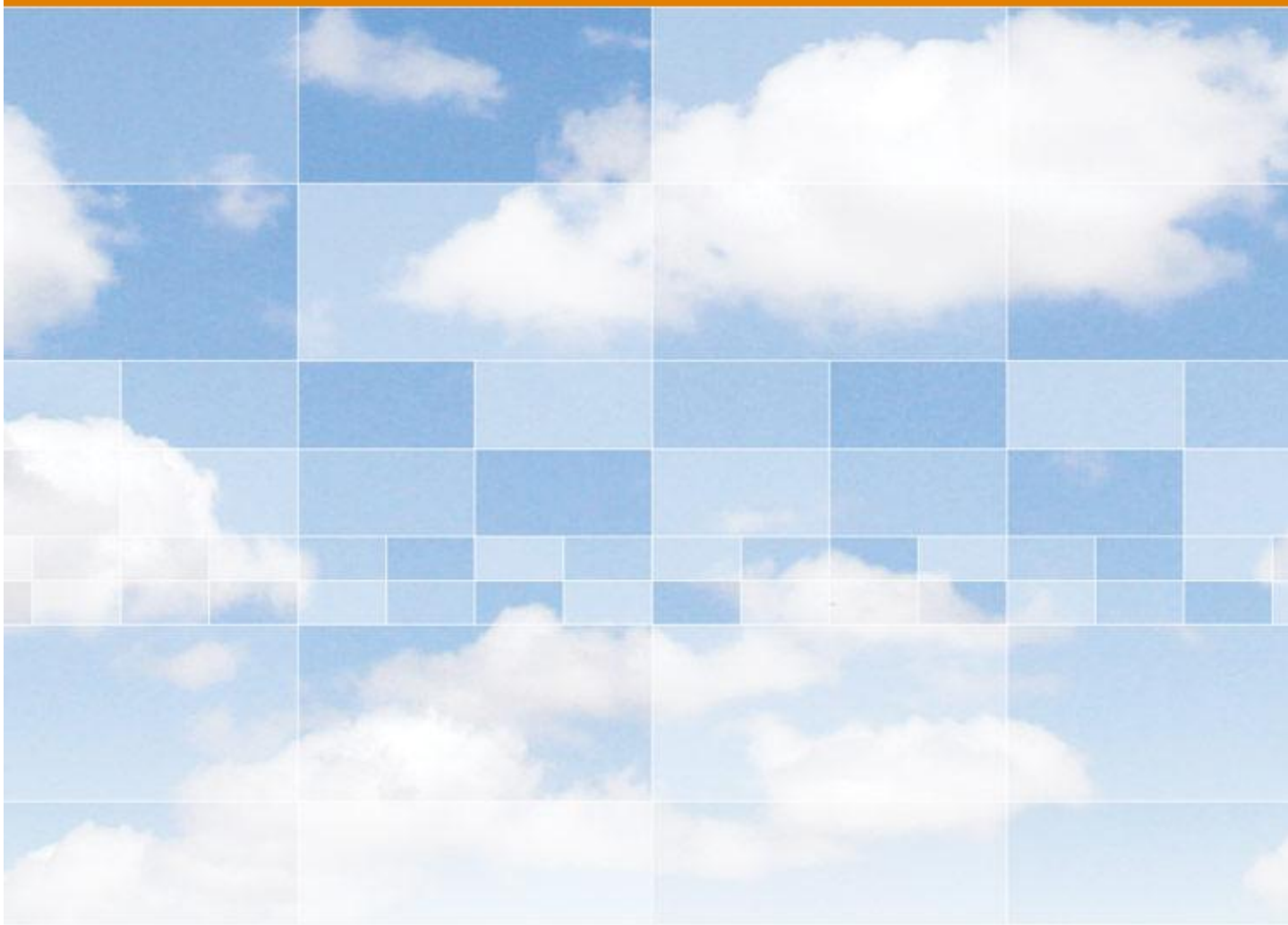




MatrikonOPC Server for SCADA DNP3

User's Manual

MatrikonOPC Server for SCADA DNP3

User's Manual

This manual is a product of Matrikon Inc.

Matrikon Inc.
Suite 1800, 10405 Jasper Avenue
Edmonton, AB T5J 3N4
Canada

Phone: +1.780.448.1010
Fax: +1.780.448.9191
www.matrikonopc.com

Document Revision History:

Date	Document Version	Description	Author
2002-10-15	1.0	Initial document.	JC
2004-01-09	1.1	Minor change to Time Bias field.	RS
2004-04-05	1.2	Changes to timestamps, DNP3 objects, and protocol fragment handling. Added Chapter 6. Minor revisions throughout manual.	RS
2004-06-22	1.3	Added Appendix D.	RS
2010-01-28	2.0	Updated software version to 1.1.0.0. Template conversion and complete rewrite.	CGAP, LB
2010-02-16	2.1	Updated Licensing, Installed Files, and Troubleshooting sections to include software and hardware licensing.	LB
2010-02-19	2.2	Removed sections referencing unused features. Corrected list of appendices.	CGAP
2010-02-23	3.0	Updated to software v1.2.0.0. Added Offline Mode and support for group 0 and 3 to OPC Data Items section. Updated Software Requirements, Installation section screenshots, Installed Files, Licensing, DNP Implementation, Appendix H – Features and Examples.	CGAP, LB
2010-03-01	3.1	Added item concerning configurations for unsolicited communication to Limitations section. Updated Output Objects in OPC Data items section.	CGAP, LB
2010-03-12	3.2	Added UDP limitation information to the network channel device link configuration and limitations section.	CGAP

2010-05-25	4.0	Updated software version to 1.2.1.0.	GW, LB
2010-05-26	4.1	Updated installed files list.	GW
2013-05-31	5.0	Updated software version to 1.2.2.0	SG
2013-11-06	6.0	Updated software version to 1.2.3.0	WXF

SOFTWARE VERSION

Version: 1.2.3.0

DOCUMENT VERSION

Version: 6.0

COPYRIGHT INFORMATION

© **Copyright 1997 - 2013**, Matrikon Inc. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, translated, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of Matrikon Inc.

CONFIDENTIAL

The information contained herein is confidential and proprietary to Matrikon Inc. It may not be disclosed or transferred, directly or indirectly, to any third party without the explicit written permission of Matrikon Inc.

LIMITATIONS

Matrikon has made its best effort to prepare this manual. Matrikon makes no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accepts no liability of any kind including without limitation warranties of merchantable quality, satisfactory quality, merchantability and fitness for a particular purpose on those arising by law, statute, usage of trade, course of dealing or otherwise. Matrikon shall not be liable for any losses or damages of any kind caused or alleged to be caused directly or indirectly from this manual.

LICENSE AGREEMENT

This document and the software described in this document are supplied under a license agreement and may only be used in accordance with the terms of that agreement. Matrikon reserves the right to make any improvements and/or changes to product specifications at any time without notice.

TRADEMARK INFORMATION

The following are either trademarks or registered trademarks of their respective organizations:

Matrikon and MatrikonOPC are trademarks or registered trademarks of Matrikon Inc.

OTHER

MatrikonOPC™ is a division of Matrikon™ Inc.

Table of Contents

Introduction	11
Who Should Use This Manual	11
Overview of Manual	11
References	12
Terminology	13
Getting Started.....	14
System Requirements	14
<i>Software Requirements</i>	<i>14</i>
<i>Hardware Requirements</i>	<i>14</i>
Installation	15
Installed Files.....	25
Licensing.....	26
Contacting Support.....	27
Configuration	28
Configuring Dynamic Data Exchange (DDE)	28
Starting the MatrikonOPC Server for SCADA DNP3.....	29
Tool Tray Menu	29
Control Panel	30
Configuration Window	31
<i>File Menu.....</i>	<i>33</i>
<i>Edit Menu</i>	<i>33</i>
<i>View Menu.....</i>	<i>34</i>
<i>Tools Menu</i>	<i>34</i>
<i>Help Menu</i>	<i>35</i>
Options Window	35
<i>General Options</i>	<i>35</i>
<i>General Logging Options.....</i>	<i>37</i>
<i>Interface Logging Options.....</i>	<i>38</i>
<i>Advanced Options.....</i>	<i>39</i>
Server Configuration.....	41
<i>Inserting New Objects</i>	<i>41</i>
<i>Creating and Configuring a Fail-Over Channel Object</i>	<i>42</i>
<i>Creating and Configuring a Network Channel Object</i>	<i>47</i>
<i>Creating and Configuring a Serial Channel Object</i>	<i>49</i>
<i>Creating and Configuring a Network Host Object</i>	<i>54</i>
<i>Creating and Configuring a Dial-Up Connection Object</i>	<i>57</i>
<i>Creating and Configuring a DNP3 Unit Object</i>	<i>63</i>
<i>Creating and Configuring a Radio Link</i>	<i>68</i>
<i>Changing Objects</i>	<i>71</i>
<i>Removing Objects.....</i>	<i>71</i>
Alias Configuration	72
<i>Inserting Alias Groups</i>	<i>72</i>
<i>Renaming Alias Groups.....</i>	<i>72</i>
<i>Inserting New Aliases.....</i>	<i>72</i>
<i>Editing Aliases.....</i>	<i>76</i>
<i>Removing Aliases</i>	<i>76</i>
<i>Removing Alias Groups.....</i>	<i>76</i>
<i>Exporting Aliases</i>	<i>76</i>
<i>Importing Aliases.....</i>	<i>77</i>
Expression Wizard	77

Item Path Browser	81
Saving a Configuration	83
Clearing a Configuration	83
Loading an Existing Configuration	83
Shutting Down the Server	83
OPC Data Items	85
<i>Device Attributes</i>	86
<i>Static Objects</i>	87
<i>Output Objects</i>	88
<i>Poll Options</i>	90
Getting Data without Being Connected to a Device	93
Diagnostics	94
Logging	94
DNP Implementation	95
Subset Level 3	95
Limitations	100
Troubleshooting	102
Problems and Solutions	102
Un-Installation	111
OPC Compliance	116
Installation	116
Common Interfaces	116
Data Access	116
<i>Groups</i>	117
<i>Items</i>	117
<i>Browsing and Item Properties</i>	117
<i>I/O Operations</i>	117

Table of Appendices

Appendix A Distributed COM (DCOM)	119
DCOM Configuration Utility	119
Default Properties	119
Security Permissions	120
Server Identity	124
Default Protocols	124
Remote Program ID	125
Appendix B Aliases	126
Scaling Expressions	126
Scaling Calculations	127
CSV File Format	129
Scaling Algorithms	131
Appendix C Standard Data Types	132
Appendix D Microsoft Excel as a DDE Client	133
DDE Read	133
DDE Write	133
Net DDE	134
Appendix E Security	135
Introduction	135
OPC Security Implementation	135
MatrikonOPC Tag Security Configuration Utility	136

Security Details	158
Appendix F Offline Mode	161
Introduction.....	161
Offline Mode Toggling	161
Offline Mode Item Values.....	161
Operational Effects	162
Appendix G SCADA Servers Connection Logic.....	163
Introduction.....	163
Polling.....	163
Connection Failures and Reconnection Logic	163
Appendix H Features and Examples.....	164
Introduction.....	164
Round-Robin Example.....	164
<i>Writes</i> OPC Item	167
<i>PacketSent</i> and <i>PacketReceived</i> OPC Items.....	167
Total Reads and Writes Indicators.....	168
Appendix I OPC Items	170
Introduction.....	170
Base OPC Items	170
Generic OPC Items	170
Network Channel Object OPC Items	172
Network Host Object OPC Items	172
Fail-Over Channel Object OPC Items.....	172
Serial Channel Object OPC Items.....	173
Radio Object OPC Items	174
Dial-Up Object OPC Items.....	175

Table of Figures

Figure 1 - InstallAware Wizard Verification Window	15
Figure 2 - License Agreement Screen	16
Figure 3 - Setup Type Window	17
Figure 4 - Destination Folder Screen	18
Figure 5 - Start Menu Screen.....	19
Figure 6 - Enter Password Screen	20
Figure 7 - Licensing Screen	21
Figure 8 - Ready to Install Screen	22
Figure 9 - Installing MatrikonOPC Server for SCADA DNP3 Screen.....	23
Figure 10 - MatrikonOPC Server for SCADA DNP3 Setup Complete Screen	24
Figure 11 - Tool Tray	29
Figure 12 - Tool Tray Menu.....	30
Figure 13 - Control Panel	30
Figure 14 - Configuration Window.....	32
Figure 15 - General Options Tab.....	36
Figure 16 - General Logging Options Tab	37
Figure 17 - Interface Logging Options Tab	39
Figure 18 - Advanced Options Tab.....	40
Figure 19 - Insert New Object Window	41
Figure 20 - Create New Fail-Over Channel Window	43
Figure 21 - Fail-Over Channel - Communication Tab	44
Figure 22 - Fail-Over Channel - Load Distribution Tab	45

Figure 23 - New Fail-Over Channel Object.....	46
Figure 24 - Create New Network Channel Window	47
Figure 25 - New Network Channel Object.....	49
Figure 26 - Create New Serial Channel Window - Communication Tab	50
Figure 27 - Create New Serial Channel Window - Data Acquisition Tab	52
Figure 28 - New Serial Channel Object	54
Figure 29 - Create New Network Host Window	55
Figure 30 - Insert New Object	56
Figure 31 - New Network Host Object	57
Figure 32 - Create New Dial-Up Connection Window - Dial-Up Tab	58
Figure 33 - Create New Dial-Up Connection Window - Modem Tab.....	60
Figure 34 - Create New Dial-Up Connection Window - Advanced Tab.....	61
Figure 35 - New Dial-Up Connection Object	63
Figure 36 - Create New DNP3 Unit - Communication Tab	64
Figure 37 - Create New DNP3 Unit - Data Acquisition Tab	66
Figure 38 - Create New DNP3 Unit - Optimization Tab	67
Figure 39 - Create New Radio Window	69
Figure 40 - Insert New Object	70
Figure 41 - New Radio Link	71
Figure 42 - Client Reference Warning Message	71
Figure 43 - Insert New Alias Window	73
Figure 44 - Insert New Alias Window Scaling Options.....	74
Figure 45 - Contents Table	75
Figure 46 - Expression Tab.....	78
Figure 47 - Expression Wizard.....	79
Figure 48 - Select Function Window	79
Figure 49 - Select Variable Window.....	80
Figure 50 - User Defined Functions Editor	80
Figure 51 - Operators Buttons.....	80
Figure 52 - Calculation Tab	82
Figure 53 - Item Path Browser	82
Figure 54 - Registry Editor	103
Figure 55 - Program ID Branch	104
Figure 56 - Add or Remove Programs.....	111
Figure 57 - Welcome to the MatrikonOPC Server for SCADA DNP3 Maintenance Screen	112
Figure 58 - Ready to Uninstall Screen	113
Figure 59 - Uninstalling MatrikonOPC Server for SCADA DNP3 Screen	114
Figure 60 - MatrikonOPC Server for SCADA DNP3 Setup Complete Screen	115
Figure 61 - Distributed COM Configuration Properties Window	121
Figure 62 - Distributed COM Configuration Security Tab	122
Figure 63 - Registry Value Permissions Window	123
Figure 64 - Add Users and Groups Window	123
Figure 65 - DDE Share	134
Figure 66 - Start Menu Navigation.....	137
Figure 67 - Enter Server Password Window	137
Figure 68 - MatrikonOPC Tag Security Configuration Utility Main Screen	138
Figure 69 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups	139
Figure 70 - Add User Window (NT).....	140
Figure 71 - Defined Users and Groups	141
Figure 72 - Add User Window (Private).....	142
Figure 73 - Add Group Window (NT)	143
Figure 74 - Add Group Window (Private)	144

Figure 75 - Enter New Name Window	144
Figure 76 - Edit <Username> Window (Permissions Tab)	146
Figure 77 - Add Permission Screen (Server Address Space)	147
Figure 78 - Add User Permission Window	148
Figure 79 - Add Permission Window: Browsing Server Address Space	149
Figure 80 - Edit <Username>: Example	150
Figure 81 - Edit <Username> Window (General Tab)	151
Figure 82 - Reset Password Window	151
Figure 83 - Edit <Groupname> Window (Permissions Tab)	152
Figure 84 - Edit <Groupname> Window (General Tab)	153
Figure 85 - Edit <Groupname> Window (Members Tab)	154
Figure 86 - Add Existing User Window	155
Figure 87 - Change Password Window	156
Figure 88 - Example	163
Figure 89 - Example 1	164
Figure 90 - Unit B Fails	165
Figure 91 - Retry Applied on Unit B Items	165
Figure 92 - Failed Polls Allowed Counter	166
Figure 93 - Unit B Confirmed Failure	166
Figure 94 - Reconnect Delay	166
Figure 95 - Reconnect Retries	166
Figure 96 - Packets Sent and Received at a Certain Point	167
Figure 97 - Server Configuration	168
Figure 98 - Monitoring Request and Reply Counters from the Client	168

Table of Tables

Table 1 - Terms and Definitions	13
Table 2 - Files Installed in "SCADA DNP3" Folder	26
Table 3 - Files Installed in "Common" Folder	26
Table 4 - Files Installed in "system32" Folder	26
Table 5 - MatrikonOPC Support Regional Contact Information	27
Table 6 - After-Hours Support	27
Table 7 - Tool Tray Menu Commands	30
Table 8 - Control Panel Commands	31
Table 9 - Configuration Window Commands	33
Table 10 - File Menu Commands	33
Table 11 - Edit Menu Commands (Server Configuration)	34
Table 12 - Edit Menu Commands (Alias Configuration)	34
Table 13 - View Menu Commands	34
Table 14 - Tools Menu Commands	35
Table 15 - Help Menu Commands	35
Table 16 - General Options Tab Fields	37
Table 17 - General Logging Options Tab Fields	38
Table 18 - Interface Logging Options Tab Fields	39
Table 19 - Advanced Options Tab Fields	40
Table 20 - Insert New Object Window Options	42
Table 21 - Fail-Over Channel - Communication Tab Components	45
Table 22 - Create New Network Channel Window Components	48
Table 23 - Create New Serial Channel Window - Communication Tab Components	52
Table 24 - Create New Serial Channel Window - Data Acquisition Tab Components	53

Table 25 - Create New Network Host Window Components	56
Table 26 - Create New Dial-Up Connection Window - Dial-Up Tab Components	59
Table 27 - Create New Dial-Up Connection Window - Modem Tab Components.....	60
Table 28 - Create New Dial-Up Connection Window - Advanced Tab Components	62
Table 29 - Create New DNP3 Unit – Communication Tab Components.....	65
Table 30 – Create New NDP3 Unit – Data Acquisition Tab	67
Table 31 - Create New DNP3 Unit – Optimization Tab	68
Table 32 - Create New Radio Window Components	70
Table 33 - Insert New Alias Window Options	74
Table 34 - Insert New Alias Window Scaling Options	74
Table 35 - Expression Wizard Options	77
Table 36 - Item Path Browser Options	81
Table 37 - Communication Options for Device Items.....	86
Table 38 - Device Attributes.....	87
Table 39 - Static Objects	88
Table 40 - Output Objects	89
Table 41 - Poll Options	91
Table 42 - DNP3 Unit Communication Configuration Parameters	93
Table 43 - Implemented Data Objects, Variations, Function Codes, and Range Qualifiers	99
Table 44 - Expressions Constructs for Alias Scaling	127
Table 45 - Calculation Operators for Alias Scaling	128
Table 46 - Calculation Functions for Alias Scaling	129
Table 47 - File Import/Export Field Descriptions	130
Table 48 - Additional File Import/Export Field Descriptions - Linear/Square Root Scaling	130
Table 49 - Additional File Import/Export Field Descriptions - Offset Scaling.....	130
Table 50 - Additional File Import/Export Field Descriptions - Expression Scaling	131
Table 51 - Additional File Import/Export Field Descriptions - Calculation Scaling	131
Table 52 - Scaling Algorithms.....	131
Table 53 - Standard Data Types	132
Table 54 - Default Tag Security	156
Table 55 - Example 1.....	157
Table 56 - Example 2: Permissions.....	157
Table 57 - Example 2: Groups and Members.....	157
Table 58 - Example 2: Permissions.....	160
Table 59 - Offline Mode Item Values	162
Table 60 - Root Device Link OPC Items	170
Table 61 - Generic OPC Items	171
Table 62 - Network Channel OPC Items.....	172
Table 63 - Network Host OPC Items	172
Table 64 - Fail-Over Channel OPC Items.....	173
Table 65 - Serial Channel Object OPC Items.....	174
Table 66 - Radio Object OPC Items	175
Table 67 - Dial-Up Object OPC Items.....	176

Introduction

The MatrikonOPC™ Server for SCADA DNP3 provides OPC access to field devices compatible with of the DNP3 protocol and supports supervisory control and data acquisition applications, even under adverse site conditions (e.g., poor throughput, line noise).

The MatrikonOPC Server for SCADA DNP3 includes support for the following communication methods:

- Multiple communications channels at the same time (serial, radio, network, and dial-up).
- Round-robin polling.
- Detailed polling schedule.
- Optimized for low-bandwidth and noisy communication channels.
- Runs as a Windows service.
- DNP3 master including level 1, level 2, and level 3 plus selected vendor extensions (strings, reporting dead band, frozen analog inputs, etc.).
- Supervisory control using single-destination and broadcast commands.

Who Should Use This Manual

This manual is intended for all users of MatrikonOPC Server for SCADA DNP3. This manual explains how to install, license, and configure the software, and how to perform common tasks. In addition and where required, technical information about OPC data items, diagnostics information, and a troubleshooting section is included.

Overview of Manual

This manual uses icons to highlight valuable information. Remember these icons and what they mean, as they will assist you throughout the manual.

	This symbol denotes important information that must be acknowledged. Failure to do so may result in the software not functioning properly.
BOLD	Font displayed in this color and style indicates a hyperlink to the applicable/associated information within this manual, or if applicable, any external sources.

The *User's Manual* has been designed so that you can click on references in the document to jump to that referenced point without having to scroll through several pages (in some cases). For example, if you were to see the sentence "Refer to Figure 1 for more information", pressing the **CTRL** key and clicking your mouse on the text "Figure 1" will automatically take you to the location of Figure 1 within the document.

This manual consists of several chapters and is structured as follows:

- **Introduction** – this introductory chapter.
- **Getting Started** – provides instructions for installing the software, and MatrikonOPC Support team contact information.

- **Configuration** – shows how to start and configure the server, and describes each component in detail including windows/screens, panels/tabs, and menu commands.
- **OPC Data Items** – describes the server's items.
- **Diagnostics** – explains how to use logging, statistical items, data qualities and timestamps, and result codes to get the most efficiency from the user's system.
- **DNP Implementation** – explains how the server fully implements the data link, transport, and application layers of the DNP protocol.
- **Limitations** – provides information on specific performance and operational limitations of the software.
- **Troubleshooting** – provides solutions for common problems that may be encountered, and answers to frequently asked questions.
- **Un-installation** – provides instructions on un-installing the software.
- **OPC Compliance** – details supported interfaces with regard to installation, common interfaces, and data access.
- **Implementation** – details the server's device-specific implementation.
- **Appendices:**
 - **A** - DCOM
 - **B** - Aliases
 - **C** - Standard Data Types
 - **D** - Microsoft Excel as a DDE Client
 - **E** - Security
 - **F** - Offline Mode
 - **G** - SCADA Servers Connection Logic
 - **H** - Features and Examples
 - **I** - OPC Items

References

This document references information found within the following documents/sites:

- www.opcfoundation.org
- www.matrikonopc.com
- www.opcsupport.com
- <http://www.dnp.org>
- *International Standard DNP3*
- *DNP3 Specification, Volume 7: IP Networking*
- *OPC Overview 1.0*
- *OPC Common Definitions and Interfaces 1.0*
- *OPC Security Custom Interface 1.0*
- *OPC Alarms and Events Interface Standard 1.10*

- OPC Data Access Custom Interface Standard 2.05a
- OPC Data Access Custom Interface Standard 3.00

Terminology

The terms *screen* and *window* are used interchangeably throughout this document.

Table 1 provides a list of definitions for terms used throughout this document.

Term/Abbreviation	Description
ADT	Asynchronous Data Transfer.
API	Application Programming Interface.
COM	Component Object Model. A method for organizing software, specifying how to build components that can be dynamically interchanged.
DA	OPC Data Access. Provides access to real-time process data.
DCOM	Distributed Component Object Model. An extension of COM that allows communication between COM components over a network.
DDE	Dynamic Data Exchange. Allows the transfer of data between two running applications.
Matrikon	Matrikon Inc.
MatrikonOPC	Matrikon's brand name for its OPC servers and clients.
OPC	The communication standards published by the OPC Foundation. Refer to www.opcfoundation.org for more information.
PLC	Programmable Logic Controller.
SCADA	Supervisory Control And Data Acquisition. Software that is interfaced to hardware via a PLC or other API.
DNP3	The Distributed Network Protocol. DNP3 is defined and managed by the DNP Users Group. Refer to www.dnp.org for more information.

Table 1 - Terms and Definitions

Getting Started

This section of the User's Manual contains important information regarding software installation and how to contact MatrikonOPC's Support team.

The **System Requirements** section shows how to avoid future problems by ensuring that the system meets the minimum software and hardware requirements. Detailed, step-by-step instructions in the **Installation** section will guide you through the installation process and provide a list of files that are installed during this process.

Once the software is installed, refer to the **Licensing** section for information on how to obtain the appropriate license. The *Licensing* section will refer you to the *Licensing Procedures* document that was installed along with the server and this *User's Manual*. The **Contacting Support** section will provide you with contact information for the MatrikonOPC Support team, should you have any problems during the installation or licensing of the software.

System Requirements

The software has **Software** and **Hardware** system requirements. These requirements must be met for the software to function properly.



Note: To install and configure a MatrikonOPC server, you must be set up as an administrative user account rather than a restricted user account.

Software Requirements

The following software is required:

- Microsoft Windows XP SP0, or
- Microsoft Windows 2003 SP0, or
- Microsoft Windows Server 2000 SP3
- Microsoft .NET 1.1 Framework (included with installation package)

Your system must have the following additional software to use the corresponding functionality:

- TCP/IP or UDP/IP terminal server



Note: It is recommended that the most current service packs are installed.

Hardware Requirements

The following hardware is required:

- Intel® Pentium® 4 Processor
- 512 MB RAM
- 40 GB 7200 RPM Hard Drive

The server requires the following additional hardware to make use of additional functionality:

- Serial communications port
- RS-232/422/485 cabling and/or converter

- Radio modem
- Hayes-compatible dial-up modem
- CDPD modem with support for the AT command set
- IP-compatible network

Installation

Once the system requirements have been met, you are ready to install the software.



Note: As part of the installation process, the **MatrikonOPC Analyzer** tool is installed and used to detect the system settings that affect the use of this software. No information is communicated back to Matrikon. Information is stored on this system **only** for future use by MatrikonOPC Support to assist with troubleshooting, if required.

To install the software:

1. Insert the MatrikonOPC Server for SCADA DNP3 CD into the CD drive.
2. If the MatrikonOPC **Welcome** screen does not automatically appear, double-click the *MatrikonOPCSCADADNP3.exe* file. The **MatrikonOPC Server for SCADA DNP3 – InstallAware Wizard** verifies its contents (Figure 1) and the **License Agreement** screen (Figure 2) appears.

Notes:

- The **Version** number located in the lower left corner indicates the version number of the software that is being installed. The text "X.X.X.X" will be replaced with the specific product version.
- From the **License Agreement** screen, you have the option of selecting the **I reject the license agreement** option. Selecting the **I reject the license agreement** option button disables the **Next** button so your options are to cancel the install by clicking on the **Cancel** button, or select the **I accept the license agreement** option button enabling you to proceed through the install.

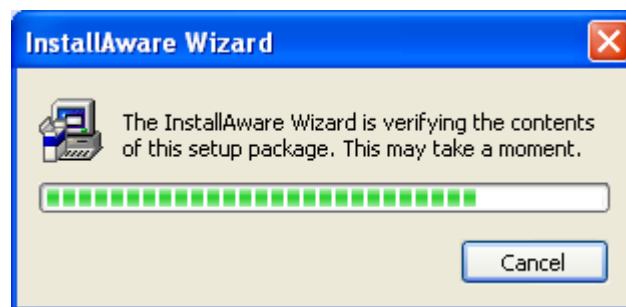


Figure 1 - InstallAware Wizard Verification Window

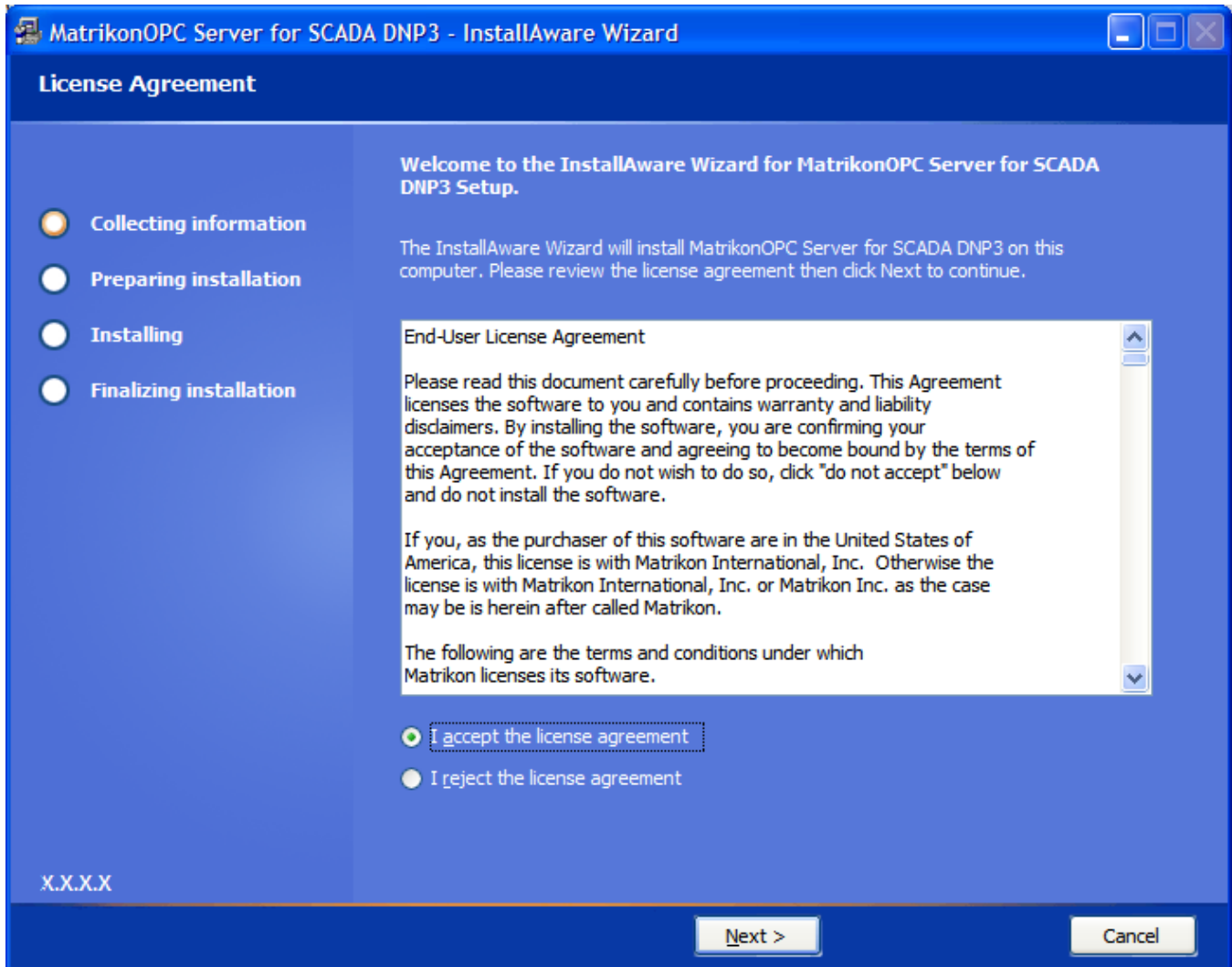


Figure 2 - License Agreement Screen

3. Read the **Software License Agreement**, using the scroll bar to view the entire message.
4. Select the **I accept the license agreement** option button.
5. Click on the **Next** button. The **Setup Type** screen (Figure 3) appears.

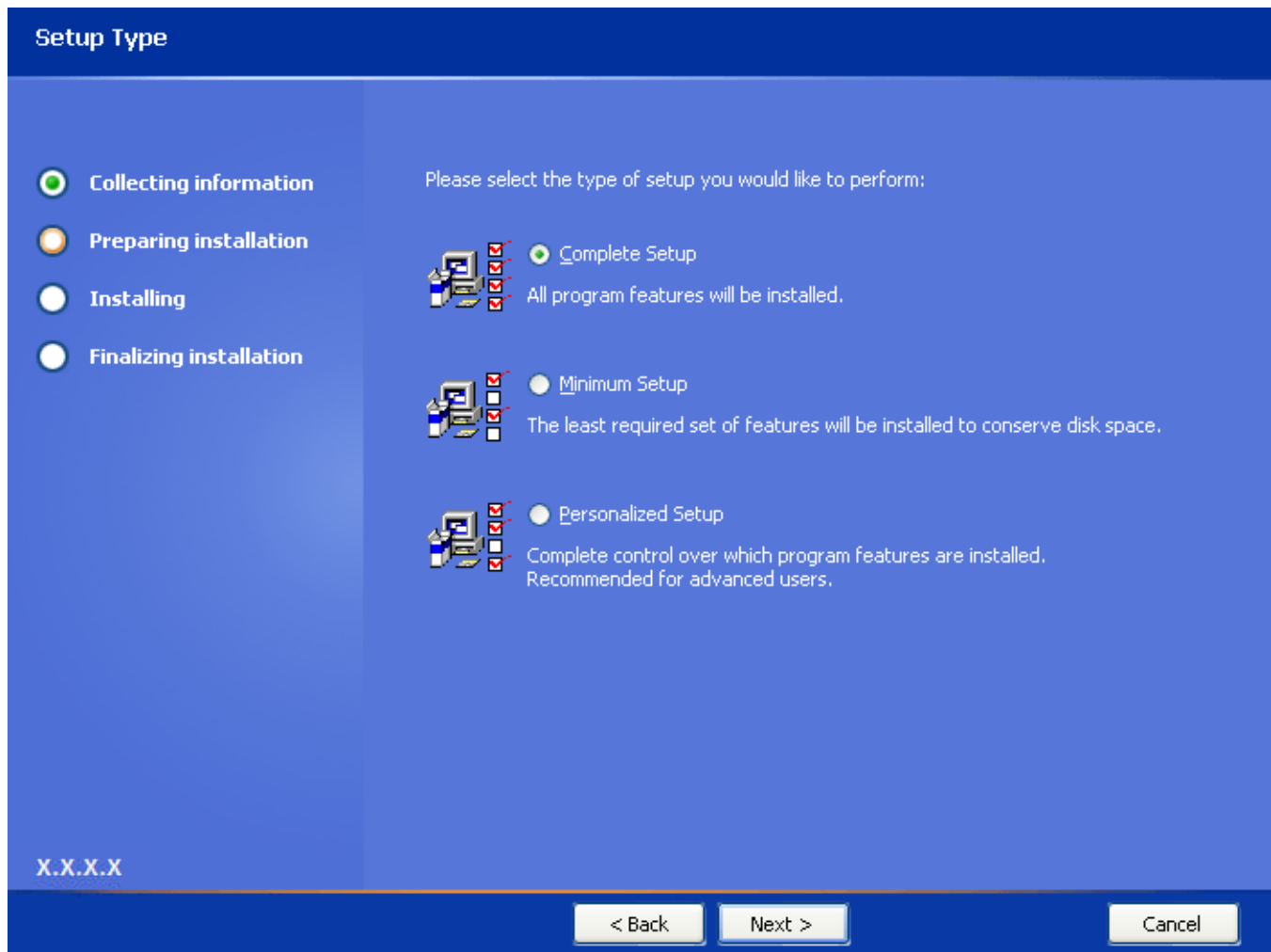


Figure 3 - Setup Type Window

6. Select the type of setup to be performed.

Note: Matrikon recommends that you select the **Complete Setup** option.

7. Click on the **Next** button. The **Destination Folder** screen (Figure 4) appears.

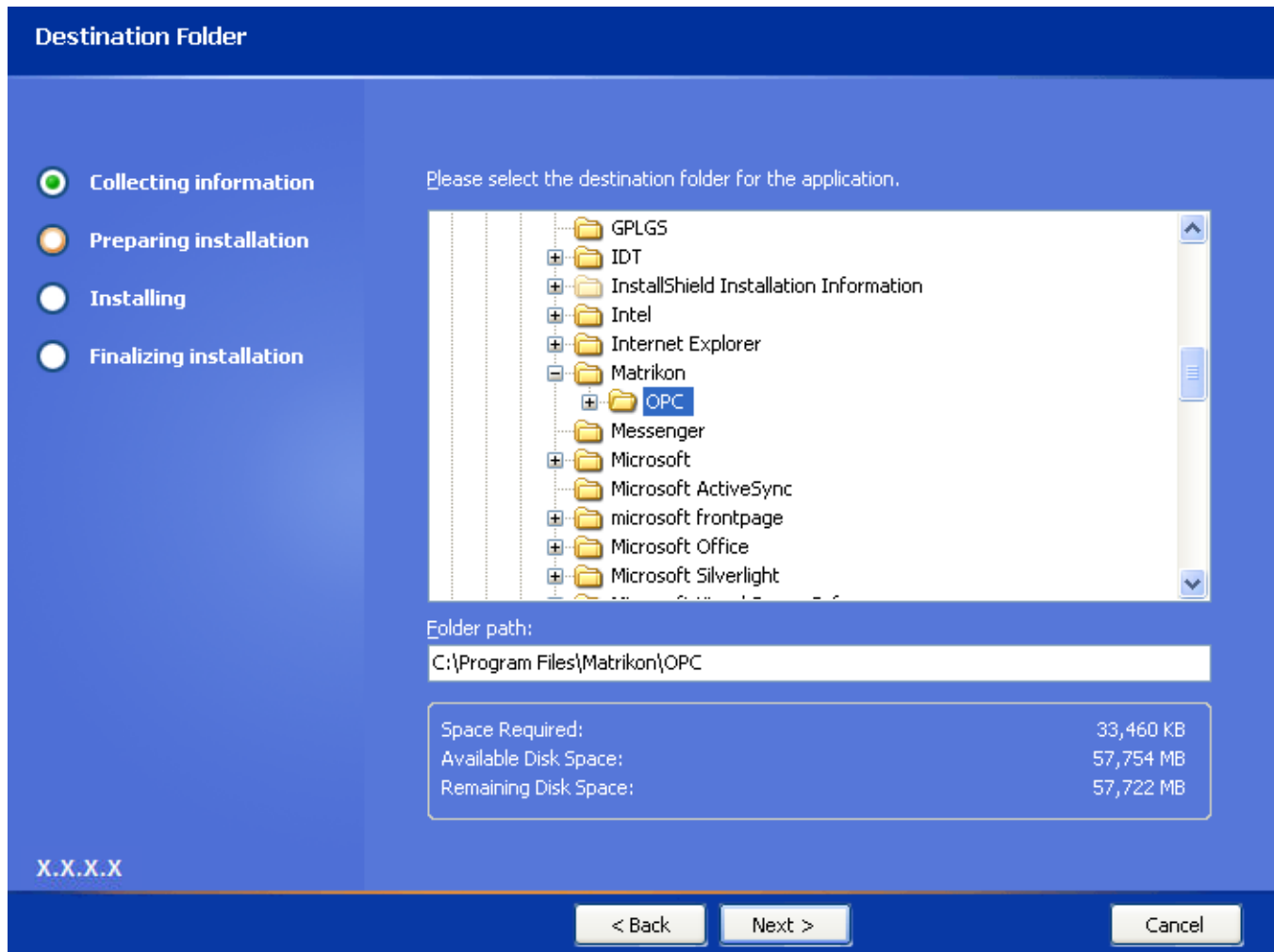


Figure 4 - Destination Folder Screen

8. Select the folder in which to install MatrikonOPC Server for SCADA DNP3, or accept the default location displayed in the **Folder path** field.
9. Click on the **Next** button. The **Start Menu** screen (Figure 5) appears.

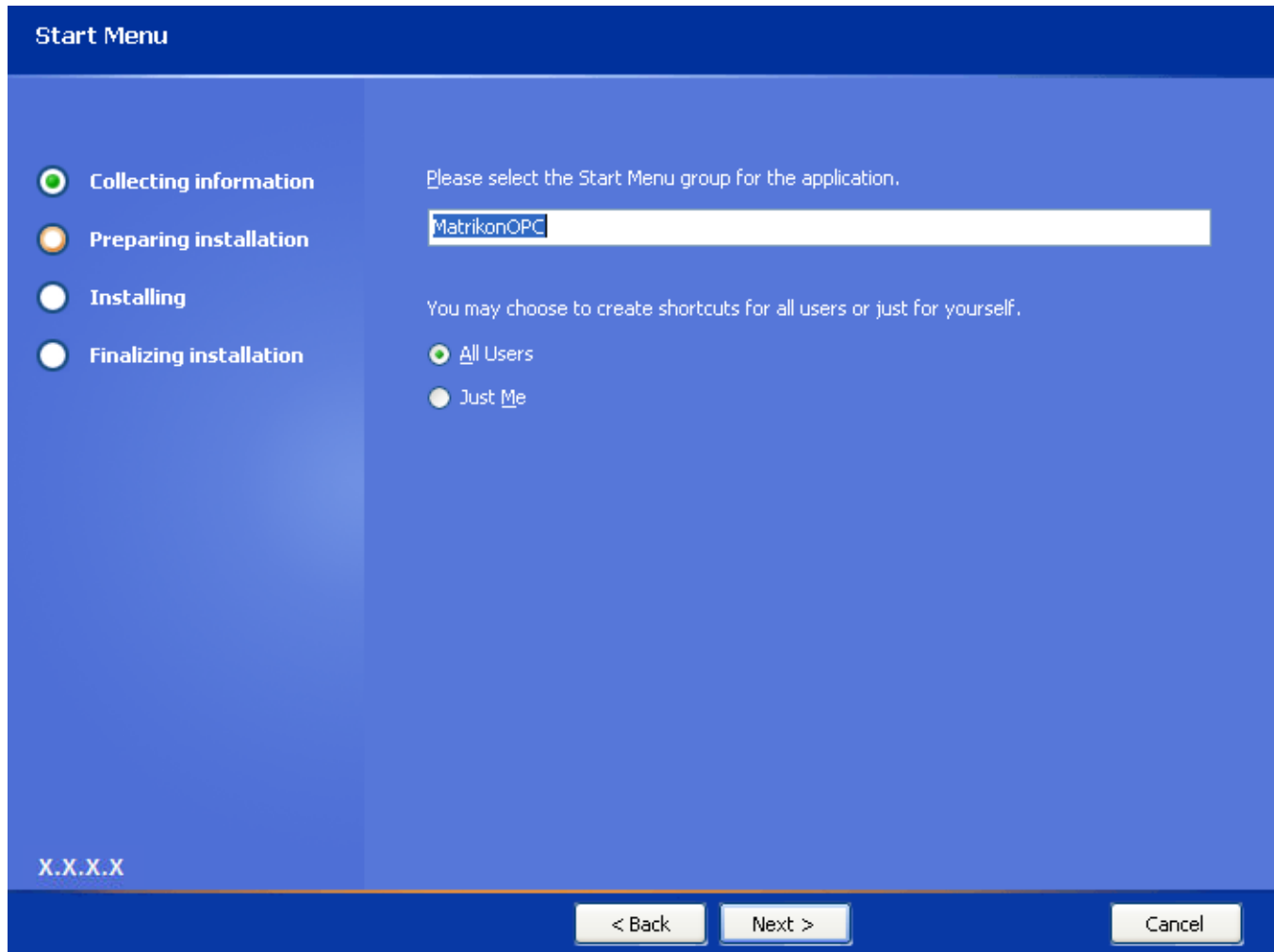
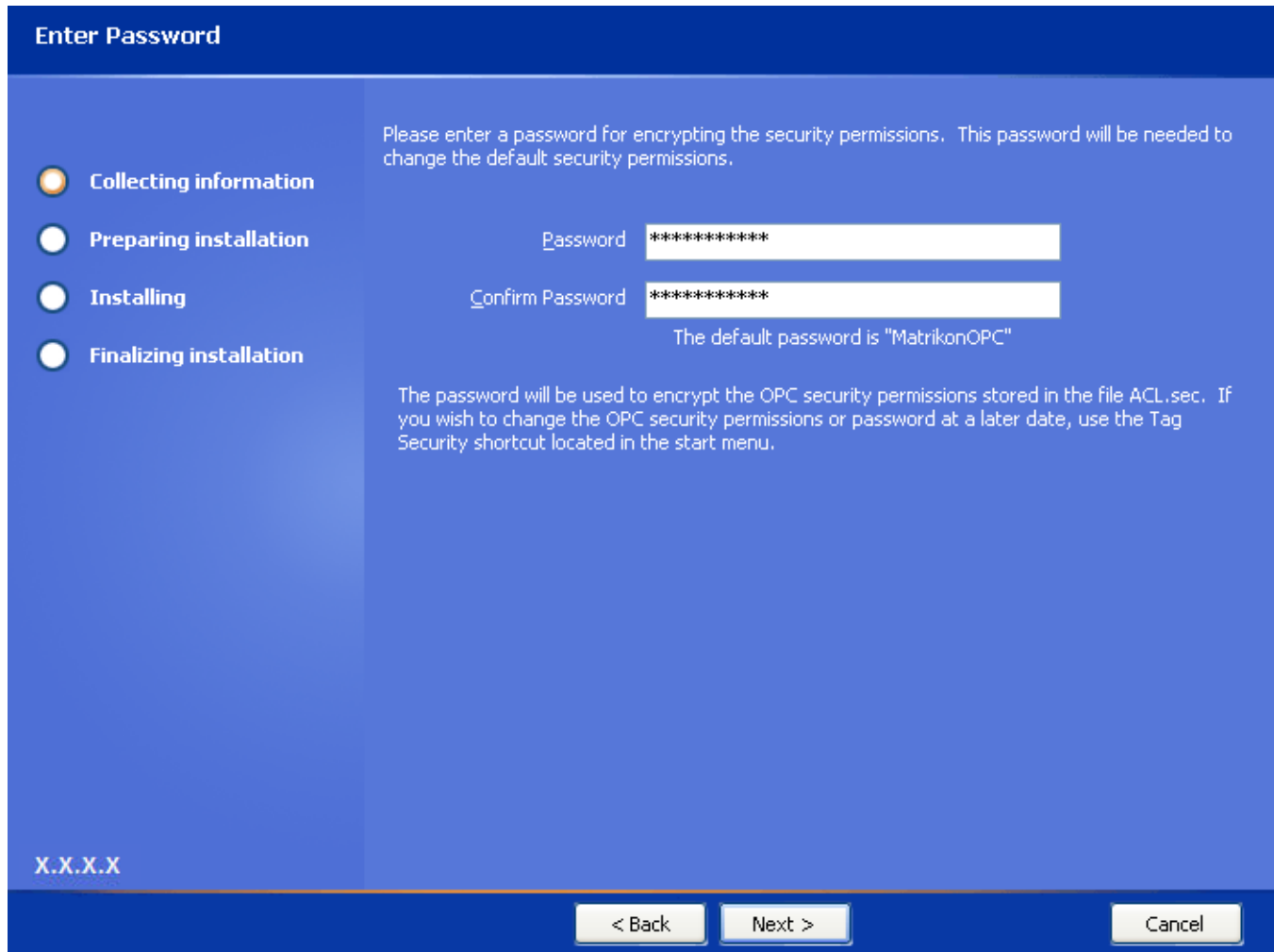


Figure 5 - Start Menu Screen

10. Select the Start Menu group and specify whether you want shortcuts created only for yourself, or for all users, by selecting the applicable option button.
11. Click on the **Next** button. The **Enter Password** screen (Figure 6) appears.



Enter Password

Please enter a password for encrypting the security permissions. This password will be needed to change the default security permissions.

☒ Collecting information
☐ Preparing installation
☐ Installing
☐ Finalizing installation

Password:
 Confirm Password:

The default password is "MatrikonOPC"

The password will be used to encrypt the OPC security permissions stored in the file ACL.sec. If you wish to change the OPC security permissions or password at a later date, use the Tag Security shortcut located in the start menu.

X.X.X.X

Figure 6 - Enter Password Screen

12. A default password is supplied for you in the **Password** and **Confirm Password** fields.

Notes:



- The default password provided for you is **MatrikonOPC**. Note this password for future reference.
- If you need to change the password at a later date, access the **Tag Security** shortcut from the **Start** menu. Click on the Windows **Start** button. Select **Programs** -> **MatrikonOPC** -> **<OPC Server Name>** -> **Tag Security**. For more information, refer to **Appendix E – Security**.

13. Click on the **Next** button to accept the default password. The **Licensing** screen (Figure 7) appears.

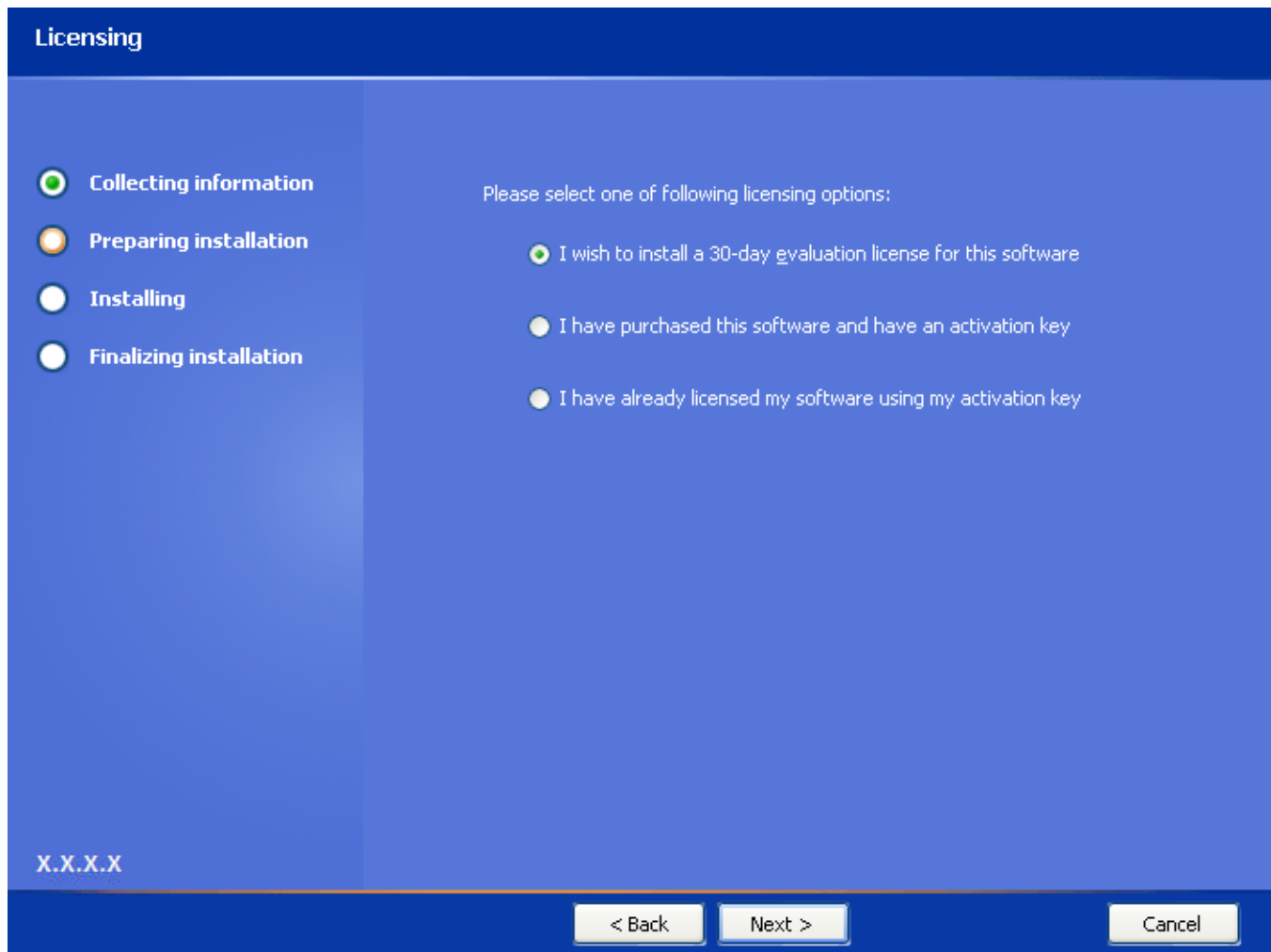


Figure 7 - Licensing Screen

14. Select one of the licensing options.
15. Click on the **Next** button to accept the selected licensing option. The **Ready to Install** screen (Figure 8) appears.

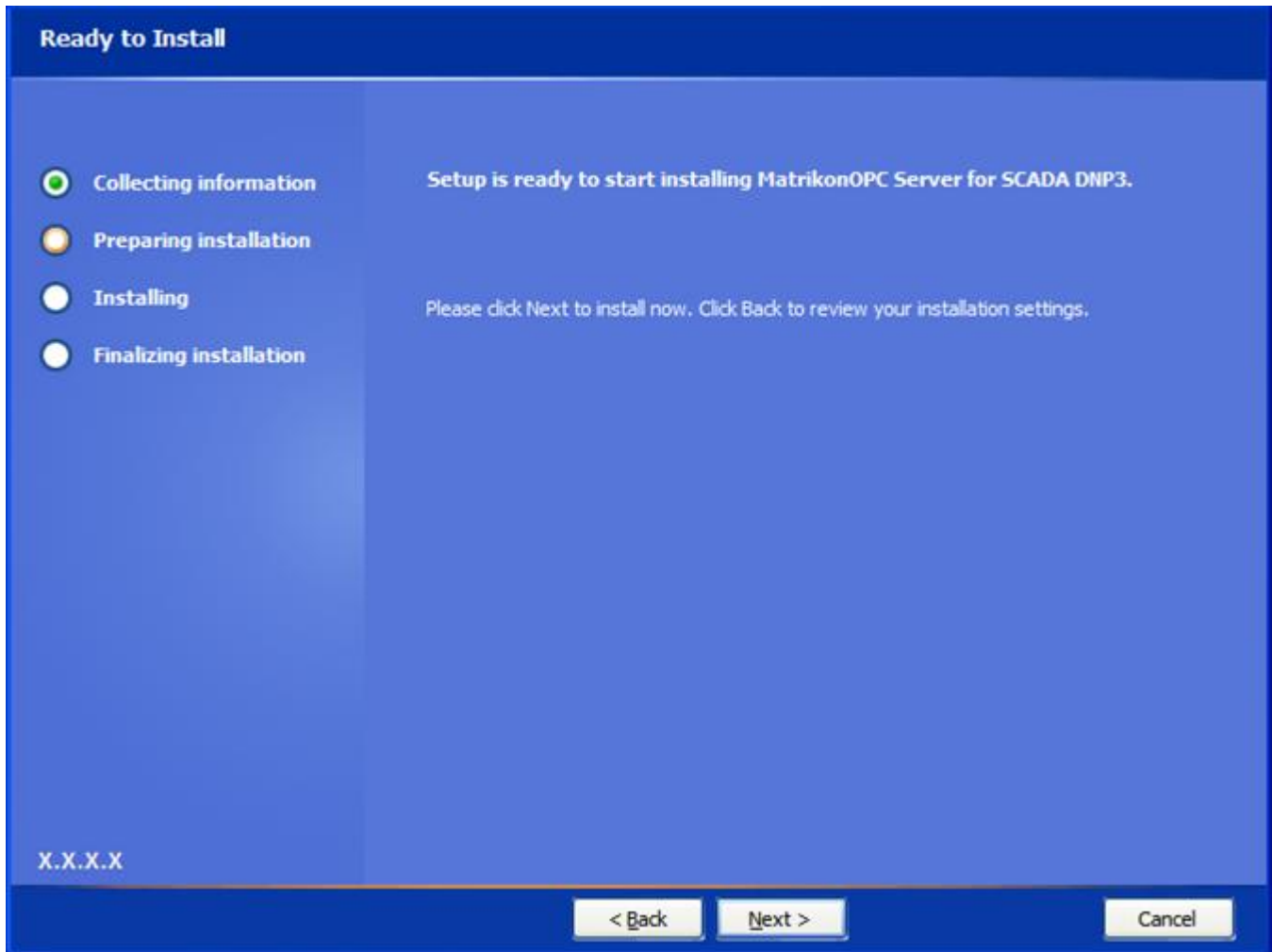


Figure 8 - Ready to Install Screen

16. Click on the **Next** button. The **Installing MatrikonOPC Server for SCADA DNP3** screen (Figure 9) appears, installation begins, and the product files are copied to the computer.

Note: Prior to starting the installation, you have the option of clicking on the **Back** button to change any of the installation information. Click on the **Cancel** button if you wish to stop or cancel the installation.



Figure 9 - Installing MatrikonOPC Server for SCADA DNP3 Screen

17. When the installation has finished, the **MatrikonOPC Server for SCADA DNP3 Setup Complete** screen (Figure 10) appears stating that MatrikonOPC Server for SCADA DNP3 has been successfully installed.

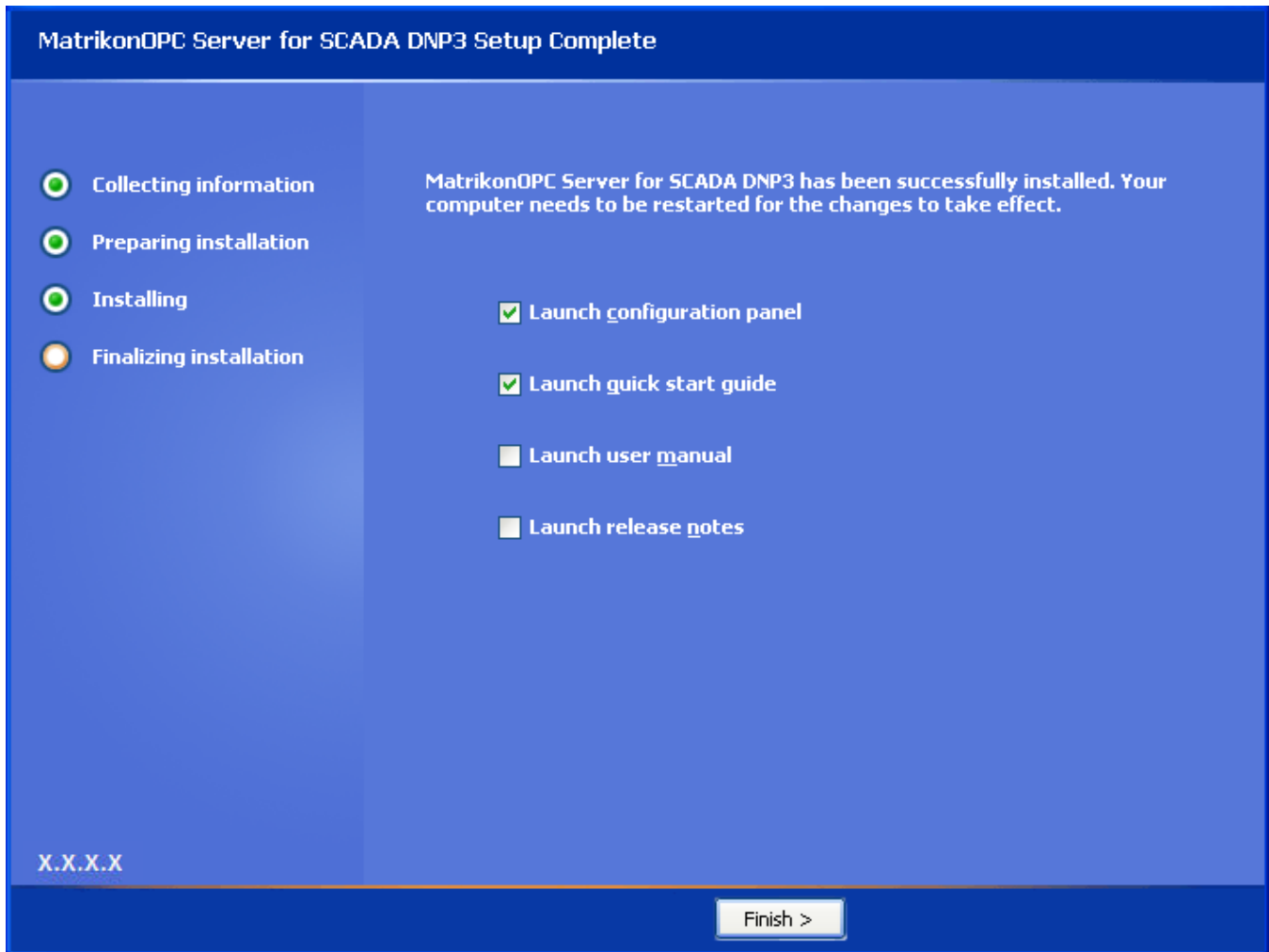


Figure 10 - MatrikonOPC Server for SCADA DNP3 Setup Complete Screen

18. At this point you have the option of launching any or all of the following by selecting the necessary checkbox or checkboxes:

- Configuration panel
- *Quick Start Guide*
- *User's Manual*
- *Release Notes*

19. Click on the **Finish** button to complete the installation and exit the Wizard.

20. The necessary files have now been copied to the target computer, the software components are registered, and shortcut icons are created in the **Start** menu.



Note: At this point, it is recommended that you verify the DCOM settings. Reference to the DCOM configuration can be found in the **DCOM Manual**. This configuration varies for different operating systems.

Installed Files

The installation program copies all necessary files to the target computer and creates shortcut icons in the **Start** menu.

The files listed in Table 2 are installed by default, in the following location:

C:\Program Files\Matrikon\OPC\SCADA DNP3

File Name	Description
ACL.sec	Access control list containing users and permissions configured for the server.
ACLSecure.exe	Command-line security utility used to encrypt/decrypt the ACL file.
AliasCalculationLib.dll Altova.dll AltovaXML.dll CalcEngine_u.dll CalcEngineResource.dll CalculationGraph.dll clipsdll.dll icudt36.dll icuin36.dll icuuc36.dll js32.dll log4cxx.dll lsapiw32.dll NTEventLogAppender.dll OpcDataDelivery_u.dll ProcessNetDataDelivery_u.dll Scheduleru_dll.dll ScriptLibrary_u.dll Xerces-c_2_7.dll	Calculation Engine binary files.
Licensing Procedures.pdf	<i>Licensing Procedures</i> document.
lsapiw32.dll	Licensing Library
MatrikonOPC Server for SCADA DNP3 Release Notes.pdf	<i>Release Notes</i> for this server.
MatrikonOPC Server for SCADA DNP3 User Manual.pdf	<i>User's Manual</i> for this server.
MatrikonOPC Server for SCADA DNP3 Quick Start.pdf	<i>Quick Start Guide</i> for this server.
OPCdnf.exe	Server executable.
ProgID.txt	Security information file used by the encryption utility.
Project Info.log	Product version information for the current build.
PSTCFGScadaLib.ocx	Server ActiveX configuration panels.
PSTCFGDnpLib.ocx	Server ActiveX configuration panels.
ServerOpts.ini	Server configuration file.

Table 2 - Files Installed in "SCADA DNP3" Folder

The files listed in Table 3 are installed by default, in the following location:

C:\Program Files\Common Files\MatrikonOPC\Common

File Name	Description
aclconfig.exe	Tag security.
EULA.pdf	End-User License Agreement in PDF format.
OEM_MATRIKON_OPC.DLL	MatrikonOPC OEM Badge Library.
OPCAuto.dll	MatrikonOPC Automation Component – enables developers to access OPC data from client applications developed using automation tools.
opcda20_auto.doc	MatrikonOPC Automation Component interface standard.
OPCDAAuto.dll	MatrikonOPC HDA Automation Component – enables developers to access OPC data from client applications developed using automation tools such as <i>Visual Basic</i> , <i>VBA</i> , and <i>VB Script</i> .
opchda_ps.dll	The proxy-stub file that allows OPC clients to make remote connections to an OPC HDA server.
opchda10_auto.doc	Developer documentation for the HDA Automation Component.
OPCHDAAUTO.DLL	MatrikonOPC HDA Automation Component – enables developers to access OPC HDA data from client applications developed using automation tools.
PSTCFG.exe	Matrikon product configuration utility.
PSTcfgps.dll	Matrikon product configuration marshalling library.
LicenseWizard.exe	Matrikon product licensing utility.
LicenseRemover.exe	Matrikon product licensing utility.

Table 3 - Files Installed in "Common" Folder

The files listed in Table 4 are installed in the **WINDOWS\system32** folder:

File Name	Description
actxprxy.dll	ActiveX Interface Marshalling Library.
ExprEval.dll	Expression Evaluation Library for Alias Scaling Equations.
opc_aeps.dll	OPC Alarms and Events 1.10 Interfaces and Marshalling Library
opccomn_ps.dll	OPC Common Interfaces and Marshalling Library
Opcenum.exe	OPC server list component.
opcproxy.dll	OPC Data Access 2.05 and 1.0a Interfaces and Marshalling Library.
opcSec_PS.dll	OPC Security Interfaces and Marshalling Library

Table 4 - Files Installed in "system32" Folder

Licensing

Most MatrikonOPC products require some form of licensing criteria be met to ensure that it functions successfully

The MatrikonOPC Server for SCADA DNP3 supports software **and** hardware licensing

IMPORTANT TO NOTE:

The following licensing information is described in detail within the *Licensing Procedures* document which accompanies the MatrikonOPC Server for SCADA DNP3 software and *User's Manual*:



- Hardware and software key licensing information.
- Information about the MatrikonOPC Licensing Utility that is used to license software, and the variety of ways in which licenses can be obtained (e.g., Internet Connection, Web Page, Email).
- Licensing Q&A and Troubleshooting.

Contacting Support

The MatrikonOPC Customer Services department (www.opcsupport.com) is available 24 hours a day, seven days a week.

Contact MatrikonOPC Support using the information below, or send an email (support@MatrikonOPC.com).

For Monday to Friday **daytime support** requests, contact MatrikonOPC Support using the regional phone numbers provided in Table 5.

Region	Office Hours	Contact Information
North America UTC/GMT -7 hours (MST)	8:00am-5:00pm	+1-877-OPC-4-ALL
Europe /Africa * UTC/GMT +1 hours (CET)	9:00am-5:00pm	+49-221-969-77-0 (Request OPC Support)
Middle East * UTC/GMT +3 hours	9:00am-5:00pm	+973-174-65363
Australia/Asia * UTC/GMT +10 hours (AEST)	9:00am-5:00pm	+61-2-4908-2198 (Request OPC Support)

* Toll-free regional numbers coming soon!

Table 5 - MatrikonOPC Support Regional Contact Information

For **after-hours support** in all regions, please use either of the following numbers. There is no extra charge from MatrikonOPC for calling their after-hours support numbers.

Region	Contact Information
All	+1-780-231-9480 +1-780-264-6714

Table 6 - After-Hours Support

Configuration

The server's Graphical User Interface (GUI) allows users to view and alter configuration parameters at run time. When a user views a configuration parameter, the information is retrieved and displayed. The updated parameters are sent as a group to the server when submitted.

Minimal configuration of the MatrikonOPC Server for SCADA DNP3 is required for the server to function properly, but users can customize the server's behavior as required. This chapter shows users how to start and configure the server and describes each component in detail, including the windows, panels, and menu commands.

The **Starting the MatrikonOPC Server for SCADA DNP3** section of this manual shows users how to start the software. The next four sections describe the **Tool Tray Menu**, **Control Panel**, **Configuration** window, and the **Options** window, in detail.

The **Server Configuration** section describes in detail how to configure the server. Instructions for configuring the MatrikonOPC Server for SCADA DNP3 as a DDE service appear in the Dynamic Data Exchange (DDE) section. The **Alias Configuration** section explains how to create user-defined aliases in place of regular OPC items, followed by four sections that cover saving, clearing, and loading configuration settings, and shutting down the server.

Configuring Dynamic Data Exchange (DDE)

The server may act as a DDE service. In this way, a DDE client can request data from the server using the following DDE commands:

- XTYP_POKE** - Write data to an item in the server.
- XTYP_REQUEST** - Read data from an item in the server.
- XTYP_ADVREQ** - Read latest data from an active advice loop.
- XTYP_ADVSTART** - Create and activate an advice loop on a single item in the server.
- XTYP_ADVSTOP** - Stop and destroy an advice loop on a single item in the server.

DDE service can be enabled or disabled using the checkbox. Note that these options will not be available if the server does not support DDE.

Items within the server can be referenced using the following syntax:

SERVICE_NAME |ITEM! SCANDETAILS

SERVICE_NAME represents the name of the DDE service. The first edit box specifies the service name used by this server.

ITEM refers to an item ID of a point within the server.

SCANDETAILS is a combination of the desired scan rate of the item, and an access path. One or more delimiting characters separate the scan rate and access path. The second edit box can be used to change the delimiters. The delimiting characters must be provided when referencing an item in the server. However, the scan rate and access path are optional. If no scan rate is specified, only data contained in the server cache will be available through DDE, and an advise loop will not be created.

Changes to the DDE options will not take effect until the server is restarted.



Note: DDE Name Syntax – DDE Names may be described in the following syntax: **SERVICE|TOPIC|NAME**

In this case, consider the **TOPIC** to be the item ID, and the **NAME** to be a combination of the scan rate and access path.

Starting the MatrikonOPC Server for SCADA DNP3

To launch the MatrikonOPC Server for SCADA DNP3, choose the appropriate shortcut from the **Start** menu.

To start the MatrikonOPC Server for SCADA DNP3:

1. Click on the Windows **Start** button and select **Programs -> MatrikonOPC -> SCADA DNP3**, and choose **MatrikonOPC Server for SCADA DNP3**.

By default, the server is installed as a Windows service. When the server is installed as a service, the splash screen does not appear, nor does the logo appear in the **Tool Tray**. Instead, the main **Configuration** window is immediately displayed. If the server is installed as a Windows service, users can also start it using the **Service Control Manager** applet (under the Windows **Control Panel**).

2. If the server is not installed as a Windows service, the server starts and the **Matrikon** logo  appears in the **Tool Tray** (Figure 11), located by default in the system tray.



Figure 11 - Tool Tray

If the server is not installed as a Windows service, the **Welcome** screen appears briefly when the server starts up.

Notes:



- If the server is not installed as a service, the server will automatically start up when a client (such as MatrikonOPC Explorer) first tries to connect to it.
- If the server is installed as a service, users can choose to run it as an application by re-registering the OPC server executable using the **/REGSERVER** command-line switch.

Tool Tray Menu

Note: If the server is installed as a Windows service, the **Tool Tray** and **Tool Tray Menu** are not available.

The **Tool Tray Menu** provides access to the **Control Panel**, the **Configuration** window, and the **About** screen. It also contains the commands to shut down the server.

To view the Tool Tray Menu:

1. Right-click your mouse on the **Matrikon logo** .
2. The **Tool Tray Menu** appears (Figure 12).

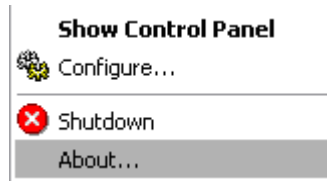


Figure 12 - Tool Tray Menu

Table 7 describes the commands in the **Tool Tray Menu**.

Command	Description
Show Control Panel	Displays the configuration control panel .
 Configure	Displays the main Configuration window .
 Shutdown	Shuts down the server.
About	Displays the server's Welcome screen, which includes information about the software.

Table 7 - Tool Tray Menu Commands

Control Panel

Note: If the server is installed as a Windows service, the **Control Panel** is not available.

The **Control Panel** displays the server's status, system time, and number of clients connected to the server. The **Control Panel** allows users to:

- Access the **Configuration** window.
- Access the **About** screen.
- Execute the command to shut down the server.

The **Control Panel** stays on top of every other window on the desktop to help monitor the status of the server.

To view the Control Panel:

1. Right-click your mouse on the **Matrikon logo** .
2. The **Tool Tray Menu** appears.
3. From the **Tool Tray Menu**, select the **Show Control Panel** menu option.
4. The **Control Panel** (Figure 13) appears.



Figure 13 - Control Panel

5. To "window shade" the **Control Panel** so that it displays only the client count, double-click your mouse on the title bar.

Table 8 describes the commands in the **Tool Tray Menu**.

Command	Description
Status	Displays the current status of the server.
Time	Displays the current time.
Clients	Displays the total number of OPC clients presently connected to the server.
Configure	Displays the main Configuration window.
Shutdown	Shuts down the server.
About	Displays the server's Welcome screen, which includes information about the software.

Table 8 - Control Panel Commands

Configuration Window

Note: If the server is installed as a Windows service, the **Tool Tray Menu** and **Control Panel** are not available. In this case, the **Configuration** window is then accessed via the Windows **Start** menu.

The **Configuration** window is used to configure the server. It displays the current configuration and allows users to change configuration parameters.

To view the Configuration window:

1. From the **Tool Tray Menu** or the **Control Panel**, select **Configure**.
2. The **Configuration** window (Figure 14) appears.

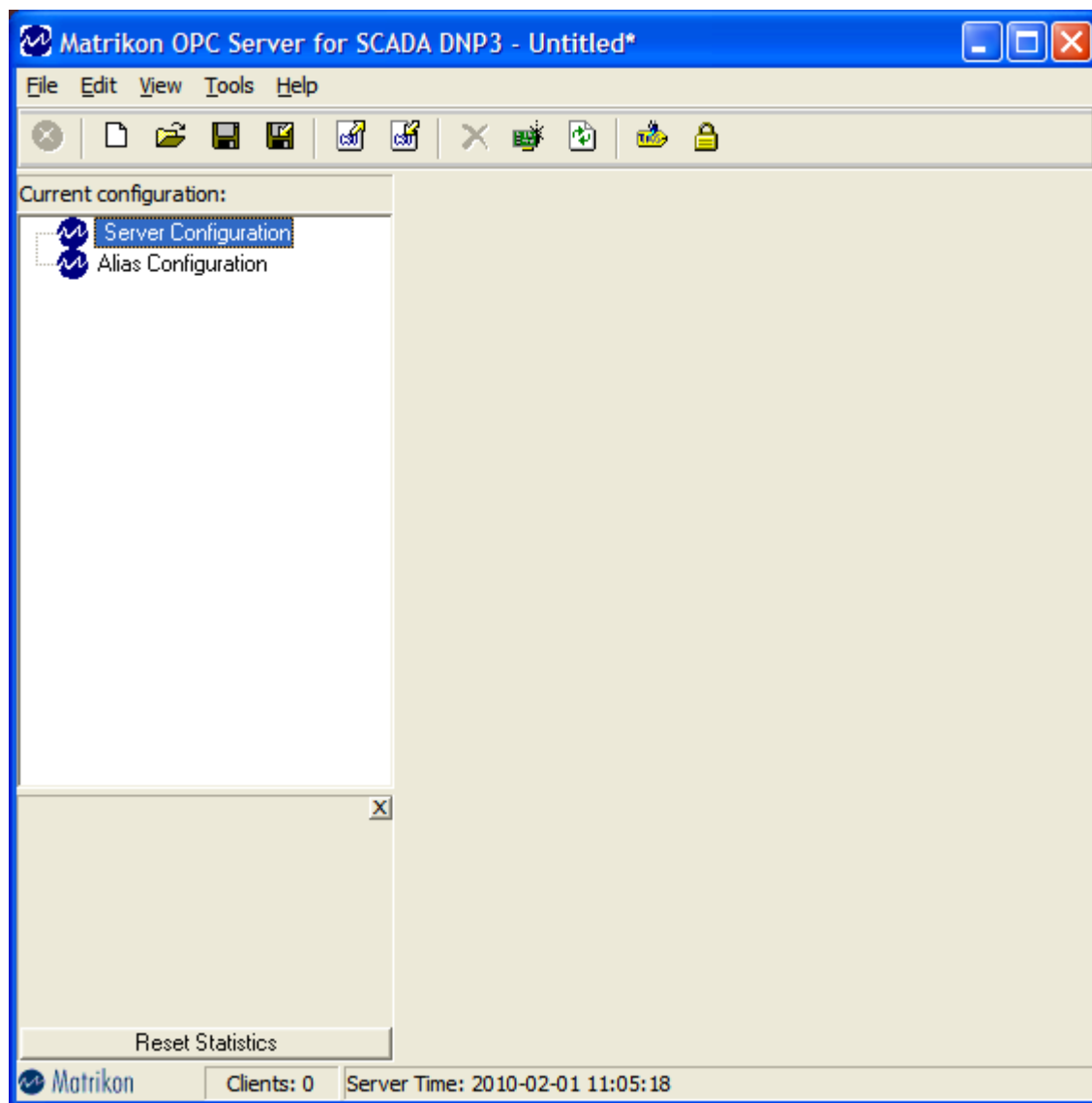


Figure 14 - Configuration Window

Table 9 describes the commands in the **Configuration** window.

Command	Description
Main Menu	Provides access to the File , Edit , View , Tools , and Help menus.
Main Toolbar	Provides shortcut buttons for commands in the Main Menu .
Current Configuration	Displays a tree of configuration objects currently defined in the server. Select an object to display its current settings in the right-hand panel.
Server Configuration	Objects under this node affect how the server communicates with the data source.
Alias Configuration	Define aliases and alias groups under this node.
Object Settings Panel	Displays the current settings of the object presently selected in the tree.
Statistics Panel	Displays available statistics for the object presently selected in the tree:

Command	Description
	Sent, Received, Timed Out, Retried, Failed, Overrun.
Reset Statistics	Resets statistics on the object presently selected in the configuration tree.
Matrikon Logo	Opens a link to the Matrikon web site.
Clients	Displays the total number of OPC clients presently connected to the server.
Server Time	Displays the current time.

Table 9 - Configuration Window Commands

The following sections describe the menus available from the **Configuration** window, and what they are used for.

File Menu

Table 10 describes the **File** menu commands.

Command	Description
 New	Clears the current configuration and starts a new one. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing.
 Open	Clears the current configuration and loads a new one from an existing file. Displays the Open Configuration window to prompt for the file name. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing.
 Save	Saves the current configuration to an XML file. Displays the Save Configuration window to prompt for a new file name if the configuration is new and has not been saved before.
 Save As	Saves the current configuration to an XML file. Displays the Save Configuration window to prompt for a new file name.
 Export Aliases	Exports all currently configured aliases to a CSV file. Displays the Export Aliases window to prompt for a file name.
 Import Aliases	Clears all aliases and imports new ones from a CSV file. Displays the Import Aliases window to prompt for an existing file name.
 Shutdown Server	Closes the current configuration and shuts down the server after signaling the shutdown event to all connected clients. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing.
Close	Hides the main Configuration window. The server shuts down after a short delay if no OPC clients are currently connected to the server.

Table 10 - File Menu Commands

Edit Menu

Table 11 describes the **Edit** menu commands that appear when the currently selected object appears under the **Server Configuration** node.

Command	Description
Undo/Can't Undo	Not implemented.

Command	Description
 Delete	Removes the currently selected object from the server configuration. Prompts the user for confirmation before continuing to see if the OPC clients have reference to items associated with the selected object or one of its children. Does not remove such objects but simply disables them and sets them to "marked for deletion".
 Define New	Displays the Insert New Object window used to create a new configuration object under the currently selected configuration object.

Table 11 - Edit Menu Commands (Server Configuration)

Table 12 describes the **Edit** menu commands that appear when the currently selected object appears under the **Alias Configuration** node.

Command	Description
Undo/Can't Undo	Not implemented.
 Rename	Renames the currently selected alias group.
 Delete Alias Group	Removes the currently selected alias group and all subordinate groups and aliases.
Delete Alias	Removes the currently selected aliases.
 Insert Alias Group	Creates a new alias group under the currently selected alias group.
Insert New Alias	Displays the Insert New Alias window used to create a new alias under the currently selected alias group.

Table 12 - Edit Menu Commands (Alias Configuration)

View Menu

Table 13 describes the **View** menu commands.

Command	Description
Statistics	Displays/hides general communication statistics for the currently selected object.
Reset Statistics	Resets all statistics for the currently selected object to zero.
Defaults	Displays the Server Defaults window used to configure the default settings for the various types of communication objects available in the server.
 Refresh	Rebuilds the tree display of the server configuration and fully expands all branches.
Options	Displays the Options window used to change general server options.

Table 13 - View Menu Commands

Tools Menu

Table 14 describes the **Tools** menu commands.

Command	Description
 DCOM Configurator	Launches the Microsoft Distributed COM Configuration Properties utility. This utility can be used to edit DCOM settings for specific COM

Command	Description
	servers to allow client applications on remote computers to connect to the server.
 View Tags	Launches MatrikonOPC Explorer, which is a general-purpose OPC client included with all MatrikonOPC servers that may be used to test the capabilities of the software. For more information, refer to the <i>MatrikonOPC Explorer User's Manual</i> .
 Security Settings	Launches the Enter server password window where you are asked to enter the security password set during the installation of the server. The default password set during the installation of this server is MatrikonOPC . The MatrikonOPC Tag Security Configuration Utility screen is then displayed which allows you to configure security settings. For more information, refer to Appendix E – Security .

Table 14 - Tools Menu Commands

Help Menu

Table 15 describes the **Help** menu commands.

Command	Description
MatrikonOPC on the Web	Opens a link to the Matrikon web site.
About	Displays the Welcome screen, which includes information about the software version.

Table 15 - Help Menu Commands

Options Window

The **Options** window is used to edit the server's options and contains three tabs: **General**, **General Logging**, and **Interface Logging**.

General Options

The **General** tab allows users to edit general server options (i.e., settings).

To view the General options:

1. On the **Configuration** window, from the **View** menu, select the **Options** menu item.
2. The **Options** window appears.
3. From the **Options** window, select the **General** tab (Figure 15).

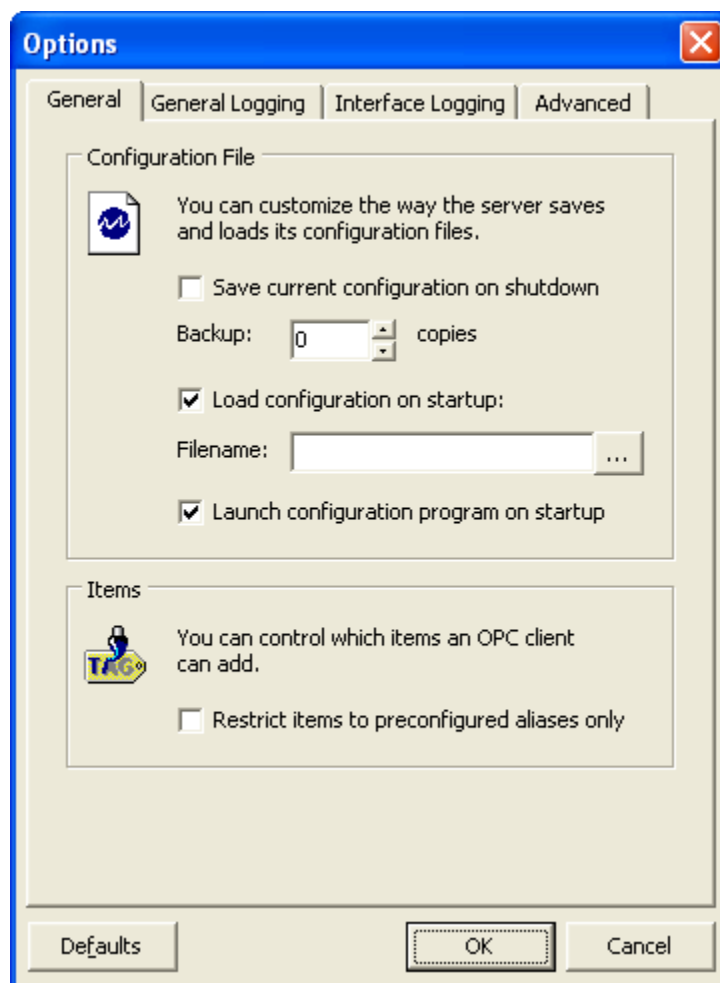


Figure 15 - General Options Tab

Table 16 describes the fields available on the **General** tab.

Field	Description
Save current configuration on shutdown	Automatically saves the current configuration to the specified file before shutting down, if selected.
Backup: X copies	Automatically keeps up to the specified number (i.e., X) of backup copies of the configuration file when saving the configuration.
Load configuration on startup	Automatically loads a configuration from the specified file when starting up, if selected.
Filename	Displays the full path of an existing file for load and save operations. Click on the ellipsis button () to display the Open window used to select an existing file name.
Launch configuration program on startup	Automatically launches the configuration utility when starting up as a local executable (rather than a Windows service), if selected.
Restrict items to preconfigured aliases	Allows you to control which items an OPC client can add. Selecting this checkbox indicates the restriction of items to pre-configured aliases only.

Field	Description
only	

Table 16 - General Options Tab Fields

Note: The server loads these settings from the Windows registry upon start-up. Changes to the **General** options settings take effect when the server is restarted.

General Logging Options

The **General Logging** tab allows users to edit general logging options.

To view the General Logging options:

1. On the **Configuration** window, from the **View** menu, select the **Options** menu item.
2. The **Options** window appears.
3. From the **Options** window, select the **General Logging** tab (Figure 16).

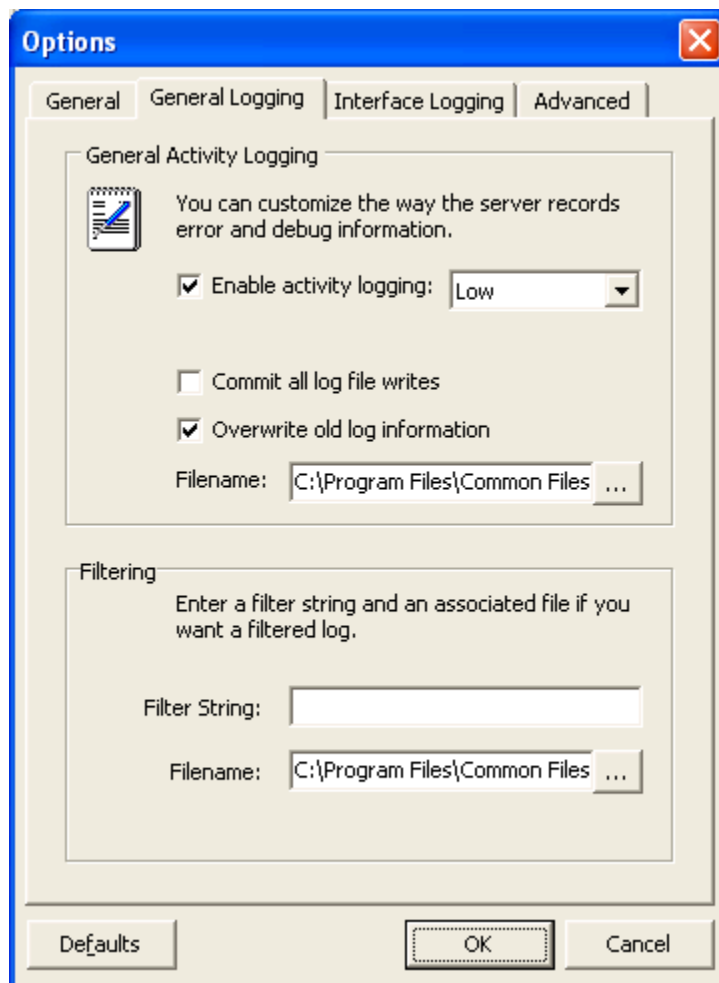


Figure 16 - General Logging Options Tab

Table 17 describes the fields available on the **General Logging** tab.

Field	Description
Enable activity logging	Enables/disables general activity logging at the specified detail level

Field	Description
	(High , Medium , Low , or None), if selected. Note: This option should not be selected unless users are debugging a problem as this will have a negative effect on performance of the OPC server. Always set this back to None when not in use.
Display activity on screen	Displays logged messages in a console window as they occur, if selected.
Commit all log file writes	Purges the file buffer after each message is logged in the event of an unexpected server shut down.
Overwrite old log information	Overwrites the old log file each time the server starts up, if selected. Otherwise, rename the old log file with a (*.bak) suffix.
General Activity Logging Filename	Displays the full path for the general activity log file. Click on the ellipsis button (...) to display the Open window used to select an existing file name. The default path is C:\Program Files\MatrikonOPC\Common\PSTCFGMatrikon.OPC.DNP.1.LOG .
Filter String	Match string for filtered log is displayed.
Filtering Filename	Displays the full path for the filtered log file. Click on the ellipsis button (...) to display the Open window used to select an existing file name.

Table 17 - General Logging Options Tab Fields

Note: General Logging options settings take effect immediately.

Interface Logging Options

The **Interface Logging** tab allows users to view and edit COM interface logging options.

To view the Interface Logging options:

1. On the **Configuration** window, from the **View** menu, select the **Options** menu item.
2. The **Options** window appears.
3. From the **Options** window, select the **Interface Logging** tab (Figure 17).

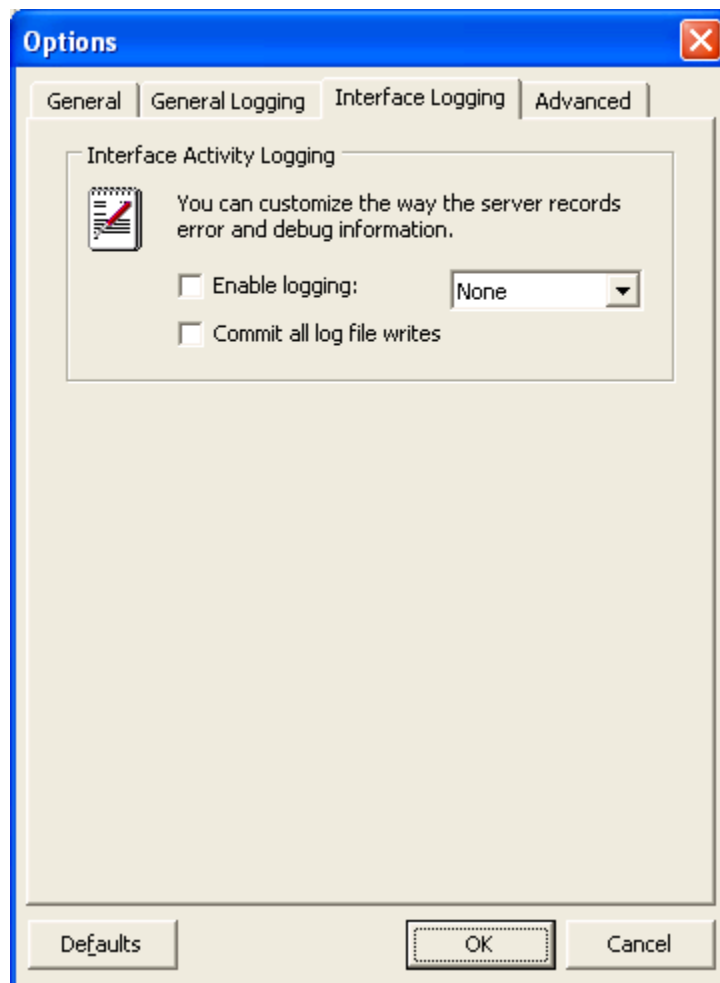


Figure 17 - Interface Logging Options Tab

Table 18 describes the fields available on the **Interface Logging** tab.

Field	Description
Enable logging	Enables/disables interface logging at the specified detail level (High , Medium , Low , or None), if selected. Generates a separate log file for each client named <i>PST###.TMP</i> in the server installation directory. Note: This option should not be selected unless users are debugging a problem as this will have a negative effect on performance of the OPC server.
Commit all log file writes	Purges the file buffer after each message is logged in the event of an unexpected server shut down.

Table 18 - Interface Logging Options Tab Fields

Note: Interface Logging options settings take effect when the next OPC client connects to the server.

Advanced Options

The **Advanced** tab allows users to view and edit advanced server options.

To view the Advanced options:

1. On the **Configuration** window, from the **View** menu, select the **Options** menu item.
2. The **Options** window appears.
3. From the **Options** window, select the **Advanced** tab (Figure 18).

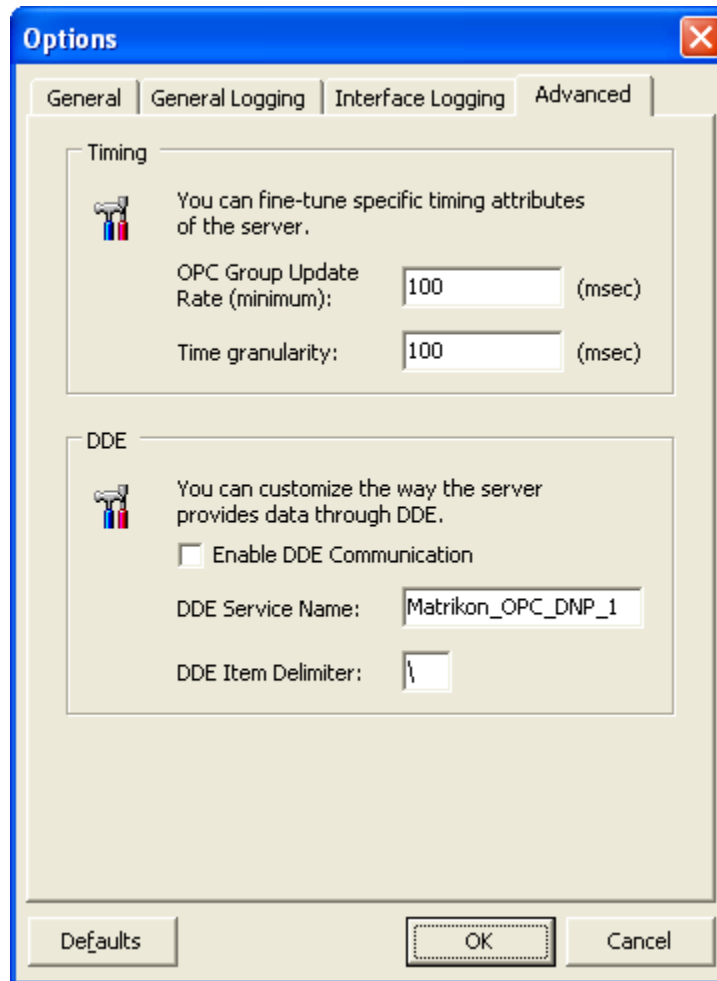


Figure 18 - Advanced Options Tab

Table 19 describes the fields available on the **Advanced** options tab.

Field	Description
OPC Group Update Rate (minimum)	Minimum update rate (milliseconds) allowed for an OPC group. Prevents OPC clients from requesting update rates that are impossible to achieve or that cause heavy CPU loads. The default value is 100 ms.
Time granularity	OPC Server group scan thread interval (milliseconds). Determines the maximum resolution for data change detection. Time granularity should always be equal to or less than the minimum group update rate.
DDE	Configures the way the server provides data through DDE.

Table 19 - Advanced Options Tab Fields

Note: The server loads these settings from the Windows registry on start-up. Changes to **Advanced** options settings take effect when the server is shut down and restarted.

Server Configuration

The server requires minimal configuration for it to run properly. You can also customize the server's behavior as required. This section shows you how to create and edit objects using the **Configuration** window.

Inserting New Objects

The **Insert New Object** and **Create New** windows are used to create **Fail-over Channel**, **Network Channel**, and **Serial Channel** objects.

Insert New Object Window

The **Insert New Object** window (Figure 19) displays a different set of options depending on the type of object selected and the types of objects already configured under it.

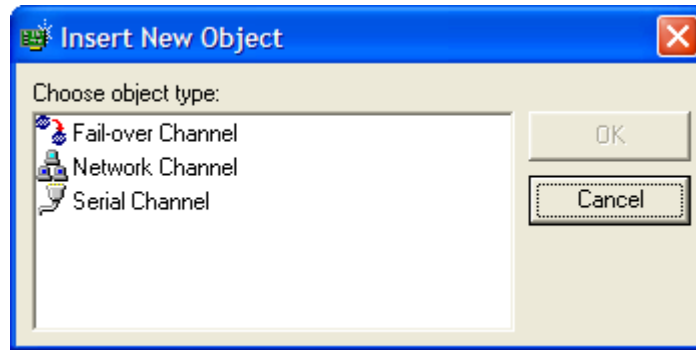


Figure 19 - Insert New Object Window

Table 20 describes the types of objects that are available for insertion as a child in the **Insert New Object** window, depending on which object is currently selected.

Selected Object	Insert New Object Window Options
Root Device Link (Server Configuration)	Fail-over Channel Network Channel Serial Channel
Fail-over Channel	<None>
Network Channel	Network Host
Network Host	Dial-up Connection DNP3 Unit
Dial-up Connection	DNP3 Unit
DNP3 Unit	<None>
Serial Channel	Dial-up Connection DNP3 Unit Radio
Dial-up Connection	DNP3 Unit
DNP3 Unit	<None>

Selected Object	Insert New Object Window Options
Radio	DNP3 Unit
DNP3 Unit	<None>

Table 20 - Insert New Object Window Options

To insert a new object:

1. On the **Configuration** window, select the **Server Configuration** node and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.
2. The **Insert New Object** window (Figure 19) appears.
3. From the displayed list, select the type of object to be created.
4. Click on the **OK** button.
5. The **Create New** window appears.

To create a newly inserted object:

1. From the **Create New** window, enter a name for the object. This name is part of the item ID that globally identifies data items from under the object. Users may also choose to enter a description of the object.
2. Edit the configuration components as desired.
3. Click on the **OK** button. The object is created.

Note: For the object to be used for communication, it must be enabled. This can be done at any time.

Create New Window

A device-specific window is displayed for each object:

- **Fail-over Channel**
- **Network Channel**
- **Serial Channel**

Creating and Configuring a Fail-Over Channel Object

The **Create New** window (Figure 20) displays the settings available when creating a **Fail-over Channel** object.

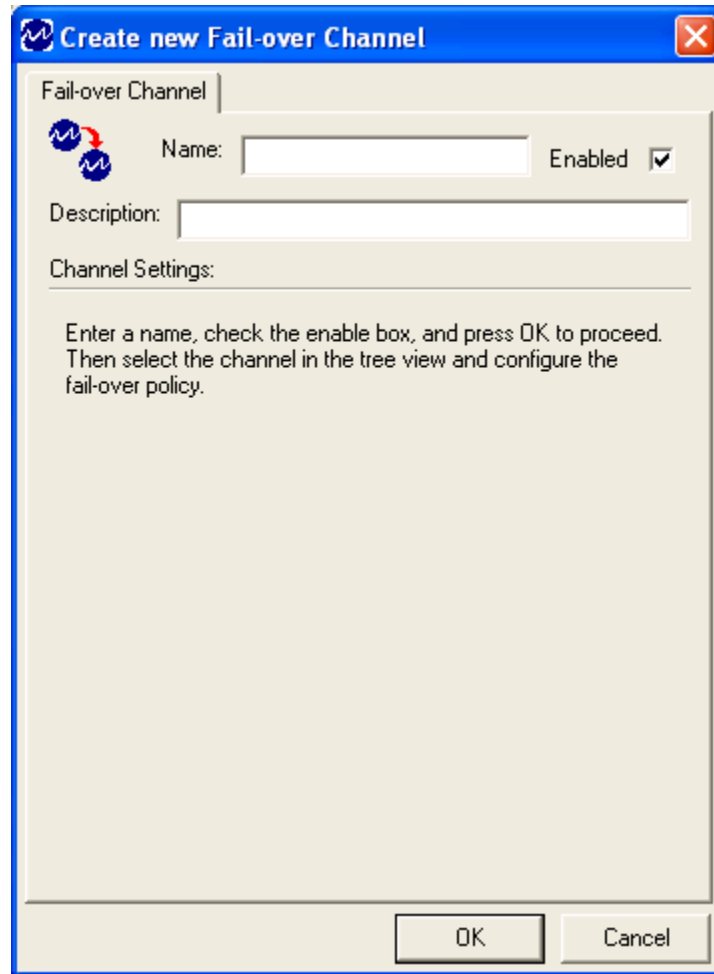


Figure 20 - Create New Fail-Over Channel Window

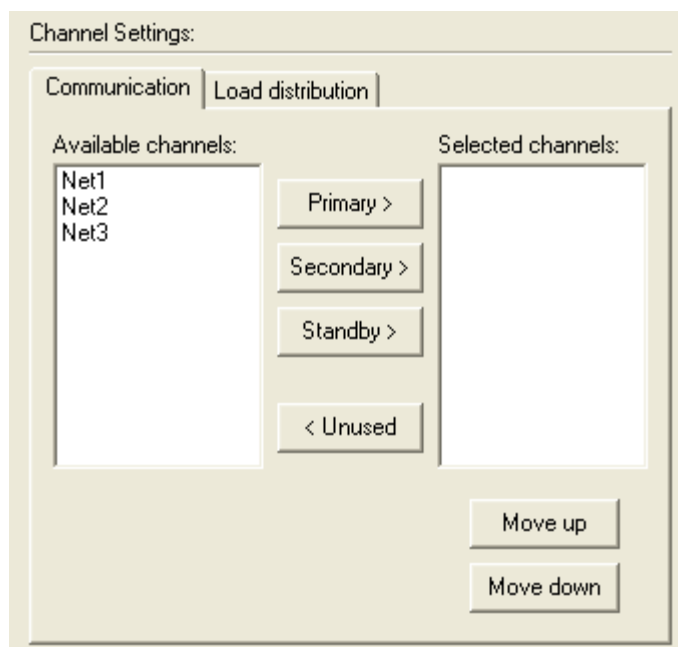
Once a Fail-over Channel object has been created, and you select it in **Current configuration** pane, the settings panel is displayed and consists of two tabs:

- **Communication**
- **Load Distribution**

The **Communication** tab (Figure 21) is not available until you have already created the Fail-over Channel. To display this tab, select the Fail-over Channel in the **Current Configuration** list and it will appear in the **Fail-over Channel Settings** window.

Communication Tab

Figure 21 displays the **Fail-over Channel – Communication** tab.



Channel Settings:

Communication | Load distribution

Available channels:

- Net1
- Net2
- Net3

Selected channels:

Primary >

Secondary >

Standby >

< Unused

Move up

Move down

Figure 21 - Fail-Over Channel - Communication Tab

Table 21 describes the components of the **Fail-over Channel - Communication** tab.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes. Note: This information stays consistent across both tabs.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected. Note: This information stays consistent across both tabs.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. Note: This information stays consistent across both tabs.
Available Channels list	Lists those communication channels not currently used in the fail-over policy.
Select Channels list	Describes the fail-over policy and the load distribution criteria for standby channels as an XML string. The default is <CFailoverDevlink/>)*
Primary	Designates the channel as a Primary fail-over channel and transfers it to the Selected channels list.
Secondary	Designates the channel as a Secondary fail-over channel and transfers it to the Selected channels list.
Standby	Designates the channel as a Standby fail-over channel and transfers it to the Selected channels list.

Component	Description
Unused	Removes the channel from the fail-over policy and transfers it back to the Available channels list.
Move up	Increases the fail-over channels priority by one and moves it up one space in the Selected channels list.
Move down	Decreases the fail-over channels priority by one and moves it down one space in the Selected channels list.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across both tabs.
Cancel	Closes the window without saving any changes made. Note: This information stays consistent across both tabs.

Table 21 - Fail-Over Channel - Communication Tab Components

Load Distribution Tab

Figure 22 displays the **Fail-over Channel – Load Distribution** tab.

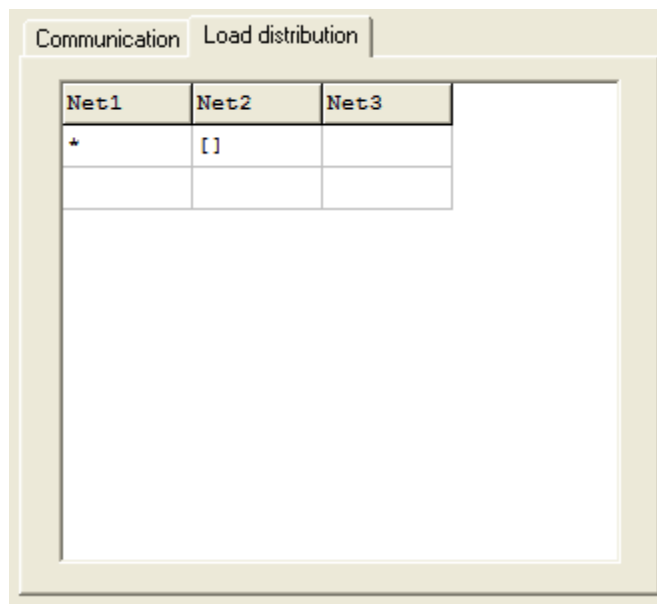


Figure 22 - Fail-Over Channel - Load Distribution Tab

Like the **Communication** tab, the **Load Distribution** tab (Figure 22) is only available after you have created the fail-over channel, in the **Fail-over Channel Settings** window.

The **Fail-over Channel** works on a tag by tag basis. If one tag is not available in Primary channel it will check the next connection in the list to attempt to get data for the tag. This also means that data can be collected from multiple different channels at the same time for **different** tags.

Notes:

- An asterisk (*) indicates all items. [] indicates no items. A load distribution can be done by typing a part of the tag string under the desired Network channel in between two asterisk (*) symbols. For example, if **Net 1** is desired to browse all tags that belong to register 4X and **Net 2** is desired to browse all tags that belong to register 3X, then you will have to type ***4000*** (or **4:**) under **Net1** and ***3000*** (or **3:**) under **Net2**.

To create a Fail-over Channel object:

1. On the **Configuration** window, select the **Server Configuration** node and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.

2. The **Insert New Object** window (Figure 19) appears.
3. From the displayed list, select the **Fail-over Channel** object type.
4. Click on the **OK** button.

5. The **Create New** window appears (Figure 20).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Fail-over Channel** is selected, then the **Create New Fail-over Channel** window is displayed.

6. From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.

7. Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.

8. Click on the **OK** button. The object is created and will appear as a child of the **Server Configuration** item as shown in Figure 23.

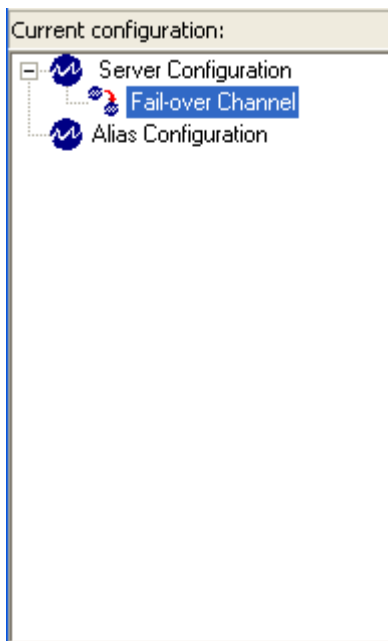


Figure 23 - New Fail-Over Channel Object

Creating and Configuring a Network Channel Object

The **Create New Network Channel** window (Figure 24) displays the settings available for configuring a **Network Channel**.

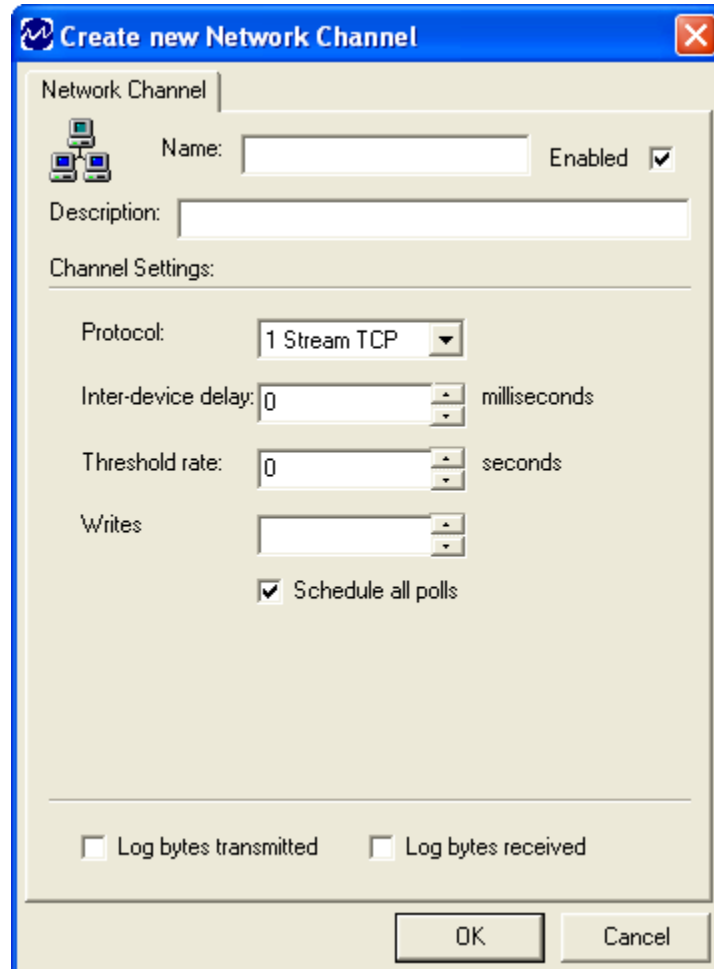


Figure 24 - Create New Network Channel Window

Table 22 describes the components of the **Create New Network Channel** window.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank.
Protocol	Allows you to select an Internet Protocol (IP) type from the drop down list.

Component	Description
	Available options are: 0 Datagram TCP, 1 Stream TCP, 2 Datagram UDP. 0 Datagram TCP and 1 Stream TCP both use TCP/IP but 0 treats the protocol as a series of discrete packets, whereas 1 treats it as a continuous stream of bytes. Default = 1 Stream TCP. Note: The channel and all units must disconnect and reconnect if this parameter changes. The UDP option will not enable DNP3 over UDP as per section 4.3.2 of the DNP3 Specification, Volume 7: IP Networking. The UDP option may be used to support DNP3 over serial through a UDP based serial to Ethernet converter.
Inter-device delay	Allows you to enter a value specifying the amount of time (in milliseconds) that the communication channel will wait sending a new request to the next unit after the data has been received from the current unit on this channel. If this is set to 0 then the option is turned off. Default = 0.
Threshold rate	Allows you to enter a value specifying the maximum achievable scan interval (in seconds) for the circuit. The server polls items with faster update rates on a continuous basis rather than as scheduled. If this is set to 0 then the option is turned off. Default = 0. Note: All units on the channel must re-optimize if this parameter changes.
Writes	Allows you to enter or select a value specifying the maximum number of writes allowed before forcing a poll.
Schedule all polls	Selecting this checkbox indicates that the server must schedule items with update rates faster than the Threshold rate to poll at the Threshold rate. Default = checkbox is selected. Note: All units on the channel must re-optimize if this parameter changes.
Log bytes transmitted	Enables (i.e., check box is selected) or disables (i.e., checkbox is cleared) the logging of bytes transmitted at Medium level. Default = checkbox is cleared.
Log bytes received	Enables (i.e., check box is selected) or disables (i.e., checkbox is cleared) the logging of bytes received at Medium level. Default = checkbox is cleared.
OK	Select this button to save any changes and close the window.
Cancel	Closes the window without saving any changes made.

Table 22 - Create New Network Channel Window Components

To create a Network Channel object:

- On the **Configuration** window, select the **Server Configuration** node and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.

2. The **Insert New Object** window (Figure 19) appears.
3. From the displayed list, select the **Network Channel** object type.
4. Click on the **OK** button.
5. The **Create New** window appears (Figure 24).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Network Channel** is selected, then the **Create New Network Channel** window is displayed.

6. From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.

7. Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.

8. Click on the **OK** button. The object is created and will appear as a child of the **Server Configuration** item as shown in Figure 25.

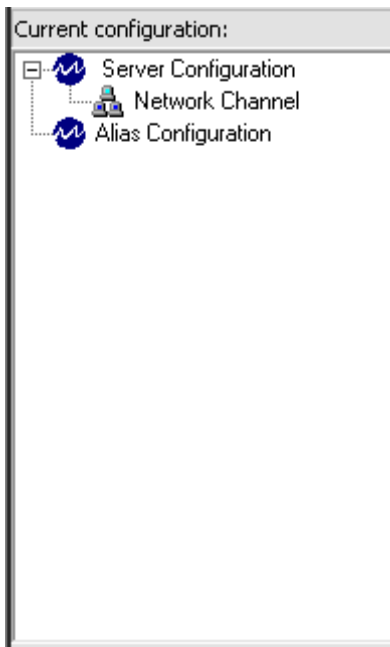


Figure 25 - New Network Channel Object

Creating and Configuring a Serial Channel Object

The **Create New** window (Figure 26) displays the settings available when creating a **Serial Channel** object.

The **Create New Serial Channel** window consists of two tabs:

- **Communication**
- **Data Acquisition**

Note: Changing the settings on this page (except for **Log bytes transmitted** and **Log bytes received**) requires that the communication channel be closed and re-opened.

Communication Tab

Figure 26 displays the **Create New Serial Channel – Communication** tab.

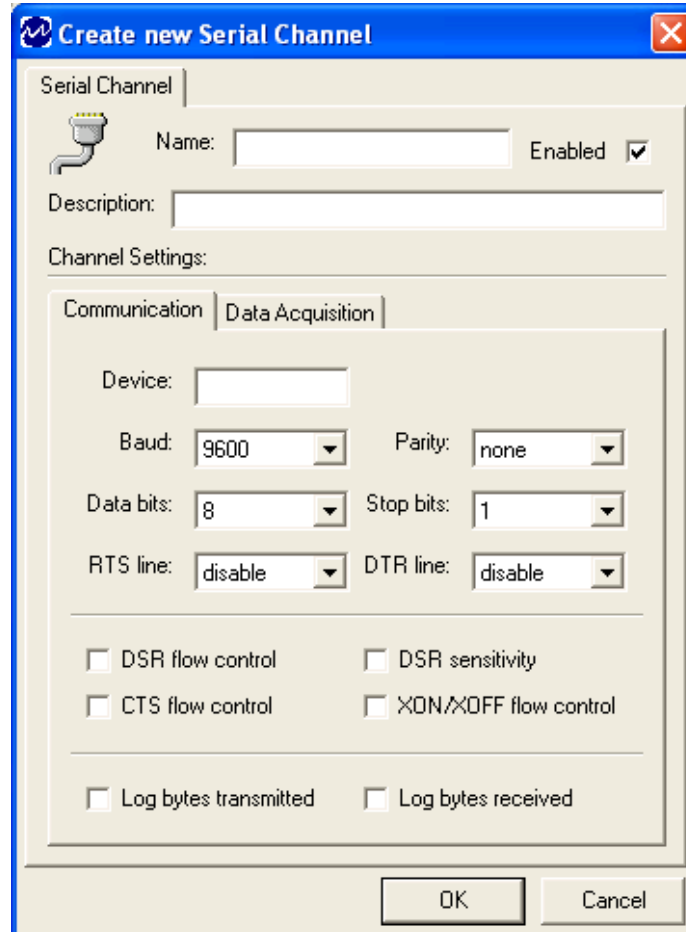


Figure 26 - Create New Serial Channel Window - Communication Tab

Table 23 describes the components of the **Create New Serial Channel – Communication** tab.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes. Note: This information stays consistent across both tabs.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected. Note: This information stays consistent across both tabs.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes.

Component	Description
	By default, this field is blank. Note: This information stays consistent across both tabs.
Device	Allows you to enter a COM port number.
Baud	Define the communication rate by selecting a value from the drop-down list. Values range between 110 and 256000 . Default = 9600 .
Parity	From the drop-down list, select the type of parity to be used. Options available are none , odd , even , mark , and space . Default = none .
Data bits	Define the number of data bits by selecting a value from the drop-down list. Values range between 4 and 8 . Default = 8 .
Stop bits	From the drop-down list, select the number of stop bits. Options available are 1 , 1.5 , and 2 . Default = 1 .
RTS line	From the drop-down list, select a Request To Send (RTS) preset. Available options are disable , enable , handshake , and toggle . Default = disable .
DTR line	Allows you to select a Data Terminal Ready (DTR) preset from the drop-down list. Available options are disable , enable , and handshake . Default = disable .
DSR flow control	This checkbox allows you to enable (i.e., select the checkbox) or disable (i.e., clear the checkbox) Data Set Ready (DSR) flow control. Default = checkbox is cleared.
DSR sensitivity	This checkbox allows you to enable (i.e., select the checkbox) or disable (i.e., clear the checkbox) Data Set Ready (DSR). Default = checkbox is cleared.
CTS flow control	This checkbox allows you to enable (i.e., select the checkbox) or disable (i.e., clear the checkbox) Clear To Send (CTS) flow control. Default = checkbox is cleared.
XON/XOFF flow control	This checkbox allows you to enable (i.e., select the checkbox) or disable (i.e., clear the checkbox) XON/XOFF software flow control. Default = checkbox is cleared.
Log bytes transmitted	Enables (i.e., check box is selected) or disables (i.e., checkbox is cleared) the logging of bytes transmitted at Medium level. Default = checkbox is cleared.
Log bytes received	Enables (i.e., check box is selected) or disables (i.e., checkbox is cleared) the logging of bytes received at Medium level. Default = checkbox is cleared.
OK	Select this button to save any changes and close the window.

Component	Description
	Note: This information stays consistent across both tabs.
Cancel	Closes the window without saving any changes made. Note: This information stays consistent across both tabs.

Table 23 - Create New Serial Channel Window - Communication Tab Components

Data Acquisition Tab

Figure 27 displays the settings available on the **Create New Serial Channel - Data Acquisition** tab.

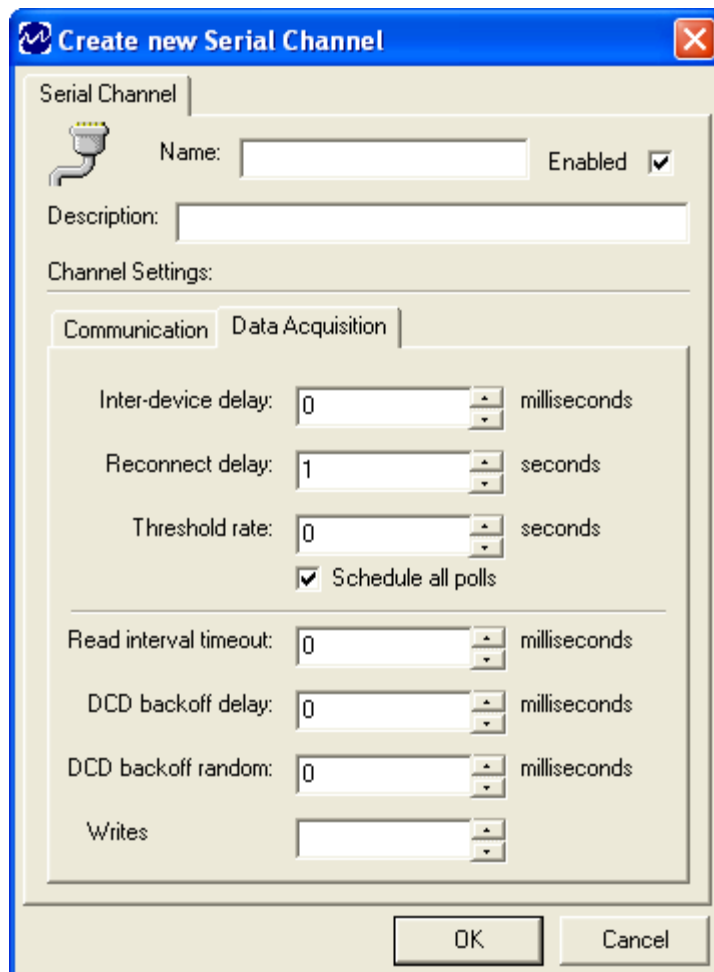


Figure 27 - Create New Serial Channel Window - Data Acquisition Tab

Table 24 describes the components of the **Create New Serial Channel – Data Acquisition** tab.

Component	Description
Inter-device delay	Allows you to enter or select a value specifying the minimum amount of time (in milliseconds) between the last request/response to/from one unit and the next request to another unit on this channel. If this option is set to 0 then it will be disabled. Default = 0 .
Reconnect delay	Allows you to enter or select a value specifying the minimum amount of

Component	Description
	time (in seconds) to wait before attempting to recover communications after the communication channel itself has failed. Default = 1 .
Threshold rate	Allows you to enter or select a value specifying the maximum achievable scan interval (in seconds) for the circuit. The server polls items with update rates faster than this on a continuous basis. Changing this option requires the server on this channel. If this is set to 0 then the option is turned off. Default = 0 . Note: All units on the channel must re-optimize if this parameter changes.
Schedule all polls	When this checkbox is selected, rather than polling them continuously, the server schedules items with update rates faster than the threshold rate to poll at the threshold rate. Default = 1 "checked" .
Read interval timeout	Allows you to enter or select a value specifying the maximum amount of time (in milliseconds) between the reception of one character and the arrival of the next. A value of 0 indicates no limit. Default = 0 .
DCD backoff delay	Allows you to enter or select a value specifying the minimum amount of time (in milliseconds) for DCD to be low before transmitting to avoid collisions. Set both DCD backoff delay and DCD backoff random fields to 0 to ignore DCD. Default = 0 .
DCD backoff random	Allows you to enter or select a value specifying the maximum amount of extra random time (in milliseconds) for DCD to be low before transmitting. Set both DCD backoff delay and DCD backoff random fields to 0 to ignore DCD. Default = 0 .
Writes	Allows you to enter or select a value specifying the maximum number of writes allowed before forcing a poll.

Table 24 - Create New Serial Channel Window - Data Acquisition Tab Components

To create a Serial Channel object:

- On the **Configuration** window, select the **Server Configuration** node and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.
- The **Insert New Object** window (Figure 19) appears.
- From the displayed list, select the **Serial Channel** object type.
- Click on the **OK** button.
- The **Create New** window appears (Figure 26).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Serial Channel** is selected, then the **Create New Serial Channel** window is displayed.

6. From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.

7. Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.

8. Click on the **OK** button. The object is created and will appear as a child of the **Server Configuration** item as shown in Figure 28.

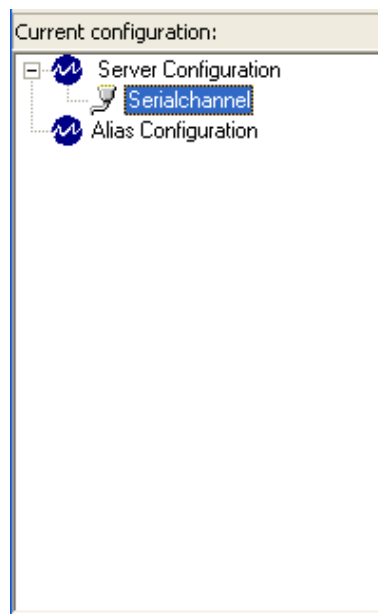
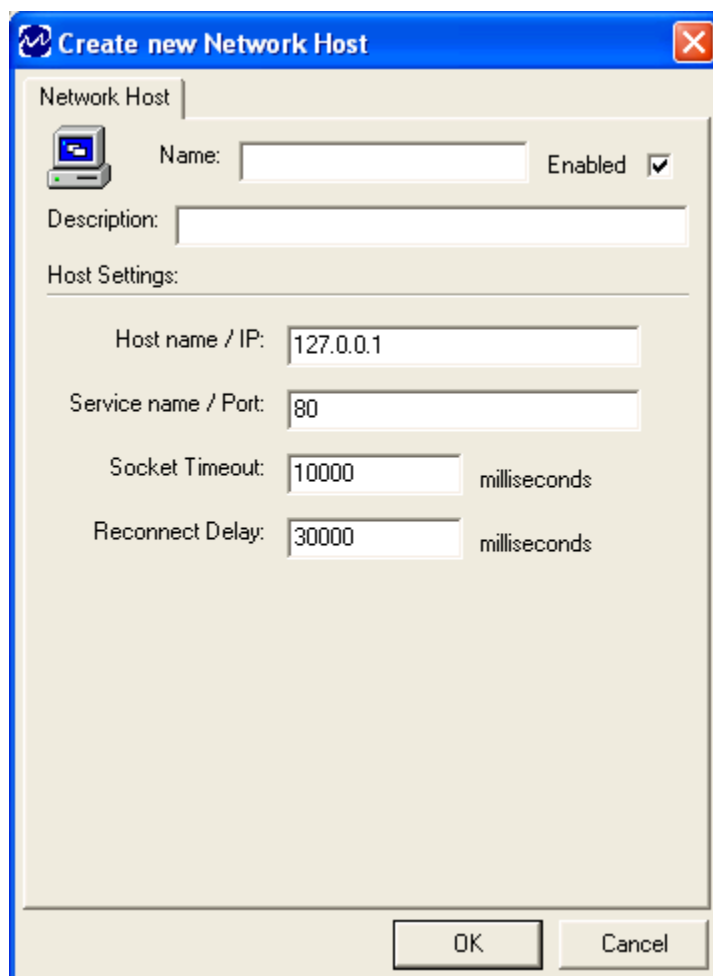


Figure 28 - New Serial Channel Object

Creating and Configuring a Network Host Object

Note: A **Network Host** can be created as a child of a **Network Channel**.

The **Create New Network Host** window (Figure 29) displays the settings available for configuring a **Network Host**.



Create new Network Host

Network Host

 Name: Enabled ☒

Description:

Host Settings:

Host name / IP:

Service name / Port:

Socket Timeout: milliseconds

Reconnect Delay: milliseconds

OK Cancel

Figure 29 - Create New Network Host Window

Table 25 describes the components of the **Create New Network Host** window.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank.
Host name/IP	Allows you to define the network name/IP address of the device.
Service name/Port	Allows you to define the service name/port for the device.
Socket Timeout	Allows you to specify the time (in milliseconds) to wait for a response on the socket.

Component	Description
Reconnect Delay	Allows you to specify the time (in milliseconds) to wait before attempting to reconnect.
OK	Select this button to save any changes and close the window.
Cancel	Closes the window without saving any changes made.

Table 25 - Create New Network Host Window Components

To create a Network Host object:

- On the **Configuration** window, select a previously-created **Network Channel** object (for assistance, refer to **Creating and Configuring a Network Channel Object**) and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.
- The **Insert New Object** window (Figure 30) appears.

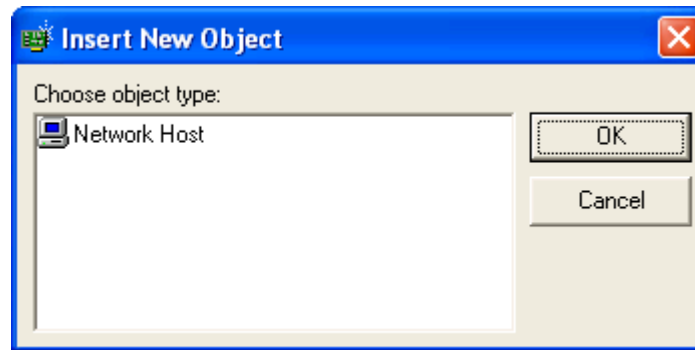


Figure 30 - Insert New Object

- From the displayed list, select **Network Host**.
- Click on the **OK** button.
- The **Create New** window appears (Figure 29).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Network Host** is selected, then the **Create New Network Host** window is displayed.
- From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.
- Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.
- Click on the **OK** button. The object is created and will appear as a child of the **Network Channel** item as shown in Figure 31.

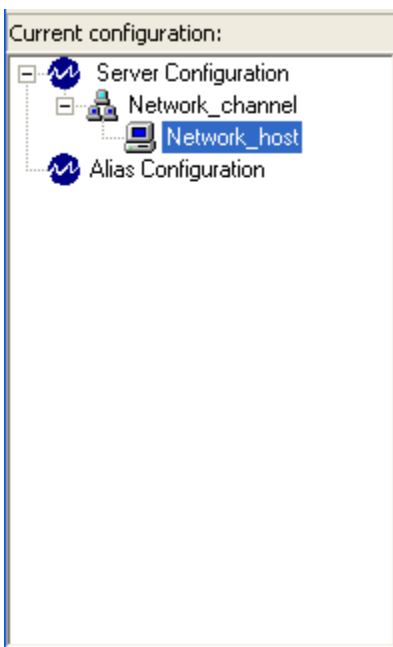


Figure 31 - New Network Host Object

Creating and Configuring a Dial-Up Connection Object

Note: A **Dial-up Connection** object can be created as a child of a **Network Host** or a **Serial Channel**. For more information, refer to [Creating and Configuring a Network Host Object](#) or [Creating and Configuring a Serial Channel Object](#).

The **Create New** window (Figure 32) displays the settings available when creating a **Dial-up Connection** object.

The **Create New Dial-up Connection** window consists of three tabs:

- **Dial-up**
- **Modem**
- **Advanced**

Dial-Up Tab

Figure 32 displays the **Create New Dial-up Connection – Dial-up** tab.

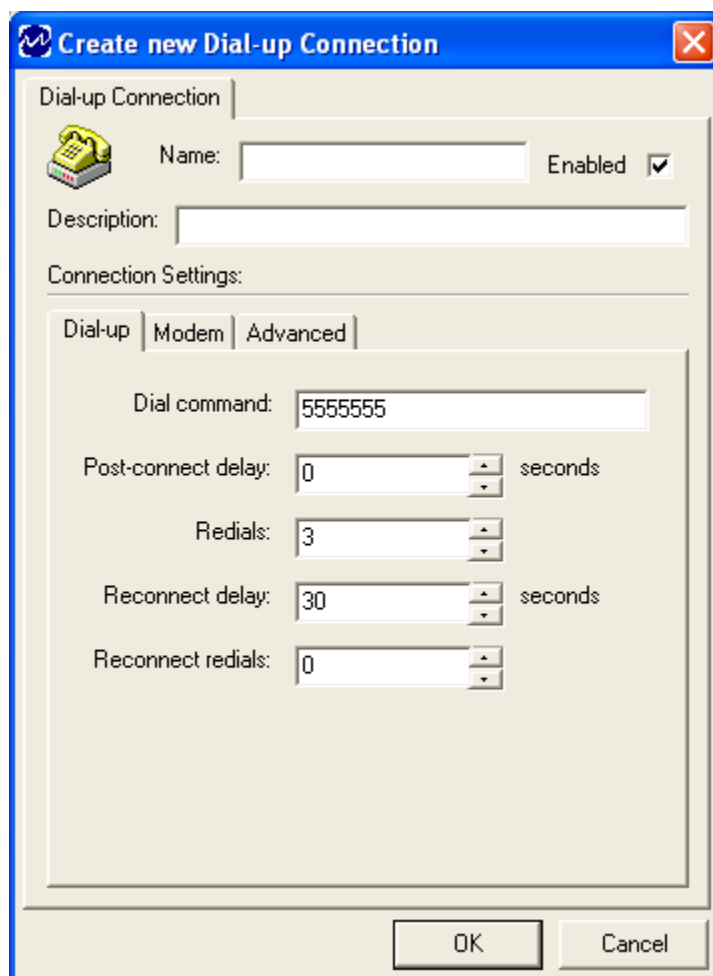


Figure 32 - Create New Dial-Up Connection Window - Dial-up Tab

Table 26 describes the components of the **Create New Dial-up Connection – Dial-up** tab.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes. Note: This information stays consistent across all tabs.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected. Note: This information stays consistent across all tabs.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank. Note: This information stays consistent across all tabs.
Dial command	Allows you to enter any valid sequence of characters that can follow an

Component	Description
	ADT command.
Post-connect delay	Allows you to enter or select a value specifying the minimum amount of time (in seconds) to wait after establishing a dial-out connection before transmitting.
Redials	Allows you to enter or select a value defining the maximum number of times to redial a connection before concluding that communication has failed with the units on that connection.
Reconnect delay	Allows you to enter or select a value specifying the minimum amount of time (in seconds) to wait before attempting to recover communications after communication has failed with the connection.
Reconnect redials	Allows you to enter or select a value defining the maximum number of times to redial when trying to reconnect after communication has failed with a dial-up connection.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Closes the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 26 - Create New Dial-Up Connection Window - Dial-Up Tab Components

Modem Tab

Figure 33 displays the settings available on the **Create New Dial-up Connection - Modem** tab.

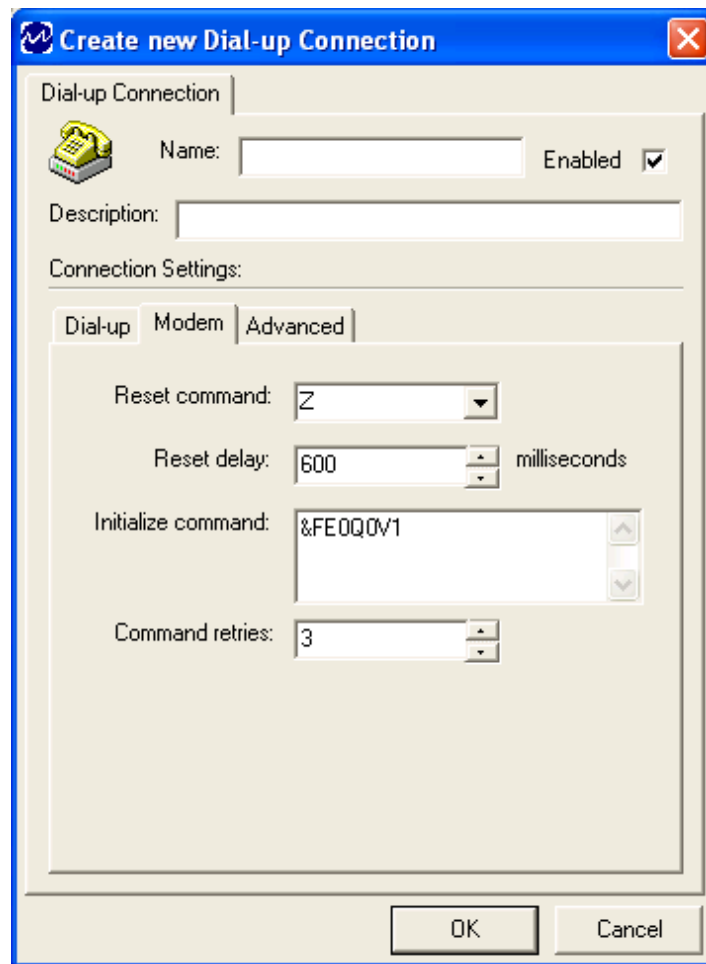


Figure 33 - Create New Dial-Up Connection Window - Modem Tab

Table 27 describes the components of the **Create New Dial-Up Connection – Modem** tab.

Component	Description
Reset command	Allows you to select, from the drop-down list, a modem reset command. This command is sent before initialization commands.
Reset delay	Allows you to enter or select a value specifying the amount of time (in milliseconds) to wait after the reset command completes.
Initialize command	Allows you to enter modem initialization command or commands, issued before dialling out and after hanging up. The command should always end with EOQOV1 .
Command retries	Allows you enter or select a value to define the maximum number of times to resend a command wait for a response before concluding that communication has failed with the modem.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Closes the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 27 - Create New Dial-Up Connection Window - Modem Tab Components

Advanced Tab

Figure 34 displays the settings available on the **Create New Dial-up Connection – Advanced** tab.

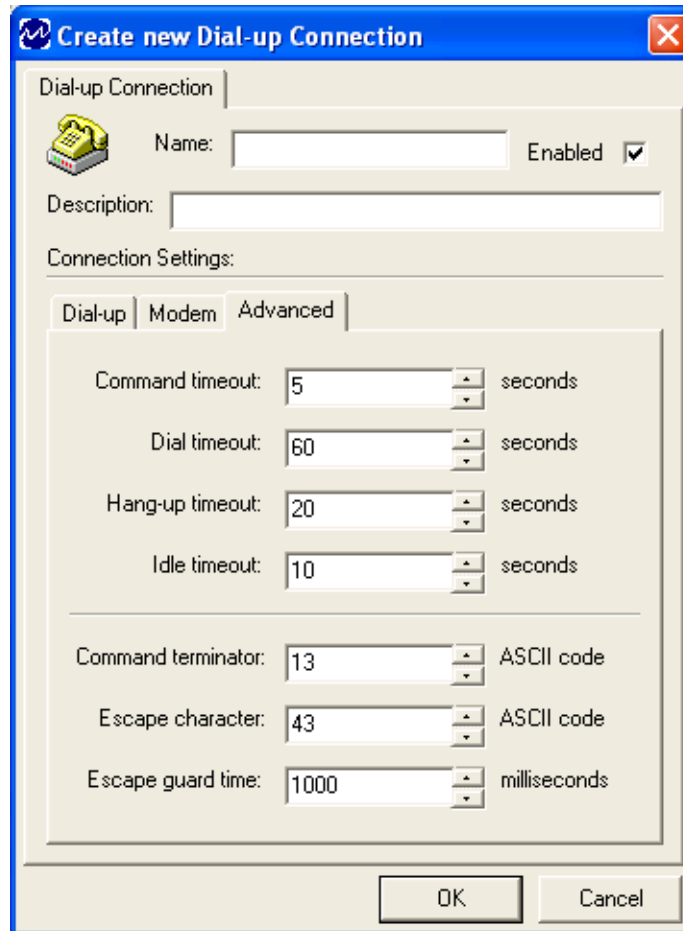


Figure 34 - Create New Dial-Up Connection Window - Advanced Tab

Table 28 describes the components of the **Create New Dial-up Connection - Advanced** tab.

Component	Description
Command timeout	Allows you to enter or select a value defining the maximum amount of time (in seconds) to wait for the modem to respond to AT commands with a valid result code.
Dial timeout	Allows you to enter or select a value defining the maximum amount of time (in seconds) to wait for the modem to receive a carrier from the dialed connection before aborting the call.
Hang-up timeout	Allows you to enter or select a value defining the maximum amount of time (in seconds) to wait for the modem to hang up after issuing the ATH0 command.
Idle timeout	Allows you to enter or select a value defining the maximum amount of time (in seconds) to allow an idle connection to continue (i.e., no communication) before hanging up.
Command terminator	Allows you to enter or select a value defining an ASCII character to be

Component	Description
	used to terminate commands and responses (usually a carriage return).
Escape character	Allows you to enter or select a value defining an ASCII character that is sent three times to escape into command mode (usually a plus sign).
Escape guard time	Allows you to enter or select a value defining the amount of time (in milliseconds) to wait before and after sending the escape sequence.

Table 28 - Create New Dial-Up Connection Window - Advanced Tab Components

To create a Dial-up Connection object:

1. On the **Configuration** window, select a previously-created **Network Host** or a previously-created **Serial Channel** (for assistance, refer to **Creating and Configuring a Network Host Object** or **Creating and Configuring a Serial Channel Object**) and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.

2. The **Insert New Object** window appears.
3. From the displayed list, select the **Dial-up Connection** object type.
4. Click on the **OK** button.
5. The **Create New** window appears (Figure 32).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Dial-up Connection** is selected, then the **Create New Dial-up Connection** window is displayed.

6. From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.

7. Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.

8. Click on the **OK** button. The object is created and will appear either as a child of the **Network Host** or **Serial Channel** item as shown in Figure 35 (depending on what the selected parent item was).

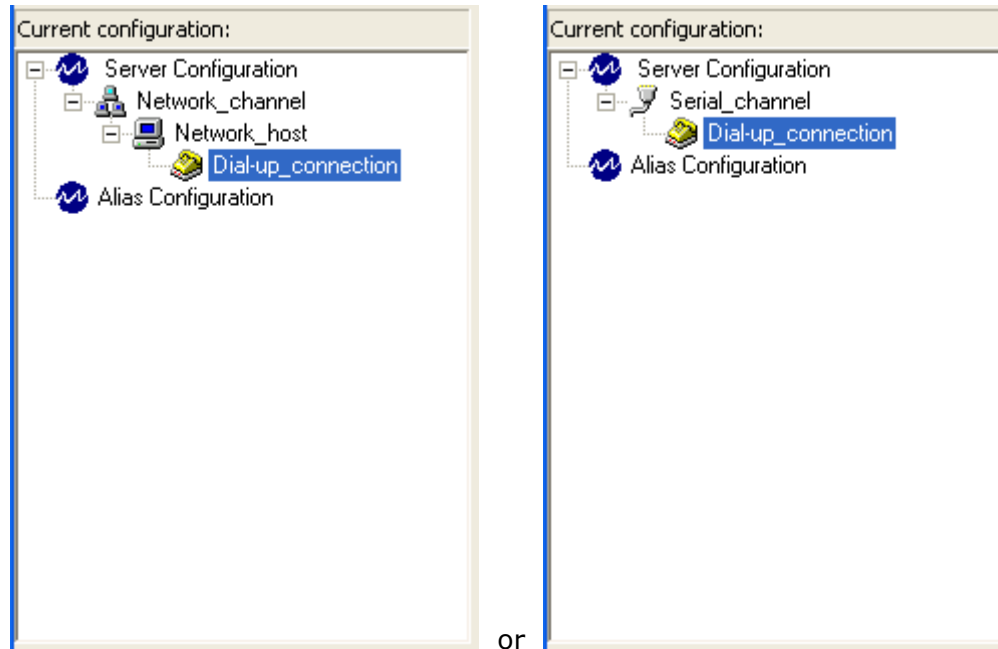


Figure 35 - New Dial-Up Connection Object

Creating and Configuring a DNP3 Unit Object

Note: A DNP3 Unit object can be created as a child of any of the following items:

- **Network Host** ([Creating and Configuring a Network Host Object](#))
- **Dial-up Connection** ([Creating and Configuring a Dial-up Connection Object](#))
- **Serial Channel** ([Creating and Configuring a Serial Channel Object](#))
- **Radio** ([Creating and Configuring a Radio Object](#))

The **DNP3 Unit Settings** panel is used to both view and to edit DNP3 unit settings. This is virtually the same as the **Create New** window for DNP3 units, with the exception that it appears after the object has been created.

The **DNP3 Unit Settings** panel includes three tabs:

- **Communication**
- **Data Acquisition**
- **Optimization**

Communication Tab

The **DNP3 Unit Settings - Communication** settings (Figure 36) include those for setting the master, station, base poll time, time bias, operate outputs, and synchronize time.

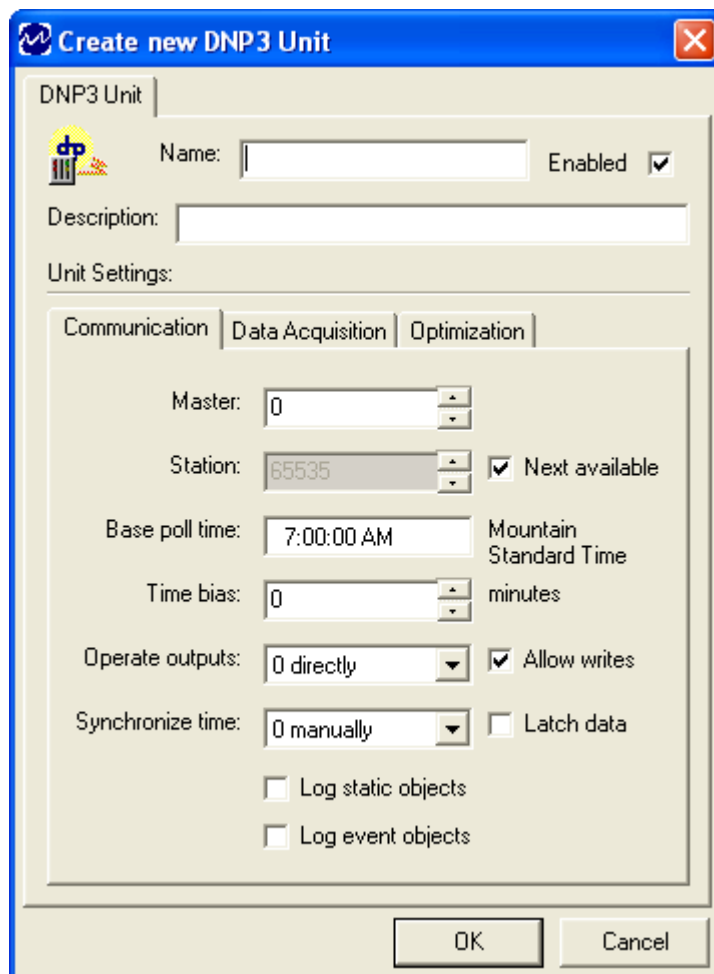


Figure 36 - Create New DNP3 Unit - Communication Tab

Table 29 describes the components of the **DNP3 Unit Settings - Communication** tab.

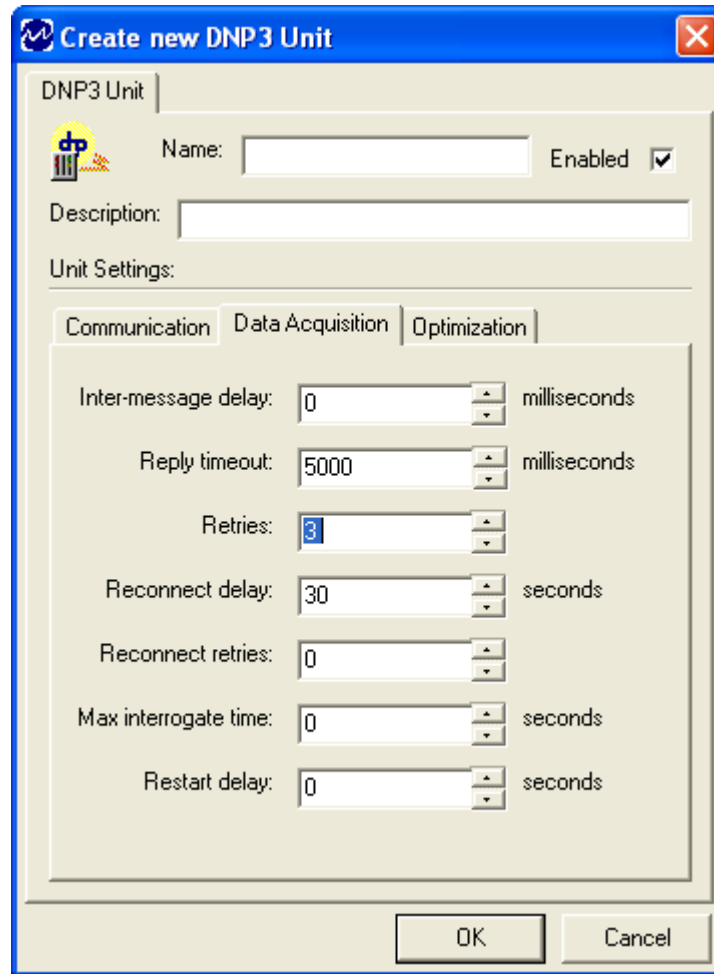
Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes. Note: This information stays consistent across all tabs.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected. Note: This information stays consistent across all tabs.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank. Note: This information stays consistent across all tabs.
Master	Allows you to enter or select a value defining the DNP3 master address. Changing this option requires the server to reset communication with this

Component	Description
	unit.
Station	Allows you to enter or select a value defining the DNP3 station address. Changing this option requires the server to reset communication with this unit.
Next available	When this checkbox is selected, the unit will default to the next available DNP3 station address on the channel. When this checkbox is selected, the Station field is disabled (i.e., grayed out).
Base poll time	Allows you to enter or select the normalization time for scheduling polls, stored as UTC. Changing this option requires the server to re-optimize communication with this unit.
Time bias	Allows you to enter or select the number of minutes to add to timestamps received from the outstation to convert them to UTC. This value is used to set the local time of the Remote Station. This must be set for timestamps received from this unit to be correct.
Operate outputs	Allows you to select, from the drop-down list, the procedure used to operate binary and analog outputs: directly , after arming , or after re-arming .
Allow writes	Select this checkbox to allow writes to the unit. Clear the checkbox to disallow writes.
Synchronize time	Allows you to select, from the drop-down list, the sort of automatic time synchronization to perform on IIN1-4: function 23 Delay Measurement, function 24 Record Current Time, or manually . Function 23 is normally used where time delays in the communication medium are constant (serial communication). Function 24 is normally used where time delays may vary (TCP communication).
Latch data	Select this checkbox to have items "freeze" at their last value/quality/timestamp when the unit is set off-scan.
Log static objects	Select this checkbox to log static objects received from the outstation at high detail level.
Log event objects	Select this checkbox to log event objects received from the outstation at high detail level.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across both tabs.
Cancel	Closes the window without saving any changes made. Note: This information stays consistent across both tabs.

Table 29 - Create New DNP3 Unit – Communication Tab Components

Data Acquisition Tab

The **DNP3 Unit Settings - Data Acquisition** settings (Figure 37) include those for setting delay times, timeouts, retries and interrogate times.



Create new DNP3 Unit

DNP3 Unit

 Name: Enabled ☒

Description:

Unit Settings:

Communication | **Data Acquisition** | Optimization

Inter-message delay: milliseconds

Reply timeout: milliseconds

Retries:

Reconnect delay: seconds

Reconnect retries:

Max interrogate time: seconds

Restart delay: seconds

OK Cancel

Figure 37 - Create New DNP3 Unit - Data Acquisition Tab

Table 30 describes all the components of the **DNP3 Unit Settings - Data Acquisition** settings.

Component	Description
Inter-message delay	Allows you to enter or select a value defining the minimum amount of time (in milliseconds) between the last request/response to/from this unit and the next request to this same unit.
Reply timeout	Allows you to enter or select a value defining the maximum amount of time (in milliseconds) to wait for the response to a request.
Retries	Allows you to enter or select a value defining the maximum number of times to resend a request and wait for a response before concluding that communication has failed with the unit.
Reconnect delay	Allows you to enter or select a value defining the minimum amount of time (in seconds) to wait before attempting to reconnect after communication has failed with a unit.
Reconnect retries	Allows you to enter or select a value defining the maximum number of times to resend a request and wait for a response when trying to reconnect after communication has failed with a unit.
Max interrogate time	Allows you to enter or select a value defining the maximum amount of time (seconds) to allow a unit to be interrogated. A value of zero indicates that

Component	Description
	interrogation must be halted manually.
Restart delay	Allows you to enter or select a value defining the minimum amount of time (in seconds) to wait following a cold/warm restart before resuming communication with the unit.

Table 30 – Create New DNP3 Unit – Data Acquisition Tab

Optimization Tab

The **DNP3 Unit Settings - Optimization** settings (Figure 38) include those for setting data link and application confirmations, as well as maximum outputs, events, and fragment size.

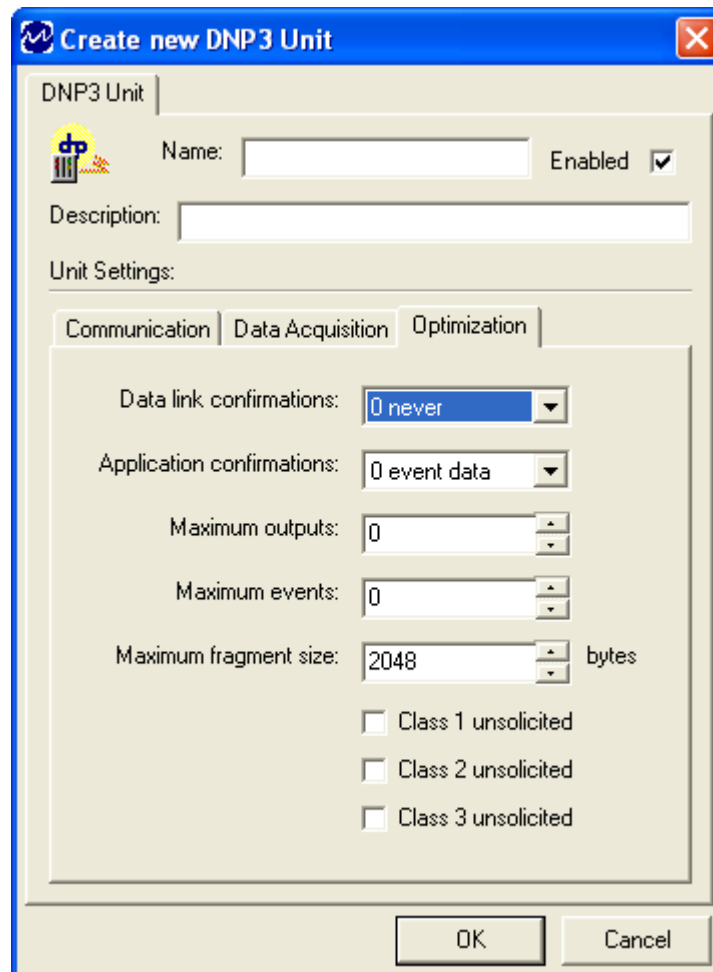


Figure 38 – Create New DNP3 Unit – Optimization Tab

Table 31 describes all the components of the **DNP3 Unit Settings, Optimization** settings.

Component	Description
Data link confirmations	Allows you to select, from the drop-down list, how often to request confirmation for FT3 frames: never , multi-frame messages only, or always .
Application confirmations	Allows you to select, from the drop-down list, how often to request confirmation for application fragments: messages containing event data only, multi-fragment messages only, or always .

Component	Description
Maximum outputs	Allows you to enter or select a value defining the maximum number of objects (control blocks) per output operation (0 = no limit).
Maximum events	Allows you to enter or select a value defining the maximum number of objects (quantity) per class/type in an event poll (0 = no limit).
Maximum fragment size	Allows you to enter or select a value defining the maximum length (bytes) of one application fragment.
Class 1 unsolicited	Select this checkbox to enable unsolicited updates for class 1 data.
Class 2 unsolicited	Select this checkbox to enable unsolicited updates for class 2 data.
Class 3 unsolicited	Select this checkbox to enable unsolicited updates for class 3 data.

Table 31 - Create New DNP3 Unit – Optimization Tab

To edit DNP3 unit settings:

1. On the **Configuration** window, select a **DNP3** unit under a previously-created **Serial Channel**, **Radio**, **Network Host**, or **Dial-up Connection** object. The **DNP3 Unit Settings** window appears.
2. Click the **Data Acquisition** tab to view and edit data acquisition settings for this **DNP3** unit.
3. When you have edited the settings, either click the **Communications** or **Optimization** tab to edit these settings, or click **Apply** to apply your changes now.

Creating and Configuring a Radio Link

Note: A **Radio** link can be created as a child of a **Serial Channel**.

The **Create New Radio** window (Figure 39) displays the settings available for configuring a **Radio** link.

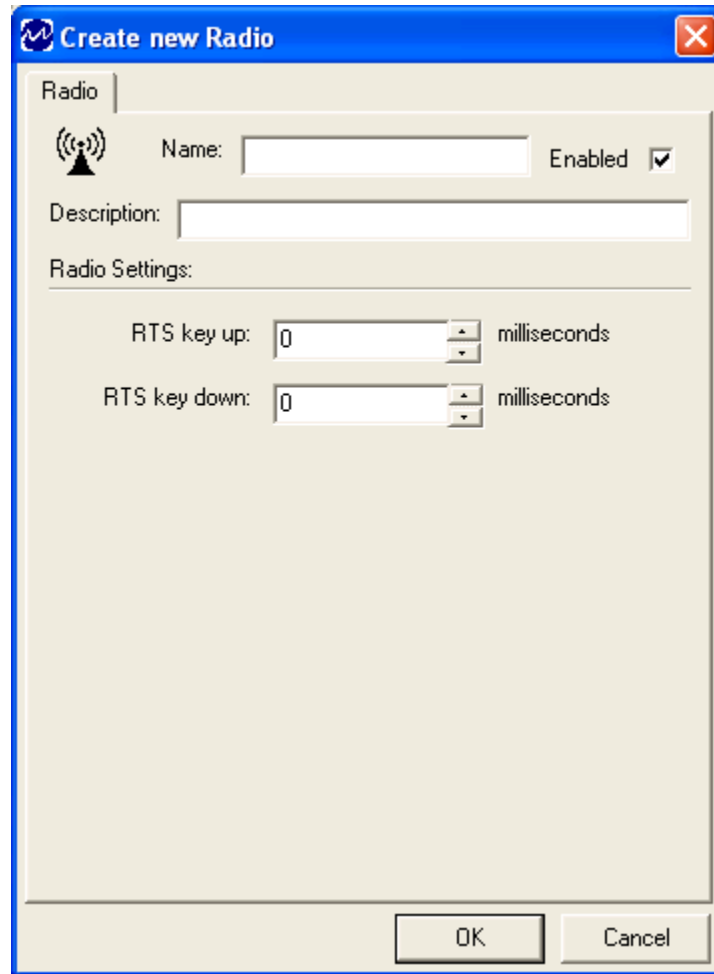


Figure 39 - Create New Radio Window

Table 32 describes the components of the **Create New Radio** window.

Component	Description
Name	Allows you to enter the name of the device link, which becomes an element of the item ID for data items. The full path of the device link must be entered. Automatically converted to title case for display purposes.
Enabled	Use this checkbox to enable (i.e., checkbox is selected) or disable (i.e., checkbox is cleared) communication for the object. By default, the checkbox is selected.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank.
RTS key up	Allows you to enter or select a value defining the minimum amount of time (in milliseconds) to wait after setting the RTS signal to allow the transceiver to "warm up".
RTS key down	Allows you to enter or select a value defining the minimum amount of time (in milliseconds) to wait before clearing the RTS signal to allow the

Component	Description
	transceiver to "cool down".
OK	Select this button to save any changes and close the window.
Cancel	Closes the window without saving any changes made.

Table 32 - Create New Radio Window Components

To create a Radio link:

- On the **Configuration** window, select a previously-created **Serial Channel** object (for assistance, refer to **Creating and Configuring a Serial Channel Object**) and either:
 - Right-click your mouse and select **Define New** from the menu that appears, or
 - Select the **Define New** menu option from the **Edit** menu, or
 - Click on the  icon.
- The **Insert New Object** window (Figure 40) appears.

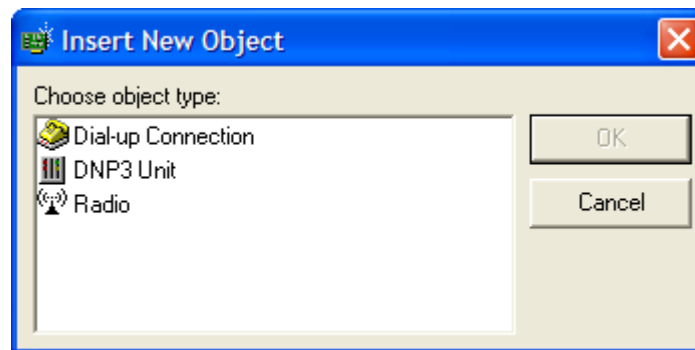


Figure 40 - Insert New Object

- From the displayed list, select **Radio**.
- Click on the **OK** button.
- The **Create New** window appears (Figure 39).

Note: The item selected in the **Insert New Object** window will determine which **Create New** window is displayed. For example, when **Radio** is selected, then the **Create New Radio** window is displayed.
- From the **Create New** window, enter a name for the object.

Note: An error message is displayed when a valid name is not entered. If the entered name is a duplicate of an existing device link, the new device link will not be created. The **Description** field is optional.
- Edit the configuration components as desired.

Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.
- Click on the **OK** button. The object is created and will appear as a child of the **Serial Channel** item as shown in Figure 41.

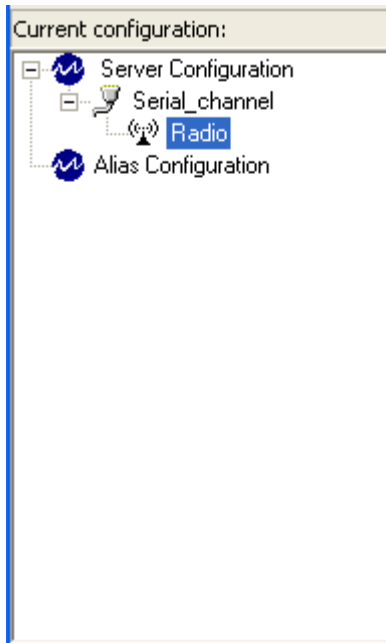


Figure 41 - New Radio Link

Changing Objects

To change an object's configuration:

1. Once an object is created, select it in the tree view (i.e., **Current configuration**) panel.
2. In the configuration panel (i.e., panel on the right), make the applicable changes.
3. Click on the **Apply** button to accept the changes, or click on the **Cancel** button to discard them.

Removing Objects

Note: Users can easily remove any object that they have created, but a warning message (Figure 42) will appear when users remove an object that has data items to which one or more OPC clients hold reference.

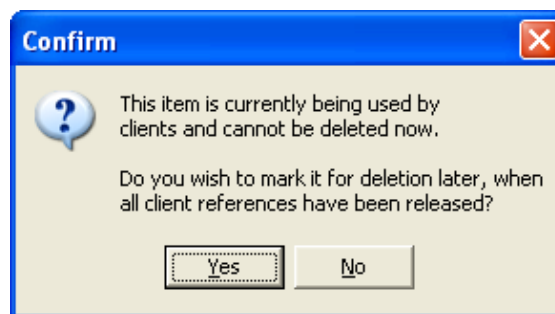


Figure 42 - Client Reference Warning Message

To remove an object:

1. In the **Configuration** window, under **Server Configuration**, select the object to be removed.
2. From the **Edit** menu, select the **Delete** menu option (or click on the  button).

Note: If one or more OPC clients hold references to data items somewhere under the selected object, a warning message (Figure 42) appears.

3. To mark the object for later deletion, click on the **Yes** button. To leave the object unmodified, click on the **No** button.

Note: Items marked for deletion are disabled and a red X appears over the icon on the right side of the window when the object is selected.

Alias Configuration

MatrikonOPC servers, including this one, provide the ability to create user-defined aliases that can be used in place of regular OPC items. This feature is particularly useful when the item path for a given server is very complex or difficult to remember, for example: *Com1.Radio1.Unit1.41.4.123*.

Servers can also be configured so that client applications have access to configured aliases only, rather than every available item.

This section of the manual describes how to create and edit aliases using the **Configuration** window.

Note: It is not necessary to define aliases before accessing server data items from an OPC client.

Inserting Alias Groups

Note: Alias Groups are used to contain one or more configured aliases.

To insert an Alias Group:

1. On the **Configuration** window, select **Alias Configuration** or a previously configured **Alias Group**.
2. From the **Edit** menu, choose **Insert Alias Group** or click on the  button.
3. A new **Alias Group** folder appears.
4. Enter a new name for the **Alias Group**, and press **Enter**.
5. The **Alias Group** is renamed.

Renaming Alias Groups

Note: Alias Groups can be renamed after they have been created.

To rename an Alias Group:

1. On the **Configuration** window, select an **Alias Group**.
2. From the **Edit** menu, choose **Rename** or click on the  button.
3. The **Alias Group** is renamed.

Inserting New Aliases

Use the **Insert New Alias** window (Figure 43) to insert a new alias into an Alias Group, or insert a new alias on its own directly under the Alias Configuration node.

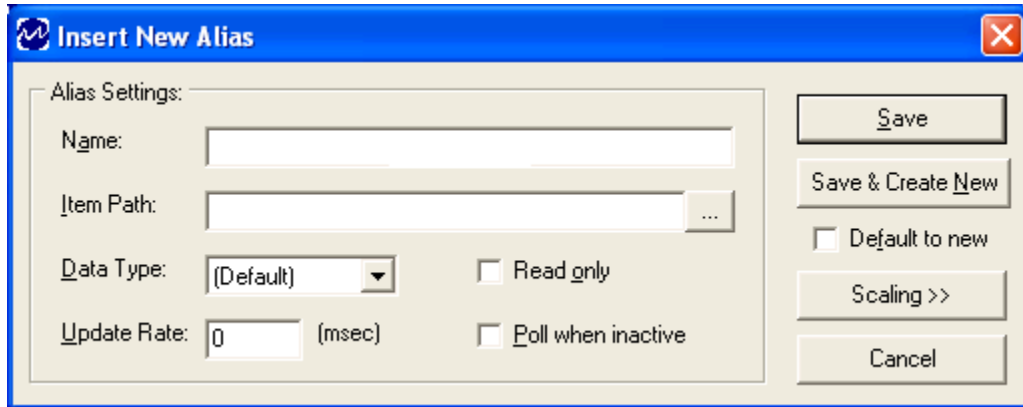


Figure 43 - Insert New Alias Window

Table 33 describes the components of the **Insert New Alias** window.

Component	Description
Name	Name for the alias (unique within the alias group).
Item Path	Fully-qualified item ID for the OPC item to which the alias refers. Click on the ellipsis button (...) to display the Item Path Browser window used to select an existing OPC item on the server. Alternatively, leave the item path blank to use the alias as a general in-memory variable. When doing so, either define the data type for the alias point as something other than Default , or have the alias set for reading and define the data type while writing values to the alias from an OPC client. Note: This component is disabled when the Calculation form of scaling is used. Item paths are specified in the calculation itself.
Data Type	Set the value of the OPC item to the specified type unless Default is selected. Also serves as the "canonical" data type for the alias.
Read only	When this checkbox is selected, it prevents OPC clients from writing values to the alias. Note: This option is not available for Calculation aliases, as they are read-only.
Update Rate	Update rate (milliseconds) to use with the Poll when inactive option.
Poll when inactive	If selected, continues updating the value for the alias at the specified update rate even if there are no OPC clients currently accessing the alias.
Save	Save changes to the alias and hide the window.
Save & Create New	Save changes to the alias and begin configuring a new one.
Default to new	Pressing Enter activates the Save & Create New button rather than the Save button, if selected.
Scaling >>	Enables scaling for the alias (displays scaling options).
<< No Scaling	Disables scaling for the alias (hides scaling options).
Cancel	Discards changes to (abandon creation of) the alias and hides the

Component	Description
	window.

Table 33 - Insert New Alias Window Options

By selecting the **Scaling >>** button, the **Insert New Alias** window can be expanded to display **Scaling Options** (Figure 44). The available forms of scaling include: Simple text **Expressions**, **Calculation**, **Linear**, **Square Root**, and **Gain/Offset**.

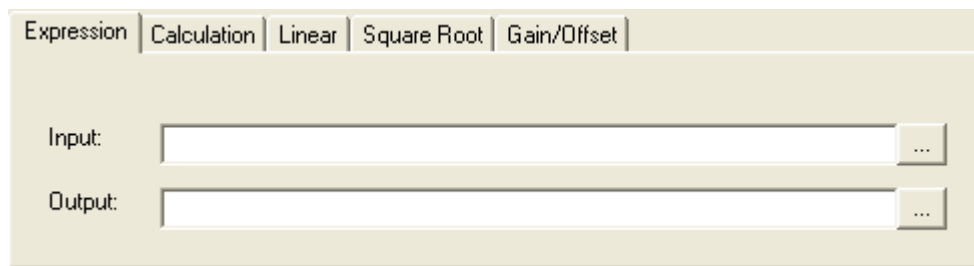


Figure 44 - Insert New Alias Window Scaling Options

Table 34 describes the **Scaling Options** for the **Insert New Alias** window.

Tab	Component	Description
Expression	Input	Simple text equation to apply to incoming values (reads). Click on the ellipsis button (...) to display the Expression Wizard screen used to help build a formula. For more information, refer to the Expression Wizard section in this manual.
	Output	Simple text equation to apply to outgoing values (writes). Click on the ellipsis button (...) to display the Expression Wizard screen used to help build a formula. For more information, refer to the Expression Wizard section in this manual.
Calculation	Input	Calculation equation to apply to incoming values (reads). Click on the ellipsis button (...) to display the Item Path Browser screen used to add item paths to this field. For more information, refer to the Item Path Browser section in this manual.
Linear and Square Root	Raw High	Maximum expected raw value of the OPC item.
	Raw Low	Minimum expected raw value of the OPC item.
	Scaled High	Maximum desired scaled value for the alias (corresponds to Raw High).
	Scaled Low	Minimum desired scaled value for the alias (corresponds to Raw Low).
	Clamp High	Clamp the scaled value at the high limit to prevent it from going out of range.
	Clamp Low	Clamp the scaled value at the low limit to prevent it from going out of range.
Gain/Offset	Gain	Scaling factor. (No limits are assumed.)
	Offset	Scaling offset.

Table 34 - Insert New Alias Window Scaling Options

Notes:



- The data type for scaled values is double-precision real unless the alias data type is specified.
- Using invalid settings, such as zero-zero for the high-low range in **Linear** scaling, may be fatal to the server, OPC clients, and communications.
- The OPC item values must be numeric for **Linear**, **Square Root**, and **Gain/Offset** scaling to work.
- The OPC item values must be non-negative for **Square Root** scaling to work. Otherwise, the scaled value will be -1 with a bad quality.
- The server may be unable to load configuration files containing invalid scaling expressions, and may fail to start up properly. If this occurs, rename the configuration file so that the server will not load it upon start-up. Alternatively, edit the XML file to correct the invalid alias settings.

To insert a new alias:

Note: It is recommended that you create a new alias under an **Alias Group** rather than directly under the **Alias Configuration** node.

1. On the **Configuration** window, select **Alias Configuration** or a previously configured **Alias Group**.
2. The **Contents** table for that **Alias Group** is displayed on the right side of the **Configuration** window (Figure 45), listing the aliases it contains.

Contents of alias group '(root)':				
Name	Item Path	Data Type	R/W	Update Rate
Alias1	Net1.Host1.Unit1.041.4.123	(Default)	R/W	
Alias2	Net1.Host1.Unit1.041.4.124	(Default)	R/W	
Alias3	Net1.Host1.Unit1.041.4.125	(Default)	R/W	

Figure 45 - Contents Table

3. From the **Edit** menu, choose **Insert New Alias**.
4. The **Insert New Alias** window (Figure 43) appears.
5. Enter a name for the alias in the **Name** field.
6. Enter the item **Path** and **ID** for the item to which the alias refers, or click on the **Browse** button to navigate to the item.
7. Click on the **Scaling** button to enable scaling for the alias. Click on the **No Scaling** button to disable scaling and hide the **Scaling Options**.

The **Scaling Options** are displayed at the bottom of the **Insert New Alias** window (Figure 44).

8. Configure the **Scaling Options** as required (see Table 34 for a description of these options), by clicking the appropriate tab for the form of scaling that maybe required.

Note: Available forms of scaling include: **Expression**, **Calculation**, **Linear**, **Square Root**, and **Gain/Offset**. **Expression**, which uses an Expression Wizard to help build equations, is used frequently and is intended to view individual bits from registers. Refer to the **Expression Wizard** section for more information. **Calculation**, which uses the Item Path Browser to add items to calculation, is intended for calculations with involve multiple items. Refer to the **Item Path Browser** section for more information.

9. Configure the remaining fields as required (see Table 33 for a description of all the components).
10. Click on the **Save** button to save the alias.

Editing Aliases

Note: Aliases can be edited after they have been created using the **Edit Alias** window. This is virtually the same as the **Insert New Alias** window (Figure 43), with the exception that it appears after the alias has been created.

To edit an alias:

1. On the **Configuration** window, select the alias you want to change, and then double-click or press **Enter**.
2. The **Edit Alias** window appears.
3. Make the changes as required.

Removing Aliases

Note: Any alias that was created can be removed.

To remove an alias:

1. On the **Configuration Window**, select one or more aliases that you want to remove.
2. From the **Edit** menu, choose the **Delete Alias** menu option.
3. The alias is removed.

Removing Alias Groups

Note: Any Alias Group that was created can be removed.

To remove an Alias Group:

1. On the **Configuration** window, select the Alias Group you want to remove.
2. From the **Edit** menu, select the **Delete Alias Group** menu option or click on the  button.
3. The **Alias Group** is removed.

Exporting Aliases

Note: Use the **Export Aliases** window to export all currently configured aliases to a CSV file.

To export all currently configured aliases:

1. From the **File** menu, select the **Export Aliases** menu option or click on the  button.
2. The **Export Aliases** window appears.
3. Enter a file name for the CSV export file.
4. Click **Save**.

5. The aliases are exported.

Importing Aliases

Note: Use the **Import Aliases** window to clear all aliases and import new ones from a CSV file.

To import aliases from a CSV file:

1. From the **File** menu, select the **Import Aliases** menu option or click on the  button.
2. The **Import Aliases** window appears.
3. Browse to the CSV file name.
4. Click **Open**.
5. The old aliases are cleared and the new ones are imported.

Expression Wizard

The **Expression** form of scaling uses an **Expression Wizard** to build formulas. The created formula is a simple text equation that is applied to either incoming values (i.e., reads), or outgoing values (i.e., writes).

Table 35 describes the **Expression Wizard** fields.

Component	Description
Input/Output Expression	Displays the expression as it is created. This field is free-form which allows you to manually enter or edit information. This field reads Input Expression when creating an input or "read" expression. It reads Output Expression when creating an output or "write" expression.
Database field	This button is reserved for future enhancements.
Function	Select this button to display the Select function window which allows you to select the necessary function from those available.
Variable	Select this button to display the Select variable window which allows you to select the necessary variable from those available.
Operators	Select the applicable button to add the corresponding operator or operators to the expression.
Clear	Select this button to clear the Input/Output Expression field.
Validate	Select this button to validate the expression that appears in the Input/Output Expression field. If the expression is invalid, an error message is displayed. If the expression is valid, a message is displayed indicating there are no errors and also stating what the result is.
OK	Select this button to accept changes to (or the creation of) the expression.
Cancel	Select this button to discard changes to (or abandon the creation of) the expression.

Table 35 - Expression Wizard Options

Notes:

- The **Expression Wizard** appears and functions the same for an input expression as it does for an output expression. The differences being the expression field label: **Input Expression**, **Output Expression**, and that one is for reads and the other for writes.
- If you are expecting to read a particular alias, create an **Input Expression**. If you are expecting to write to a particular alias, create an **Output Expression**.

To create an Input or Output Expression:

1. On the **Configuration** window, select **Alias Configuration** or a previously configured **Alias Group**.
2. The **Contents** table for that **Alias Group** is displayed on the right side of the **Configuration** window (Figure 45), listing the aliases it contains.
3. Either create a new alias (for instructions, see **To insert a new alias**), or
Double-click your mouse on an existing alias, or
Right-click your mouse on an existing alias and select the **Edit Alias** option from the displayed menu.
4. The **Edit Alias** window appears.
5. Click on the **Scaling** button to enable scaling for the alias. The **Scaling Options** are displayed at the bottom of the **Insert New Alias** window (Figure 44) or the **Edit Alias** window.

Note: Whether the **Insert New Alias** window or the **Edit Alias** window is displayed depends on whether you are creating a new alias or editing an existing one.

6. Select the **Expression** tab (Figure 46).

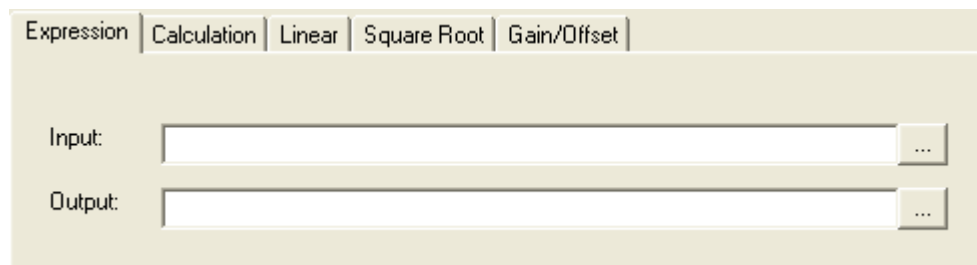


Figure 46 - Expression Tab

7. Click on the ellipsis button adjacent to the **Input** field (or **Output** field).
8. The **Expression Wizard** (Figure 47) is displayed.



Figure 47 - Expression Wizard

9. Manually enter your new expression in the **Input/Output Expression** field and proceed to step 14, or
 Perform steps 9 through 13 using a combination of the **Function**, **Variable**, and **Operators** buttons to create your expression, which will be displayed in the **Input/Output Expression** field as you build it.
10. Click on the **Function** button to go to the **Select function** (Figure 48) window. After selecting the required function, click on the **Continue** button to close the **Select function** window and return to the **Expression Wizard**.

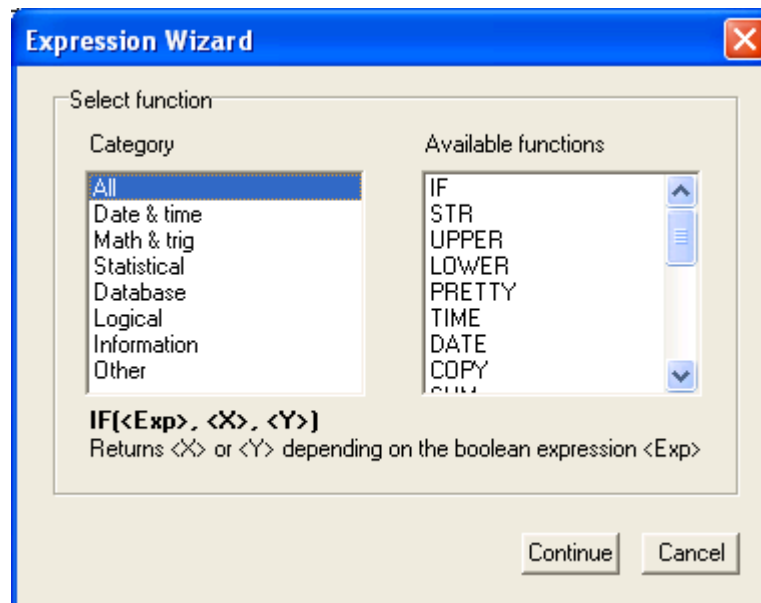


Figure 48 - Select Function Window

11. Click on the **Variable** button to go to the **Select variable** (Figure 49) window. After selecting the required variable, click on the **OK** button to close the **Select variable** window and return to the **Expression Wizard**.

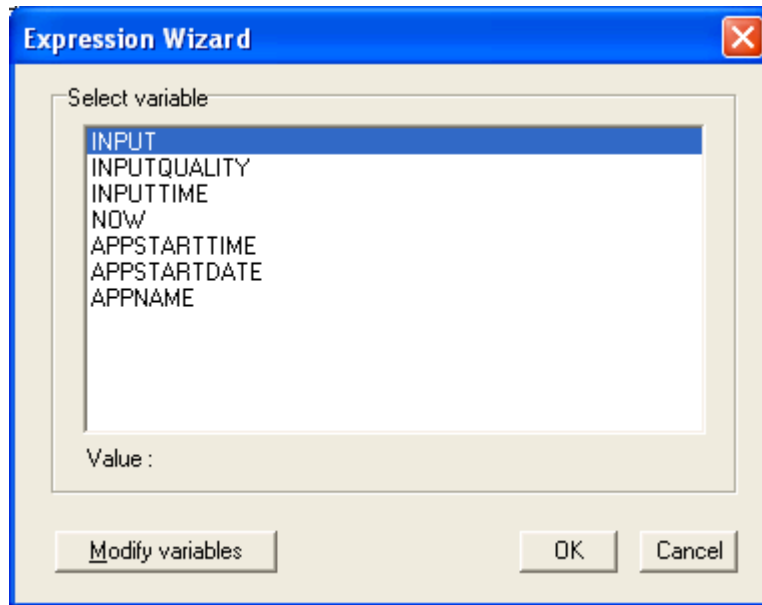


Figure 49 - Select Variable Window

12. If required, from the **Select variable** window, click on the **Modify variables** button to access the **User Defined Functions Editor** (Figure 50) which allows you to add, change, or delete variables.

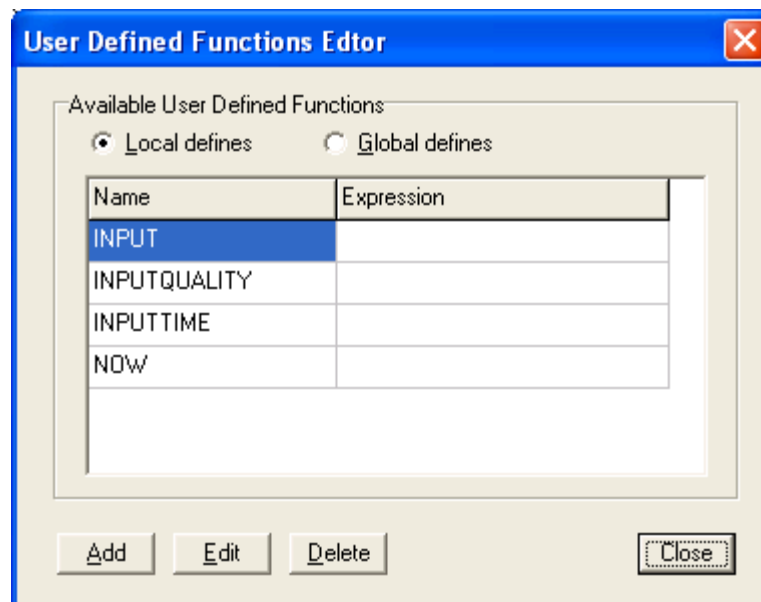


Figure 50 - User Defined Functions Editor

13. The **Operators** buttons (Figure 51) allow you to enter an operation descriptor based on the selected button.

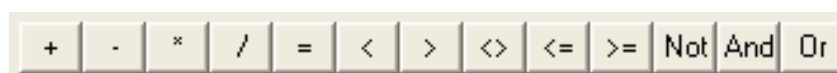


Figure 51 - Operators Buttons

14. Click on the **Validate** button to determine whether or not the expression is valid.

15. If the expression is valid (i.e., a confirmation message is displayed), click on the **OK** button to close the message window and return to the **Expression Wizard** screen.
16. Click on **OK** button on the **Expression Wizard** screen to close the wizard and display the expression in either the **Input** or **Output** field, depending on which expression you defined.
17. From either the **Insert New Alias** or **Edit Alias** window, click on the **Save** button.
18. The **Insert New Alias** or **Edit Alias** window closes and you are returned to the **Configuration** window.

Item Path Browser

The **Calculation** form of scaling uses the **Item Path Browser** to add item paths. The created formula is a simple text equation that is applied to either incoming values (i.e., reads), or outgoing values (i.e., writes).

Table 36 describes the **Item Path Browser** fields.

Component	Description
Branch Hierarchy	Displays the branch hierarchy of the OPC server when browsing actions are being performed. The +/- symbols can be used to display/hide the branches below the specified branch. Left-clicking a branch displays its leaves in the Leaf List component.
Leaf List	Displays the list of leaves belonging to a selected branch from the Branch Hierarchy . Left-clicking a leaf enables the OK button.
OK	Select this button to add the selected item from the Leaf List to the Input/Output component of the Insert New Alias form.
Cancel	Select this button to exit the Item Path Browser without adding any item paths.
Refresh	Select this button to refresh the browsing hierarchy in the Branch Hierarchy component.

Table 36 - Item Path Browser Options

Note: The **Item Path Browser** appears and functions the same for an input calculation as it does for an output calculation.

To create an Input or Output Calculation with item paths:

1. On the **Configuration** window, select **Alias Configuration** or a previously configured **Alias Group**.
2. The **Contents** table for that **Alias Group** is displayed on the right side of the **Configuration** window (Figure 45), listing the aliases it contains.
3. Either create a new alias (for instructions, see [To insert a new alias](#)), or
Double-click your mouse on an existing alias, or
Right-click your mouse on an existing alias and select the **Edit Alias** option from the displayed menu.
4. Click on the **Scaling** button to enable scaling for the alias. The **Scaling Options** are displayed at the bottom of the **Insert New Alias** window (Figure 44) or the **Edit Alias** window.

Note: Whether the **Insert New Alias** window or the **Edit Alias** window is displayed depends on whether you are creating a new alias or editing an existing one.

5. Select the **Calculation** tab (Figure 52).

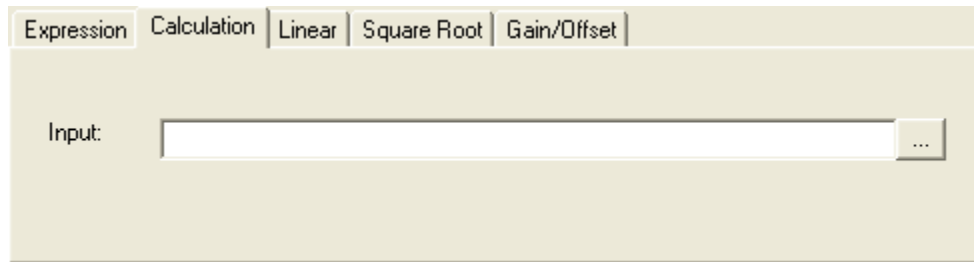


Figure 52 - Calculation Tab

6. Click on the ellipsis button adjacent to the **Input** field (or **Output** field).
7. The **Item Path Browser** (Figure 53) is displayed.

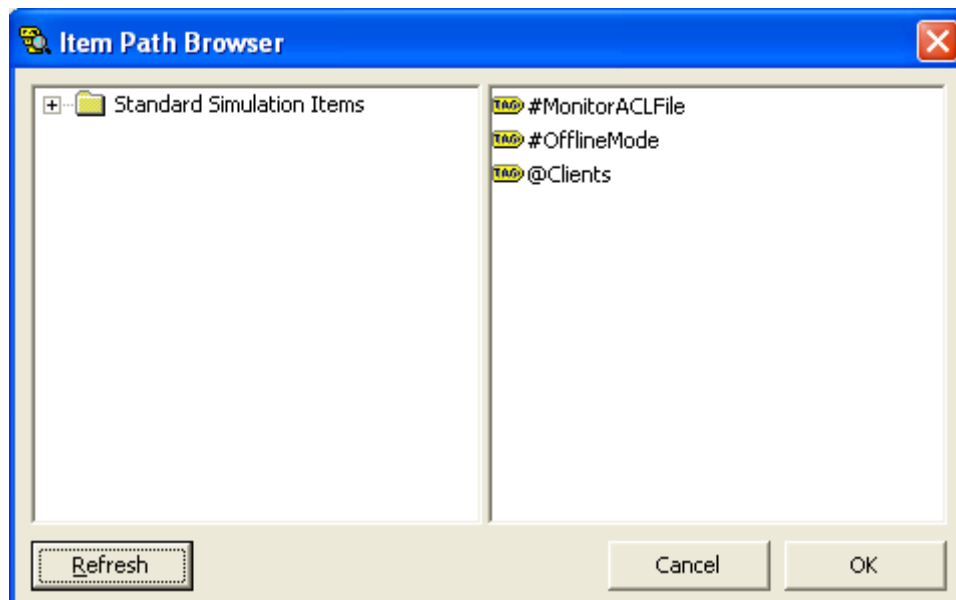


Figure 53 - Item Path Browser

8. Browse the **Branch Hierarchy** until you find the branch containing the leaf you are interested in.
9. Left-click your mouse on the leaf in the **Leaf List** and press the **OK** button. The item path is inserted (surrounded by square brackets) into the **Input/Output** component of the **Insert New Alias** form.
10. Edit the calculation in the Input/Output component until the syntax is finalized. Refer to Table 45 and Table 46 for more information on the calculation syntax.
11. Perform steps 9 through 11 for any additional item paths you wish to add to the calculation.
12. From either the **Insert New Alias** or **Edit Alias** window, click on the **Save** button.
13. The **Insert New Alias** or **Edit Alias** window closes and you are returned to the **Configuration** window.

Saving a Configuration

Note: When the server configuration is complete, use the **Save Configuration** window to save the configuration to an XML file.

To save a configuration to an XML file:

1. From the **File** menu, select the **Save As** menu option or click on the  button (alternatively, users can choose **Save** or click .
2. The **Save Configuration** window appears.
3. Enter a file name if saving the file for the first time.
4. Click **Save**.
5. The configuration is saved.

Clearing a Configuration

Note: Starting a new configuration will clear the existing one.

To clear a configuration:

1. From the **File** menu, choose the **New** menu option or click on the  button.
2. If OPC clients are still connected to the server, a warning message appears.
3. Click **OK**.
4. The configuration is cleared.

Loading an Existing Configuration

To load an existing configuration file:

1. From the **File** menu, select the **Open** menu option or click on the  button.
2. The **Open Configuration** window appears.
3. Browse for the configuration file that you want to load.
4. Click **Open**.
5. If OPC clients are still connected to the server, a warning message appears.

Notes:

- At this stage, the connection between the server and the client needs to be broken.
 - When the new configuration is completely loaded, the changes will take effect in the OPC client.
6. Click **OK**.
 7. The old configuration is cleared and the new configuration is loaded from the file.

Shutting Down the Server

To shut down the server:

1. On either the **Control Panel** or the **Tool Tray Menu**, select **Shutdown**. If the server is running as a local executable, choose **Shutdown Server** from the **File** menu or click on the  button.

2. If OPC clients are still connected to the server, a warning message appears.
3. Click **OK**.
4. The server is shut down.



Note: The shutdown command is not available for the server if it runs as a Windows service. Services can be shut down only from the **Service Control Manager** applet in the Windows **Control Panel**.

OPC Data Items

This section describes the OPC data items used in the MatrikonOPC Server for SCADA DNP3.

The MatrikonOPC Server for SCADA DNP3 supports **g.v.x** notation for addressing individual objects on a DNP3 unit. In addition, the server:

- tries to extract a valid object address from a given item ID.
- accepts any valid object group for **g** as a decimal value between **1** and **254**.
- accepts any valid object variation for **v** as a decimal value between **0** and **255**.
- accepts any index for **x** as a decimal value between **0** and **4,294,967,295 ($2^{32} - 1$)**. All objects that support this index will have an **x** as the last entry in the Object ID. The **x** must be replaced with a valid index number.
- requires at least the channel and unit names prefixed to the object address, each element separated by a period (e.g., **COM1.RTU1.30.0.1**), to differentiate between objects on different units and different communication channels.

When addressing individual DNP3 items the client has the option to include a text description with the item. By default all applicable items come with the basic text description.

Example, the following are all referencing the same item (analog input number one):

- **COM1.RTU1.AnalogInput 30.0.1**
- **COM1.RTU1.AnalogInputCycleHz 30.0.1**
- **COM1.RTU1.CycleHz 30.0.1**
- **COM1.RTU1.30.0.1**

A text description may be added/edited for any item where an Object ID is given. The description must come immediately after the period (.) separating the unit name from the object number. It may not contain any special characters including periods or spaces. The Description must end with a single space before the object number.

The MatrikonOPC Server for SCADA DNP3 accepts communication options specified in the access path for individual data items to allow users to customize communication for those items. Whether the server actually uses these options for data acquisition depends on the unit configuration settings.

The communication options listed in Table 37 are supported for device items. Changes to the options for an item may require the server to re-optimize the unit where the item is located.

Component	Description
+	Indicates that the server polls this item when communication is first established (or re-established) with the unit, even if its scan interval is greater than the threshold rate. These items are optimized separately from other items scheduled at the same scan interval.
interval	Scan interval (milliseconds) for the item. It overrides the update rate for the OPC group where the item is added. If the same item is requested several times at different scan intervals, then fastest one is used.
!	Indicates that the server polls the item at a high priority (honoring fastest scan rate). If the same item is requested several times, then the item is polled at high priority if any of the requested access paths contain this flag.

Component	Description
-	Indicates that the server does not poll this item. The server will retain this item and update its value if it receives it via some other poll method. (Cannot be used with above options.)

Table 37 - Communication Options for Device Items

Any combination of the communication options is valid provided it maintains the order initial poll, interval, priority. Alternatively, if the access path contains just a dash (-), then this indicates that the server does not poll the individual item (quiescent). Use this latter option when receiving unsolicited updates or some alternative form of polling.

The MatrikonOPC Server for SCADA DNP3 supplies the data items listed in the following sections, with the specified data type, read access (R), and write access (W), for each DNP3 unit.

Device Attributes

Device Attributes, listed in Table 38, provide configuration information about the DNP3 unit. Unlike other object types, variations represent different values, rather than different views of the same value. Devices may have more than one set of attributes, which are addressed through the index.

Each attribute is listed by its Item ID. By default, each attribute has a text description that may be modified or omitted by the client.

Example: **COM1.RTU1.DevAttrDeviceManuName 000.252.x**

Item ID	Data Type	R	W	Comments
0.211.x	VT_BSTR	✓		Identifier of support for user-specific attributes.
0.212.x	VT_UINT8	✓		Number of master-defined data set prototypes.
0.213.x	VT_UINT8	✓		Number of outstation-defined data set prototypes.
0.214.x	VT_UINT8	✓		Number of master-defined data sets.
0.215.x	VT_UINT8	✓		Number of outstation-defined data sets.
0.216.x	VT_UINT8	✓		Max number of binary outputs per request.
0.217.x	VT_UINT8	✓		Local timing accuracy.
0.218.x	VT_UINT8	✓		Duration of timing accuracy.
0.219.x	VT_INT8	✓		Support for analog output events.
0.220.x	VT_UINT8	✓		Max analog output index.
0.221.x	VT_UINT8	✓		Number of analog outputs.
0.222.x	VT_INT8	✓		Support for binary output events.
0.223.x	VT_UINT8	✓		Max binary output index.
0.224.x	VT_UINT8	✓		Number of binary outputs.
0.225.x	VT_INT8	✓		Support for frozen counter events.
0.226.x	VT_INT8	✓		Support for frozen counters.
0.227.x	VT_INT8	✓		Support for counter events.
0.228.x	VT_UINT8	✓		Max counter index.

Item ID	Data Type	R	W	Comments
0.229.x	VT_UINT8	✓		Number of counter points.
0.230.x	VT_INT8	✓		Support for frozen analog inputs.
0.231.x	VT_INT8	✓		Support for analog input events.
0.232.x	VT_UINT8	✓		Maximum analog input index.
0.233.x	VT_UINT8	✓		Number of analog input points.
0.234.x	VT_INT8	✓		Support for double-bit binary input events.
0.235.x	VT_UINT8	✓		Maximum double-bit binary input index.
0.236.x	VT_UINT8	✓		Number of double-bit binary input points.
0.237.x	VT_INT8	✓		Support for binary input events.
0.238.x	VT_UINT8	✓		Max binary input index.
0.239.x	VT_UINT8	✓		Number of binary input points.
0.240.x	VT_UINT8	✓		Max transmit fragment size.
0.241.x	VT_UINT8	✓		Max receive fragment size.
0.242.x	VT_BSTR	✓		Device manufacturer's software version.
0.243.x	VT_BSTR	✓		Device manufacturer's hardware version.
0.245.x	VT_BSTR	✓		User-assigned location name.
0.246.x	VT_BSTR	✓		User-assigned ID code/number.
0.247.x	VT_BSTR	✓		User-assigned device name.
0.248.x	VT_BSTR	✓		Device serial number.
0.249.x	VT_BSTR	✓		DNP subset and conformance.
0.250.x	VT_BSTR	✓		Device manufacturer's product name and model.
0.252.x	VT_BSTR	✓		Device manufacturer's name.
0.254.x	VT_EMPTY	✓		Non-specific all attributes request.
0.255.x	VT_BSTR	✓		List of attribute variations device supports.

Table 38 - Device Attributes

Static Objects

Static objects, listed in Table 39, represent the current state of inputs, measurements, and other information on the outstation. Each object may have an associated status value (**S**) and/or a timestamp (**T**) supplied by the outstation. Some items may have event history (**E**) and some items may be broadcast (**B**).

Each object is listed by its Item ID. By default each object has a text description that may be modified or omitted by the client.

Example: **COM1.RTU1.AnalogInput 30.0.x**

Item ID	Data Type	R	W	S	T	E	B	Comments
1.0.x	VT_BOOL	✓		✓		✓		Binary input.

Item ID	Data Type	R	W	S	T	E	B	Comments
								Binary input change events (2.0).
3.0.x	VT_UI1	✓		✓				Double bit binary values.
10.0.x	VT_BOOL	✓		✓				Binary output.
20.0.x	VT_UI4	✓	✓	✓		✓	✓	Counter. Counter change events (22.0). Write non-zero values to freeze or zero values to freeze and clear (DNP3 level 3).
21.0.x	VT_UI4	✓		✓	✓	✓		Frozen counter. Frozen counter events (23.0).
30.0.x	VT_R8	✓	✓	✓		✓	✓	Analog input. Analog change events (32.0). Write non-zero values to freeze or zero values to freeze and clear (DNP3 level 3).
31.0.x	VT_R8	✓		✓	✓	✓		Frozen analog input. Frozen analog events (33.0).
40.0.x	VT_R8	✓		✓			✓	Analog output status.
50.1	VT_DATE	✓	✓					Date and time (function 23). Write any value to perform time synchronization.
50.3	VT_DATE		✓					Last recorded date and time (function 24). Write any value to perform time synchronization.
80.1.x	VT_BOOL	✓	✓					Internal indication.
81.1.x	VT_ARRAY VT_UI1	✓						Storage object (3 elements).
101.1.x	VT_BSTR	✓						Small packed BCD (4 digits).
101.2.x	VT_BSTR	✓						Medium packed BCD (8 digits).
101.3.x	VT_BSTR	✓						Large packed BCD (16 digits).
102.1.x	VT_UI1	✓	✓					Byte.
110.0.x	VT_BSTR	✓				✓		String (maximum 255 characters). String events (111.0).

Table 39 - Static Objects



Note: Use the quiescent option (-) with indexed items when communicating with a level 1 or level 2 device. Use a poll option item to indicate the actual method of acquiring the data.

Output Objects

Output objects, listed in Table 40, provide a mechanism for controlling outputs on the outstation using the OPC write functionality. The current value for this type of item is the status of the last operation performed on that object. The server supports supervisory control using single-destination and broadcast commands.

Each object is listed by its Item ID. By default each object has a text description that may be modified or omitted by the client.

Example: **COM1.RTU1.BinaryOutput 010.0.x**

Item ID	Data Type	R	W	B	Comments
10.1.x	VT_BOOL		✓		Write binary output without status.
10.2.x	VT_UI1		✓		Write binary output with status.
12.1.x	VT_BSTR	✓	✓	✓	Control relay output block. Write an individual control code, or a string of up to four numbers (code ¹ , count, on time, off time). After a write is performed, the item repeats back the parameters sent, with an additional status code ² from the device (e.g., code, count, on time, off time, status).
12.2.x	VT_BSTR	✓	✓	✓	Pattern control block (DNP3 level 3). Write an individual control code, or a string of up to four numbers (code ¹ , count, on time, off time). Output guaranteed to be simultaneous.
40.1.x	VT_I4		✓		Write 32-bit analog output (online).
40.2.x	VT_I2		✓		Write 16-bit analog output (online).
40.3.x	VT_R4		✓		Write short floating-point analog output (online).
40.4.x	VT_R8		✓		Write long floating-point analog output (online).
41.1.x	VT_I4	✓	✓	✓	32-bit analog output block. Write an individual 32-bit value.
41.2.x	VT_I2	✓	✓	✓	16-bit analog output block. Write an individual 16-bit value.
41.3.x	VT_R4	✓	✓	✓	Short floating-point analog output block. Write an individual short floating-point value.
41.4.x	VT_R8	✓	✓	✓	Long floating-point analog output block. Write an individual long floating-point value.

Table 40 - Output Objects

¹ The operation codes are numeric and are defined by the DNP3 specification as follows:

- 0: NUL
- 1: PULSE_ON
- 2: PULSE_OFF
- 3: LATCH_ON
- 4: LATCH_OFF
- 5 to 15: Undefined

² The status codes are numeric and are defined by the DNP3 specification as follows:

- 0: SUCCESS
- 1: TIMEOUT

- 2: NO_SELECT
- 3: FORMAT_ERROR
- 4: NOT_SUPPORTED
- 5: ALREADY_ACTIVE
- 6: HARDWARE_ERROR
- 7: LOCAL
- 8: TOO_MANY_OBJS
- 9: NOT_AUTHORIZED
- 10: AUTOMATION_INHIBIT
- 11: PROCESSING_LIMITED
- 12: OUT_OF_RANGE
- 13 to 125: RESERVED
- 126: NON_PARTICIPATING
- 127: UNDEFINED

Poll Options

The items listed in Table 41 provide a means to control the polling method used by the server to acquire data for static objects. The current value for this type of item is meaningless, but simply referencing the item is enough to cause the server to use the specified polling technique.

Each object is listed by its Item ID. By default each object has a text description that may be modified or omitted by the client.

Example: **COM1.RTU1.BinaryInputAny 001.0**

Item ID	Data Type	R	W	Comments
1.0	VT_BOOL	✓		All binary inputs (any variation).
2.0	VT_EMPTY	✓		All binary input changes (any variation).
10.0	VT_BOOL	✓		All binary outputs (any variation).
20.0	VT_UI4	✓	✓	All counters (any variation). Write non-zero values to freeze or zero values to freeze and clear.
21.0	VT_UI4	✓		All frozen counters (any variation).
22.0	VT_EMPTY	✓		All counter change events (any variation).
23.0	VT_EMPTY	✓		All frozen counter events (any variation).
30.0	VT_R8	✓	✓	All analog inputs (any variation). Write non-zero values to freeze or zero values to freeze and clear.
31.0	VT_R8	✓		All frozen analog inputs (any variation).
32.0	VT_EMPTY	✓		All analog change events (any variation).
33.0	VT_EMPTY	✓		All frozen analog events (any variation).
40.0	VT_R8	✓		All analog output statuses (any variation).
60.1	VT_EMPTY	✓		All class 0 (static) data.

Item ID	Data Type	R	W	Comments
60.2	VT_EMPTY	✓		All class 1 (event) data.
60.3	VT_EMPTY	✓		All class 2 (event) data.
60.4	VT_EMPTY	✓		All class 3 (event) data.
111.0	VT_EMPTY	✓		All string events.

Table 41 - Poll Options

The MatrikonOPC Server for SCADA DNP3 supplies the communication configuration parameters listed in Table 42 for all DNP3 units.

Item ID	Description	Default
#OfflineMode	When true, the DNP3 Unit operates in offline mode. Refer to Appendix F – Offline Mode for more information.	False
master	DNP3 master station number (0-65535). Unit disconnects and reconnects if this parameter changes.	0
station	DNP3 slave station number (0-65535). Unit disconnects and reconnects if this parameter changes. Note that addresses 65520 through 65535 are reserved for broadcast operations.	next available
mode	Indicates how the unit behaves. 0 = DNP3 master 1 = DNP3 slave (not implemented) Unit disconnects and reconnects if this parameter changes.	0
basePollTime	Normalization time for scheduling polls, stored as UTC HH:MM:SS. Unit re-optimizes if this parameter changes.	00:00:00
timeBias	Minutes to add to a timestamp from the outstation to convert it to UTC.	0.0
ArmOutputs (Select before operate)	Indicates whether to arm outputs with the <i>select</i> command (function 3) before issuing an <i>operate</i> command (function 4) rather than just issuing a <i>direct operate</i> command (function 5) when controlling binary or analog outputs. 0 = direct operate 1 = select-then-operate 2 = rearm on select retry Arming outputs before operating enables the server to safely make a “best effort” to operate an output exactly once (using time-outs and retries) without the need for operator intervention.	0
synchronize	Indicates the type of time synchronization to perform automatically when IIN1-4 detected. 0 = no synchronization 1 = function 23 (serial) 2 = function 24 (network).	0
allowWrites	Allow/disallow output operations (functions 2 through 10) to unit.	TRUE
latchData	When true, items “freeze” at their last value/quality/timestamp rather than going to bad qualities	FALSE

Item ID	Description	Default
	when the unit is set off scan.	
logStatics	Enable/disable the logging of static objects received at high level.	FALSE
logEvents	Enable/disable the logging of event objects received at high level.	FALSE
interMessageDelay	Minimum amount of time (milliseconds) between the last request/response to/from this unit and the next request to this same unit.	0
replyTimeout	Maximum amount of time (milliseconds) to wait for the response to an application function.	5000
retries	Maximum number of times to resend a request and wait for a response before concluding that communication has failed with the unit.	3
reconnectDelay	Minimum amount of time (milliseconds) to wait before attempting to reconnect after communication has failed with a unit.	30000
reconnectRetries	Maximum number of times to resend a request and wait for a response when trying to reconnect after communication has failed with a unit.	0
maxInterrogate	Maximum amount of time (seconds) to allow a unit to be interrogated. A value of zero indicates that interrogation must be halted manually.	0
restartDelay	Minimum amount of time (milliseconds) to wait following a cold/warm restart before resuming communication with the unit.	0
dataLink	Indicates how often to request confirmation for FT3 frames. 0 = never 1 = multi-frame messages only 2 = always This option has no effect on broadcast units.	0
application	Indicates how often to request confirmation for application fragments. 0 = messages containing event data only 2 = multi-fragment messages only 3 = always This option has no effect on broadcast units. Fragment confirmation should only be used for units emulating slave devices.	0
maxOutputs	Maximum number of objects (values, control blocks, pattern masks) per output operation. 0 = no limit	0
maxEvents	Maximum number of objects (quantity) per event poll (class 1/2/3 or type). Unit re-optimizes if this parameter changes. 0 = no limit	0

Item ID	Description	Default
fragment	Maximum number of bytes in an application fragment. Unit re-optimizes if this parameter changes.	2048
unsolicited1 unsolicited2 unsolicited3	Enable/disable unsolicited updates for Class 1, 2, or 3 data. The server reissues the ENABLE command whenever it receives IIN1-7 (device restart), and issues DISABLE and ENABLE commands as these settings change.	FALSE FALSE FALSE

Table 42 - DNP3 Unit Communication Configuration Parameters

Getting Data without Being Connected to a Device

The MatrikonOPC Server Framework supports “offline mode”, which allows OPC clients to obtain changing good quality data without being connected to a device. This is useful if you wish to test an HMI or other OPC client without worrying about the connection to the device, or the quality of the data provided. For more information, refer to **Appendix F - Offline Mode**.

Diagnostics

The server supplies diagnostic information to assist operators and support personnel with troubleshooting communication problems and software faults.

Logging

All MatrikonOPC servers produce log files that record errors and debugging information. The log files can be extremely valuable for troubleshooting. As such, it is important to note that the default log level is set to low. The **General Logging** tab of the **Options** dialogue in the main configuration window contains settings to control server logging.

General Activity Logging records information about the internal workings of the OPC server. It is useful for troubleshooting problems with configuration and device communication. Interface Activity Logging records information about the client/server OPC communication. It is useful for troubleshooting compliance issues.

For General logging, the higher the log level, the more information that is recorded. However, server performance may decrease at higher log levels. The recommended operating level is **Medium**. More log levels are available for both types of logging which record more detailed information, as well as the ability to output log statements to a console window at run time. Contact **MatrikonOPC Support** for further instructions on how to enable the higher log levels and console logging.

For Interface logging, the log level can be considered very high and therefore should never be used during normal operation of the OPC server unless specifically working on problems related to interfacing.

MatrikonOPC Sniffer is a useful tool for logging OPC client/server communication. It enhances the Interface Activity Logging by recording the client-side transactions. It can also be used with other OPC servers. MatrikonOPC Sniffer is a utility used to troubleshoot OPC client/server interoperability issues. Contact the MatrikonOPC Sales department for further information about this product, or use the following link to access the **Matrikon Sniffer Download**.

In general, the server logs all errors and other information of immediate importance to the user at the low detail level, all warnings and other information of moderate importance to the user at a medium detail level, and additional information concerning the normal functioning of the software at a high detail level. The server also logs further information of concern to support personnel at the debug log level.



Note: The higher the log level, the slower the performance of the server. It is recommended that the log level be left at the default, unless troubleshooting needs to be performed.

DNP Implementation

For more information on DNP, view the documents listed below (as well as others) at <http://www.dnp.org>.

- *DNP V3.00 Data Link Layer 0.02*
- *DNP V3.00 Transport Functions 0.01*
- *DNP V3.00 Application Layer 0.03*
- *DNP V3.00 Data Object Library 0.02*
- *DNP V3.00 Subset Definitions 2.00*
- *Transporting DNP V3.00 over Local and Wide Area Networks 1.0*
- *DNP V3.00 Technical Bulletins (1997 through 2000)*
- *DNP3-2001 IED Certification Procedure*

The MatrikonOPC Server for SCADA DNP3 User's Manual conforms to level 3 of the **DNP V3.00** specification as a master. However, the server accommodates slave devices that support levels 1 and 2 as well. The server fully implements the data link, transport, and application layers of the DNP protocol as outlined in the subset definitions for level 3.

Subset Level 3

The MatrikonOPC Server for SCADA DNP3 User's Manual supports the following application commands as a master.

- Function 1 Read
- Function 2 Write
- Functions 3 and 4 Select and Operate
- Functions 5 and 6 Direct Operate (with and without acknowledgement)
- Functions 7 and 8 Immediate Freeze (with and without acknowledgement)
- Functions 9 and 10 Freeze and Clear (with and without acknowledgement)
- Functions 13/14 Cold/Warm Restart
- Function 20/21 Enable/Disable Unsolicited Messages
- Function 23/24 Delay Measurement/Record Current Time (for time synchronization)

The server supports broadcast to (hexadecimal) station addresses `FFFF`, `FFFE`, and `FFFD` for functions 6, 8, and 10 (no request for confirmation).

The server implements the data objects, variations (VA), function codes (FC), and range qualifiers (Q) listed in Table 43 to comply with the level 1, level 2, and level 3 DNP subset requirements and support common vendor extensions.

Data Object	Request			Response			Operation
	FC	VA	Q (hex)	FC	VA	Q (hex)	
0	1	211-250, 252, 254, 255	00 ³ 01 ³ 02 ⁺ 06	129	211-250, 252, 254, 255	00 01 02	Read Device Attributes.
1	1	0	00 ³ 01 ³ 02 ⁺ 06	129	1, 2	00 01 02	Read binary inputs.
	—	—	—	130	1, 2	00 01 02	Unsolicited update for binary inputs.
2	1	0	06 07 ² 08 ² 09 ⁺	129	1-3	17 28 39	Read binary input changes.
	—	—	—	130	1-3	17 28 39	Unsolicited update for binary input changes.
3	1	0,1,2	06 07 ² 08 ² 09 ⁺	129	0-2	17 28 39	Double Bit Binary Inputs.
10	1	0	00 ³ 01 ³ 02 ⁺ 06	129	1, 2	00 01 02	Read binary outputs.
	2	1 ⁺ , 2 ⁺	00 01 02	129			Write binary outputs (deprecated).
	—	—	—	130	1, 2	00 01 02	Unsolicited update for binary outputs.
12	3 4	1	17 28 39 ⁺	129	1	17 28 39	Select then operate control relay output blocks.
	3 4	2 ⁺ , 3 ⁺	00 01 02 07(R=1)	129	2, 3	00 01 02 07(R=1)	Select then operate pattern control blocks and pattern masks.
	5	1	17 28 39 ⁺	129	1	17 28 39	Directly operate output blocks. Echo request.
	6	1	17 28 39 ⁺				Directly operate output blocks. No response.
	5	2 ³ , 3 ³	00 01 02 07(R=1)	129	2, 3	00 01 02 07 (R=1)	Directly operate pattern control blocks and pattern masks. Echo request.
	6	2 ³ , 3 ³	00 01 02 07(R=1)				Directly operate pattern control blocks and pattern masks. No response.
20	1 ²	0	00 ³ 01 ³ 02 ⁺ 06	129	1-8	00 01 02	Read counters.
	7 ² 9 ⁺	0	00 ³ 01 ³ 02 ⁺ 06	129			Immediate freeze or freeze and clear counters.

Data Object	Request			Response			Operation
	FC	VA	Q (hex)	FC	VA	Q (hex)	
	8 ² 10 ⁺	0	00 ³ 01 ³ 02 ⁺ 06				Immediate freeze or freeze and clear counters. No response.
	—	—	—	130	1-8	00 01 02	Unsolicited update for counters.
21	1 ²	0	00 ³ 01 ³ 02 ⁺ 06	129	1-12	00 01 02	Read frozen counters.
	—	—	—	130	1-12	00 01 02	Unsolicited update for frozen counters.
22	1 ²	0	06 07 08 09 ⁺	129	1-8	17 28 39	Read counter change events.
	—	—	—	130	1-8	17 28 39	Unsolicited update for counter change events.
23	1 ³	0	06 07 08 09 ⁺	129	1-8	17 28 39	Read frozen counter events.
	—	—	—	130	1-8	17 28 39	Unsolicited update for frozen counter events.
30	1 ²	0	00 ³ 01 ³ 02 ⁺ 06	129	1-6	00 01 02	Read analog inputs.
	7 ⁺ 9 ⁺	0	00 01 02 06	129			Immediate freeze or freeze and clear analog inputs.
	8 ⁺ 10 ⁺	0	00 01 02 06				Immediate freeze or freeze and clear analog inputs. No response.
	—	—	—	130	1-6	00 01 02	Unsolicited update for analog inputs.
31	1 ⁺	0	00 01 02 06	129	1-8	00 01 02	Read frozen analog inputs.
	—	—	—	130	1-8	00 01 02	Unsolicited update for frozen analog inputs.
32	1 ²	0	06 07 08 09 ⁺	129	1-8	17 28 39	Read analog change events.
	—	—	—	130	1-8	17 28 39	Unsolicited update for analog change events.
33	1 ⁺	0	06 07 08 09	129	1-8	17 28 39	Read frozen analog events.
	—	—	—	130	1-8	17 28 39	Unsolicited update for frozen analog events.
34	1 ⁺	1-3	00 01 02 06	129	1-3	00 01 02	Read analog input reporting dead-bands.

Data Object	Request			Response			Operation
	FC	VA	Q (hex)	FC	VA	Q (hex)	
40	1	0	00 ³ 01 ³ 02 ⁺ 06	129	1-4	00 01 02	Read analog output statuses.
	2 ⁺	1-4	00 01 02	129			Write analog output statuses (deprecated).
	—	—	—	130	1-4	00 01 02	Unsolicited update for analog output statuses.
41	3 4	1 ³ , 2 3 ⁺ , 4 ⁺	17 28 39 ⁺	129	1-4	17 28 39	Select then operate analog outputs.
	5	1 ³ , 2 3 ⁺ , 4 ⁺	17 28 39 ⁺	129	1-4	17 28 39	Directly operate analog outputs. Echo request.
	6	1 ³ , 2 3 ⁺ , 4 ⁺	17 28 39 ⁺				Directly operate analog outputs. No response.
50	1	1 ³	07(R=1)	129	1	07(R=1)	Read time and date.
	2	1, 3 ⁺	07(R=1)	129			Write time and date (time synchronization).
51	—	—	—	129 130	1, 2	07(R=1)	Common absolute time of occurrence (possibly unsynchronized) for relative time references.
52	13 14 ⁺ 23			129	1, 2	07(R=1)	Time delay (seconds or milliseconds) to wait after issuing the restart command or the calculated delay measurement.
60	1	1	06	129			Read all class 0 (static) data objects.
	1	2-4	06 07 08 09 ⁺	129			Read class 1, 2, or 3 (event) data objects.
	20 ³ 21 ³	2-4	06	129			Enable/disable spontaneous messages for class 1, 2, or 3 event data objects.
80	1 ³	1	00 01 02 ⁺	129	1	00 01 02	Read internal indications.
	2	1	00 01 ⁺ 02 ⁺	129			Write internal indications.
81	1 ⁺	1	00 01 02	129	1	00 01 02	Read storage objects.
101	1 ⁺	1-3	00 01 02	129	1-3	00 01 02	Read packed BCD values.
102	1 ⁺	1	00 01 02	129	1	00 01 02	Read bytes.
	2 ⁺	1	00 01 02	129			Write bytes.

Data Object	Request			Response			Operation
	FC	VA	Q (hex)	FC	VA	Q (hex)	
110	1 ⁺	0	00 01 02	129	N	00 01 02	Read byte strings of length N.
111	1 ⁺	0	06 07 08 09	129	N	17 28 39	Read string events of length N.
	—	—	—	130	N	17 28 39	Unsolicited update for string events of length N.

Table 43 - Implemented Data Objects, Variations, Function Codes, and Range Qualifiers

² The specified function/object/variation/qualifier combination requires a DNP level 2 device.

³ The specified function/object/variation/qualifier combination requires a DNP level 3 device.

⁺ The specified function/object/variation/qualifier combination requires an extended DNP device.

Additionally, the server parses range qualifiers 18, 19, 27, 29, 37, 38, 40, 41, 42, 50, 51, 52, 60, 61, and 62 (hexadecimal) if they occur in a *slave* response.

Note: Not all DNP units support the same data objects, variations, function codes, or range qualifiers.

The server records the internal indication bits received with each response from an outstation in the item cache for the 80.1.x objects. The server clears 80.1.7 (restart) with a write command (function 2) as soon as it receives this notification. The server continues to poll class 1/2/3 data (function 1) while 80.1.1/2/3 are set in order to completely empty the buffers.

Limitations

MatrikonOPC Server for SCADA DNP3 has the following limitations:

1. The MatrikonOPC Server for SCADA DNP3 User's Manual does not support the DNP data link function 1 (**Reset User Process**). This function is deprecated.
2. The server does not support explicit polling for specific (non-zero) variations of data objects that support variation zero at this time.
3. The server does not support DNP device application commands at this time. The specific functions and data objects not supported are as follows.
 - Function 16 Initialize Application
 - Function 17 Start Application
 - Function 18 Stop Application
 - Function 19 Save Configuration
 - Object 90 Variation 1 Application Identifier
4. The server does not support DNP file commands at this time. The specific functions, range qualifiers, and data objects not supported are as follows.
 - Functions 25 and 26 Open and Close
 - Function 27 Delete
 - Function 28 Get File Information
 - Function 29 Authenticate
 - Function 30 Abort
 - Qualifiers 1B, 2B, 3B, 4B, 5B, and 6B (hexadecimal) Free-format
 - Object 70 Variation 1 File Identifier (deprecated)
 - Object 70 Variation 2 Authentication
 - Object 70 Variation 3 File Command
 - Object 70 Variation 4 File Command Status
 - Object 70 Variation 5 File Transport
 - Object 70 Variation 6 File Transport Status
5. The server does not support the following DNP application functions at this time.
 - Functions 11 and 12 Freeze with Time (with and without acknowledgement)
 - Function 15 Initialize Data (reset object to initial or default settings)
6. The server does not support the DNP application function 22 (**Assign Classes**) at this time. Although this functionality is technically required for DNP Level 3 compliance, it is not generally used.
7. The server does not support the following DNP data objects at this time.
 - Object 50 Variation 2 Time and Date with Interval
 - Object 82 Variation 1 Device Profile
 - Object 83 Variation 1 Private Registration Object

- Object 83 Variation 2 Private Registration Object Descriptor
 - Object 100 Variation 1 Short Floating Point
 - Object 100 Variation 2 Long Floating Point
 - Object 100 Variation 3 Extended Floating Point
 - Object 112 Virtual Terminal Output Block
 - Object 113 Virtual Terminate Event Data
8. The server does not support the following DNP range qualifiers (hexadecimal) for virtual addressing. Virtual addressing is normally used only for diagnostic or manufacturing tests, as intimate knowledge of the outstation is required to properly interpret the response.
- Qualifiers 03, 04, and 05 one/two/four-byte start and stop addresses in range field
9. Qualifiers 43, 54, and 65 one/two/four-byte start and stop addresses in range field and each object prefixed with one/two/four-byte object size.
10. If a DNP device is being used with the MatrikonOPC Server for SCADA DNP3 where all the configured points have the access path option '\-', and data is expected to arrive through purely unsolicited means, the device automatically disconnects and no data is received. This is caused by the SCADA framework attempting to economise on data traffic by disconnecting from a device with no active communications. **Workaround:** Subscribe to at least one static point on the device with a large OPC Update rate. This keeps the device connected and listening for unsolicited communications without constantly communicating with the device.
11. The MatrikonOPC Server for SCADA DNP3 does not support DNP over UDP as specified by section 4.3.2 of the ***DNP3 Specification, Volume 7: IP Networking***. The UDP option for the Network Channel Device Link cannot be used to communicate in this way. The UDP option, is intended to support communication to a DNP3 device over a serial line with a UDP to serial converter.

Refer to the *MatrikonOPC Server for SCADA DNP3 Release Notes* for known issues.

Troubleshooting

The following section addresses some of the most common problems encountered, and questions asked, while using this OPC server. Please check the following **Problems and Solutions** before contacting the MatrikonOPC Support team.

Problems and Solutions

Server stops updating client with item values after two hours

Problem:	The server stops updating the client with item values after two hours.
Solution:	The server may be licensed with a hardware key and the hardware key may not be properly detected. Alternatively, try running the MatrikonOPC Licensing utility from the shortcut menu. Click on the Check Licenses button to see the status of all MatrikonOPC product licenses. Then, run the HINSTALL program that is located in the Program Files\Common Files\MatrikonOPC\Common directory.

Server stops updating client with item values after 30 days

Problem:	The server stops updating the client with item values after 30 days.
Solution:	The evaluation period for the license has expired. Contact the MatrikonOPC Support team.

Server shuts down after five minutes when no clients connected

Problem:	The server automatically shuts down after five minutes when there are no clients connected.
Solution:	This is standard behavior for COM servers. However, this behavior can be overridden as shown in the following example:  Note: Microsoft highly recommends that you back up the registry before editing it or making changes to it. 1. From the Run command, enter REGEDIT. 2. The Registry Editor (Figure 54) is launched. 3. In the Registry Editor, under HKEY_CLASSES_ROOT, look for the required program ID (e.g., <i>Matrikon.OPC.Simulation.1</i>).

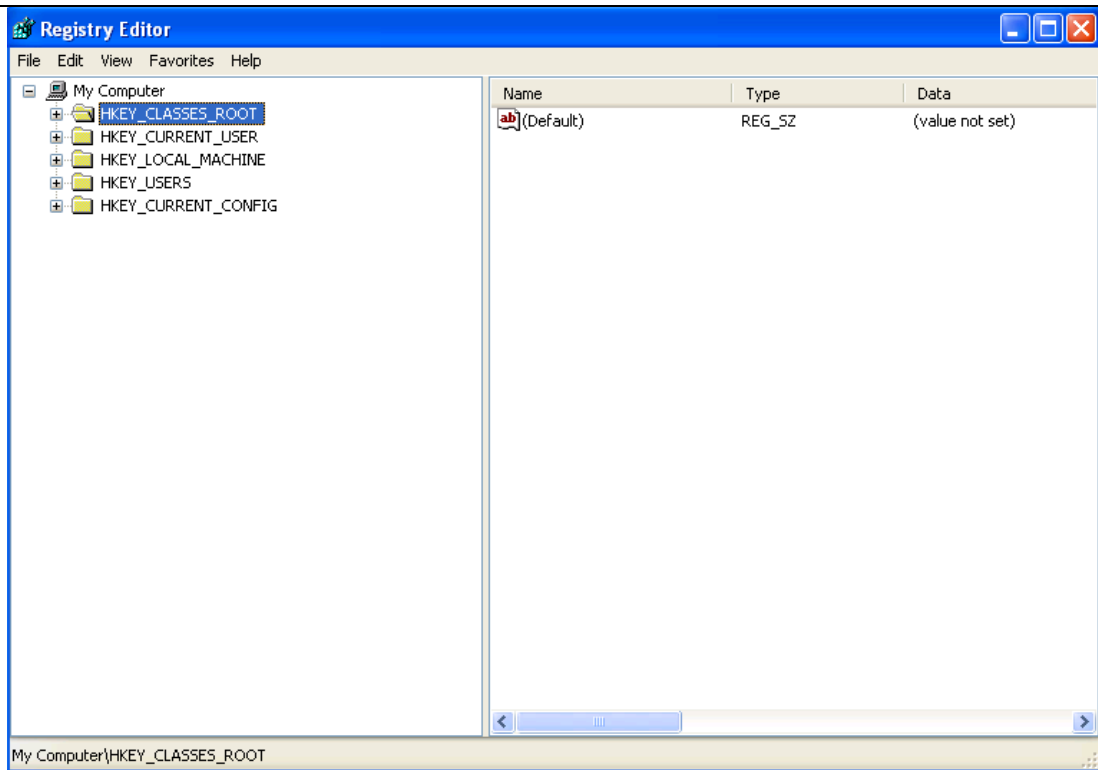


Figure 54 - Registry Editor

4. Expand the program ID branch.
5. Click on the CLSID branch.
6. Record the global universal ID (GUID).

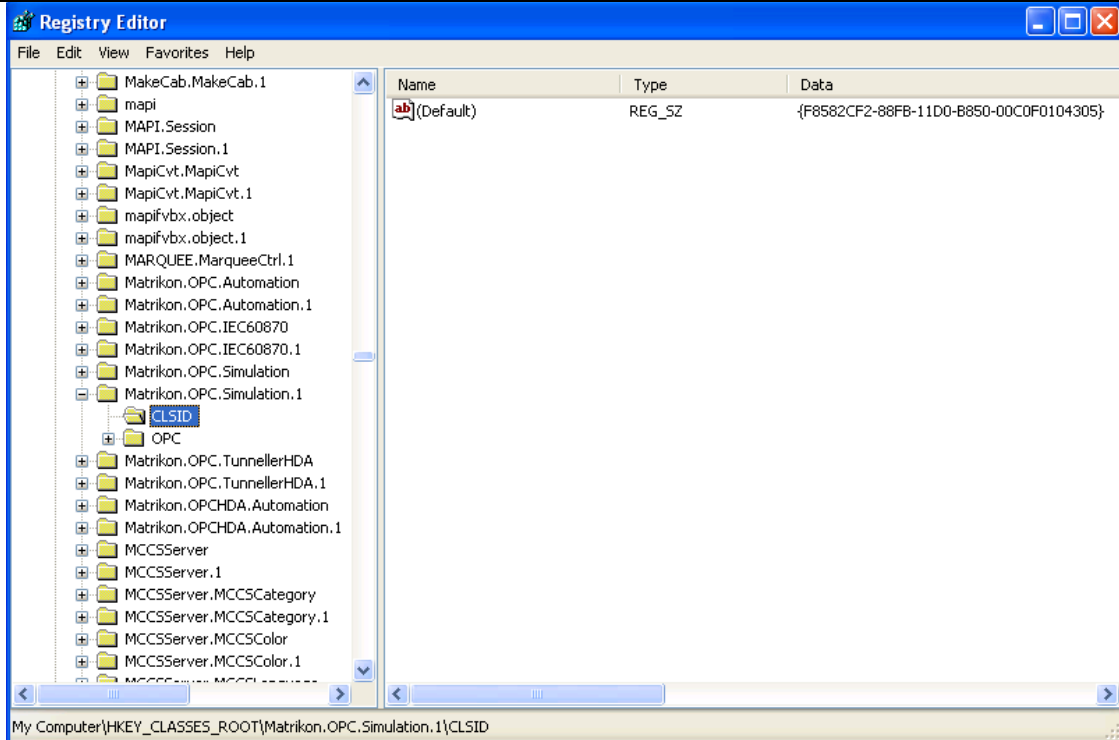


Figure 55 - Program ID Branch

7. Under the **HKEY_CLASSES_ROOT\CLSID** branch, search for the GUID retrieved in the previous step (e.g., **HKEY_CLASSES_ROOT\CLSID\{024C7FFC-9CC3-476f-867A-BC3CAD79F4FE}**).
8. Create a string value called **LockServer** in the Options branch underneath the GUID (e.g., **HKEY_CLASSES_ROOT\CLSID\{024C7FFC-9CC3-476f-867A-BC3CAD79F4FE}\Options**).
9. Create a new value using the context menu and choose **New String Value** from the menu.
10. Set the value of the **LockServer** entry to **1**.
Note: To edit the value, select the entry and select the **Modify** menu option from the **Edit** menu.
11. Shut down the server and restart it for the change to take effect.

Cannot configure client access paths, so cannot configure item options

Problem: The OPC client does not provide a means to configure access paths, making it difficult to correctly specify the data acquisition options for the items.

Solution: The server provides a global parameter for configuring an escape character, to allow users to append communication options to the end of an item ID which would accommodate clients that do not support access paths.

Perform the following steps as shown (with example) below:



Note: Microsoft highly recommends that you back up the registry before editing it or making changes to it.

1. From the **Run** command, enter **REGEDIT**.
2. The **Registry Editor** is launched.
3. In the **Registry Editor**, under **HKEY_CLASSES_ROOT**, look for the required program ID (e.g., Matrikon.OPC.Simulation.1).
4. Expand the program ID branch.
5. Click on the CLSID branch.
6. Record the global universal ID (GUID).
7. Under the **HKEY_CLASSES_ROOT\CLSID** branch, search for the GUID retrieved in the previous step (e.g., **HKEY_CLASSES_ROOT\CLSID\{024C7FFC-9CC3-476f-867A-BC3CAD79F4FE}**).
8. Create a string value called **ItemIDEscapeCharacter** in the Options branch underneath the GUID (e.g., **HKEY_CLASSES_ROOT\CLSID\{024C7FFC-9CC3-476f-867A-BC3CAD79F4FE}\Options**).
Note: To create a new value, use the context menu and select the **New String Value** menu option.
9. Set the value of **ItemIDEscapeCharacter** to a single character, such as "|" (pipe).
Note: To edit the value, select the entry and select the **Modify** menu option from the **Edit** menu.
10. Shut down the server and restart it for the change to take effect.
11. Configure the **ItemIDEscapeCharacter Item ID** in the OPC client with the access path appended to the end with the configured escape character (e.g., **ITEMID|ACCESSPATH**).

More than one HASP attached to parallel port, but only first one is recognized

Problem:	There is more than one HASP hardware key from Matrikon attached to the parallel port, but the software recognizes only the first one.
Solution:	HASP keys from the same vendor cannot be chained together. Send an email to the MatrikonOPC Support team to obtain a HASP key containing the combined codes of all installed MatrikonOPC Servers.

Server cannot be configured; no MatrikonOPC logo in Tool Tray

Problem:	The server cannot be configured because there is no MatrikonOPC logo  in the Tool Tray .
Solution:	If the Server is running as a service, the MatrikonOPC logo  does not appear in the Tool Tray . To configure the server, start the configuration utility by using the shortcut to the OPC

server in the Windows **Start** menu (this shortcut starts the **Configuration** utility as well as the OPC Server).



Note: If the server configuration utility generates an “access denied” error on launch, the DCOM permissions have not been configured properly.

OPC client unable to create or read items under configured object (device)

Problem: The OPC client is unable to create or read items under a configured object or device.

Solution: Check the object configuration. Ensure that the **Enabled** checkbox is selected, and verify the access credentials are correct (e.g., **Username**, **Password**).

Server does not retain settings

Problem: The server does not retain its previous settings and needs to be reconfigured each time it starts up.

Solution: In the **Configuration** window, choose **Options** from the **View** menu. Under the **General** tab, ensure that the **Load configuration on start-up** checkbox is selected and that the correct file name appears in the edit box (see **General Options**).

Server cannot save configuration in XML

Problem: The OPC server cannot save the configuration in XML format.

Solution: Microsoft Internet Explorer 4.01 (or later) must be installed to use the XML format.

Server does not show up in the list of locally available program IDs in OPC client application

Problem: The server does not show up in a list of locally available program IDs in the OPC client application.

Solution: Make sure that a user with local administrative rights installs the OPC server so that it can create the necessary entries in the registry.

Ensure OPCEnum is registered as a service, DCOM permissions are configured properly, and the OPCEnum service is running.

Also, especially for older OPC clients that do not use the OPC server browser, make sure the client is running as a user that has *read* access to the registry.

Server does not show up as a program ID in a remote OPC client application

Problem: The server does not show up in a list of available program IDs in the OPC client application on a remote machine.

Solution: Follow the steps found in **DCOM Manual** to copy the program ID from the server machine to the OPC client machine.

Access denies or time-out error when connecting to remote server via DCOM

Problem:	Access Denied error message appears, or time out occurs when trying to connect to a remote OPC server via DCOM.
Solution:	Ensure that the access and launch permissions for the OPC server are set correctly on the server machine. For more information, refer to the DCOM Manual .

Server does not start up or client cannot connect

Problem:	A client tries to connect to the server and fails, or the server does not start up.
Solution:	Ensure that the access and launch permissions for the OPC server are set correctly. For more information, refer to the DCOM Manual .

About screen and Configuration window do not show up

Problem:	The About screen and Configuration window do not show up when a remotely-connected client, or a client that runs as an NT service (such as Aspen Technologies CIMIO OPC Manager) tries to launch the OPC server.
Solution:	Either set the identity for the OPC server to the interactive user, or else consider running the server as an NT service. For more information, refer to the DCOM Manual .

DA 2.0 asynchronous I/O does not work

Problem:	After installing an older OPC server, DA 2.0 asynchronous I/O no longer works.
Solution:	The old installation program installed and registered its own (older) version of the OPC proxy/stub DLL. Reinstall the standard OPC proxy/stub DLLs, using an up-to-date installation program or re-register them using the REGSVR32 command-line utility (refer to the OPC Compliance - Installation section in this manual).

Trouble communicating through a Network

Problem:	Problems communicating to the Modbus device through a network.
Solution:	Make sure users can ping the device. Use Start -> Run with command, CMD, to bring up a command window. Enter the following: <pre> Ping ipaddress (e.g. C:\temp>ping 127.0.0.1 Pinging 127.0.0.1 with 32 bytes of data: Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Reply from 127.0.0.1: bytes=32 time<10ms TTL=128 Ping statistics for 127.0.0.1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), </pre>

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms)

Where **ipaddress** is the IP address of the user's machine. If it says "no response", then there are likely network issues between the user's machine and the remote machine.

Note: Refer to the **DCOM Manual** to further diagnose DCOM issues.

Can I connect it to my computer's serial ports?

Problem: I don't have any familiarity with RS-485/RS-422. Is it similar to RS-232? How can my computer "talk" to an RS-485/RS-422 device? Can I connect it to my computer's serial ports?

Solution: Computers come standard with RS-232 serial ports. RS-485 serial ports must either be specially purchased, or an RS-232/RS-485 converter must be purchased.

RS-485 and RS-422 allow you to serially chain all of the devices to a single communications port. The devices then take turns on the communication port. This allows reduced cost due to having to provide only a single communication port. This also results in reduced bandwidth since the total bandwidth provided to all devices cannot exceed the bandwidth of the communications port.

How can OPC data be accessed through other applications?

Problem: How can I access OPC data in *Microsoft Excel*, *Microsoft Word*, or another application with support for *Visual Basic*, *VBA*, or *VB Script*?

Solution: Use the MatrikonOPC **Automation Component** to create a *Visual Basic* script that connects to a server, creates groups and items, and receives data change updates. Contact MatrikonOPC Support for examples of how to do this in *Excel*, *Visual Basic*, or in an *HTML* document.

Minimizing communications to the devices

Problem: I wish to minimize communications with my device.

Solution: Consider which items change frequently and which do not. Having your OPC client or clients read different items at different rates (different OPC group update frequency) can result in reduced communications.

If some items are not needed for a considerable period, consider having your OPC client either remove them or disable/deactivate them. MatrikonOPC Modbus will not scan items unless they are actively demanded by at least one OPC client.

Trouble scheduling poll cycles

Problem: I need more options to schedule my polls at specific times or better manage the fairness of data access among devices.

Solution: MatrikonOPC Server for SCADA DNP3 allows significantly more configuration options and is preferable in SCADA environments.

Noisy communications

Problem:	I am having interference problems when communicating with my SCADA devices.
Solution:	MatrikonOPC Modbus has some head and tail squall squelch capabilities. However, you may consider using MatrikonOPC Server for SCADA DNP3 for enhanced features.

Reads and writes time out

Problem:	My device does not seem to wish to communicate. All of my reads and writes time out.
Solution:	Check your configuration to make sure it matches the configuration of your Modbus device. In particular, make sure that the data/parity/stop settings match (serial), make sure you are using the correct node number or numbers, and make sure you have the correct IP address and port number (Ethernet Modbus). If your device is a Daniel (32-bit) device supporting Modbus-like protocol, you will need to use the 3W and 4W registers because this device will send and receive twice as much data per register as a normal Modbus device.

Serial and TCP connections

Problem:	Serial Device links do not work as fast as TCP Device links
Solution:	Serial communications are much slower than TCP communications. As the number of items increase, The time it will take to update all items will increase as well

Using the 3W and 4W registers, or the 3 and 4 registers

Problem:	Should I be using the 3W and 4W registers, or the 3 and 4 registers?
Solution:	The difference between the 3W and 4W registers is the assumption as to the width of one register point. For example, in standard Modbus devices, register 4:1 will send and receive 16 bits of data. Daniel devices using a variant of the Modbus protocol (also called Daniel Modbus) use 32-bit registers, and send and receive 32 bits for each register requested or sent. The actual protocol is different, and they are mutually incompatible. A standard Modbus device will not correctly accept data fed to it using the 3W and 4W registers, and a Daniel Modbus device will not correctly accept data fed to it using the 3 and 4 registers. Your Modbus device <i>User's Manual</i> should indicate whether the device registers are standard (16-bit) or Daniel (32-bit). Generally, if one type does not work, try the other.

Removing the server as a service

Problem:	How do I remove the OPC server as a service?
Solution:	Re-register the OPC server executable using the /REGSERVER command-line switch.

Starting the server manually when installed as a service

Problem: Does the server need to be started manually when it is installed as a service?
Solution: No, the first OPC client that tries to connect will start the OPC server.

Search the *MatrikonOPC Support Knowledge Base* at www.opcsupport.com to find the answers to other commonly-asked MatrikonOPC Server for SCADA DNP3 questions.

Un-Installation

To successfully un-install MatrikonOPC Server for SCADA DNP3 using the **Add or Remove Programs** from the Microsoft Windows **Control Panel** is recommended.

To un-install MatrikonOPC Server for SCADA DNP3:

1. Click on the **Start** button and highlight the **Control Panel** item.
2. From the displayed menu, select **Add or Remove Programs**.
3. The **Add or Remove Programs** window (Figure 56) is displayed.
4. Scroll through the list of currently installed programs and updates to find and select **MatrikonOPC Server for SCADA DNP3**.

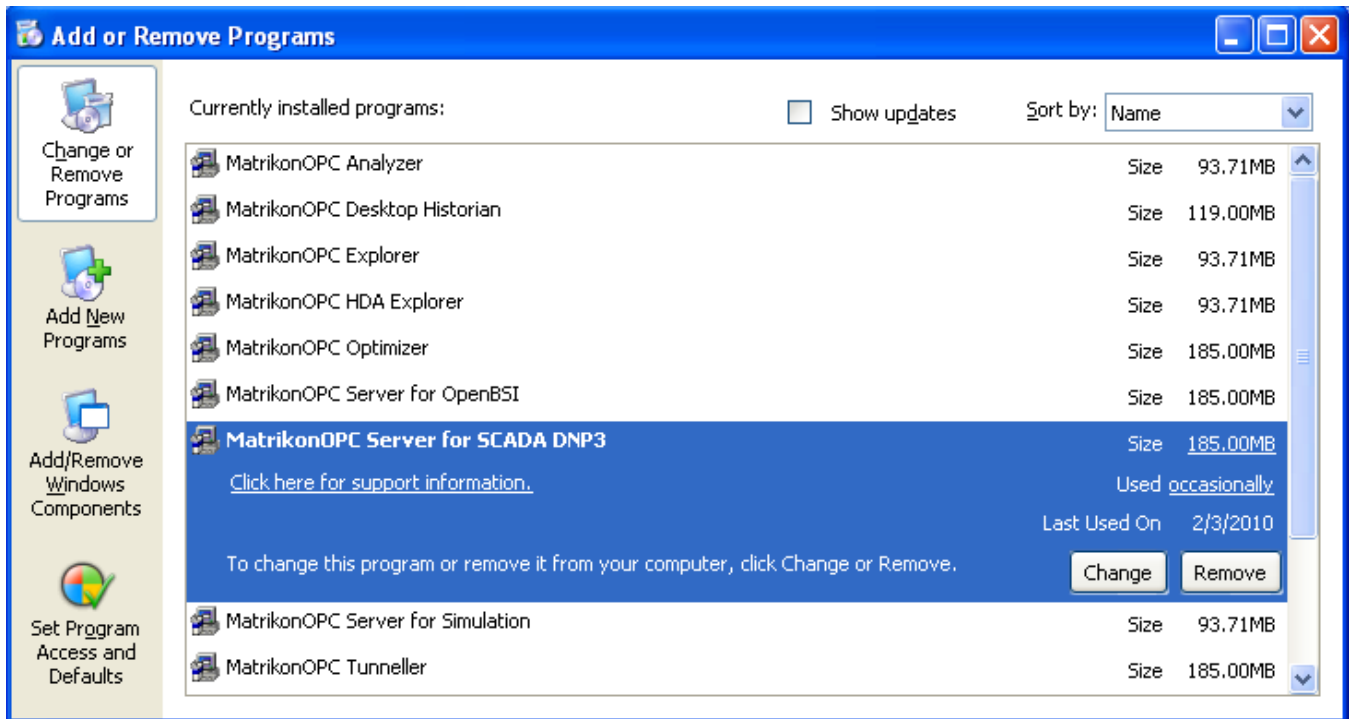


Figure 56 - Add or Remove Programs

5. Click on the **Remove** button associated with the MatrikonOPC Server for SCADA DNP3 program to initiate the un-install process.
6. The **MatrikonOPC Server for SCADA DNP3 – InstallAware Wizard** appears, and the **Welcome to MatrikonOPC Server for SCADA DNP3 Maintenance** screen (Figure 57) is displayed.

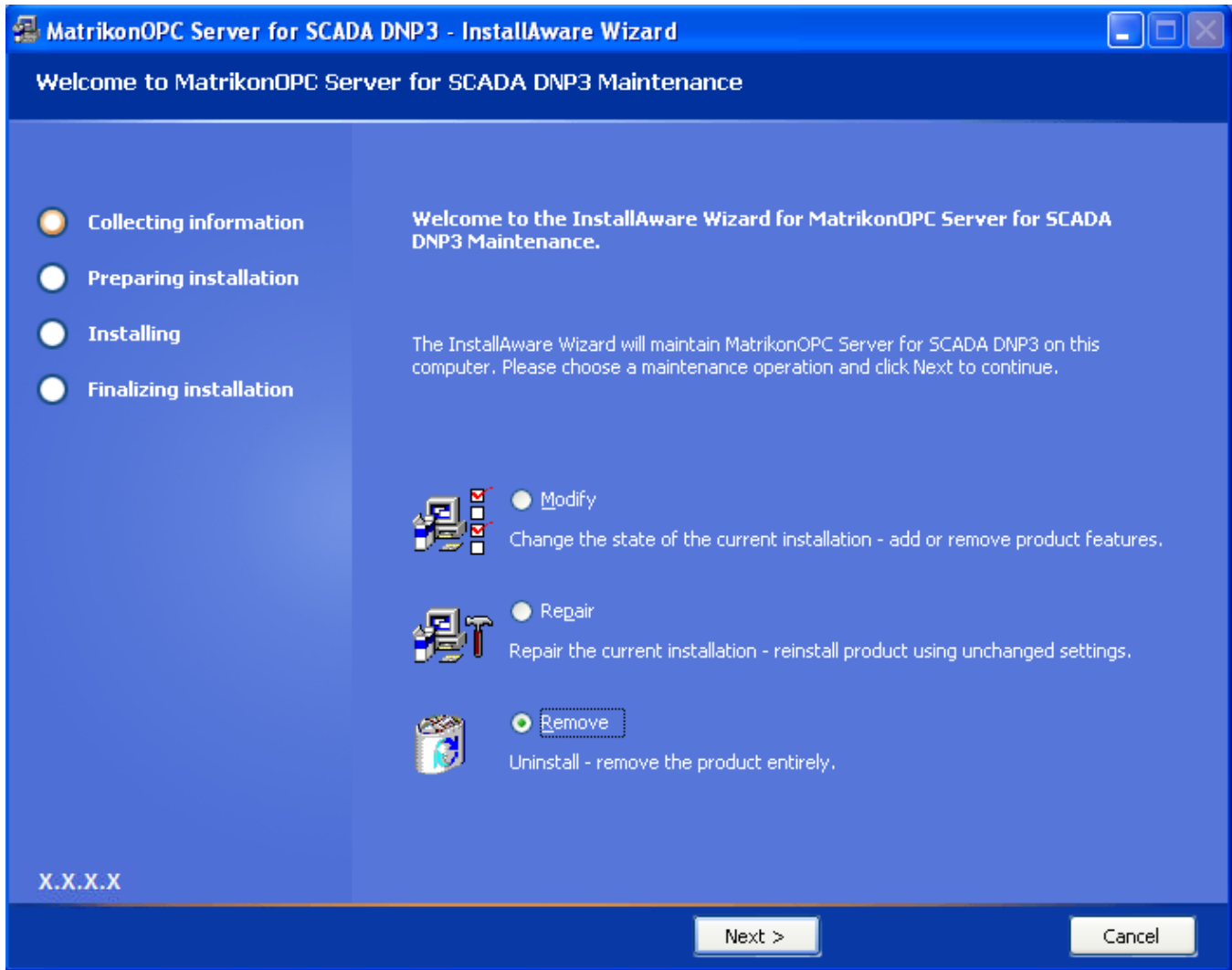


Figure 57 - Welcome to the MatrikonOPC Server for SCADA DNP3 Maintenance Screen

7. Ensure the **Remove** option button is selected to un-install MatrikonOPC Server for SCADA DNP3 entirely.
8. Click on the **Next** button. The **Ready to Uninstall** screen (Figure 58) is displayed.

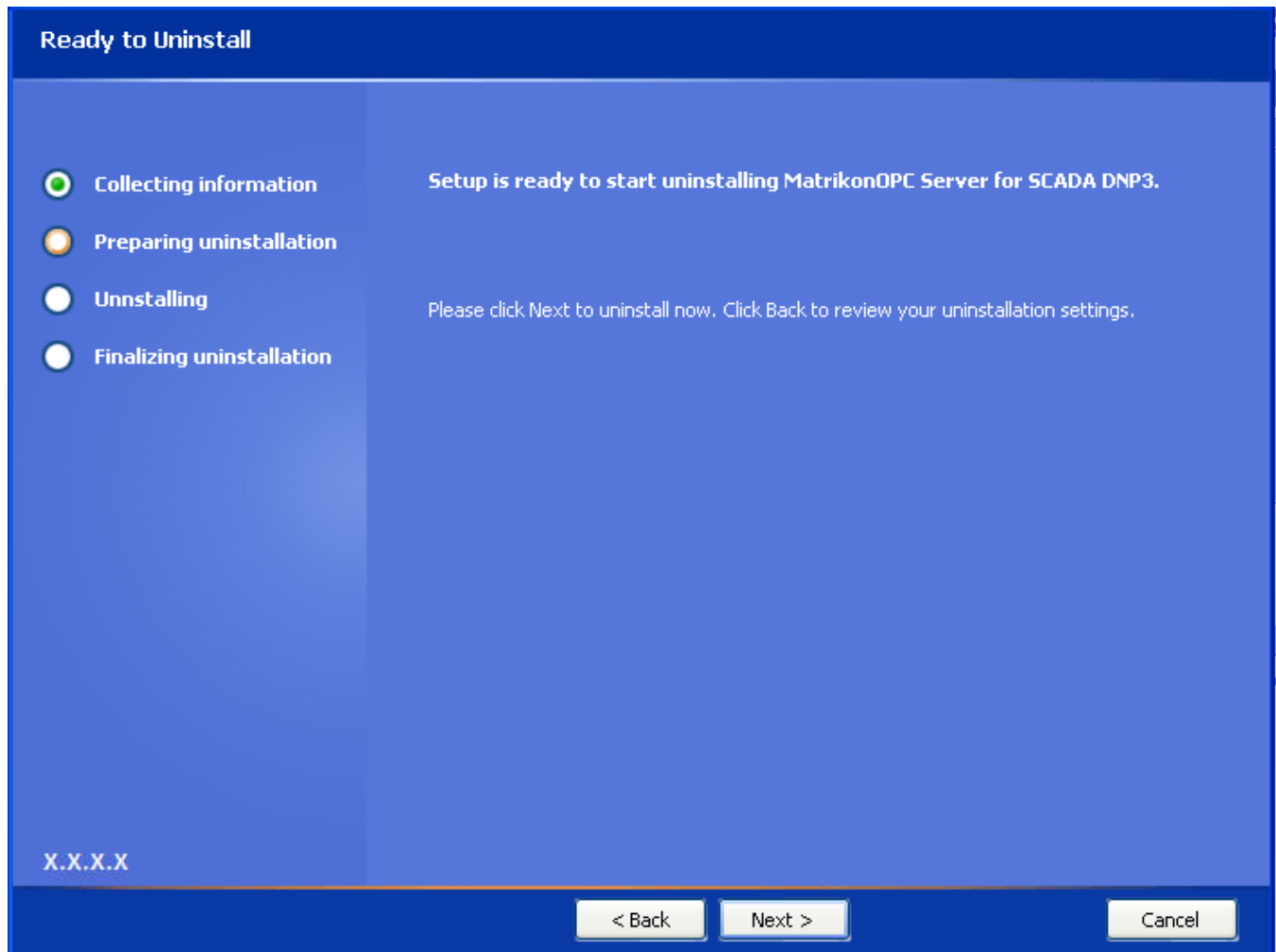


Figure 58 - Ready to Uninstall Screen

9. Click on the **Next** button.
10. The **Uninstalling MatrikonOPC Server for SCADA DNP3** screen (Figure 59) appears and the un-install takes place.

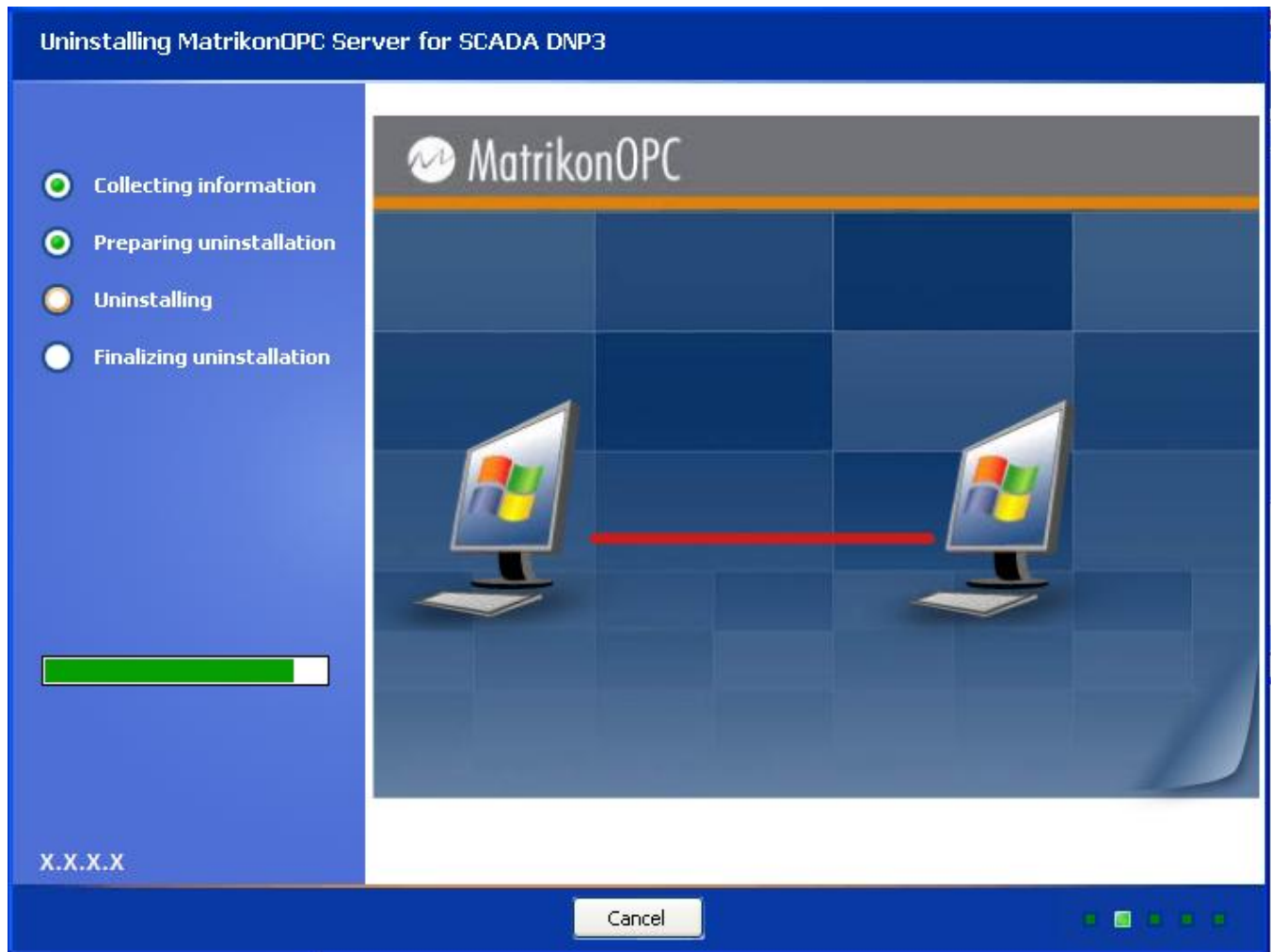


Figure 59 - Uninstalling MatrikonOPC Server for SCADA DNP3 Screen

11. When the un-install has finished, the **MatrikonOPC Server for SCADA DNP3 Setup Complete** screen (Figure 60) appears stating that MatrikonOPC Server for SCADA DNP3 was successfully un-installed.

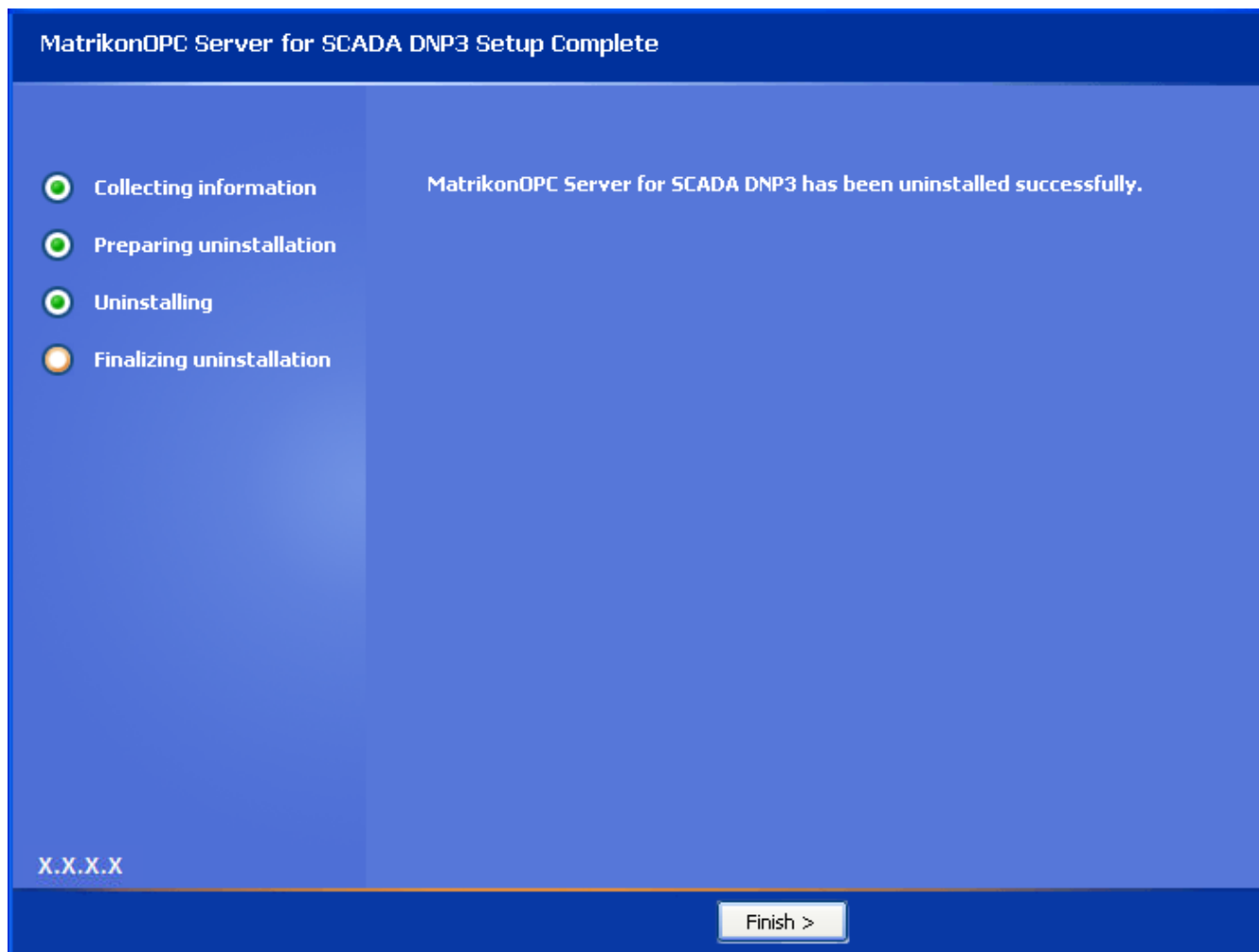


Figure 60 - MatrikonOPC Server for SCADA DNP3 Setup Complete Screen

12. Click on the **Finish** button to complete the un-install and exit the Wizard.
13. The program no longer appears listed in the **Add or Remove Programs** window.

OPC Compliance

For more information on OPC, view the documents listed below (as well as other OPC Specifications) at <http://www.opcfoundation.org>. MatrikonOPC supports the following interfaces:

- *OPC Overview 1.0*
- *OPC Common Definitions and Interfaces 1.0*
- *OPC Security Custom Interface 1.0*
- *OPC Alarms and Events Interface Standard 1.10*
- *OPC Data Access Custom Interface Standard 2.05a*
- *OPC Data Access Custom Interface Standard 3.00*

Installation

The server is by default installed as a local out-of-process COM server and enters its registration information in the Windows registry when instructed to do so with the **/REGSERVER** command-line option. The server installs itself as a Windows service and enters its registration information in the Windows registry when instructed to do so with the **/SERVICE** command-line option.

- Version-independent program ID is **Matrikon.OPC.DNP**.
- Version-specific program ID is **Matrikon.OPC.DNP.1**.
- OPC sub-key and vendor information string.
- Globally unique application ID (e.g., **81BD69CB-47A4-49bc-B5BD-2CD55ACC2DDE**).
- Globally unique class ID number (e.g., **F1F07BB3-D2CB-4e68-A4BF-488CE1FD9F2**).
- Full path of 32-bit local server executable.
- OPC Data Access Server 1.0 and 2.05a implemented component categories.

The server removes its registration information from the Windows registry when commanded to do so with the **/UNREGSERVER** command-line option.

Common Interfaces

The server supports the mandatory functionality specified in *OPC Common Definitions and Interfaces*. The server supports the following locales for result code translation:

- US English (0x0409)
- System default (0x0800)
- User default (0x0400)
- Neutral (0x0000).

The server allows the client to set the client name for each connection. The server supports the shutdown event notification client-side interface.

Data Access

The server supports the mandatory functionality specified in the *OPC Data Access Custom Interface Standard*.

Groups

The server supports the addition, removal, and cloning of private groups. The server allows the client to manage group state.

- Name
- Active state
- Update rate (100 millisecond resolution)
- Time bias
- Dead-band (percent of analog item high-low range)

Items

The server supports the addition, removal, and validation of items in a group. The server allows the client to manage item configuration.

- Active state
- Requested data type
- Dead-band (percent of analog item high-low range)
- Sampling rate
- Buffer values (used only when sampling rate is enabled and is sampling faster than the group update rate).

Browsing and Item Properties

The server supports address space browsing.

- Hierarchical address space
- Simulate flat address space
- Branch/leaf name filter (pattern matching)
- Item data type filter
- Item access rights filter

The server supports the following mandatory item properties.

- Value, quality, and timestamp
- Canonical data type
- Access rights
- Scan rate

I/O Operations

The server supports synchronous I/O operations.

- Read active item values from cache.
- Read item values from device.
- Read items value from device based on how old the cache items value is.
- Read items without adding the item to an OPC group.
- Write control values to items (on device).

- Write control value, quality, and/or timestamp to items (if the server supports such features).
- Write control values without adding the item to an OPC group.

The server supports asynchronous I/O operations as defined for **DA 3.00**.

- Read items value from device based on how old the cache items value is.
- Write control value, quality, and/or timestamp (if the server supports such feature).

The server supports the data change event notification client-side interface as defined for **DA 3.00**.

- Keep-alive call-back indicating server is alive.

The server supports asynchronous I/O operations as defined for **DA 2.05a**.

- Read items values from device.
- Write control values to items (on device).
- Refresh active items from cache.
- Cancel outstanding operations.
- Enable/disable event notifications.

The server supports the data change event notification client-side interface as defined for **DA 2.05a**.

- Data change or dead-band exceeded.
- Asynchronous refresh operation complete.
- Asynchronous read operation complete.
- Asynchronous write operation complete.
- Asynchronous operation cancellation complete.

The server supports asynchronous I/O operations as defined for **DA 1.0**.

- Read items values from device.
- Read items values from cache.
- Write control values to items (on device).
- Refresh active items from cache.
- Cancel outstanding operations.

The server supports the data change event notification client-side interface as defined for **DA 1.0**.

- Data change or dead-band exceeded – data with timestamps.
- Data change or dead-band exceeded – data without timestamps.
- Asynchronous write operation complete.

The server supports OPC Alarms and Events as defined for **AE 1.10**.

Appendix A Distributed COM (DCOM)

DCOM is an object protocol that enables COM components (such as OPC clients and servers) to communicate directly with each other across a network. A certain amount of configuration is required on the system where the OPC server is installed to allow remote clients to connect to it over the network.

Readers should be familiar with DCOM and with Windows 2000 security features and security administration. Information regarding Distributed COM and various links to related sites, white papers, specifications, and so on, can be found at

<http://www.microsoft.com/com/default.msp>.

Notes:



- The following steps are suggestions only. Ask your Windows Network Administrator for more information about the settings that you should use, especially between different domains.
- The steps provided in this appendix apply to Windows NT operating systems only. For information on how to configure DCOM settings for newer Windows operating systems, please refer to the MatrikonOPC Online Support page on **DCOM Settings**.

DCOM Configuration Utility

Start the DCOM configuration utility either from the server configuration utility or from the command-line (**DCOMCNFG**). Answer, **yes** to any message boxes that appear (allowing the utility to assign application ID entries to those servers that don't already have them).

The main window for **DCOMCNFG** allows the user to either configure default settings for all COM servers or else to configure settings for a specific server chosen from the list. The former will affect all servers configured to use the default settings. The latter will affect the selected server only.



Note: DCOM settings are stored in the registry and loaded by COM (and OPC) servers at start-up. Therefore, server processes must be shut down and re-started for these changes to take effect.

Default Properties

The **Default Properties** tab contains settings that affect all DCOM communication on the machine.

- First of all, ensure that the **Enable Distributed COM on this computer** is selected in so that the machine is available to others via DCOM.
- Select the **Enable COM Internet Services on this computer** to allow DCOM access to the machine from the Internet (check with your administrator).
- In general, the other settings do not need to be changed.

The **Authentication Level** specifies when COM should authenticate the identity of calling clients (each call, each packet, etc).

- Normally, it should be set to **Connect**, indicating that COM should authenticate clients when they first connect to a server. If it is set to **None**, then COM performs no authentication and ignores any access permission settings.

The **Impersonation Level** specifies whether servers can ascertain the identity of calling clients and whether they can then perform operations on the client's behalf (as if the server is the client).

- Normally, it should be set to **Identify**, allowing the server to identify the calling client to see if it is allowed access to a certain resource but not to actually access any of these resources as the client.
- Select the **Provide additional security for reference tracking** to make even the reference counting on COM objects secure. This setting is not generally required.

Security Permissions

The most important DCOM settings for an OPC server are the security permissions. There are two ways for you to set these:

1. Change the specific settings for the server (recommended).
2. Change the default settings (not recommended) and make sure that the OPC server will use these.

Either way, be certain that the access and launch permissions are correct for the server.

Setting Security Permissions

To set the security permissions for an OPC Server:

1. Open the DCOM configuration utility.
2. Select the OPC server, and then click **Properties**.
3. The **Distributed COM Configuration Properties** window (Figure 61) appears.

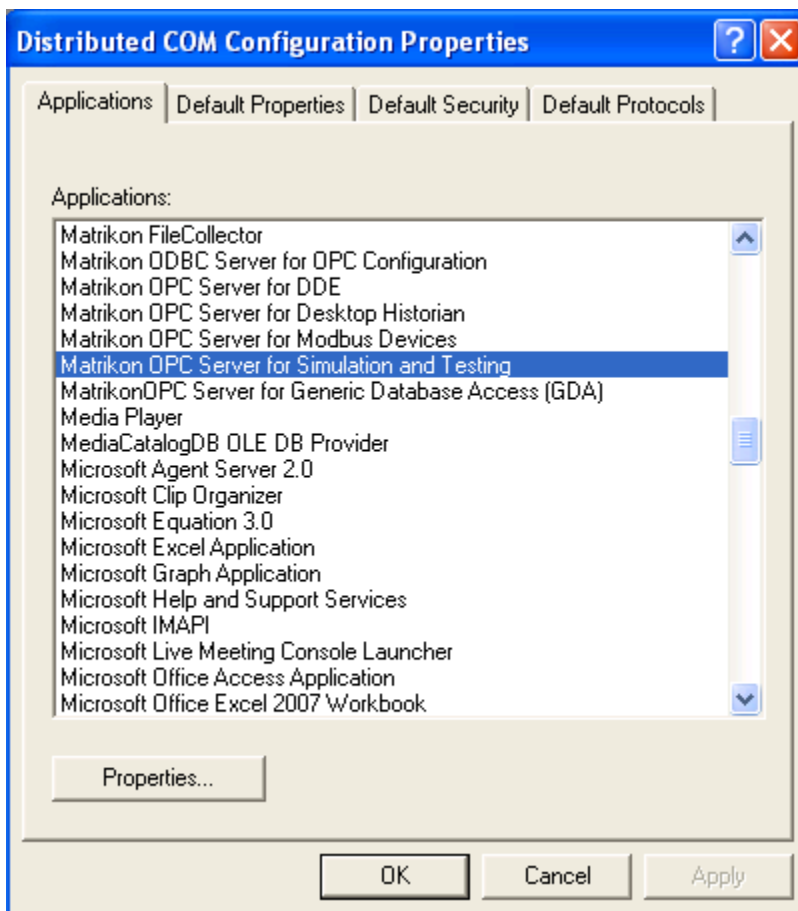


Figure 61 - Distributed COM Configuration Properties Window

4. Click on the **Security** tab to set the security for the server.
5. The **Distributed COM Configuration Security** tab (Figure 62) appears.

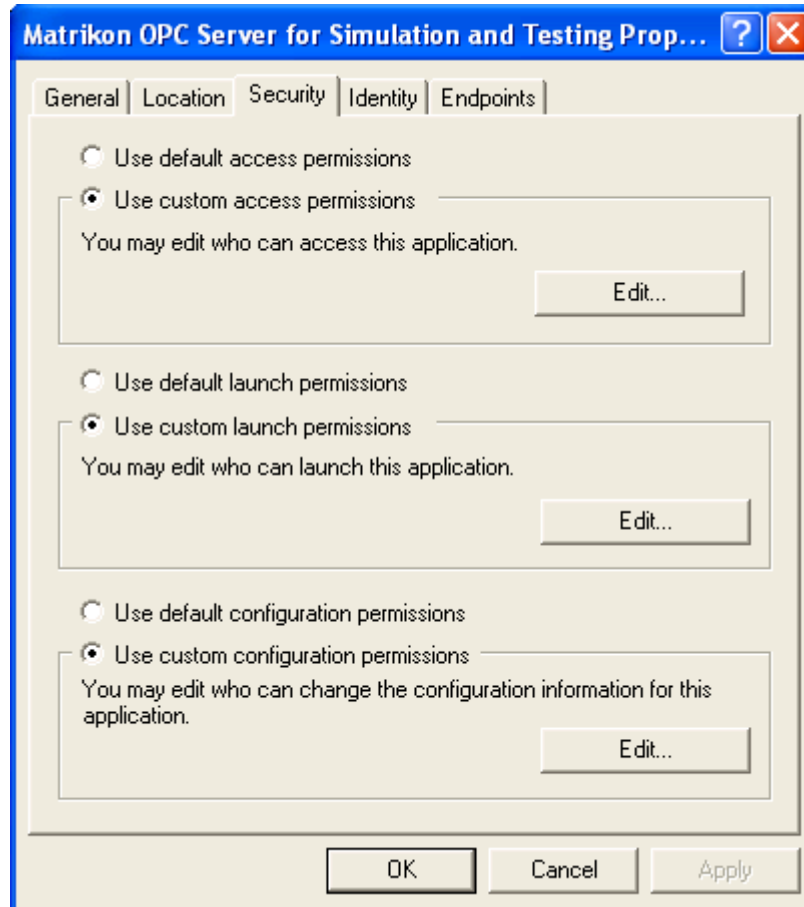


Figure 62 - Distributed COM Configuration Security Tab

Notes:

- The **Access Permissions** contain an *Access Control List* of principals that are allowed to interact with objects supplied by a server.
 - The **Launch Permissions** contain an *Access Control List* of principals that are allowed to start up a server process or service.
6. Include the names of users or user groups from trusted domains that you wish to be able to use the OPC server on this machine. Include the **Everyone** group to allow access to all users on a particular domain.
 7. To set the Access permissions, click **Use custom access permissions** and then click **Edit**.
 8. The **Registry Value Permissions** window (Figure 63) appears.

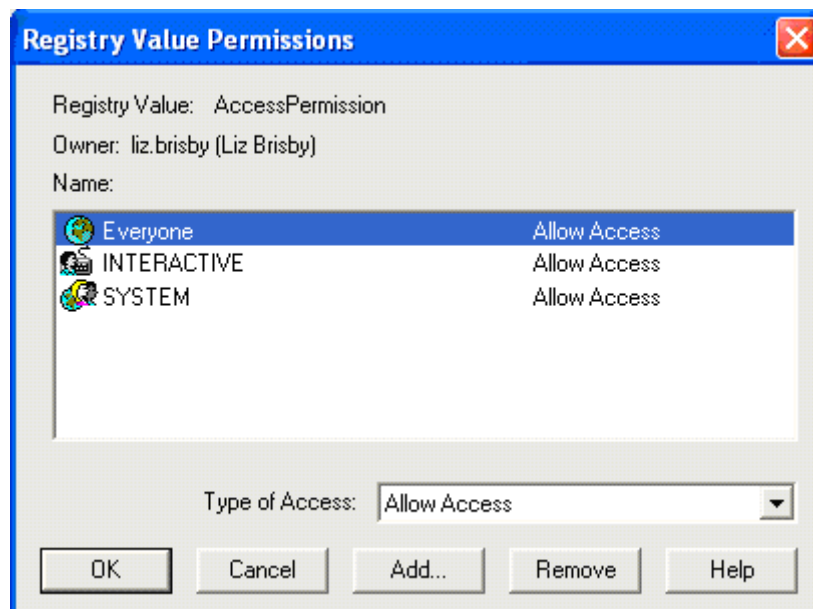


Figure 63 - Registry Value Permissions Window

9. To add users to the list click **Add**.
10. The **Add Users and Groups** window (Figure 64) appears.

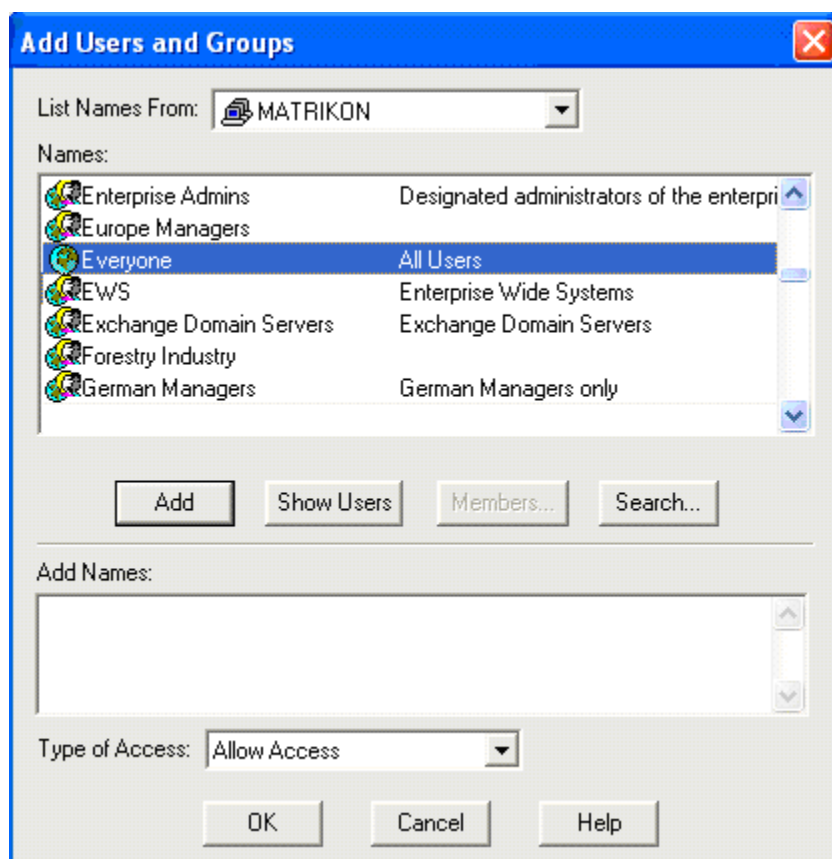


Figure 64 - Add Users and Groups Window

11. To add a user to the list, select the user, and then click **Add**. If the user you wish to add does not appear then click **Show Users**.

12. When you are done adding users, click **OK** to close the **Add Users and Groups** window. You can then choose to **Allow Access** or **Deny Access** for each user.

Notes:

- The procedure to set the launch permissions is similar to the above, but instead of choosing **Allow Access** for a user you would choose **Allow Launch**.
- The Configuration Permissions contain an *Access Control List* of principals that are allowed to modify the configuration information for a server. In other words, it indicates who is allowed to alter the registry entries for installed servers as well as who is able to access the registry for the purposes of installing new servers. It is usually simpler to install and configure servers as a user with local administrative rights.

13. To connect to an OPC server from outside of the domain, create a local user account on both the server and the client machine with identical *username* and *password*. Then, add the local user on the OPC server to the DCOM permissions. Use the local account on the client machine to connect to the OPC server.

Server Identity

The **Identity** tab for a selected COM (or OPC) server specifies the user account that should be used when COM starts up the process. The available settings are different for servers that run as local executables as opposed to those that run as NT services.



Note: It is strongly recommended that OPC servers should be installed to run as NT services if they are going to be accessed by remote clients via DCOM. This ensures that the server can always be accessed even if no one is presently logged on to the machine, and only one server process ever starts up. It also adds a greater degree of security in terms of who is able to shut down the server process.

Servers that run as local executables have the option of running as the launching user (the calling client—this is the default), the interactive user (the one currently logged onto the machine), or a specified user. It is usually best to use the interactive user or a specified user. Otherwise, remote clients might start up multiple separate server processes that are not accessible to others.

Servers that run as NT services should generally run as the local **System** account. Alternatively, the server can be set to run as a specified user, although this is usually done from the **Service Control Manager** applet rather than DCOMCNFG. *Access* and *Launch* permissions are particularly important when installing a server to run as an NT service.

Default Protocols

The **Default Protocols** tab specifies the communication protocols available to DCOM. The order that protocols appear in the list indicates the priority in which they will be used (the topmost having the highest priority).

The more protocols that appear in the list, the better the chances of connecting to an OPC server on an unknown remote machine (such as at an OPC Interoperability Workshop). However, it may also take longer for DCOM to time out if a server machine is not present since it has to try each protocol in turn.

For most situations, it is best to remove all unused protocols from the list and only include those that are necessary for your network. For example, on a TCP/IP network, one would include the **Connection-oriented TCP/IP** protocol. Contact your IT personnel for more information about your network.



Note: Evidence indicates that there are problems with the datagram-oriented protocols (such as UDP/IP) that can cause memory leaks in DCOM. Therefore, it is strongly recommended that these protocols be removed from the list of default protocols. Datagram-oriented protocols are not supported under Windows 2000 at all (although the DCOM configuration utility still allows you to configure them).

Remote Program ID

Before the **OPC Server Browser** became available, OPC client applications had to search the registry to generate a list of available OPC servers. Therefore, some older OPC clients need to have a program ID in the local registry in order to connect to a particular OPC server.

The simplest solution is to install the OPC server software on the client machine even if it is not used. Alternatively, use the following steps to copy a program ID to the client machine.

Note: This method may not work for every OPC client. Please check the client documentation for more information.



WARNING: Any changes made to the registry must be made with **extreme caution!**

1. Back up your registry.
2. On the server machine, run **REGEDIT** as a user that has access rights to the local registry.
3. Expand the **HKEY_CLASSES_ROOT** key.
4. Find the program ID(s) for the desired OPC server(s).

Note: In the case of MatrikonOPC Servers, the ID has the form *Matrikon.OPC.Device*. If you quickly type the first few letters then **REGEDIT** should jump to the location of that key. Some servers may have both a version-specific as well as a version-independent program ID. In this case both IDs should be copied to the client machine.
5. For each program ID, select the key and choose **Export Registry File** from the **Registry** menu. Enter a file name, and then click **Save**. Be careful not to overwrite other export files that you are creating.
6. Copy the exported **REG** files to the client machine.
7. Merge the **REG** files into the registry of the client machine.

Note: This should simply be a matter of double clicking on the file from the desktop of the client machine. Alternatively, run **REGEDIT** on the client machine and choose **Import Registry File** from the **Registry** menu, selecting each file in turn. This must be done as a user who has write access to the local registry.
8. Use **REGEDIT** to check that the program IDs have in fact, been copied.
9. Delete the **REG** files since they are no longer needed.

Appendix B Aliases

Scaling Expressions

Alias scaling expressions may use any of the expression constructs listed in Table 44.

Construct	Description	Examples
'text'	Text value (single quotation marks).	'hello' 'Joe's Alias'
+ - * /	Addition (or Append), Subtraction, Multiplication, and Division.	(3 * 7 + 1) / 8 - 2 'hi' + 'there'
= < > <> <= >=	Equal To, Less Than, Greater Than, Unequal To, Less or Equal To, Greater or Equal To.	3 < 4
Not And Or	Logical Not, Logical And, Logical Or. May also be used for binary math.	(7 >= 3) And (1 <> 0) (12 And 5) = 4
TIME	Current time as text.	'The time is' + TIME
DATE	Current date as text.	'Today is' + DATE
INT(x)	Returns the integer part of x.	INT(3.14) = 3
FRAC(x)	Returns the fractional part of x.	FRAC(3.14) = 0.14
SQRT(x)	Returns the square root of x.	SQRT(16) = 4
DIV(x, y)	Divides x by y.	DIV(42, 7) = 6
IF(expr, x, y)	Returns x if expression evaluates to TRUE, otherwise returns y.	IF(6 <= 12, 'OK', 'Bad') = 'OK'
TRUE FALSE	Constant Boolean true and false.	(5 > 6) = FALSE
TYPEOF(x)	Returns the data type of x as a text description ('STRING', 'INTEGER', 'FLOAT', 'BOOLEAN', 'ERROR').	TYPEOF('hello') = 'STRING'
STR(x)	Converts the numeric value x to text.	STR(3.14) = '3.14'
UPPER(x) LOWER(x) PRETTY(x)	Converts the text value x to all upper case or lower case letters, or the first letter upper case and the rest lower.	UPPER('alarm') = 'ALARM' LOWER('ALARM') = 'alarm' PRETTY('ALARM') = 'Alarm'
COPY(x, start, length)	Returns a sub-string of the x, copying length characters starting at start.	COPY('FIDDLE', 2, 4) = 'IDDL'
FORMATNUMERIC(mask, x)	Converts the numeric value x to text using the format mask.	FORMATNUMERIC('####.#', 123.4567) = '123.5'
INPUT	The incoming value read from OPC.	INPUT * 3.1415
OUTPUT	The outgoing value written to OPC.	OUTPUT / 3.1415

Construct	Description	Examples
'text'	Text value (single quotation marks).	'hello' 'Joe's Alias'

Table 44 - Expressions Constructs for Alias Scaling

Scaling Calculations

Calculations may contain references to any OPC item in the server's syntax. However, they may not contain references to other alias items. There are no limits on how many items can be used in a calculation. The only limiting factor may be performance related. To reference another OPC item in the calculation, wrap the items full item path in square brackets. For example to add the items **Com1.Rtu.Reg1** and **Com1.Rtu.Reg2** together, the correct expression would be:

[Com1.Rtu.Reg1] + [Com1.Rtu.Reg2]

If the OPC item being referenced in a calculation is not found within the servers address space, the server attempts to add it. If successful, the OPC server uses the update rate of the alias to update the OPC item.

If the OPC item being referenced in a calculation is found within the servers address space, the server creates a subscription to it using the lowest update rate of the item and the alias. For example, if the update rate of **Com1.Rtu.Reg1** is ten seconds and a subscription is created to an alias with an update rate of one second, the new update rate of the OPC item is one second.

When the subscription to the alias is cancelled, the item returns to using the previous update rate. However, if the option **Poll Always** is enabled for the alias, the server will always have a subscription to that alias and therefore the lower update rate of the alias is used.

In the event that the server cannot create a subscription to the OPC item, the alias quality reports *Bad, bad configuration*.

Alias scaling calculations may use any of the operators listed in Table 45.

Construct	Description	Examples
-	Minus operator.	x - y
-	Unary minus operator.	-x
!	Not logical operator. Returns 1 if x is 0, else returns 0.	!x
!=	Not equal logical operator. Returns 1 if true, 0 if false.	x != y
%	Modulo; find remainder of the division of x by y.	x % y
&	And logical operator. Returns 1 if true, 0 if false.	x & y
*	Multiplication operator.	x * y
/	Division operator.	x / y
^	Calculates x raised to the power of y.	x ^ y
	Or logical operator. Returns 1 if true, 0 if false.	x y

Construct	Description	Examples
+	Addition operator.	$x + y$
<	Lesser than logical operator. Returns 1 if true, 0 if false.	$x < y$
<=	Lesser than or equal logical operator. Returns 1 if true, 0 if false.	$x <= y$
==	Equal logical operator. Returns 1 if true, 0 if false.	$x == y$
>	Greater than logical operator. Returns 1 if true, 0 if false.	$x > y$
>=	Greater than or equal logical operator. Returns 1 if true, 0 if false.	$x >= y$

Table 45 - Calculation Operators for Alias Scaling

Alias scaling calculations may use any of the functions listed in Table 46.

Construct	Description	Examples
abs	Absolute value.	abs(x)
acos	Arccosine	acos(x)
asin	Arcsine	asin(x)
atan	Arctangent	atan(x)
avg	Returns the average of a set of values.	avg(v1,v2,v3,...)
bin	Converts a binary number to a decimal number.	bin(binNumber)
ceil	Ceiling.	ceil(x)
cos	Cosine.	cos(x)
cosh	Hyperbolic cosine.	cosh(x)
derivate	Differentiate the expression with respect to one variable at the specified point.	derivate(expression, variable, point)
fact	Returns the factorial of x: $x*(x-1)*(x-2)*...(x-x+1)$.	fact(x)
floor	Floor.	floor(x)
hex	Converts an hexadecimal number to a decimal number.	hex(hexNumber)
if	If the condition is true, returns val1 else returns val2.	if(condition, val1, val2)

Construct	Description	Examples
isNaN	Returns 1 if the number is a NaN value.	isNaN(value)
log	Natural logarithm.	log(x)
log10	Base-10 logarithm	log10(x)
max	Returns larger of a set of values.	max(v1,v2,v3,...)
max	Returns larger of two values.	max(x,y)
max	Returns larger of three values.	max(x,y,z)
min	Returns smaller of a set of values.	min(v1,v2,v3,...)
min	Returns smaller of two values.	min(x,y)
min	Returns smaller of three values.	min(x,y,z)
rand	Random value between 0 and 1.	rand()
rand	Random value between min and max.	rand(min, max)
round	Round the fractional part of a number.	round(x)
sin	Sine.	sin(x)
sinh	Hyperbolic sine.	sinh(x)
solve	Finds the variable's value that yields the desired result using the Newton's numerical approximation method.	solve(expression, variable, result, [v0=0], [tol=0.01],[maxIter=100])
sqrt	Square root.	sqrt(x)
sum	Returns the sum of a set of values.	sum(v1,v2,v3,...)
tan	Tangent.	tan(x)
tanh	Hyperbolic tangent.	tanh(x)
trapezoid	Compute a numerical approximation to the integral between a and b.	trapezoid(expression, variable, a, b, [step=0.1])

Table 46 - Calculation Functions for Alias Scaling

CSV File Format

The alias import/export file contains lines of comma-separated values. Values containing commas or spaces are enclosed in double-quotation marks (" "). Double-quotation marks occurring inside quoted values are escaped with an extra double-quotation mark. Lines beginning with a hash mark (#) are ignored (used for comments). Each line contains the fields listed in Table 47.

Field	Description
Alias Group	Name of the alias group folder where the alias belongs. Periods in the name indicate subfolders below the root (e.g., North.FIC101 = alias group North under the Alias

Field	Description
	Configuration root and alias group FIC101 under that).
Alias Name	Name of the alias. Full alias path name composed of the alias group path, a period, and the alias name (e.g., North.FIC101.CV for an alias named CV).
Item Path	Fully qualified item ID for the OPC item to which the alias refers.
Data Type	Decimal number indicating the data type for the alias.
Read-only	Specifies whether the alias is read-only or read-write. 0 = read-write 1 = read-only
Poll Always	Specifies whether the alias is polled continuously or not. 0 = only poll as requested by an OPC client (normal) 1 = poll continuously at the specified update rate
Update Rate	Update rate (milliseconds) to use with the Poll Always option.
Scaling	Scaling type for the alias. 0 = none 1 = linear 2 = square root 3 = gain/offset 4 = expression 5 = calculation

Table 47 - File Import/Export Field Descriptions

When the scaling field specifies linear (1) or square root (2) scaling, the line contains the additional fields listed in Table 48.

Field	Description
High Raw	Raw value range (double-precision real).
Low Raw	
High Scaled	Scaled value range (double-precision real).
Low Scaled	
Clamp	Clamp options. 0 = none 1 = clamp low value 2 = clamp high value 3 = clamp both high and low values

Table 48 - Additional File Import/Export Field Descriptions - Linear/Square Root Scaling

When the scaling field specifies gain/offset (3) scaling, the line contains the additional fields listed in Table 49.

Field	Description
Gain	Scaling factor (double-precision real).
Offset	Scaling offset (double-precision real).

Table 49 - Additional File Import/Export Field Descriptions - Offset Scaling

When the scaling field specifies expression (4) scaling, the line contains the additional fields listed in Table 50.

Field	Description
Input Expression	Simple formula applied to the value read from the OPC item.
Output Expression	Simple formula applied to values written to the OPC item. The output formula should be the reciprocal of the input formula.

Table 50 - Additional File Import/Export Field Descriptions - Expression Scaling

When the scaling field specifies calculation (5) scaling, the line contains the additional fields listed in Table 51.

Field	Description
Input Calculation	Calculation applied to the value read from the OPC item.

Table 51 - Additional File Import/Export Field Descriptions - Calculation Scaling

Scaling Algorithms

For each type of scaling, a different algorithm (Table 52) is applied to values read from the OPC item. A reverse algorithm is applied to any values written to the OPC item.

Scaling	Algorithm/Example	Reverse Algorithm/Example
Linear	$(x - Raw_{Low}) \left(\frac{Scaled_{High} - Scaled_{Low}}{Raw_{High} - Raw_{Low}} \right) + Scaled_{Low}$	$(x - Scaled_{Low}) \left(\frac{Raw_{High} - Raw_{Low}}{Scaled_{High} - Scaled_{Low}} \right) + Raw_{Low}$
Square Root	$\sqrt{x - Raw_{Low}} \left(\frac{Scaled_{High} - Scaled_{Low}}{\sqrt{Raw_{High} - Raw_{Low}}} \right) + Scaled_{Low}$	$(x - Scaled_{Low})^2 \left(\frac{Raw_{High} - Raw_{Low}}{(Scaled_{High} - Scaled_{Low})^2} \right) + Raw_{Low}$
Gain/Offset	$Gain \cdot x + Offset$	$\frac{x - Offset}{Gain}$
Expression	$SQRT(INPUT) + 5$	$(OUTPUT - 5) * (OUTPUT - 5)$
Calculation	$round([Random.Real4])$	N/A

Table 52 - Scaling Algorithms

Appendix C Standard Data Types

The Standard data types and their descriptions are listed in Table 53.

Hex	Dec	Data Type	Description
0000	0	VT_EMPTY	Default/Empty (nothing)
0002	2	VT_I2	2-byte signed integer
0003	3	VT_I4	4-byte signed integer
0004	4	VT_R4	4-byte (single-precision) real
0005	5	VT_R8	8-byte (double-precision) real
0006	6	VT_CY	Currency
0007	7	VT_DATE	Date
0008	8	VT_BSTR	Text (UNICODE)
000A	10	VT_ERROR	Error code
000B	11	VT_BOOL	Boolean (TRUE = -1, FALSE = 0)
0011	16	VT_I1	1-byte signed integer
0012	17	VT_UI1	1-byte unsigned integer
0013	18	VT_UI2	2-byte unsigned integer
0014	19	VT_UI4	4-byte unsigned integer
2002	8194	VT_ARRAY VT_I2	Array of 2-byte signed integers
2003	8195	VT_ARRAY VT_I4	Array of 4-byte signed integer
2004	8196	VT_ARRAY VT_R4	Array of 4-byte (single-precision) real
2005	8197	VT_ARRAY VT_R8	Array of 8-byte (double-precision) real
2006	8198	VT_ARRAY VT_CY	Array of currency values
2007	8199	VT_ARRAY VT_DATE	Array of dates
2008	8200	VT_ARRAY VT_BSTR	Array of text values
200A	8202	VT_ARRAY VT_ERROR	Array of error codes
200B	8203	VT_ARRAY VT_BOOL	Array of Boolean values
2011	8208	VT_ARRAY VT_I1	Array of 1-byte signed integers
2012	8209	VT_ARRAY VT_UI1	Array of 1-byte unsigned integers
2013	8210	VT_ARRAY VT_UI2	Array of 2-byte unsigned integers
2014	8211	VT_ARRAY VT_UI4	Array of 4-byte unsigned integers

Table 53 - Standard Data Types

Appendix D Microsoft Excel as a DDE Client

Microsoft Excel can act as both DDE client and DDE server. When using Excel as the client, DDE items can be bound to specific cells in a spreadsheet, creating a read-only “hot link” to the DDE items. Using Visual Basic, Excel can also be used to transmit (write) the data contained in a specific cell of a spreadsheet to a DDE server.

DDE Read

To perform a DDE Read using Excel, simply enter a DDE Item as a formula in some spreadsheet cell:

=SERVICE|TOPIC! NAME

Excel will initiate a DDE Advise loop, or “hot link”, to the topic and item within the service. The DDE Management system (in this case, Windows) will forward any update sent by the DDE service, to the appropriate DDE client (in this case, Microsoft Excel). The DDE service is responsible for update rate/behavior.

To disable a specific hotlink in Excel, use the **Links** menu option under the **Edit** menu.

Special Characters in Excel

Excel reserves the use of specific characters for use in any cell. If a **SERVICE**, **TOPIC**, or **NAME** contains any special characters, surround the specific field with single quotation characters (' '):

=SERVICE|TOPIC!'NAME'

=SERVICE|'TOPIC'!'NAME'

=SERVICE|'TOPIC'!NAME

To include single quotation characters in the name, enter two simultaneous single quotation characters:

=matrikon_opc_simulation_1|'Power.Generator's Value'!'1000\'

DDE Write

To perform any DDE command other than requests (read) or advise (hot link), a Visual Basic (VB) function must be used. Most DDE commands are available by using the application object. For example, the following function will poke (write) the contents of column 1, row 1 to an item in the OPC Simulation server:

```
Sub WriteToDDE()  
  
' open a DDE channel. Field 1 = SERVICE, Field 2 = TOPIC  
'channel = DDEInitiate("matrikon_opc_simulation", "Bucket Brigade.Real4")  
  
' poke to the Item 1000\, the value of cell A1  
DDEPoke channel, "1000\", Worksheets("Sheet1").Range("A1")  
  
' close the channel  
DDETerminate channel  
  
End Sub
```

Net DDE

Since DDE commands are routed by the operating system, it is not possible to establish a DDE session between two computers unless some transport mechanism is used. This is usually supplied as a plug-in component of the operating system. In the Windows Environment, the NetDDE Windows Service allows DDE communication between two computers.

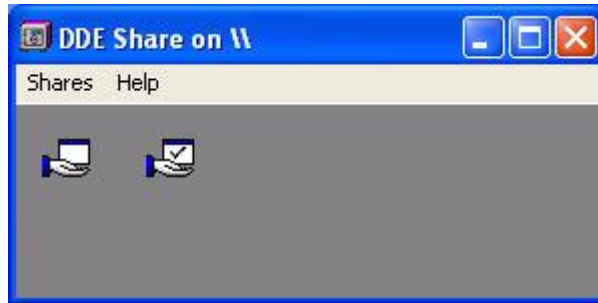


Figure 65 - DDE Share

NetDDE must first be configured using the DDEShare application (*DDEShare.exe*) as shown in Figure 65. Each SERVICE and TOPIC pair, or "NetDDE Share", that is to be available through NetDDE must be assigned a unique name.

Appendix E Security

Introduction

The OPC Framework has implemented the OPC Security Customer Interface version 1.0 of the specification. Both the *IOPCSecurityNT* and *IOPCSecurityPrivate* interfaces are fully supported (there are no optional pieces).

IOPCSecurityNT describes how NT authentication is used in OPC Security. *IOPCSecurityPrivate* describes how proprietary user credentials are used in OPC Security. The OPC Security specification defines how user credentials are passed from client to server, but very little else. The type of functionality in an OPC server that is controlled by OPC Security is vendor-determined.

Appendix Structure

This appendix is structured as follows:

- **Introduction** – this introductory section.
- **OPC Security Implementation** – description of user access dependencies.
- **MatrikonOPC Tag Security Configuration Utility** – describes the utility that is used to configure security for MatrikonOPC servers.
- **Security Details** – describes how permissions are applied, how security settings are stored, and other important details.

OPC Security Implementation

Whether a user has access or not will depend on:

1. **Identity** – the user behind the OPC client's actions.
2. **Location** – the OPC item ID or hierarchy path being accessed.
3. **Type** – the type of functionality the user is trying to perform.

Identity

Using the *IOPCSecurityNT* interface for OPC Security, the identity of the OPC client is the domain user that is running the OPC client and connecting to the OPC server. The OPC Framework will attempt to impersonate the client that is connected to the server, and use the name from those credentials for access control. This method does not require any implementation of OPC Security by the OPC client, since no interface calls are necessary.

Using the *IOPCSecurityPrivate* interface for OPC Security, the OPC client must make a call to the OPC server to log on with a user name and password. In this scenario, the OPC client must implement and follow the OPC Security specification in terms of following the calls necessary to provide credentials. The credentials provided through the private interface override those provided from the NT interface. The OPC client may choose to log off, at which point the NT credentials are used until the log on call is made again.

Location

Some of the interface calls made from an OPC client to an OPC server require the client to provide an OPC item ID. The OPC Framework will take the OPC item ID provided, and determine whether access to that location is allowed or not. A particular server installation may want to control access to a particular device or branch in the hierarchy, and is able to do so by setting permissions for a partial item ID or path.

Other interface calls do not provide an ID, but may depend on the state of the server with respect to previous calls. OPC Browsing (DA 2.0) is an example of this. In this case, the full path up to that particular location is used for determining access rights.

Type

There are four types of interface functionality in the OPC Framework (specifically the OPC Outer Layer) that are controlled using OPC Security:

1. Browsing
2. Adding items
3. Reading
4. Writing

Browsing is the least intrusive, followed by adding items, reading values from the items, and finally writing to the items being the most intrusive. There are multiple interfaces, and functions within those interfaces, that can be used to perform the types of functionality listed above. Thus, security control has been added to each possible entry. For example, read control has been added to group subscriptions call-backs as well as synchronous reads and asynchronous reads – denying read control would disable reads for the possible types.

A location that is being accessed by an OPC client may have different permissions for the different types of access. For example, one particular item may be browseable, added, and read, but the writing permissions might be restricted so that the user cannot interfere with the operation of the end device.

Note: Of the four functionality types listed above, three of them make use of the full OPC item ID when an interface call is made from the client to the server: Adding Items, Reading, or Writing. When browsing, only a partial path leading to an OPC item may be known at any location in the browsing hierarchy.

MatrikonOPC Tag Security Configuration Utility

The tag security settings for MatrikonOPC servers are configured and managed via the **MatrikonOPC Tag Security Configuration Utility**, a tool that is installed with the server. This utility allows users to define, per MatrikonOPC server, the following:

- Who has permission
- Which tags/locations they have permissions for
- The type of permissions for those locations

Security settings configured using this utility are read by the OPC Framework and populated in memory upon server start-up, and are monitored for changes.

Note: In order for the **MatrikonOPC Tag Security Configuration Utility** to work properly, the windows user running the utility must have Administrator rights to the computer.

The **MatrikonOPC Tag Security Configuration Utility** is a component of an OPC server installation, and is installed in the following location:

C:\Program Files\Common Files\MatrikonOPC\Common\ACLConfig.exe

The **MatrikonOPC Tag Security Configuration Utility** can be run either directly from its installed location, or from a shortcut found in the **Start Menu**. If the utility is run from the installed location, then the user must select the OPC server for which security will be configured. If the **MatrikonOPC Tag Security Configuration Utility** is run from the shortcut, then it will configure security for the OPC server to which the shortcut belongs.

To run the MatrikonOPC Tag Security Configuration Utility from its shortcut:

1. Click on the Windows **Start** button.
2. Select **Programs -> MatrikonOPC -> <OPC Server Name> -> Tag Security**.

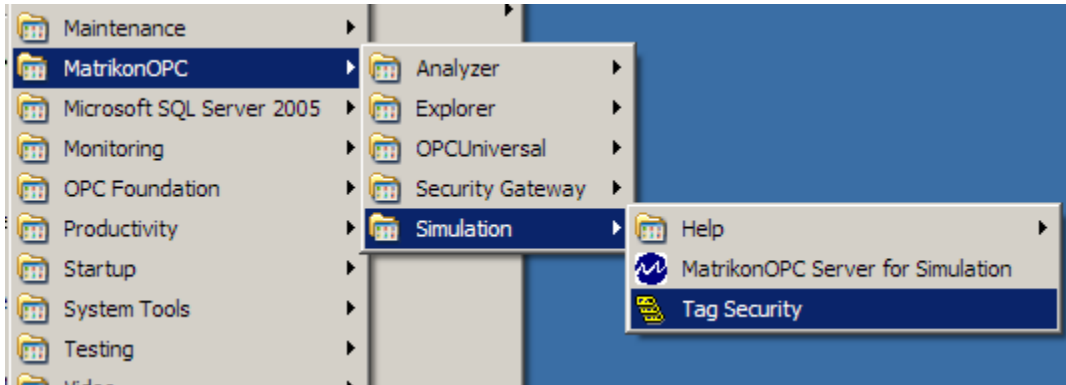


Figure 66 - Start Menu Navigation

After the MatrikonOPC Tag Security Configuration Utility is run:

1. A window appears asking for a password to be entered. This protects the security settings and prevents unauthorized individuals from accessing these settings. For servers that required a security password to be entered during their installation, the **Enter server password** window (Figure 67) appears.



Figure 67 - Enter Server Password Window

2. Enter the password created during the installation of the OPC server.
Note: The default password provided for you during installation (if you chose to use the default) is **MatrikonOPC**.
3. Click on the **OK** button.
4. The **MatrikonOPC Tag Security Configuration Utility** screen (Figure 68) appears.

Layout

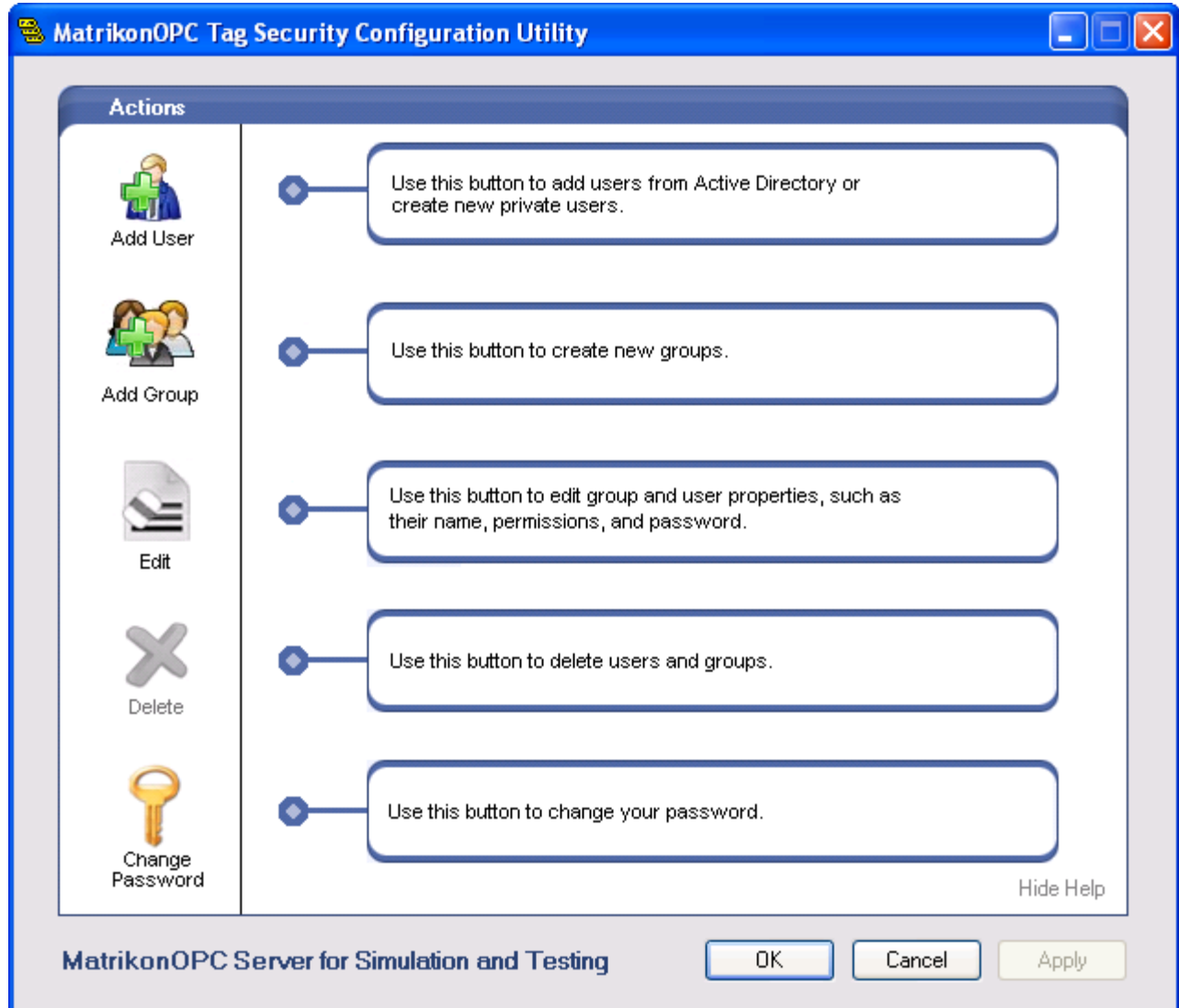


Figure 68 - MatrikonOPC Tag Security Configuration Utility Main Screen

The **MatrikonOPC Tag Security Configuration Utility** screen displays the name of the OPC server that is being configured for tag security. In Figure 68 above, the **Utility** screen shows that the **MatrikonOPC Server for Simulation and Testing** tag security is being configured.

The left-hand side of the **Utility** screen shows a column of action icons that can be clicked upon. These actions are further described later in this appendix. Some actions may not be applicable, depending on the context in which they are used, and are identified by grayed-out icons.

In the center of the **Utility** screen there are descriptions for each of the actions that can be performed. The appearance of these descriptions can be toggled at any time by clicking on the **Hide Help/Show Help** link that exists in the bottom-right corner of the **Utility** screen. When the **Help** screen is hidden, a list of users and groups that have been added appears (Figure 69). By default, there is always a user named **Everyone** in the **Users & Groups** list. This user defines the permissions used for other NT users that are not configured.

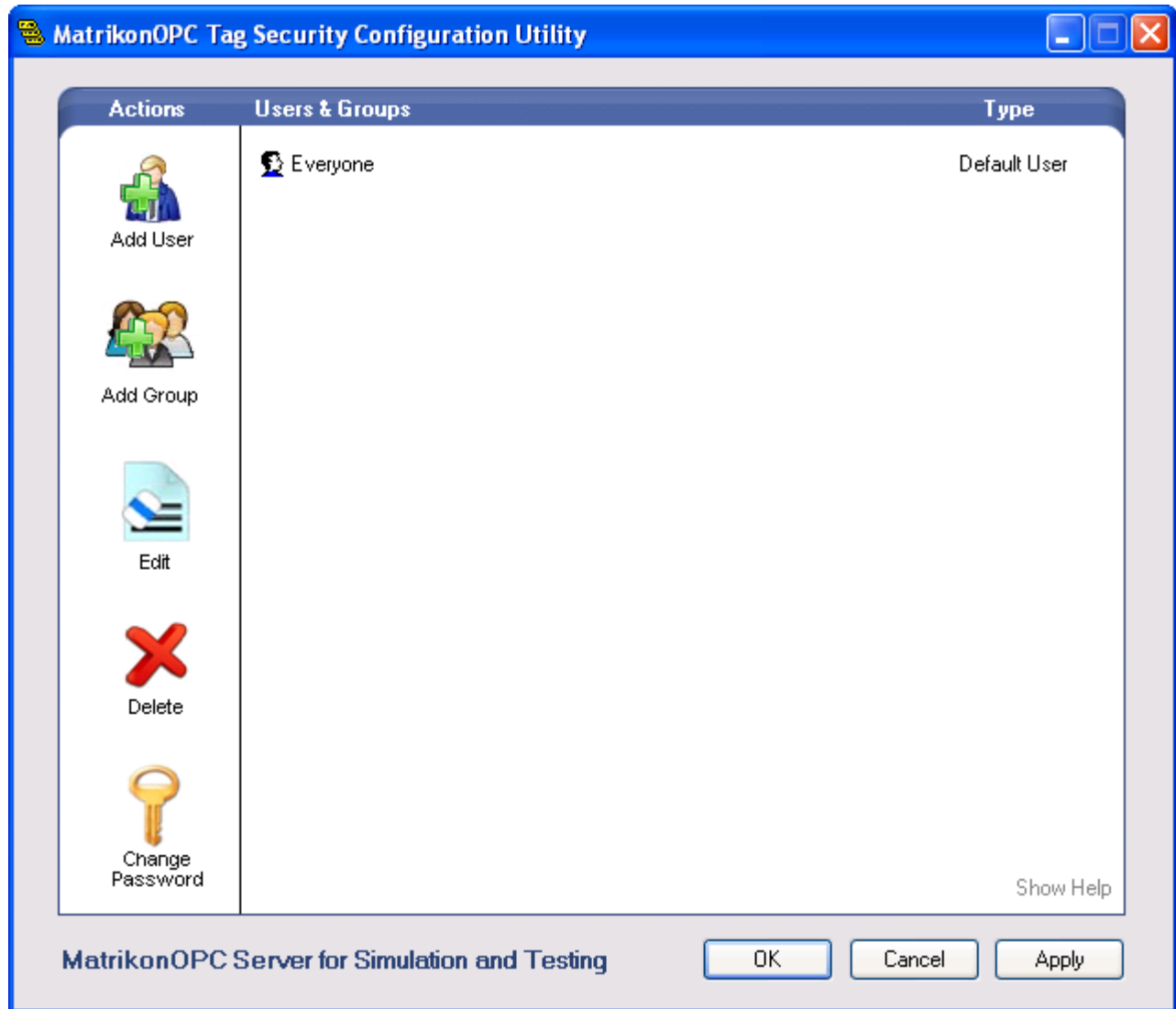


Figure 69 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups

Note: After any action is performed, the changes made do not take effect until either the **OK** or **Apply** button has been selected. Clicking on the **OK** button saves the changes and closes the **Utility** screen. Clicking on the **Apply** button saves the changes and keeps the **Utility** screen open. Clicking on the **Cancel** button or the **X** button on the top-right of the screen, discards any changes made.

Add User

There are two types of users for which security can be configured: *NT Users* and *Private Users*. Adding a user to the configuration will allow permissions to be defined for that user. For NT users, the *IOPCSecurityNT* interface is used, and for Private users, the *IOPCSecurityPrivate* interface is used.

NT User

To add an NT user:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add User** button.

2. The **Add User** window (Figure 70) appears. The **NT User** option button is selected by default. This will allow the addition of a user from a Windows NT Domain.

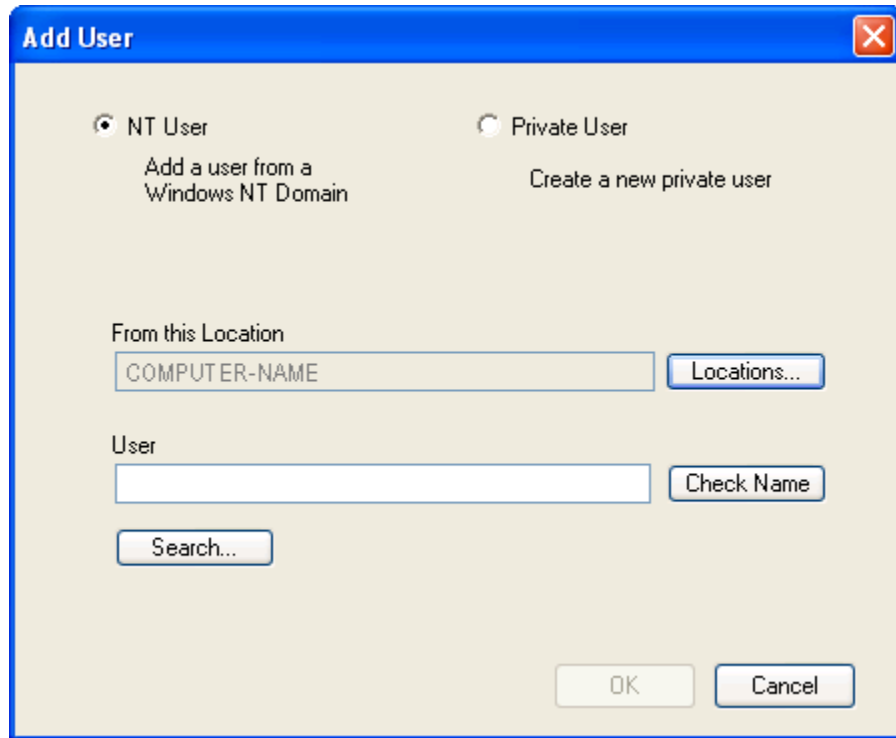


Figure 70 - Add User Window (NT)

3. By default, the local machine name appears in the **From this Location** field. To browse to a different location, click the **Locations** button.
4. The **User** field can be entered manually. Clicking on the **Check Name** button performs validation on the entered user. The user names are the same as the Windows NT domain names used on the network. To avoid manually entering a user, click on the **Search** button, and select a user from the displayed list of users.
5. To add the selected user, click on the **OK** button. The user is then added to the list of users and/or groups currently defined (refer to Figure 71 for a sample list of defined users and groups).
6. The **Edit <Username>** window (Figure 76) appears. Follow the instructions in the **Edit User** section for adding permissions.

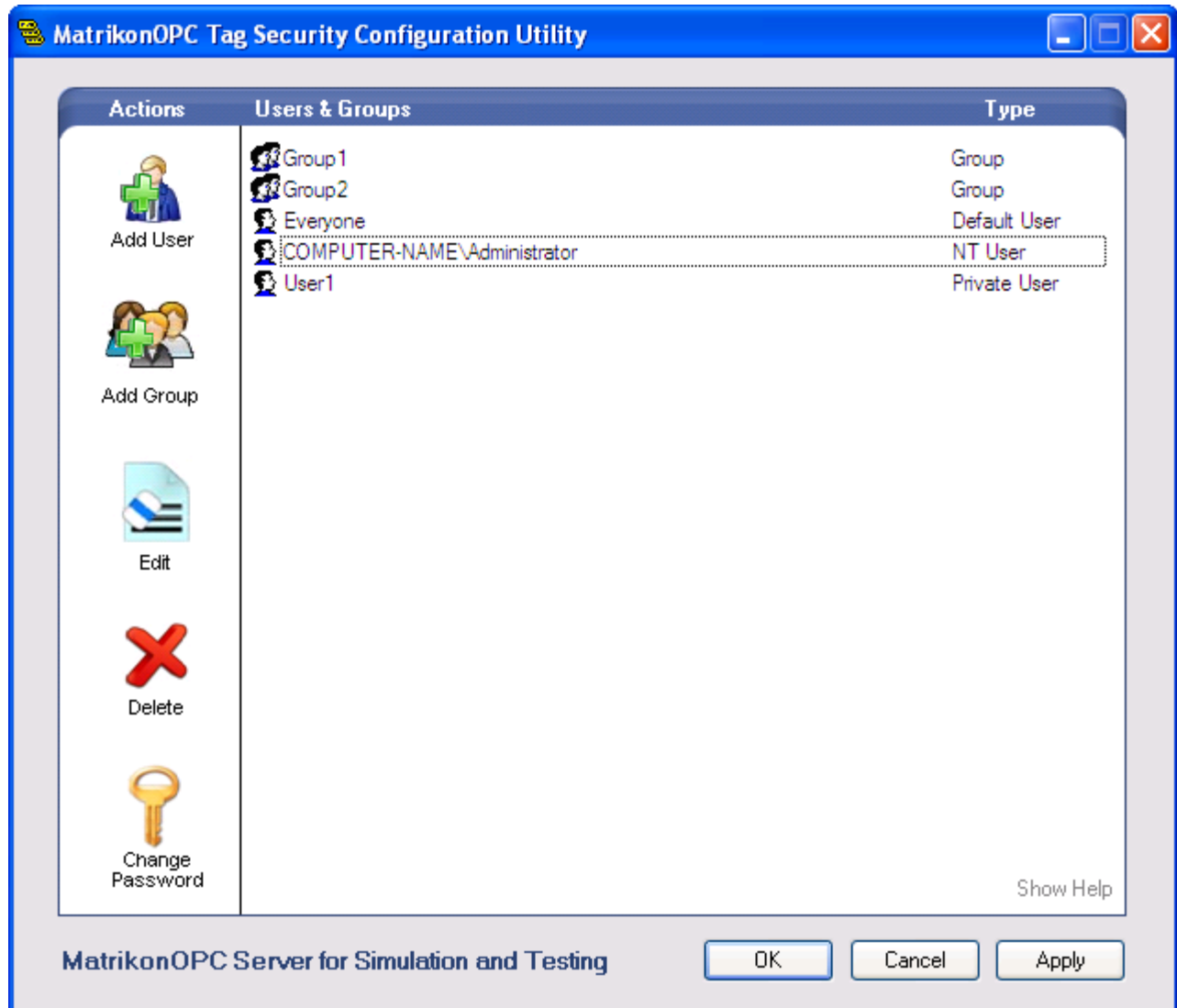


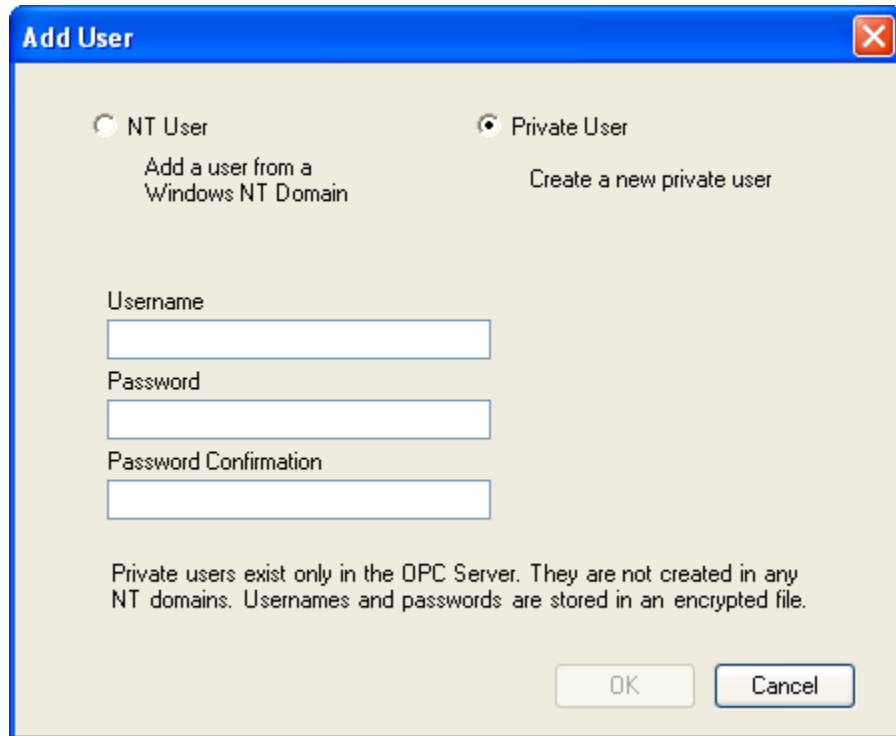
Figure 71 - Defined Users and Groups

Private User

Private users have names and passwords associated with them, custom to the OPC client application, which must implement the OPC Security Private interface for this section to be meaningful. Private users exist only in the OPC server. They are not created in any NT domains.

To add a Private user:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add User** button.
2. The **Add User** window (Figure 70) appears.
3. Select the **Private User** option button (Figure 72).



The 'Add User' dialog box has a blue title bar with a close button. It contains two radio buttons: 'NT User' (unselected) and 'Private User' (selected). Below 'NT User' is the text 'Add a user from a Windows NT Domain'. Below 'Private User' is the text 'Create a new private user'. There are three text input fields: 'Username', 'Password', and 'Password Confirmation'. At the bottom, there is a note: 'Private users exist only in the OPC Server. They are not created in any NT domains. Usernames and passwords are stored in an encrypted file.' and two buttons: 'OK' and 'Cancel'.

Figure 72 - Add User Window (Private)

4. In the **Username** field, enter a user name.
5. In the **Password** field, enter a password.
6. In the **Password Confirmation** field, re-enter the new password.
7. Click **OK** to create the Private user. It will be added to the list of users and/or groups currently defined (refer to Figure 71 for a sample list of defined users and groups).

Note: The user name cannot be added if there is already a configured User or Group with that same name.

Add Group

Groups are used to group users together so that they can share common permissions. Groups are not necessary to use OPC Security. However, they are convenient when you need to apply common permissions to multiple users. A group must contain at least one user, and any combination of users can be grouped together.

Note: A user can exist in multiple groups, but if two or more of the groups have the same configured path (refer to the **Edit User** section), and each group defines a permission (Allow/Deny) for the type of access, then the group whose name alphabetically comes first is used.

There are two types of groups for which security can be configured: **NT Groups** and **Private Groups**.

NT Group

To add an NT group:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add Group** button.

- The **Add Group** window (Figure 73) appears. The **NT Group** option button is selected by default. This will allow the addition of an NT group from a Windows NT Domain.

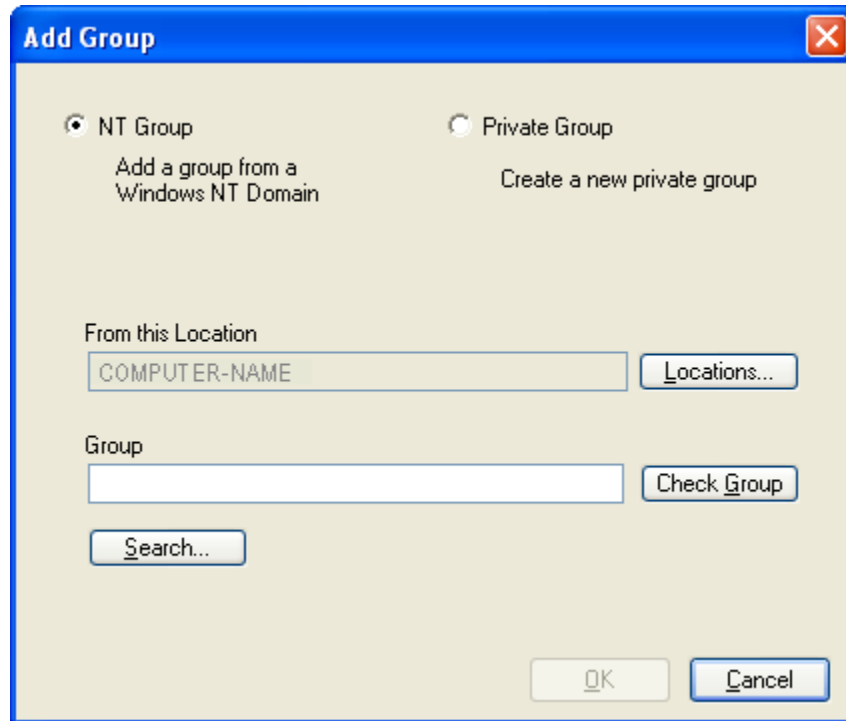


Figure 73 - Add Group Window (NT)

- By default, the local machine name appears in the **From this Location** field. To browse to a different location, click the **Locations** button.
- The **Group** field can be entered manually. Clicking on the **Check Group** button performs validation on the entered group. The group names are the same as the Windows NT domain group names used on the network. To avoid manually entering a group, click on the **Search** button, and select a group from the displayed list of groups.
- To add the selected group, click on the **OK** button. The group is then added to the list of users and/or groups currently defined (refer to Figure 71 for a sample list of defined users and groups).
- The **Edit <Groupname>** window (Figure 83) appears (for NT Groups, there is only the **Permissions** tab). Follow the instructions in the **Edit Group** section for adding permissions.

Private Group

To add a Private Group:

- From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add Group** button.
- The **Add Group** window (Figure 73) appears.
- Select the **Private Group** option button (Figure 74).

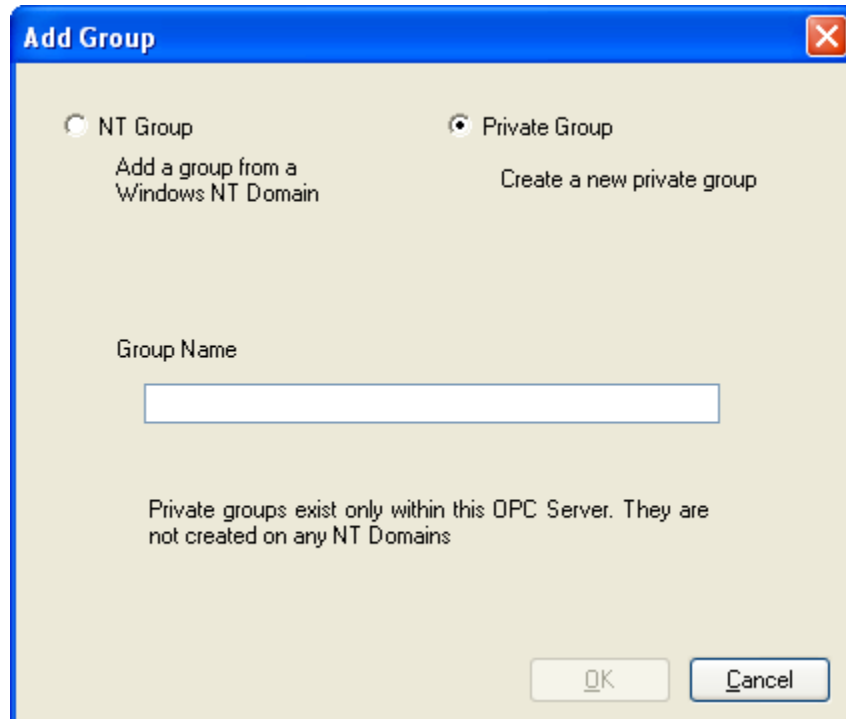


Figure 74 - Add Group Window (Private)

4. Enter a name for the group to be created. The group is private and will only exist in the OPC server. The group cannot be created if there is already a configured user or group with that same name.
5. Click on the **OK** button to create the group. It will be added to the list of users and/or groups currently defined (refer to Figure 71 for a sample list of defined users and groups).
6. The **Edit <Groupname>** window (Figure 83) appears. Follow the instructions in the **Edit Group** section for adding permissions.

Duplicate

Another way to create a new user or group is to duplicate an existing one.

To create a new user or group via duplication:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, right-click your mouse on the user or group you wish to duplicate.
2. From the displayed menu, select **Duplicate**.
3. The **Enter New Name** window (Figure 75) appears.

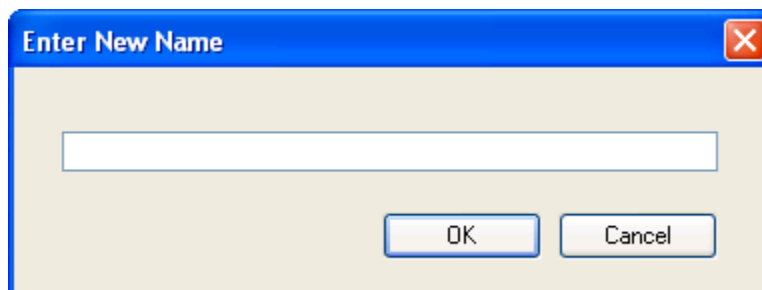


Figure 75 - Enter New Name Window

4. Enter a name for the new user or group to be created.
5. Click on the **OK** button. There must not already be a configured user or group with that same name. The new user or group will then appear in the list, and will contain the same properties as the duplicated parent (i.e., original) user or group.

Edit

Once the desired users and/or groups are defined, they must be edited to configure their respective permissions.

Note: Permissions can also be defined for the user **Everyone**, which is defined as the default user. For every NT user not configured in the MatrikonOPC Tag Security Configuration Utility, the user **Everyone** is used for determining security permissions.

Permissions for allowing/denying browsing, adding items, reading items, and writing items can be configured. Permissions are defined for users and groups for a particular location in the server's address space hierarchy. A location can either be a tag (i.e., OPC Item ID) or a path leading up to an item.

Edit User

To edit a user:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, either:
 - Double-click your mouse on the user you wish to edit, or
 - Right-click your mouse on the required user and select **Edit User** from the displayed menu, or
 - Click your mouse on the required user, and then select the **Edit** button.
2. The **Edit <Username>** window (Figure 76) appears.

Notes:

- In this example, the user being edited is **User1** so the window's title reads **Edit User1**.
- There are two tabs on this window: **Permissions** and **General**. The **General** tab only appears for private users.

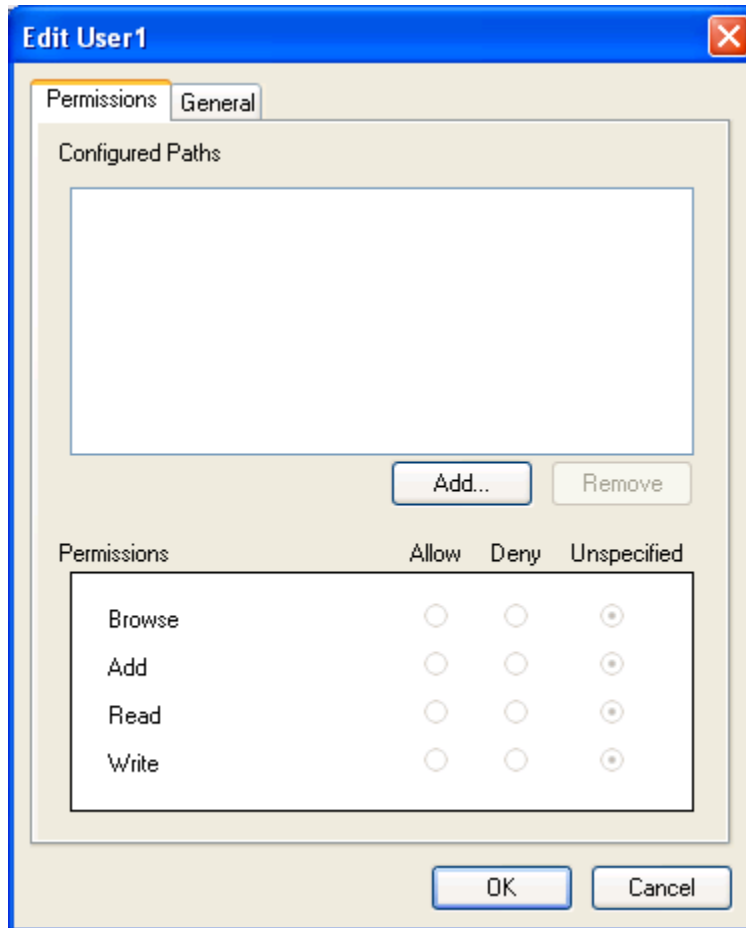


Figure 76 - Edit <Username> Window (Permissions Tab)

Permissions

On the **Permissions** tab, the permissions associated with this user relating to browsing, adding, reading, and writing for any specific paths or OPC items are configured. The **Configured Paths** screen section lists the paths and/or OPC items for which permissions are defined. The **Permissions** screen section indicates those permissions with option buttons, which can be set to **Allow**, **Deny**, or **Unspecified**. Selecting **Unspecified** directs the OPC Framework to look for the permission higher up in the hierarchy.

From the **Permissions** tab, when the **Add** button is selected, the **Add Permission** screen is displayed. In the **Server Address Space** screen section, folders and items are shown as nodes are selected and expanded.

Red folders indicate a null branch. This means that the item names below this branch do not contain the branch name, so permissions set on the branch will not reflect on **Add**, **Write**, and **Read** permissions for the items below the branch. To properly set permissions on the items below the branch, they have to be set on the items themselves.

Figure 77 provides an example of a null branch and items below it, all of which are outlined in black.

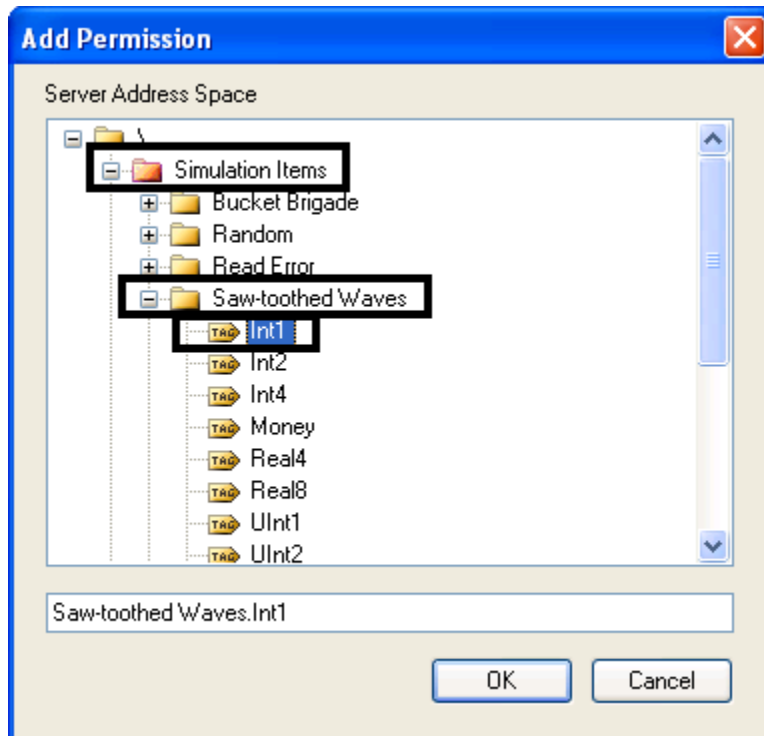


Figure 77 - Add Permission Screen (Server Address Space)

When browsing, using the example in the diagram above, **Simulation Items** is a null branch (identified by the red folder), **Saw-toothed Waves** is a non-null branch, and **Int1** is an item.

Setting permissions on the **Simulation Items** branch does not affect **Read**, **Write**, and **Add** permissions for the **Saw-toothed Waves** branch of the **Int1** item below that. This is because when adding the **Int1** item, the item ID of the **Int1** item is actually **Saw-toothed Waves.Int1** and not **Simulation Items\Saw-toothed Waves.Int1**.

Setting **Read**, **Write**, and **Add** permissions for the **Saw-toothed Waves** branch will affect the items below as **Saw-toothed Waves** is part of the item ID of the **Int1** item (**Saw-toothed Waves.Int1**), and therefore the **Saw-toothed Waves** folder does not appear as a red folder like the **Simulation Items** folder does.

Note: User permissions override group permissions. For example, if a defined group is denied writing privileges to an OPC item, **Random.Int4**, while a defined user (a member of that group) is allowed writing privilege to Random items (**Random.<itemID>**), then the user permissions would take precedence for that OPC item (even though the permissions relating to the group are a better match for the OPC item, **Random.Int4**).

To edit a user's permissions:

1. Click on the **Add** button to begin configuring permissions for the current user.
2. The **Add User Permission** window (Figure 78) appears. This window allows you to browse the OPC server address space to find either a path in the hierarchy, or a particular OPC item.

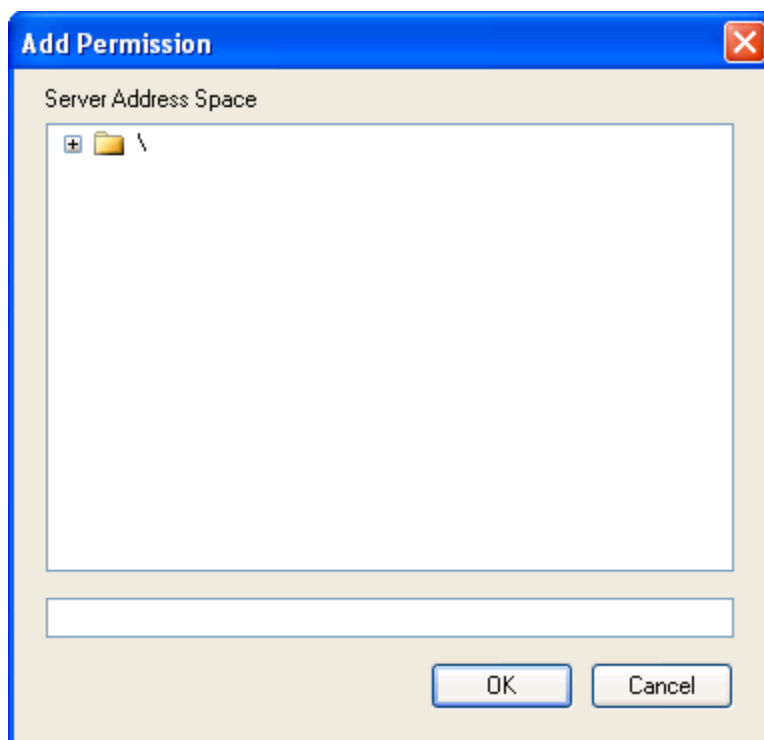


Figure 78 - Add User Permission Window

3. Expand on the server address space's root node and continue to browse to the desired path in the hierarchy, or the desired OPC item.

Note: Branches (i.e., folders) that are red in colour (see Figure 79) are not part of an item's path, but rather are used for browsing organization. Configuring permissions for adding, reading, and writing will not affect items below it. For more information, refer to **Permissions**.

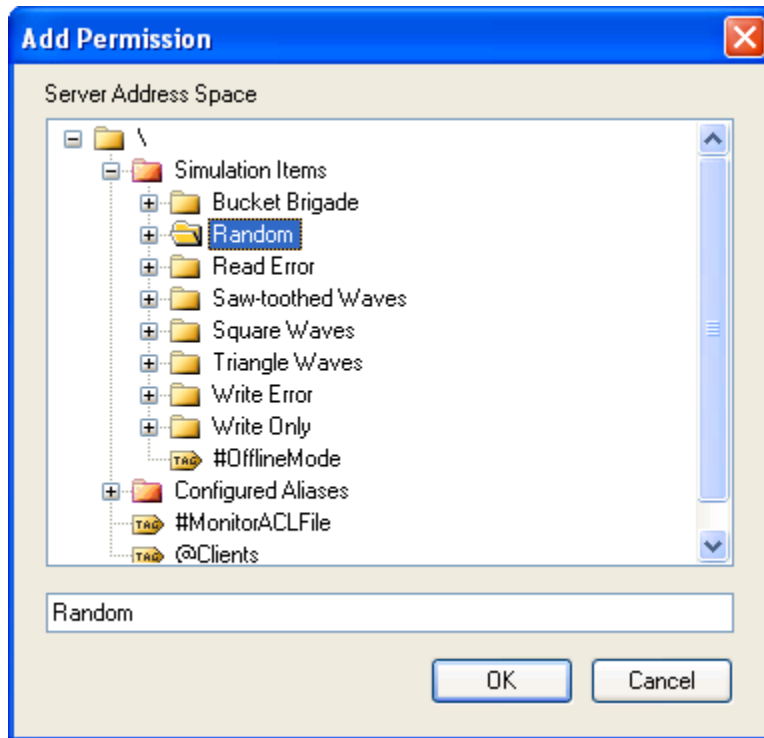


Figure 79 - Add Permission Window: Browsing Server Address Space

4. Click on the **OK** button.
5. The selected path or item will be listed in the **Configured Paths** screen section of the **Edit User** window. Permissions can now be assigned, as in the example depicted in Figure 80.

Note: In this example, **User1** is allowed to browse the **Random** path of the OPC server's address space. Adding privileges are denied, and Reading and Writing privileges are unspecified.

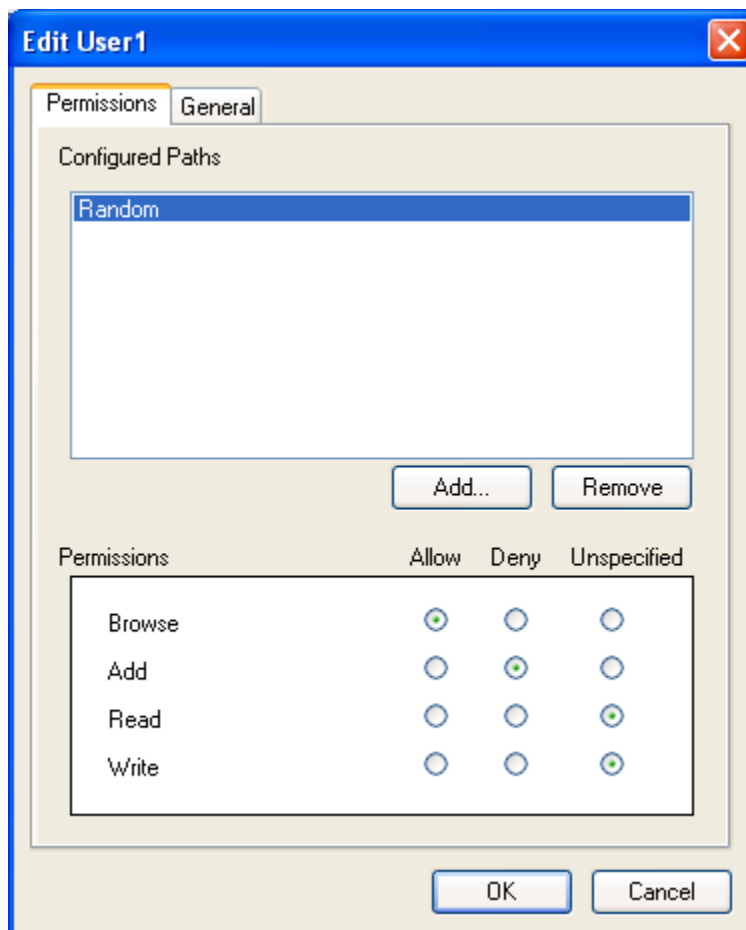


Figure 80 - Edit <Username>: Example

On the **General** tab (Figure 81) of the **Edit <Username>** window, the name and password of the user can be changed.

To edit a user's name:

1. Enter a new name in the **Name** field.
2. Click on the **OK** button.

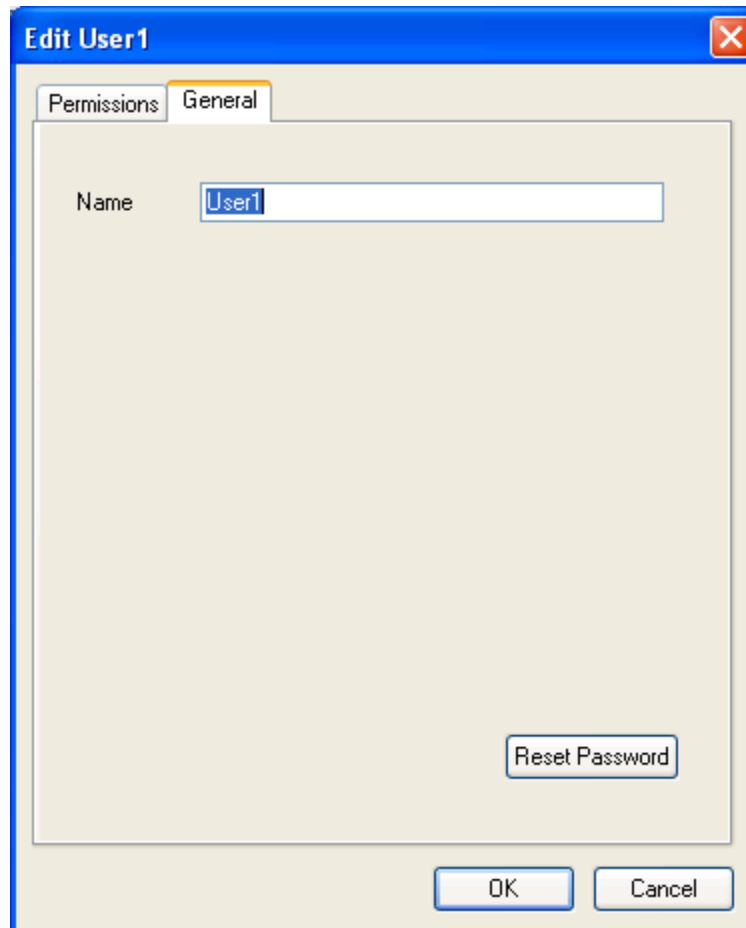


Figure 81 - Edit <Username> Window (General Tab)

To change the user's password:

1. Click on the **Reset Password** button. The **Reset Password** window (Figure 82) appears.

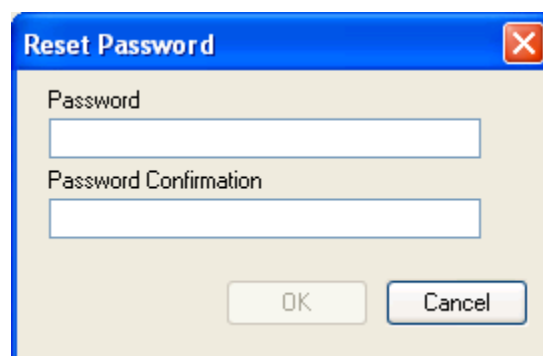


Figure 82 - Reset Password Window

2. Enter the new password in the **Password** field.
3. Re-enter the password in the **Password Confirmation** field.
4. Click on the **OK** button.

Edit Group

To edit a group:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, either:
 - Double-click your mouse on the group you wish to edit, or
 - Right-click your mouse on the required group and select **Edit Group** from the displayed menu, or
 - Click your mouse on the required group and then select the **Edit** button.
2. The **Edit <Groupname>** window (Figure 83) appears.

Notes:

- In this example, the group being edited is **Group1** so the window's title reads **Edit Group1**.
- For Private Groups, there are three tabs on this window: **Permissions**, **General**, and **Members**. For NT Groups, there is only the **Permissions** tab.

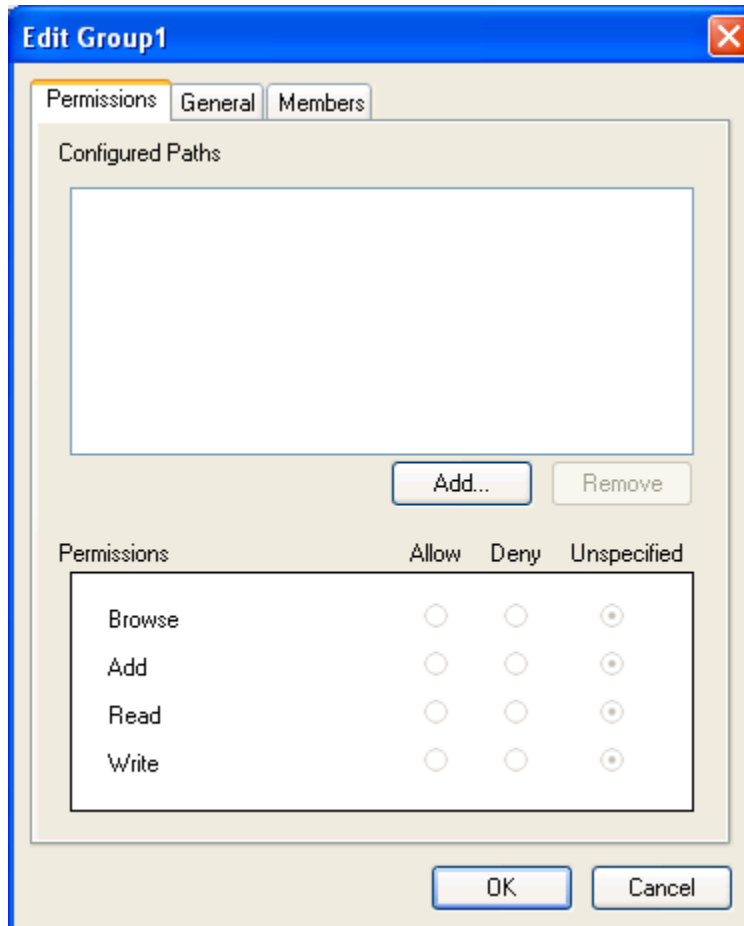


Figure 83 - Edit <Groupname> Window (Permissions Tab)

On the **Permissions** tab, the permissions associated with this group relating to browsing, adding, reading, and writing for any specific paths or OPC items are configured. Refer to the **Edit User** section regarding configuration on the **Permissions** tab. Group and user permissions are configured in the same way.

On the **General** tab (Figure 84) of the **Edit <Groupname>** window, the name of the group can be changed.

To edit a group's name:

1. Enter a new name in the **Name** field.
2. Click on the **OK** button.

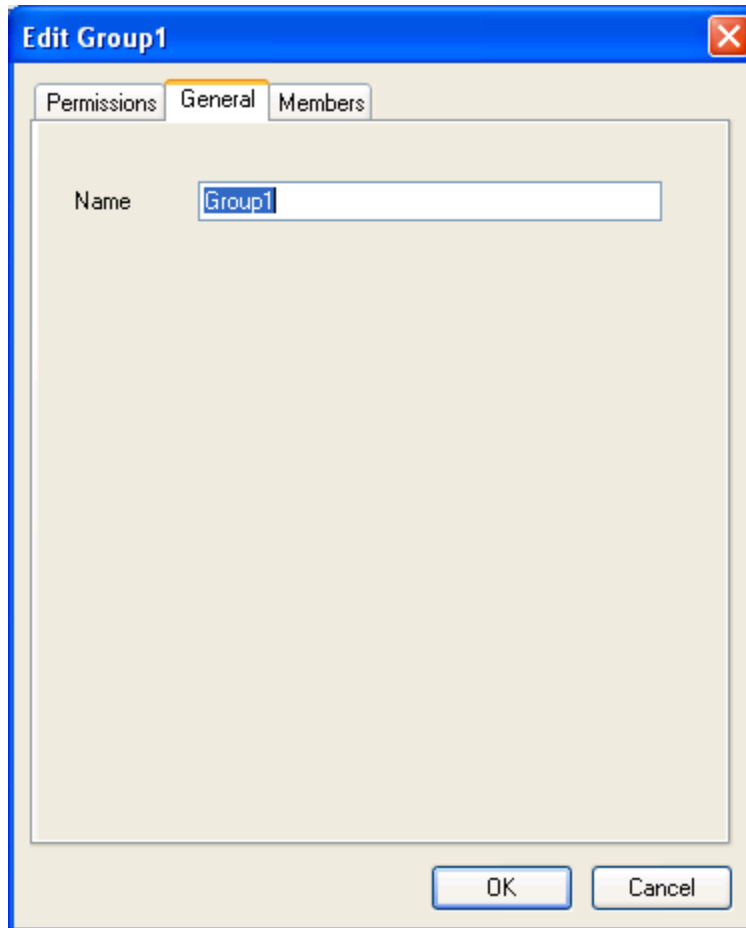


Figure 84 - Edit <Groupname> Window (General Tab)

On the **Members** tab (Figure 85), the users that are part of the current group are defined. By default, the **Group Members** screen section is empty. In Figure 85, **User1** has been added to **Group1**.

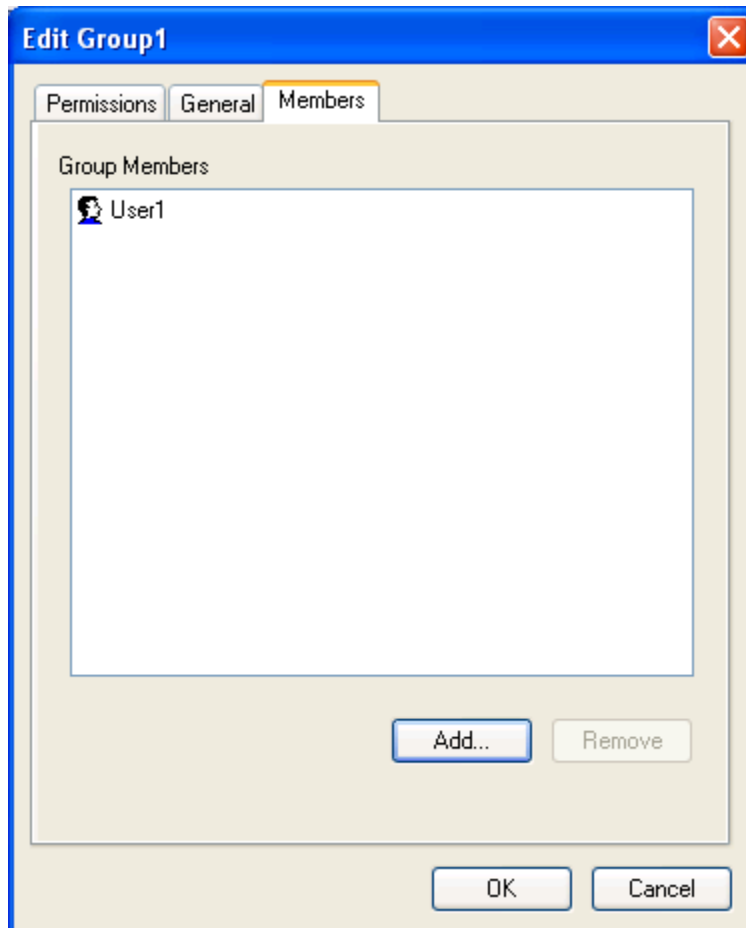


Figure 85 - Edit <Groupname> Window (Members Tab)

To add one or more members to the group:

1. Click on the **Add** button. The **Add Existing User** window (Figure 86) appears.

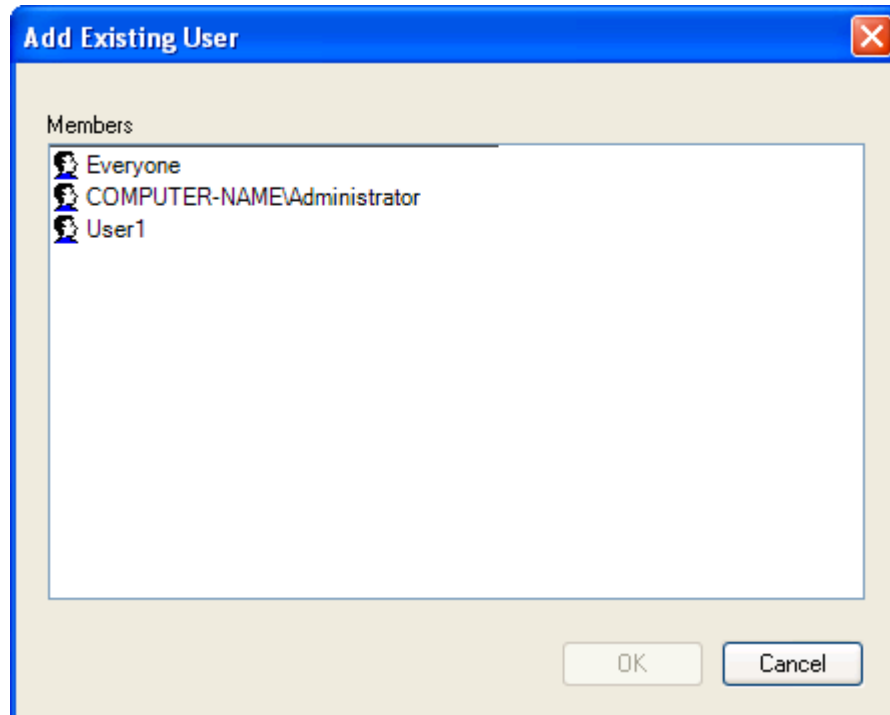


Figure 86 - Add Existing User Window

2. The **Members** screen section lists all the defined users from which you may choose. Select one or more desired users to become members of the group.
3. Click on the **OK** button. The selected user or users appear in the **Group Members** screen section on the **Members** tab (Figure 85).

To remove a user from the group:

1. Select that user in the **Group Members** screen section.
2. Click on the **Remove** button.

Notes:

- If a user name and a group name (to which the user belongs) have permissions defined for the same location, the user name will be used. If a user belongs to two groups that have permissions defined for the same location, the group that is alphabetically first will be used.
- The exact location (full item ID for reading, writing, and adding, or the full path for browsing) is always looked for first when determining the permission for a particular user. If the exact location is not found, or is found but does not contain a defined permission, then the closest match in location is looked at next, and so on. The root location (i.e., empty string) will always match, and is used if no partial location match is made.

Delete

To delete a previously added user or group:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, either:
 - Select the required user or group from the list and click on the **Delete** button (Figure 71), or

- For a group, right-click your mouse on the required group and select **Delete Group** from the displayed menu, or
- For a user, right-click your mouse on the required user and select **Delete User** from the displayed menu

Change Password

To change the security password for the OPC server:

1. From the **MatrikonOPC Security Configuration Utility** main screen, click on the **Change Password** button (Figure 68).
2. The **Change Password** window (Figure 87) appears.



The dialog box titled "Change Password" contains three text input fields. The first field is preceded by the text "Please enter the old password for this OPC Server". The second field is preceded by "Please enter the new password for this OPC Server". The third field is preceded by "Please confirm the new password". To the left of the input fields is a small icon of a padlock. At the bottom right of the dialog are "OK" and "Cancel" buttons.

Figure 87 - Change Password Window

3. Enter the old password for the current OPC server.
4. Enter and confirm the desired new password.
5. Click on the **OK** button.

Note: Changes are applied in the Utility main window by clicking on either the **OK** or **Apply** button.

Examples

This section contains examples of tag security settings made via the MatrikonOPC Tag Security Configuration Utility, and the impact of these settings.

Default

The default tag security configuration provided is quite simplistic as is shown in Table 54:

User/Group	Configured Paths	Browse	Add	Read	Write
Everyone	\	Allow	Allow	Allow	Allow

Table 54 - Default Tag Security

As no users or groups are defined, any NT user connecting to the OPC server will use the **Everyone** default user for permissions. Only the root level location is defined under the **Configured Paths** list, which gives full permissions to the entire OPC server. An administrator will want to change these default settings for the OPC server to provide more security on its tags.

Example 1

Table 55 contains a possible tag security configuration enforces complete restricted access except for the NT user **DOMAIN\Admin**:

User/Group	Configured Paths	Browse	Add	Read	Write
Everyone	\	Deny	Deny	Deny	Deny
DOMAIN\Admin	\	Allow	Allow	Allow	Allow

Table 55 - Example 1

At this point, more users can be added which belong to a more restricted group. This group may be denied write capability or restricted to certain areas in the server hierarchy.

Example 2

Following is an example of a tag security configuration for the MatrikonOPC Server for Simulation and Testing, with sample use-cases. Table 56 lists all defined users and groups and their associated permissions. Table 57 indicates which users are members of the defined groups.

Unspec. permission indicates *Unspecified*. Groups in this example are Private Groups.

User/Group	Configured Paths	Browse	Add	Read	Write
Everyone	\	Allow	Deny	Deny	Deny
Everyone	Configured Aliases	Deny	Unspec.	Unspec.	Unspec.
DOMAIN\john.doe					
DOMAIN\fred.stone					
DOMAIN\sally.simpson					
DOMAIN\the.admin					
Supervisor	\	Deny	Allow	Allow	Deny
Restricted (group)					
Common (group)	\	Allow	Allow	Allow	Deny
Common (group)	Triangle Waves	Deny	Deny	Deny	Deny
Admin (group)	\	Allow	Allow	Allow	Allow
Admin (group)	Bucket Brigade.Int4	Unspec.	Unspec.	Unspec.	Deny

Table 56 - Example 2: Permissions

User/Group	Configured Paths
Restricted	DOMAIN\john.doe
Common	DOMAIN\fred.stone, DOMAIN\sally.simpson
Admin	DOMAIN\the.admin

Table 57 - Example 2: Groups and Members

Tip 1

Adding a user name and not defining any permissions for that user name (or any group it belongs to), will completely restrict their access to information in the OPC server.

Case 1

User **DOMAIN\john.doe** connects. The user is unable to perform any function at any level, since no permissions have been defined for this user name or the **Restricted** group to which it belongs.

Tip 2

Use the root location to define permissions for locations that have not been defined. Use the default user to define permissions for users that are not listed.

Case 2

User **DOMAIN\no.name** connects. This name is not defined so the default user permissions are used. At the root level location, the default user can browse but no more. The only other location where permissions are defined for the default user is **Configured Aliases** – here browsing is denied and adding, reading, and writing permissions are not defined. Thus, **DOMAIN\no.name** will be able to browse the entire server except the **Configured Aliases** branch and all aliases under it. Also, **DOMAIN\no.name** will not be able to do any item addition, reading, or writing. Since item addition, reading, and writing permissions were not defined for the default user for under **Configured Aliases**, it would use the permissions defined at the root level.

Case 3

User **DOMAIN\fred.stone** connects. This user belongs to the defined group **Common**. At the root level, the group Common can browse, add, and read items, but writing is denied. The only other location which defines permissions for this group is **Triangle Waves**. This location has denied all permissions for the **Common** group.

Case 4

User **Supervisor** connects through the private security interface and logs on. This user does not belong to any group, but its name has a root level permission which allows it to add and read items. No other locations have permissions defined. Since the user cannot browse, it will need to know the item syntax for any items it wishes to add and read.

Case 5

User **DOMAIN\the.admin** connects. This user belongs to the **Admin** group, which at the root level has all permissions allowed. The only other location where the **Admin** group has permissions defined, is the full item ID **Bucket Brigade.Int4**. This user is unable to write to that item. However, the root permissions for browsing, adding, and reading the item apply as they are not defined at this level.

Security Details

ACL File

The permissions that the **MatrikonOPC Tag Security Configuration Utility** creates are stored in a file named **ACL.sec** that is located in the same directory as the MatrikonOPC server executable: **C:\Program Files\Matrikon\OPC\< OPC Server Name >**.

ACL.sec is encrypted with 256-bit AES using the password key that was provided during installation (or changed in the security utility).

If **ACL.sec** is missing from its location above, then the OPC server will deny all users access to all browsing, adding, reading, and writing functionality.

Note: It is advised that this file is backed up and stored somewhere safe, once tag security configuration has been completed. In the event that this file is lost or deleted by accident, simply transfer the stored backup (if one was made) to the directory stated above. If **ACL.sec** becomes deleted and no backup was made, tag security will need to be re-configured.

Run-Time Tag Security Configuration

Tag security can be configured and updated while a MatrikonOPC server is running. This run-time security configuration can be controlled using the **#MonitorACLFile** OPC item (found in the root branch when browsing the server).

The **#MonitorACLFile** is a boolean OPC tag that has a default value of **True** when the server starts which indicates that the tag security permissions are monitored and applied while the server is running. By adding this item to an OPC group and writing a value of **False** to this item, the server no longer applies tag security configuration changes while the server is running. The server would need to be stopped and restarted for the changes to take effect.

By disabling the ability of run-time tag security configuration, a malicious user that has access to the machine cannot delete the ACL file and thus remove all user permissions for OPC security. Run-time tag security configuration can be re-enabled when changes to the tag security need to be made, and then disabled again once they have been applied.

Security should be applied to the **#MonitorACLFile** tag so that unauthorized users are unable to control this ability described above.

Client Connections and Private Log On

When an OPC client connects to the server, the OPC Framework impersonates the client and determines the name of the NT user that is running the client. This client name (consisting of the domain name and the user for that domain) is what the OPC Framework uses when checking permissions set in the **MatrikonOPC Tag Security Configuration Utility**. If this NT user was not added in the **Users & Groups** list (Figure 71), then the user **Everyone** is used instead.

If the OPC client chooses to use the *IOPCSecurityPrivate* interface, it must call the *Logon()* function and provide a name and password. The OPC Framework will immediately look for the private user in the **Users & Groups** list (Figure 71). If the user is found and the password provided is correct, the *Logon()* result is successful and the user name provided replaces the NT user that was obtained through impersonation. If not found, the *Logon()* result is failure and the NT user remains as the name used for security permissions. When the OPC client calls *Logoff()*, the NT user becomes the name used for security permissions.

Determining Permission

Whenever a browsing, item addition, read, or write operation is performed by the OPC client, the OPC Framework will call a permission routine to determine if permission is allowed or denied. Three pieces of information are always sent to this routine call:

1. Identity
2. Location
3. Type

Identity is the user name described in the previous section – either the NT domain name, a private name, or the default user **Everyone**. In addition, identity includes any groups (private or NT) that the user belongs to. Location is either the full item ID or a partial path in the server hierarchy. Type is the access type: browsing, item addition, reading, or writing. Each piece of information is checked in the order listed above.

The following information details the procedure used in determining permission rights:

1. Look for a permission match with the NT domain name or private name. This step occurs only if the NT domain name or private name has been defined in the **Users & Groups** list.

2. If a permission match was not yet found, look for one using each group defined in the **Users & Groups** list that the NT domain name or private name belongs to. The first group that contains a permission match will be the one used. An NT domain name does not need to be defined in the **Users & Groups** list for a group it belongs to, to have a permission match. The NT domain name must be part of **Group Members** for private groups, or in the Active Directory for NT groups.
3. If a permission match was not yet found, look for a permission match using the default user **Everyone**.

The procedure used in finding a permission match for a particular identity is as follows:

1. Check whether the exact location is found in the **Configured Paths** list for the **identity**. If found:
 - a. Check whether the permission type (**browse**, **add**, **read**, or **write**) is specified (Figure 80). If the permission type is specified for the action being performed, a match is found and the permission (either allow or deny) is used.
2. If a permission match was not found in step 1a, check whether a partial match of the location is found in the **Configured Paths** list for the **identity**. A partial match is always a sub-string of the given location that starts with the same characters. This represents starting from the root location and moving down the browsing hierarchy.

For example, the location **Random** is a partial match of the full item ID **Random.String**. However, **String** is not a partial match (even if it is a sub-string) because it does not match the first seven characters. The root location **** is considered a partial match for every full item ID.

For each partial match from step 2, apply step 1a. The best partial match (i.e., the one that has the most characters) that is successful in step 1a is the one whose permission is used.

Example

The following is an example of a tag security configuration. Table 58 lists all defined users and their associated permissions.

User/Group	Configured Paths	Browse	Add	Read	Write
Everyone					
DOMAIN\john.doe	\	Allow	Allow	Allow	Allow
DOMAIN\john.doe	Random	Allow	Deny	Deny	Deny
DOMAIN\john.doe	Random.Int	Allow	Allow	Allow	Allow

Table 58 - Example 2: Permissions

The user **DOMAIN\john.doe** wants to read the item **Random.Int4**. The permission routine would not be able to find an exact location match under the **Configured Paths** list. However, it would loop through each partial match in the Configured Paths list looking for a defined permission. The location **Random.Int** would be the closest match and the permission would be **ALLOW**.

The user **DOMAIN\john.doe** wants to read the item **Random.Real4**. The permission routine would not be able to find an exact location match under the **Configured Paths** list. However, it would loop through each partial match in the Configured Paths list looking for a defined permission. The location **Random** would be the closest match and the permission would be **DENY**.

Appendix F Offline Mode

Introduction

Offline mode allows the MatrikonOPC Server Framework to be disconnected to the end device, but still return data as if the data was coming from it. This is useful in two situations:

1. A configuration can be set up with to interact with any hardware, allowing any problems in the configuration to be worked out without having them affect the device.
2. Diagnosing problems becomes much simpler when an implementer can remove the device hardware from the architecture.

Offline mode can be applied to the entire configuration of a MatrikonOPC server or to a portion of it.

Offline Mode Toggling

A Boolean control item, named **#OfflineMode**, is provided at each branch in a MatrikonOPC server browsing hierarchy. Adding this item will allow an OPC client to monitor the offline mode for that location using read operations and provide the ability to toggle offline mode for that location using write operations.

When reading the item **#OfflineMode**, the value **True** represents enabled and the value **False** represents disabled. Likewise, writing a value of **True** to **#OfflineMode** enables offline mode and writing a value of **False** to **#OfflineMode** disables offline mode. When offline mode is toggled at a particular location in the hierarchy, it also toggles offline mode for all branches underneath it in hierarchy. For example, if offline mode was enabled at the root in the hierarchy, every branch would have its offline mode enabled. Upon server start-up, every branch has the **#OfflineMode** item set to **False** (i.e., offline mode is disabled).

Offline Mode Item Values

When offline mode is enabled at a particular location in the browsing hierarchy, all OPC items at that location generate random values according to their data type (the **Date** data type is the one exception to this). Table 59 shows the value behavior for each data type:

Data Type	Behavior
Boolean (VT_BOOL)	True or False .
Character (VT_I1)	Value between -128 and 127 .
16-bit Integer (VT_I2)	Value between -32768 and 32767 .
32-bit Integer (VT_I4 and VT_INT)	Value between -2147483648 and 2147483647 .
Byte (VT_UI1)	Value between 0 and 255 .
Word (VT_UI2)	Value between 0 and 65525 .
Double Word (VT_UI4 and VT_UINT)	Value between 0 and 4294967295 .
Float (VT_R4)	Value between -13388.5962 and 13388.5962 .
Double (VT_R8)	Value between -8345.512588035 and 8345.512588035 .
Date (VT_DATE)	Current system time.

Data Type	Behavior
String (VT_BSTR)	<i>Simulated</i> or <i>Data</i> .

Table 59 - Offline Mode Item Values

Operational Effects

When offline mode is enabled at a particular location in a server's hierarchy, there is no communication between the server and the end-device/application to which the location refers.



Note: Some servers allow communication to multiple devices/applications. To ensure there is no communication in the entire server, offline mode should be enabled at the root level.

To ensure that there is no communication when offline mode is enabled, the MatrikonOPC Server Framework will disable the object associated with that branch. When an object is disabled due to offline mode, the **Enabled** checkbox will be cleared (i.e., unselected) in its panel within the configuration utility. Enabling the object will have no effect while the object has offline mode enabled. When offline mode is disabled for that particular object, the MatrikonOPC Server Framework will re-enable it and the **Enabled** checkbox will be selected (i.e., checked) once again.

Appendix G SCADA Servers Connection Logic

Introduction

In MatrikonOPC SCADA servers the data is polled in a round-robin mechanism (as long as the items belong to the same Channel Device link). This means that the OPC items will be scanned in sequence depending on the unit device links to which they belong. If one of the device links fails, then the server will apply the retry sequence on this device link. If after applying the retry sequence, the device link is still failing, the server will move to the next device link in the sequence. The failing device link will be treated differently then the rest of the working device links based on the failure and reconnection logic settings that were entered for that particular device link.

Polling

Polling is described as the operation where the server requests and extracts data from the device. As explained in the Introduction section of this appendix, polling is done in a round-robin mechanism depending on which device links are currently being scanned.

Every Channel device link does its own polling for all of its sub-device links. If your server configuration contains multiple Channel device links then they will do the polling independently of each other.

Note: If a unit device link does not have any items added by an OPC client, it will disconnect until a client requests items that belong to that unit device link. Some servers, like the MatrikonOPC Server for SCADA DNP3, may have an option to force a unit device link to stay connected at all times.

Connection Failures and Reconnection Logic

In the case of a connection failure, the reconnection logic (meaning the timeout values, retries counts, and other related options) applied will depend on the type of device link that failed.

Example:

Suppose in our configuration we have a Network Channel device link called **Channel**. Under the Network Channel device link we have a Network Host device link named **Host**. Under the Host device link we have multiple unit device links (**U1**, **U2**).

If failure happens due to an IP Address problem, the reconnection logic applied will depend on the values and options defined in the **Host** device link.

If a failure happens due to a Unit Address problem, the reconnection logic parameters will be those defined in the unit device link that failed.

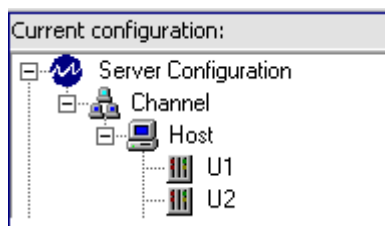


Figure 88 - Example

Appendix H Features and Examples

Introduction

This appendix describes the common features and newest enhancements added for the MatrikonOPC Server for SCADA DNP3, complete with examples.

Round-Robin Example

As explained in **Appendix G – SCADA Servers Connection Logic**, all of the MatrikonOPC SCADA servers poll in a round-robin mechanism. The MatrikonOPC Server for SCADA DNP3 is not an exception to that. The best way to explain that is by an example:

Example 1 (Unit Device Link Failure)

Suppose your OPC client is currently scanning the following items (or tags):

- **A1, A2, and A3** from device link **Unit A**
- **B1, B2, and B3** from device link **Unit B**
- **C1, C2, and C3** from device link **Unit C**.

During polling, scanning will go through device link **Unit A** followed by device link **Unit B**, and finally device link **Unit C**. The items are then read in the following order:

A1, A2, A3, B1, B2, B3, C1, C2, C3

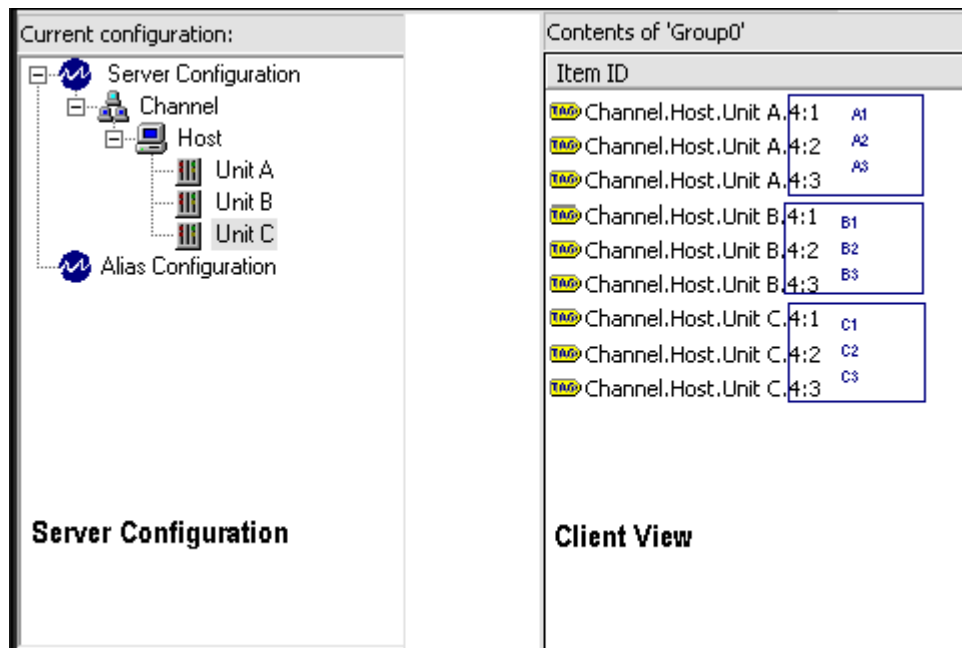


Figure 89 - Example 1

Suppose that the communication on **Unit B** failed for any reason. For this example, we will imagine that the failure came from the unit device link itself and that all of its parent device links are fine. In the next polling cycle, items **A1, A2, and A3** are scanned and the server identifies the fact that there is a problem accessing the items that belong to **Unit B**. The server then applies the number of connection retries defined in the **Retries** field on the **Data Acquisition** tab.

After the specified number of retries is consumed, scanning will continue on to the next device link, and then the next, in order. In the next polling cycle, if **Unit B** is still failing the server will check

the **Failed Polls Allowed** option on the **Data Acquisition** tab. This option is used to specify how many more cycles the server will try the number of retries defined in the **Retries** field before determining the connection has failed and setting the **Quality** for all to **Bad, Last Known Value**.

After the number of poll cycles defined in the **Failed Polls Allowed** field has elapsed, the device link will no longer be in the polling sequence. This means that **Unit C** will be scanned directly after **Unit A**, and **Unit B** will be skipped.

At this point the server will check the **Reconnect delay** option defined in **Unit B** and it will only try to connect to **Unit B** at that delay interval. That is, if **Reconnect delay** is set to **X**, the server will try to connect to **Unit B** every **X** seconds. Then, every time the server tries to connect to **Unit B** it will apply the number of retries defined in the **Reconnect retries** field.

The previous scenario can be summed up in the following steps:

1. **Unit B** disconnects due to a communication failure.

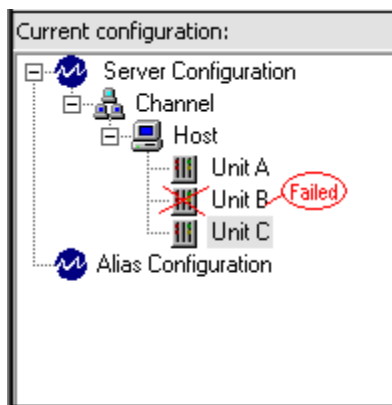


Figure 90 - Unit B Fails

2. The retry sequence is applied to **Unit B** and the server continues scanning the remaining device links.

Retries and Allowed Polls

Retries:

Reconnect retries:

Failed polls allowed:

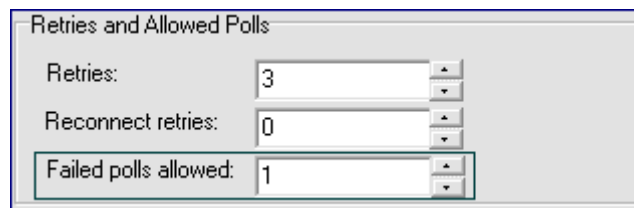
Item ID	Value	Quality
Tag Channel.Host.Unit A.4:1	4	Good, non-specific
Tag Channel.Host.Unit A.4:2	5	Good, non-specific
Tag Channel.Host.Unit A.4:3	0	Good, non-specific
Tag Channel.Host.Unit B.4:1	4	Good, non-specific
Tag Channel.Host.Unit B.4:2	5	Good, non-specific
Tag Channel.Host.Unit B.4:3	0	Good, non-specific
Tag Channel.Host.Unit C.4:1	4	Good, non-specific
Tag Channel.Host.Unit C.4:2	5	Good, non-specific
Tag Channel.Host.Unit C.4:3	0	Good, non-specific

Retry sequence will be applied for items that belong to unit B

Quality will stay Good as long as the Failed Polls Allowed counter has not been exceeded.

Figure 91 - Retry Applied on Unit B Items

3. The server checks the **Failed Polls Allowed** counter. If the counter has not yet been exceeded, the same retry sequence is applied to **Unit B** in the next poll, and the **Quality** for the items stay **Good**.



Retries and Allowed Polls

Retries: 3

Reconnect retries: 0

Failed polls allowed: 1

Figure 92 - Failed Polls Allowed Counter

- After the **Failed Polls Allowed** counter has been exceeded, the **Quality** of the those items that belong to **Unit B** will change to **Bad** and it is removed from the polling sequence.

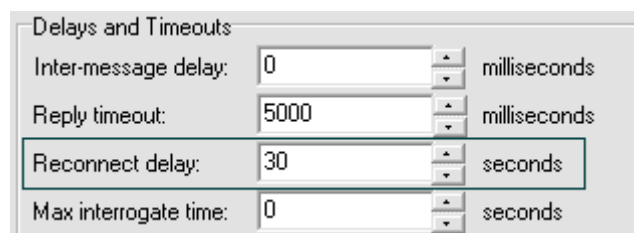
Item ID	Value	Quality
 Channel.Host.Unit A.4:1	4	Good, non-specific
 Channel.Host.Unit A.4:2	5	Good, non-specific
 Channel.Host.Unit A.4:3	0	Good, non-specific
 Channel.Host.Unit B.4:1	4	Bad, last known value
 Channel.Host.Unit B.4:2	5	Bad, last known value
 Channel.Host.Unit B.4:3	0	Bad, last known value
 Channel.Host.Unit C.4:1	4	Good, non-specific
 Channel.Host.Unit C.4:2	5	Good, non-specific
 Channel.Host.Unit C.4:3	0	Good, non-specific

After the Failed Polls Allowed counter has been exceeded, the Quality will go to *Bad* and Unit B will be removed from the polling sequence.

Client View

Figure 93 - Unit B Confirmed Failure

- The server checks the **Reconnect delay** interval and if it passes, the server tries to reconnect to **Unit B** again.



Delays and Timeouts

Inter-message delay: 0 milliseconds

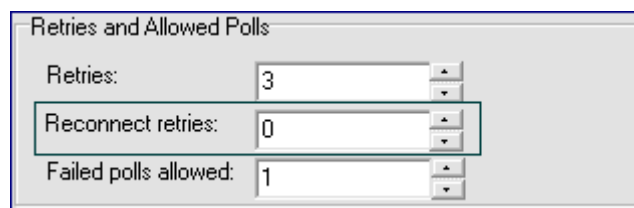
Reply timeout: 5000 milliseconds

Reconnect delay: 30 seconds

Max interrogate time: 0 seconds

Figure 94 - Reconnect Delay

- Thereafter, the number of retries applied is that which has been defined in the **Reconnect retries** field of **Unit B**.



Retries and Allowed Polls

Retries: 3

Reconnect retries: 0

Failed polls allowed: 1

Figure 95 - Reconnect Retries

Note: The reconnection logic applied depends on which type of device link failed to connect. For example, if what fails is the Modbus Unit address (defined in the unit device link) then the reconnection logic applied will depend on the options defined in the unit device link. On the other hand, if what fails is the Socket then the reconnection logic applied will depend on the options defined in the Network Host device link.

Writes OPC Item

Under any Channel device link, there is an OPC item called **Writes**. This OPC item was designed to prevent the writes from taking up the whole channel bandwidth. This item can be accessed and edited through OPC. This item indicates the number of successive writes allowed before forcing the next poll in the queue for that specific Network Channel. If the value of that item is set to **0** then the feature will be turned off. After the forced poll is completed, the server will reschedule the polls for that specific network channel starting now.

Example:

Suppose the OPC client is currently scanning items **A**, **B**, and **C** from the **Network Channel**, as well as the **Writes** OPC item. Suppose the OPC client's update rate is set to **23** seconds.

Assume we performed the following actions:

- Wrote **10** in the **Writes** OPC item.
- Wrote **4** successive values in **Item A** in a time span of 4 seconds.
- Wrote **3** successive values in **Item B** in a time span of 3 seconds.
- Wrote **5** successive values in **Item C** in a time span of 5 seconds.

Since the client's update rate is 23 seconds, the data is requested from the client every 23 seconds, which means polling happens every 23 seconds.

The server will perform the 4 successive writes to **Item A**, then 3 successive writes to **Item B**, and then it will do only 3 of the 5 writes to **Item C**. The server then forces the next poll to occur immediately instead of waiting for it until 10 writes have passed. The polls are then rescheduled for this specific Network Channel starting now, meaning the next poll will happen exactly 23 seconds from now, and so on.

PacketSent and PacketReceived OPC Items

PacketSent and **PacketReceived** OPC items are found only under the unit device links and they can only be accessed through OPC. The **PacketSent** item shows the last packet that was sent from the server in a hexadecimal format. The **PacketReceived** OPC item shows the last packet that was received from the device in a hexadecimal format.

 Nc.H2.U.PacketReceived	02 03 0A 00 00 00 00 00 00 00 00 04	Good, non...	01/06/200...	Active
 Nc.H2.U.PacketSent	02 36 00 00 00 06 02 03 00 00 00 05	Good, non...	01/06/200...	Active

Figure 96 - Packets Sent and Received at a Certain Point

Note: These OPC items update at the rate the client requests. So, if the packets are sent out or received faster than the update rate, the OPC client will miss some of the hexadecimal data.

Total Reads and Writes Indicators

For any type of device link in the MatrikonOPC Server for SCADA DNP3, there are four OPC items (or counters) that can be used to monitor the total number of write or read request packets that are being sent by the server. This is also the case for the total number of reply packets received from the device. Those items are accessible through OPC and can be found under any type of a device link. The four items are defined as follows:

- **TotalReadsSent** - the number of read request packets sent by the server through this specific device link until now.
- **TotalReadsReceived** - the number of reply packets received from the device until now, in response to the read requests.
- **TotalWritesSent** - the number of write request packets sent by the server through this specific device link until now.
- **TotalWritesReceived** - the number of reply packets received from the device until now, in response to the write requests.

Figure 97 shows an example where the number of packets is being monitored for every type of device link. The server configuration being used contains the Network Channel device link **Nc**, the Network Host device link **H2** and the Modbus Unit device link **U**.

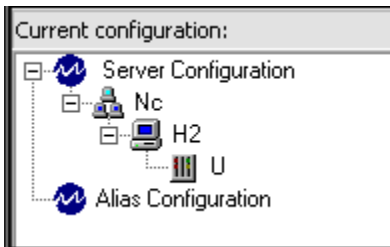


Figure 97 - Server Configuration

Item ID	Access Path	Value	Quality	Timestamp	Status
Nc.H2.TotalReadsReceived		5620	Good, non-specific	01/06/2009 12:23:21.020 PM	Active
Nc.H2.TotalReadsSent		2811	Good, non-specific	01/06/2009 12:23:21.005 PM	Active
Nc.H2.TotalWritesReceived		2	Good, non-specific	01/06/2009 11:37:00.170 AM	Active
Nc.H2.TotalWritesSent		1	Good, non-specific	01/06/2009 11:37:00.154 AM	Active
Nc.H2.U.TotalReadsReceived		5620	Good, non-specific	01/06/2009 12:23:21.020 PM	Active
Nc.H2.U.TotalReadsSent		2811	Good, non-specific	01/06/2009 12:23:21.005 PM	Active
Nc.H2.U.TotalWritesReceived		2	Good, non-specific	01/06/2009 11:37:00.170 AM	Active
Nc.H2.U.TotalWritesSent		1	Good, non-specific	01/06/2009 11:37:00.154 AM	Active
Nc.TotalReadsSent		2811	Good, non-specific	01/06/2009 12:23:21.005 PM	Active
Nc.TotalWritesReceived		2	Good, non-specific	01/06/2009 11:37:00.170 AM	Active
Nc.TotalWritesSent		1	Good, non-specific	01/06/2009 11:37:00.154 AM	Active
Nc.Totalreceived		2811	Good, non-specific	01/06/2009 12:23:21.020 PM	Active

Figure 98 - Monitoring Request and Reply Counters from the Client

In Figure 98 we can see that the number of read packets sent by **Nc.H2.U** (which is the full path of the unit device link **U**) was **2811**. The same unit device link received **5620** packets meaning that for every request packet being sent by the server, there is an average of approximately **2** reply packets received from the device.

We can also see that the total number of write requests that was sent by the server (i.e., **TotalWritesSent**) is **1** which means that only one write operation was done up until this point. This write operation had **2** reply packets received from the device to indicate success or failure.

In this example, the values of those counters were the same for the different type of device links. It should be noted that is not always the case. If the Network Host device link had two unit device links being scanned instead of one, the values of the counters on the Network Host device link will be more than those of its individual unit device links. This is because it will be the summation of the number of packets of all of its sub-device links that are currently being scanned by the OPC client.

Note: The qualities of any of the four OPC items will be **Bad** until a write or a read operation is completed for the device link to which they belong.

Appendix I OPC Items

Introduction

This appendix explains the OPC items that can be found in SCADA servers and what they are used for.

Base OPC Items

These OPC items are found in the Root Device Link of the server. This link is the root for all of the configured device links.

OPC Item	Description
#MonitorACLFile	A Boolean that indicates if the server is currently monitoring the Access List file or not (i.e., if the security is enabled or not).
@Clients	A string the shows the clients the server is currently connected to.
Purge	If 1 is written to that item, all of the device links that are marked for deletion will be removed as long as they are neither enabled nor connected to a client.

Table 60 - Root Device Link OPC Items

Generic OPC Items

OPC Item	Description
Bpsin	Number of bytes received by the server per second.
Bpsout	A counter indicating the number of bytes sent from the server per second.
Broadcast	Number of broadcast packets sent until now.
Bytesin	Number of bytes received by the server until now.
Bytesout	Number of bytes sent from the server until now.
Checksumerror	A counter indicating the number of times a check sum error or invalid response occurs.
Commfail	A Boolean that indicates whether communication failed or not on that specific device link. This option exists in all types of device links
Configuration	Shows the configuration for that type of device link in a string format. This option exists for all types of device links
Connected	A Boolean that indicates whether that specific device link is connected or not.
Currentunit	Indicates the full path for the unit device link in a blank string that is currently polling. It should be noted that if the polling operation is very fast, you might not have a chance to see the value because when the polling is done the value returns to a blank string.
Deleted	Disables the device link and mark it for deletion.
Description	Description defined for the current device link.
Enabled	Indicates whether the device link is enabled or not.
Errorresponse	The number of errors received from the device until now for the current

	object.
Failure	Number of failures that happened up until now, for the current object. The same value can be seen in the server's GUI in the lower left-hand side under the name Failed .
Incomplete	A counter indicating the number of incomplete responses from the device.
Invalid	A counter that indicates the number of invalid or incomplete responses from the server.
Lastresponse	A timestamp that shows the time of the last response received from the device.
Lastsent	A timestamp that shows the time the last packet was sent to the device.
Name	The name of the current object.
Noresponse	A counter that increments when there is no response from the device.
Overrun	A counter that indicates the number of overruns that happened up until now. This counter can also be seen in the server's GUI the lower left-hand side.
Precentreturn	The percentage of number of packets received compared to the number of packets sent.
Percentvalid	The percentage between (the total packets initially sent + the retries) and (the total packets received + the error responses).
Pollcomplete	The number of polls completed up until now.
Received	The number of packets received up until now.
reconnectDelay	The value set for the reconnect delay option in the server's GUI.
Resetstats	Resets the statistics of the server.
Retried	A counter for the number of retries accomplished up until now.
Scan	A Boolean that is True if the object is currently scanning.
Sent	A counter that indicates the number of packets sent from this object up until now. This option can only be seen in the lower left-hand side of the server's GUI.
TimeOut	A counter indicating the number of timeouts.
TotalReadsReceived	The total number of read packets received to the current object up until now.
TotalReadsSent	The total number of read packets sent from the current object up until now.
TotalWritesReceived	The total number of write packets received to the current object up until now.
TotalWritesSent	The total number of write packets sent from the current object up until now.
Totalsent	Total number of packets sent from the current object and any sub-objects.
Totalreceived	Total number of packets received to the current object and any sub-objects.
Unsolicited	A counter indicating the number of unsolicited messages.

Table 61 - Generic OPC Items

Network Channel Object OPC Items

OPC Item	Description
InterDeviceDelay	An OPC item that gives access to the Inter-Device Delay option which allows you to enter a value specifying the minimum amount of time (in milliseconds) between the last response from one unit, and the next request to another unit on this channel.
LogRx	An OPC item that gives access to the Log bytes received option which shows the hexadecimal format of the packets received in the log file (-1 means the option is enabled and 0 means the option is disabled).
LogTx	An OPC item that gives access to the Log bytes transmitted option which shows the hexadecimal format of the packets sent in the log file (-1 means the option is enabled and 0 means the option is disabled).
MaxUnsolicited	Maximum unsolicited messages allowed. Default is 2048 .
MinUnsolicited	Minimum unsolicited messages allowed. Default is 4 .
Writes	This OPC item is fully explained in Appendix H – Features and Examples .
Scheduleallpolls	This OPC item allows access to the Schedule all polls checkbox in the server's GUI.
Threshold	This OPC item allows access to the Threshold rate field in the server's GUI. The OPC item is measured in milliseconds, whereas the field itself in the server's interface is in seconds.

Table 62 - Network Channel OPC Items

Network Host Object OPC Items

OPC Item	Description
SocketTO	The value of the socket timeout. This is the same as the Socket timeout field in the server's GUI for the network host object.
Host	The IP address of the remote device. This is the same as the Host name/IP field in the server's GUI for the network host object.
Service	The port number of the remote device. This is the same as the Service name/port field in the server's GUI for the network host object.
Reconnectdelay	The reconnect delay configured for the connection. This is the same as the Reconnect delay field in the server's GUI for the network host object.

Table 63 - Network Host OPC Items

Fail-Over Channel Object OPC Items

OPC Item	Description
Name	User name assigned to the object, which becomes an element of the item ID for data items. Automatically converted to title case for display purposes.
Enabled	Enables or disables communication for the object.
Description	User-defined text (64-character maximum) for documentation purposes.

Configuration	Shows the configuration for the Fail-Over Channel object.
----------------------	---

Table 64 - Fail-Over Channel OPC Items

Serial Channel Object OPC Items

OPC Item	Description
Name	User name assigned to the object, which becomes an element of the item ID for data items. Automatically converted to title case for display purposes.
Enabled	Enables or disables communication for the object.
Description	User-defined text (64-character maximum) for documentation purposes.
Device	This OPC item allows you to enter the COM port number for the connected device.
Baud	This OPC item is for entering the Baud rate of the communication through OPC. Values range between 110 and 256000 . Default = 9600 .
Parity	This OPC item displays and allows selecting the type of parity to be used. Options available are 0-none , 1-odd , 2-even , 3-mark , and 4-space . Default = none .
Databits	This OPC item is for entering the number of data bits through OPC. Values range between 4 and 8 . Default = 8 .
Stopbits	This OPC item is for entering the number of stop bits through OPC. Values available are 1 , 1.5 , and 2 . Default = 1 .
RTScontrol	Same as the RTS Line option in the GUI. Select a Request To Send (RTS) preset. Available options are 0-disable , 1-enable , 2-handshake , and 3-toggle . Default = disable .
DTRcontrol	Same as the DTS Line option in the GUI. Allows you to select a Data Terminal Ready (DTR) Available options are 0-disable , 1-enable , and 2-handshake . Default = disable .
OutxDsrFlow	This OPC item allows you to enable or disable Data Set Ready (DSR) flow control. Default = 0 . A value of -1 indicates that the option is enabled and a value of 0 indicates the option is disabled.
DSRsensitivity	This OPC item allows you to enable or disable Data Set Ready (DSR). Default = 0 . A value of -1 indicates that the option is enabled and a value of 0 indicates the option is disabled.
OutxCtsFlow	This OPC item allows you to enable or disable Clear To Send (CTS) flow control. Default = 0 . A value of -1 indicates that the option is enabled and a value of 0 indicates the option is disabled.

OPC Item	Description
OutxOnOffFlow	This OPC item allows you to enable or disable XON/XOFF software flow control. Default = 0 . A value of -1 indicates that the option is enabled and a value of 0 indicates the option is disabled.
Interdevicedelay	This OPC item allows you to enter a value specifying the minimum amount of time (in milliseconds) between the last request/response to/from one unit and the next request to another unit on this channel. If this OPC Item is set to 0 then the option will be disabled. Default = 0 .
Reconnectdelay	This OPC item allows you to enter a value specifying the minimum amount of time (in seconds) to wait before attempting to recover communications after the communication channel itself has failed. Default = 1 .
Threshold	This OPC item allows you to enter a value specifying the maximum achievable scan interval (in seconds) for the circuit. The server polls items with update rates faster than this on a continuous basis. Changing this option requires the server re-optimize communications with all units on this channel. If it is set to 0 then the option is turned off. Default = 0 . Note: All units on the channel must re-optimize if this parameter changes.
ScheduleAllPolls	This OPC item is the same as the Schedule all polls option in the server's GUI. When this option is enabled, rather than polling them continuously, the server schedules items with update rates faster than the threshold rate to poll at the threshold rate. Default = 1 .
ReadIntervalTimeout	This OPC item allows you to enter a value specifying the maximum amount of time (in milliseconds) between the reception of one character and the arrival of the next. A value of 0 indicates no limit. Default = 0 .
backoffDelay	This OPC item allows you to enter a value specifying the minimum amount of time (in milliseconds) for DCD to be low before transmitting to avoid collisions. Set both backoff delay and backoff random items to 0 to ignore DCD. Default = 0 .
backoffRandom	This OPC item allows you to enter a value specifying the maximum amount of extra random time (in milliseconds) for DCD to be low before transmitting. Set both backoff delay and backoff random items to 0 to ignore DCD. Default = 0 .

Table 65 - Serial Channel Object OPC Items

Radio Object OPC Items

OPC Item	Description
Name	User name assigned to the object, which becomes an element of the item ID

OPC Item	Description
	for data items. Automatically converted to title case for display purposes.
Enabled	Enables or disables communication for the object.
Description	User-defined text (64-character maximum) for documentation purposes.
Keyup	This OPC item allows you to enter a value defining the minimum amount of time (in milliseconds) to wait after setting the RTS signal to allow the transceiver to "warm up".
keydown	This OPC item allows you to enter a value defining the minimum amount of time (in milliseconds) to wait before clearing the RTS signal to allow the transceiver to "cool down".

Table 66 - Radio Object OPC Items

Dial-Up Object OPC Items

OPC Item	Description
Answered	Indicates that a call has been answered.
Busy	Indicates that the line was busy.
Carrier	A Boolean that indicates if there is a carrier for the Dial-Up object or not.
Dialout	Indicates that a dial out occurred.
Lastanswered	The date of the last time a call was answered.
Lastdialout	The date the last time a dial out occurred.
Lastresponse	The date of the last response.
Lastsent	Last sent time.
Nocarrier	Indicates that no carrier was found in the response.
Nodialtone	Indicates that there is no dial tone.
Noresponse	Indicates that there is no response.
Percentanswered	The percentage of calls answered based on the number of dial outs.
Name	User name assigned to the object, which becomes an element of the item ID for data items. Automatically converted to title case for display purposes.
Enabled	Enables or disables communication for the object
Description	User-defined text (64-character maximum) for documentation purposes.
Dial	This OPC item allows you to enter any valid sequence of characters that can follow an ADT command.
PostConnectDelay	This OPC item allows you to enter a value specifying the minimum amount of time (in seconds) to wait after establishing a dial-out connection before transmitting.
Redials	This OPC item allows you to enter a value defining the maximum number of times to redial a connection before concluding that communication has failed with the units on that connection.

ReconnectDelay	This OPC item allows you to enter a value specifying the minimum amount of time (in seconds) to wait before attempting to recover communications after communication has failed with the connection.
ReconnectRedials	This OPC item allows you to enter a value defining the maximum number of times to redial when trying to reconnect after communication has failed with a dial-up connection.
Reset	This OPC item allows you to select a modem reset command. This command is sent before initialization commands.
ResetDelay	This OPC item allows you to enter a value specifying the amount of time (in milliseconds) to wait after the reset command completes.
Initialize	This OPC item allows you to enter modem initialization command or commands, issued before dialling out and after hanging up. The command should always end with <i>EOQOV1</i> .
CommandRetries	This OPC item allows you enter a value to define the maximum number of times to resend a command wait for a response before concluding that communication has failed with the modem.
CommandTimeout	This OPC item allows you to enter a value defining the maximum amount of time (in seconds) to wait for the modem to respond to AT commands with a valid result code.
DialTimeout	This OPC item allows you to enter a value defining the maximum amount of time (in seconds) to wait for the modem to receive a carrier from the dialed connection before aborting the call.
HangupTimeout	This OPC item allows you to enter a value defining the maximum amount of time (in seconds) to wait for the modem to hang up after issuing the ATH0 command.
Idle timeout	This OPC item allows you to enter a value defining the maximum amount of time (in seconds) to allow an idle connection to continue (i.e., no communication) before hanging up.
CarriageReturn	This item is the same as the Command terminator option in the GUI. Allows you to enter or select a value defining an ASCII character to be used to terminate commands and responses (usually a carriage return).
EscapeCharacter	This OPC item allows you to enter a value defining an ASCII character that is sent three times to escape into command mode (usually a plus sign).
EscapeGuardTime	This OPC item allows you to enter or select a value defining the amount of time (in milliseconds) to wait before and after sending the escape sequence.

Table 67 - Dial-Up Object OPC Items