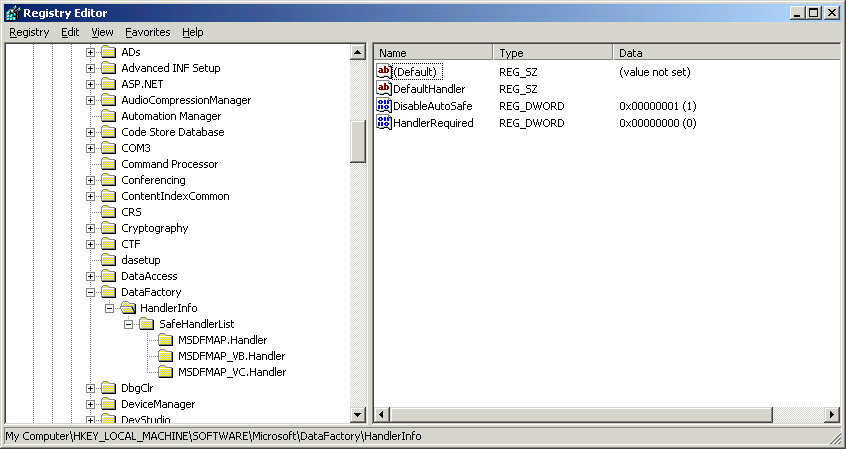
**Windows 2000**

* Locate the Handunsf.reg file located in the *System Drive Letter*:\Program Files\Common Files\System\msadc directory.
* Double click to run this file
* Reboot the computer, IIS will now be running in unsafe mode and it is possible to configure logging over HTTP
* It is possible to run IIS back to safe mode by running the handsafe.reg file and rebooting the computer – note the configuration for over HTTP will not work in safe mode.

**Windows XP and 2003 Server**

* Handunsf.reg has been removed from Windows 2003 for security reasons.
* In order to run IIS in unsafe mode it is required to change specific settings in the registry
* Click start>run>regedit
* Locate the Key HKEY\_LOCAL\_MACHINE \SOFTWARE\Microsoft\DataFactory\HandlerInfo\
* Locate the sub key HandlerRequired and change the value to 0 for “unsafe mode” (1 is for “safe mode”)
* Locate the sub key DefaultHandler and remove the MSDFMAP.Handler value

**Unsafe Mode Registry Values**



**Safe Mode Registry Values**

****

* Reboot the computer and IIS will now be running in unsafe mode and it is possible to configure logging over HTTP

**Configuring a Logger to log to an Access database over HTTP**

On the Loggers General Tab select database. On the Advanced tab click the user defined radio button in the Logger Database section.

Below is an example of a connection string which could be used with this configuration:

Provider=MS Remote;Remote Server= http://mesxp148/product\_name;Remote Provider=Microsoft.Jet.OLEDB.4.0;Data Source=\product\_name\database\Authors.mdb

In the example above Authors.mdb is the name of the Database to be used. In the example above mesxp148 is the computer name.

**Configuring a Logger to log to a SQL Server database over HTTP**

On the Loggers General Tab select database. On the Advanced tab click the user defined radio button in the Logger Database section.

Below is an example of a connection string which could be used with this configuration:

Provider=MS Remote;Remote Server=http://mesxp148/product\_name;Remote Provider=SQLOLEDB;Data Source=(local);Initial Catalog=Data;User ID=sa;Password=sa

In the example above Data is the name of the Database to be used. In the example above mesxp148 is the computer name.

**\*Note: The Database specified must exist on the Server.**

# Exposing SQL Server Logged data to Web Pages via XML

On the Web Server IIS for SQL Server XML Support must be installed and configured. IIS for SQL Server XML Support is only installed when SQL Server is installed on the server.

To configure IIS for SQL Server XML Support:

1. On the start menu, point to Program Files, click Microsoft SQL Server and then click IIS for SQL Server XML Support in IIS
2. Expand your server, right-click the Default Web Site folder, select New and then Select Virtual Directory.
3. On the General tab of the properties page, type XMLLoggedData for the virtual directory name.
4. For Local Path, type c:\reskit\xmlloggeddata. From Windows Explorer create this directory structure.
5. On the Security tab, enter a user name and password with administrator permissions in the Database where the logged data exists.
6. On the Database tab, enter the database server name, and then enter the Database name of the database which contains the logged data.
7. On the settings tab, select Virtual URL Queries and Template Queries
8. On the Virtual Names tab, click New and then add new virtual name of queries with a type of template and a path to c:\reskit\xmlloggeddata
9. Click OK to save the settings, and then close the Virtual Directory Management Tool.

To retrieve XML using a Transact-SQL statement in a URL

1. Launch Internet Explorer
2. In the address bar type a query similar to the following example:

http://*MachineName*/XMLLoggedData?sql=SELECT+*dt*,+*c5*+FROM+*LOGGER\_1\_DATA*+FOR+XML+raw&root=root

In the example above *MachineName* can be placed with the computer name where the database is located.

In the example above *dt* and *c5* are the two fields which are to be returned from the database. *LOGGER\_1\_DATA*  is the name of the table where the data is located.

# Select First Available Server

The sel\_first\_server.exe is installed to the product\bin folder when the Client is installed. When the application is run it will search the network for the first available server. The utility searches the network for the product name. When it finds a server it adds the server name to the Key: ServerName which is found in HKey\_Current\_User\Software\Measuresoft\Product\_Name

# Disabling Purge of Configuration Sub Directories

When a configuration is opened, the service is stopped and restarted. When the service starts it purges any device or processor subdirecties containing a config file which do not belong to the current configuration. E.g Old configuration contains modbu,1 in devcap.txt and new configuration contains modbu,2 in devcap.txt. When the new configuration is opened modbu\_2 is created and when service re-starts modbu\_1 is deleted.

This functionality can be stopped by setting the following registry entry.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\*PurgeConfigSubdirs** OFF

# Enabling Debug for the PID Controller

The PID Controller contains a debug facility which allows it to be debugged at run-time should an error occur. To enable this facility a number of **Registry Entries** must be set:

## Switching Debugging On

To switch debugging on for all PID Controller loops simply add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\PID\_Debug*** and set its value to “**ON”.**

To switch debugging on for a PID Controller specific loop simply add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\PID\_<No>\_Debug*** and set its value to “**ON”.**

## Selecting the Debug Type

The PID Controller allows you to output the debug information to a Console Window, Text File or as a Trace Statement which can be displayed by applications such as DBWIN32.EXE.

To enable these facilities for all PID Controller loops add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\PID\_DebugType***

To switch debugging on for a PID Controller specific loop simply add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\PID\_<No>\_DebugType***

The values of this key can be as follows:

**“CON”** to send output to a console window

**“FILE”** to send the output to a text file or

**“TRACE”** to send the output as a trace statement.

These can be concatenated to send the output to multiple types by using the **|** symbol.

e.g. “**FILE|CON”** would send the output to both File and Console Window.

When sending output to the **FILE** type you must specify the file.

**Note:** Console (CON) is not supported on Windows Vista. Instead set the output mode to TRACE, and to view the debug data you must use SysInternals Debug Viewer. This can be downloaded from <http://www.microsoft.com/technet/sysinternals/Utilities/DebugView.mspx>

In order for Console mode to work on Windows XP the service must be configured to logon as the System Account with Interact with Desktop enabled

# Adding directories on a Save

When a configuration is saved the CURRENT\_CONFIG, REPLAY\_OPTIONS and SAVED\_VALUES directories are saved in a single file.

Additional directories can be added to the saved file by setting the following registry entry.

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\*ExtraSaveDirs** CMONITORS;TRENDS;C:\DIR

Directories are separated by a ;. If the path is not absolute, then it is a product subdirectory.

# Adding registry entries on a setup

If a product.reg is dropped into the DISK1 directory containing setup.exe, the setup will automatically apply the registry settings in the product.reg file during the setup. The product.reg file must be in the format of the Windows registration file format generated when exporting parts of the registry using regedit e.g.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<PRODUCT NAME>]

"TagSize"=dword:00000008

"DescSize"=dword:00000016

# Storing Digital States as Text in Database Logs

The database loggers can store digital state as 32 character text instead of an integer.

To switch debugging on add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\DatabaseDigitalText*** and set its value to RES\_SZ value of “**ON”.**

To store as a varchar(32) instead of a char(32) set the key to varchar(32).

# Storing DATATIME in UTC format in Database Logs

The database loggers by default store local time in databases.

To store in Universal Coordinated Time add the following registry key

***HKEY\_LOCAL\_MACHINE\SOFTWARE\Measuresoft\<ProductName>\DatabaseUTC*** and set its value to RES\_SZ value of “**ON”.**

**Note: This does not work under Windows 2000.**