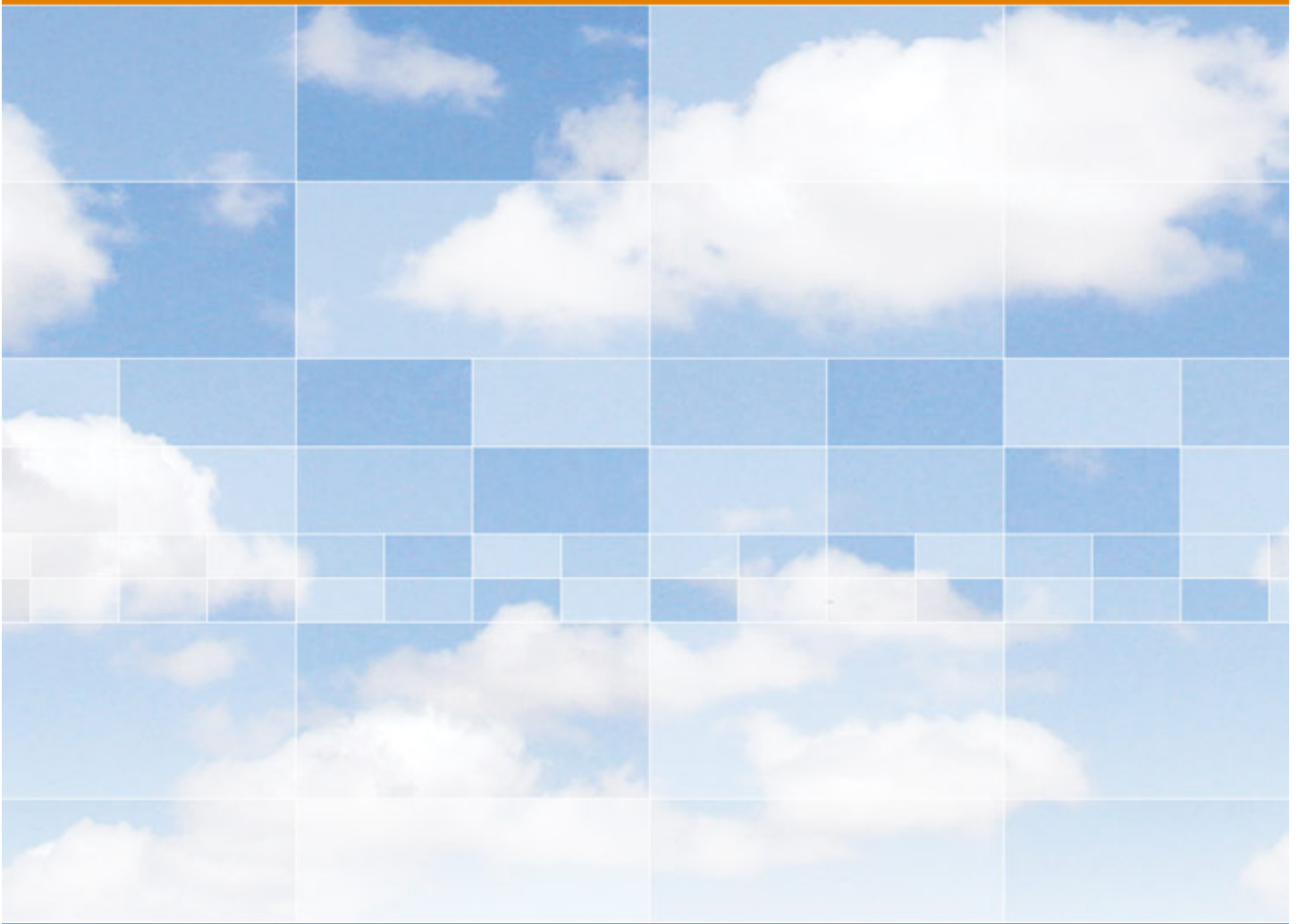




MatrikonOPC Server for IEC 60870

User's Manual

MatrikonOPC Server for IEC 60870

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
2003-02-25	1.0	Initial document.	JC
2007-05-09	2.0	Converted to new template, general edit, updated to reflect functionality changes.	LB
2007-10-02	3.0	Updated software version, added analyzer install note to Installation section, added Expression Wizard information.	JFY
2008-11-10	3.1	Updated to software version 1.0.3.1.	BS
2009-01-22	4.0	Updated to software version 1.0.4.0. Implemented Security and Framework changes. Updated the Installation section. Updated the Configuration Window screenshot to display the View Tags and Security Settings icons. Updated Tools Menu Commands table to include descriptions of View Tags and Security Settings icons. Updated Un-Installation section. Added Security and Offline Mode appendixes. Common and IEC60870 folders updated in Installed Files section. Added Server Status List Device Link OPC Items table to OPC Data Items section. Added Creating and Configuring a Server Status List Object to Configuration section. Added Getting Data without Being Connected to a Device to OPC Data Items section.	CGAP, LB

2009-09-15	5.0	Updated to software version 1.0.5.0. Added Beta tag lines. Added item about treating unsigned integer values as Booleans to Troubleshooting section. Removed DEP settings point from note in Installation section. Updated Contacting Support section. Updated Appendix A – Distributed COM (DCOM) introduction.	DOC, LB
2009-09-18	5.1	Beta tag lines removed.	LB
2009-09-18	5.2	Limitations section added.	LB
2009-09-24	5.3	Replaced Destination Folder and Setup Complete screenshots in Installation section.	LB

SOFTWARE VERSION

Version: 1.0.5.0

DOCUMENT VERSION

Version: 5.2

COPYRIGHT INFORMATION

© **Copyright 1997 - 2009**, 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	12
Who Should Use This Manual	12
Overview of Manual	12
References	13
Terminology	14
Getting Started	15
System Requirements	15
Software Requirements	15
Hardware Requirements	15
Installation	16
Installed Files	26
Licensing	27
Contacting Support	28
Configuration	29
Dynamic Data Exchange (DDE)	29
Starting the MatrikonOPC Server for IEC 60870	30
Tool Tray Menu	30
Control Panel	31
Configuration Window	32
File Menu	34
Edit Menu	34
View Menu	35
Tools Menu	35
Help Menu	36
Options Window	36
General Options	36
General Logging Options	38
Interface Logging Options	39
Advanced Options	40
Server Configuration	42
Creating Objects	42
Creating and Configuring a Fail-Over Channel Object	44
Creating and Configuring a Network Channel Object	48
Creating and Configuring a Serial Channel Object	51
Creating and Configuring a Server Status List Object	56
Creating and Configuring a Network Host Object	60
Creating and Configuring a Dial-Up Connection Object	63
Creating and Configuring an IEC 60870 Unit Object	70
Creating and Configuring a Radio Object	79
Creating and Configuring Server Defaults	82
Changing Objects	83
Removing Objects	83
Alias Configuration	84
Inserting Alias Groups	84
Renaming Alias Groups	85
Inserting New Aliases	85
Editing Aliases	88
Removing Aliases	88
Removing Alias Groups	88
Exporting Aliases	88

<i>Importing Aliases</i>	88
Expression Wizard	89
Saving a Configuration	92
Clearing a Configuration	93
Loading an Existing Configuration	93
Shutting Down the Server	93
OPC Data Items	95
IEC 60870 Items	95
<i>Data Items</i>	96
Configuration Items	100
<i>Common Parameters</i>	100
<i>Communication Channel Parameters</i>	101
<i>Serial Channel Parameters</i>	101
<i>Radios</i>	102
<i>Network Channels</i>	103
<i>Network Hosts</i>	103
<i>Fail-Over Channels</i>	103
<i>Dial-Up Connections</i>	103
<i>IEC 60870 Units</i>	104
<i>Dynamic Object Creation</i>	107
Control Items	107
Getting Data without Being Connected to a Device	108
SCADA Communication	109
Channels	109
<i>Serial</i>	109
<i>Radio</i>	109
<i>Network</i>	109
<i>Dial-Up</i>	109
Poll Optimization	110
Transactions	110
<i>Continuous</i>	110
<i>Scheduled</i>	111
<i>Instantaneous</i>	112
Integrity	112
<i>Transmission</i>	112
<i>Reception</i>	112
<i>Failure and Recovery</i>	113
<i>Redundancy and Fail-Over</i>	113
Diagnostics	117
Logging	117
Statistical Items	117
Data Qualities and Timestamps	120
Result Codes	121
Limitations	122
Troubleshooting	123
Problems and Solutions	123
Questions and Answers	129
Un-Installation	131
OPC Compliance	136
Installation	136
Common Interfaces	136
Data Access	136
<i>Groups</i>	137

Items	137
Browsing and Item Properties	137
I/O Operations	137
IEC 80670 Interoperability.....	139
IEC 60870-5-101 Interoperability Profile	139
System or Device	139
Network Configuration	139
Physical Layer	140
Link Layer	140
Application Layer	141
IEC 60870-5-104 Interoperability Profile	148
System or Device	148
Application Layer	148

Table of Appendices

Appendix A Distributed COM (DCOM)	157
DCOM Configuration Utility	157
Default Properties	157
Security Permissions.....	158
Server Identity	161
Default Protocols.....	161
Remote Program ID.....	162
Appendix B Aliases	163
Scaling Expressions	163
CSV File Format	164
Scaling Algorithms	165
Appendix C Standard Data Types.....	166
Appendix D Microsoft Excel as a DDE Client.....	167
DDE Read	167
DDE Write.....	167
Net DDE	168
Appendix E Common IEC 60870 Item Configurations	169
Configuring an Access Path Option.....	169
Non-Polled Items	169
Initial Interrogation	169
OPC Group Subscription Update Rate vs. Access Path Poll Rate	169
IEC 60870 Interrogation Commands	170
Appendix F Security.....	171
Introduction	171
OPC Security Implementation	171
MatrikonOPC Tag Security Configuration Utility.....	172
Security Details	194
Appendix G Offline Mode	197
Introduction	197
Offline Mode Toggling	197
Offline Mode Item Values	197
Operational Effects	198
Appendix H SCADA Servers Connection Logic.....	199
Introduction	199
Polling	199

Connection Failures and Reconnection Logic	199
Appendix I Features and Examples	200
Introduction	200
Round-Robin Example	200
Scanning and <i>Stay Connected</i> Option	202
<i>Writes</i> OPC Item	203
<i>PacketSent</i> and <i>PacketReceived</i> OPC Items	203
Appendix J OPC Items	204
Introduction	204
Base OPC Items	204
Generic OPC Items	204
Network Channel Object OPC Items	205
Network Host Object OPC Items	206
Fail-Over Channel Object OPC Items	206
Serial Channel Object OPC Items	206
Radio Object OPC Items	208
Dial-Up Object OPC Items	209

Table of Figures

Figure 1 - InstallAware Wizard Verification Window	16
Figure 2 - License Agreement Screen	17
Figure 3 - Product Registration Screen	18
Figure 4 - Setup Type Screen	19
Figure 5 - Destination Folder Screen	20
Figure 6 - Start Menu Screen	21
Figure 7 - Enter Password Screen	22
Figure 8 - Ready to Install Screen	23
Figure 9 - Installing MatrikonOPC Server for SCADA IEC Screen	24
Figure 10 - MatrikonOPC Server for SCADA IEC Setup Complete Screen	25
Figure 11 - Tool Tray	30
Figure 12 - Tool Tray Menu	31
Figure 13 - Control Panel	31
Figure 14 - Configuration Window	33
Figure 15 - General Options Tab	37
Figure 16 - General Logging Options Tab	38
Figure 17 - Interface Logging Options Tab	40
Figure 18 - Advanced Options Tab	41
Figure 19 - Insert New Object Window	42
Figure 20 - Create New Fail-Over Channel Window	44
Figure 21 - Fail-Over Channel Settings Communication Tab	45
Figure 22 - Fail-Over Channel Settings Load Distribution Tab	46
Figure 23 - New Fail-Over Channel Object	47
Figure 24 - Create New Network Channel Window	48
Figure 25 - New Network Channel Object	50
Figure 26 - Create New Serial Channel Window - Communication Tab	51
Figure 27 - Create New Serial Channel Window - Data Acquisition Tab	54
Figure 28 - New Serial Channel Object	56
Figure 29 - Create New Server Status List Window	57
Figure 30 - New Server Status List Object	60
Figure 31 - Create New Network Host Window	61
Figure 32 - Insert New Object	62

Figure 33 - New Network Host Object	63
Figure 34 - Create New Dial-Up Connection Window - Dial-Up Tab	64
Figure 35 - Create New Dial-Up Connection Window - Modem Tab.....	66
Figure 36 - Create New Dial-Up Connection - Advanced Tab	67
Figure 37 - Insert New Object Window	69
Figure 38 - New Dial-Up Connection Object	70
Figure 39 - Create New IEC 60870 Unit Window - Communication Tab	71
Figure 40 - Create New IEC 60870 Unit Window - Data Acquisition Tab.....	73
Figure 41 - Create New IEC 60870 Unit Window - Parameters Tab	75
Figure 42 - Create New IEC 60870 Unit Window - Advanced Tab	77
Figure 43 - Create New Radio Window	80
Figure 44 - Insert New Object.....	81
Figure 45 - New Radio Object.....	82
Figure 46 - Server Defaults Window.....	83
Figure 47 - Client Reference Warning Message	84
Figure 48 - Insert New Alias Window	85
Figure 49 - Insert New Alias Window Scaling Options.....	86
Figure 50 - Contents Table	87
Figure 51 - Expression Tab.....	90
Figure 52 - Expression Wizard.....	90
Figure 53 - Select Function Window	91
Figure 54 - Select Variable Window.....	91
Figure 55 - User Defined Functions Editor	92
Figure 56 - Operators Buttons.....	92
Figure 57 - Server Configuration Scenario.....	113
Figure 58 - F0V1 Server Configuration Scenario.....	114
Figure 59 - Fail-Over Channel Settings for F0V1.....	114
Figure 60 - Registry Editor	124
Figure 61 - Program ID Branch	125
Figure 62 - Edit Alias Window	130
Figure 63 - Add/Remove Programs	131
Figure 64 - Welcome to the MatrikonOPC Server for SCADA IEC Maintenance Screen ..	132
Figure 65 - Ready to Uninstall Screen	133
Figure 66 - Uninstalling MatrikonOPC Server for SCADA IEC Screen	134
Figure 67 - MatrikonOPC Server for SCADA IEC Setup Complete Screen.....	135
Figure 68 - Distributed COM Configuration Properties Window	158
Figure 69 - Distributed COM Configuration Security Tab	159
Figure 70 - Registry Value Permissions Window	160
Figure 71 - Add Users and Groups Window	160
Figure 72 - DDE Share	168
Figure 73 - Start Menu Navigation.....	173
Figure 74 - Enter Server Password Window	173
Figure 75 - MatrikonOPC Tag Security Configuration Utility Main Screen	174
Figure 76 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups	175
Figure 77 - Add User Window (NT).....	176
Figure 78 - Defined Users and Groups	177
Figure 79 - Add User Window (Private).....	178
Figure 80 - Add Group Window (NT)	179
Figure 81 - Add Group Window (Private)	180
Figure 82 - Enter New Name Window.....	180
Figure 83 - Edit <Username> Window (Permissions Tab)	182
Figure 84 - Add Permission Screen (Server Address Space).....	183

Figure 85 - Add User Permission Window.....	184
Figure 86 - Add Permission Window: Browsing Server Address Space	185
Figure 87 - Edit <Username>: Example.....	186
Figure 88 - Edit <Username> Window (General Tab).....	187
Figure 89 - Reset Password Window	187
Figure 90 - Edit <Groupname> Window (Permissions Tab)	188
Figure 91 - Edit <Groupname> Window (General Tab)	189
Figure 92 - Edit <Groupname> Window (Members Tab)	190
Figure 93 - Add Existing User Window	191
Figure 94 - Change Password Window	192
Figure 95 - Example	199
Figure 96 - Example 1	200
Figure 97 - Unit B Fails.....	201
Figure 98 - Retry Applied on Unit B Items.....	201
Figure 99 - Unit B Confirmed Failure	202
Figure 100 - Reconnect Delay.....	202
Figure 101 - Reconnect Retries	202
Figure 102 - Packets Sent and Received at a Certain Point	203

Table of Tables

Table 1 - Terms and Definitions.....	14
Table 2 - Files Installed in "IEC60870" Folder.....	26
Table 3 - Files Installed in "Common" Folder	27
Table 4 - Files Installed in "system32" Folder.....	27
Table 5 - MatrikonOPC Support Regional Contact Information	28
Table 6 - After-Hours Support	28
Table 7 - Tool Tray Menu Commands.....	31
Table 8 - Control Panel Commands.....	32
Table 9 - Configuration Window Commands.....	34
Table 10 - File Menu Commands.....	34
Table 11 - Edit Menu Commands (Server Configuration)	35
Table 12 - Edit Menu Commands (Alias Configuration).....	35
Table 13 - View Menu Commands.....	35
Table 14 - Tools Menu Commands	36
Table 15 - Help Menu Commands	36
Table 16 - General Options Tab Fields	38
Table 17 - General Logging Options Tab Fields.....	39
Table 18 - Interface Logging Options Tab Fields	40
Table 19 - Advanced Options Tab Fields.....	42
Table 20 - Insert New Object Window – Available Objects.....	43
Table 21 - Fail-Over Channel - Communication Tab Components.....	46
Table 22 - Create New Network Channel Window Components.....	50
Table 23 - Create New Serial Channel Window - Communication Tab Components	53
Table 24 - Create New Serial Channel Window - Data Acquisition Tab Components	55
Table 25 - Create New Server Status List Window Components	59
Table 26 - Create New Network Host Window Components	62
Table 27 - Create New Dial-Up Connection Window - Dial-Up Tab Components	65
Table 28 - Create New Dial-Up Connection Window - Modem Tab Components.....	67
Table 29 - Create New Dial-Up Connection Window - Advanced Tab Components.....	68
Table 30 - Create New IEC 60870 Unit Window - Communication Tab Components	72
Table 31 - Create New IEC 60870 Unit Window - Data Acquisition Tab Components.....	74

Table 32 - Create New IEC 60870 Unit Window - Parameters Tab Components	76
Table 33 - Create New IEC 60870 Unit Window - Advanced Tab Components	78
Table 34 - Create New Radio Window Components	81
Table 35 - Insert New Alias Window Options	86
Table 36 - Insert New Alias Window Scaling Options	86
Table 37 - Expression Wizard Options	89
Table 38 - Communication Options for Device Items.....	96
Table 39 - Access Path Option Examples	96
Table 40 - Monitor Items.....	97
Table 41 - Process Control Items	97
Table 42 - System Control Items.....	98
Table 43 - Parameter Control Items.....	100
Table 44 - Common Configuration Parameters	101
Table 45 - Communication Channel Configuration Parameters.....	101
Table 46 - Serial Channel Configuration Parameters	102
Table 47 - Radio Configuration Parameters.....	102
Table 48 - Network Channel Configuration Parameters.....	103
Table 49 - Network Host Configuration Parameters	103
Table 50 - Dial-Up Connection Configuration Parameters.....	104
Table 51 - IEC 60870 Unit Communication Configuration Parameters.....	107
Table 52 - Communication Object Control Item.....	107
Table 53 - Unit Control Item.....	108
Table 54 - Dial-Up Connection Control Item	108
Table 55 - Server Status List Device Link OPC Items.....	108
Table 56 - Reset Statistics Control Item	118
Table 57 - Communication Objects Statistical Items	119
Table 58 - Communication Channels Statistical Items.....	119
Table 59 - IEC 60870 Unit Statistical Item	119
Table 60 - Dial-Up Connection Statistical Items	119
Table 61 - OPC Quality Codes	120
Table 62 - OPC Result Codes	121
Table 63 - Expressions Constructs for Alias Scaling	164
Table 64 - File Import/Export Field Descriptions	164
Table 65 - Additional File Import/Export Field Descriptions - Linear/Square Root Scaling	165
Table 66 - Additional File Import/Export Field Descriptions - Offset Scaling.....	165
Table 67 - Additional File Import/Export Field Descriptions - Expression Scaling	165
Table 68 - Scaling Algorithms.....	165
Table 69 - Standard Data Types	166
Table 70 - Default Tag Security	192
Table 71 - Example 1.....	193
Table 72 - Example 2: Permissions.....	193
Table 73 - Example 2: Groups and Members.....	193
Table 74 - Example 2: Permissions.....	196
Table 75 - Offline Mode Item Values	198
Table 76 - Root Device Link OPC Items	204
Table 77 - Generic OPC Items	205
Table 78 - Network Channel OPC Items	206
Table 79 - Network Host OPC Items.....	206
Table 80 - Fail-Over Channel OPC Items.....	206
Table 81 - Serial Channel Object OPC Items.....	208
Table 82 - Radio Object OPC Items	209
Table 83 - Dial-Up Object OPC Items.....	210

Introduction

This manual is designed to teach you how to install and configure the MatrikonOPC™ Server for IEC 60870.

This MatrikonOPC Server for IEC 60870 provides connectivity to any RTU, IED (Intelligent Electronic Device), PLC, meter, transducer, relay, etc., compatible with either the IEC 60870-5-101 protocol or the IEC 60870-5-104 protocol.

The MatrikonOPC IEC 60870 server includes support for:

- IEC 60870 controlling station, including transmission protocols IEC 60870-5-101 and IEC 60870-5-104.
- Multiple communications channels at the same time (serial, radio, network, and dial-up).
- Supervisory control using single-destination and broadcast commands.
- Redundancy, including channel redundancy, and fail-over and fail-back.
- Round-Robin polling
- Detailed polling schedule
- Optimized for low-bandwidth and noisy communication channels
- Runs as a Windows service

The purpose of the MatrikonOPC IEC server is to maintain a robust connection to a device supporting the SCADA IEC protocol. This server is used in control, processing, and manufacturing industries.

Who Should Use This Manual

This manual is intended for all users of MatrikonOPC Server for IEC 60870. This manual explains how to install, license, and configure the software, and how to perform common tasks. In addition, technical information about OPC data items, diagnostics information, and a troubleshooting section are included.

Overview of Manual

This document 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 chapter in this document are 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.
- **SCADA Communication** – discusses channels, poll optimization, transactions, and integrity.
- **Diagnostics** – explains how to use logging, statistical items, data qualities and timestamps, and result codes to get the most efficiency from your system.
- **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 the server's OPC compliance with regard to installation of common interfaces and data access.
- **IEC 60870 Implementation** – outlines how the server conforms to IEC 60870 specifications.
- **Appendices:**
 - o **A** - DCOM
 - o **B** – Aliases
 - o **C** – Standard Data Types
 - o **D** – Microsoft Excel as a DDE Client
 - o **E** – Common IEC 60870 Item Configurations
 - o **F** – Security
 - o **G** – Offline Mode
 - o **H** – SCADA Servers Connection Logic
 - o **I** – Features and Examples
 - o **J** – OPC Items

References

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

- www.opcfoundation.org
- www.matrikonopc.com
- www.opcsupport.com
- www.iec.ch
- <http://www.iec.org>
- *OPC Overview 1.0*
- *OPC Common Definitions and Interfaces 1.0*
- *OPC Security Custom Interface 1.0*
- *OPC Data Access Custom Interface (Version 3.0) Specification*
- *OPC Data Access Custom Interface (Version 2.05) Specification*

- *OPC Data Access Custom Interface (Version 1.0a) Specification*
- *International Standard IEC 60870-5-101*
- *International Standard IEC 60870-5-104*

Terminology

The following terms are used interchangeably throughout this document:

- *screen and window*
- *tab and panel*
- *device link and object*
- *MatrikonOPC Server for SCADA IEC 60870 and MatrikonOPC Server for IEC 60870 and MatrikonOPC Server for SCADA IEC*

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

Term / Abbreviation	Description
CDPD	Cellular Digital Packet Data.
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.
HDA	OPC Historical Data Access.
IEC	International Electrotechnical Commission. A non-for-profit, non-governmental international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies.
Matrikon	Matrikon Inc.
MatrikonOPC	Matrikon's brand name for its OPC-compliant servers and clients.
OPC	A communication standard. Refer to www.opcfoundation.org for more information.
PLC	Programmable Logic Controller.
PPP	Point-to-Point Protocol.
SCADA	Supervisory Control and Data Acquisition.

Table 1 - Terms and Definitions

Getting Started

This section of the *User's Manual* contains important information regarding MatrikonOPC Server for IEC 60870 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 **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 minimum **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

At a minimum, the following software is required:

- Microsoft Windows XP or 2003 or 2000
- Internet Explorer 4.01 Service Pack 1 (or better)



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

Hardware Requirements

At a minimum, the following hardware is recommended:

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

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

- Serial communications port
- RS232/422/485 cabling and/or converters
- Radio modem
- Hayes-compatible modem (dial-up, leased line, CDPD)
- IP-compatible network
- TCP/IP or UDP/IP terminal server

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 IEC 60870 CD into the CD drive.
2. If the MatrikonOPC **Welcome** screen does not automatically appear, double-click the *MatrikonOPCSCADAIEC.exe* file. The **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.

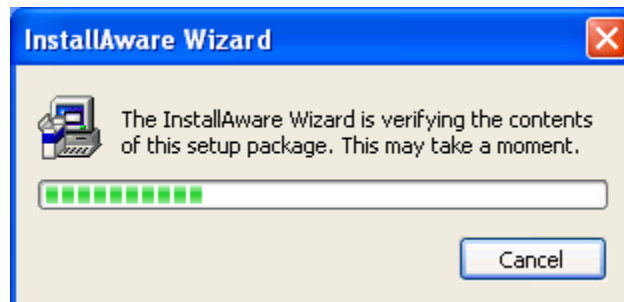


Figure 1 - InstallAware Wizard Verification Window

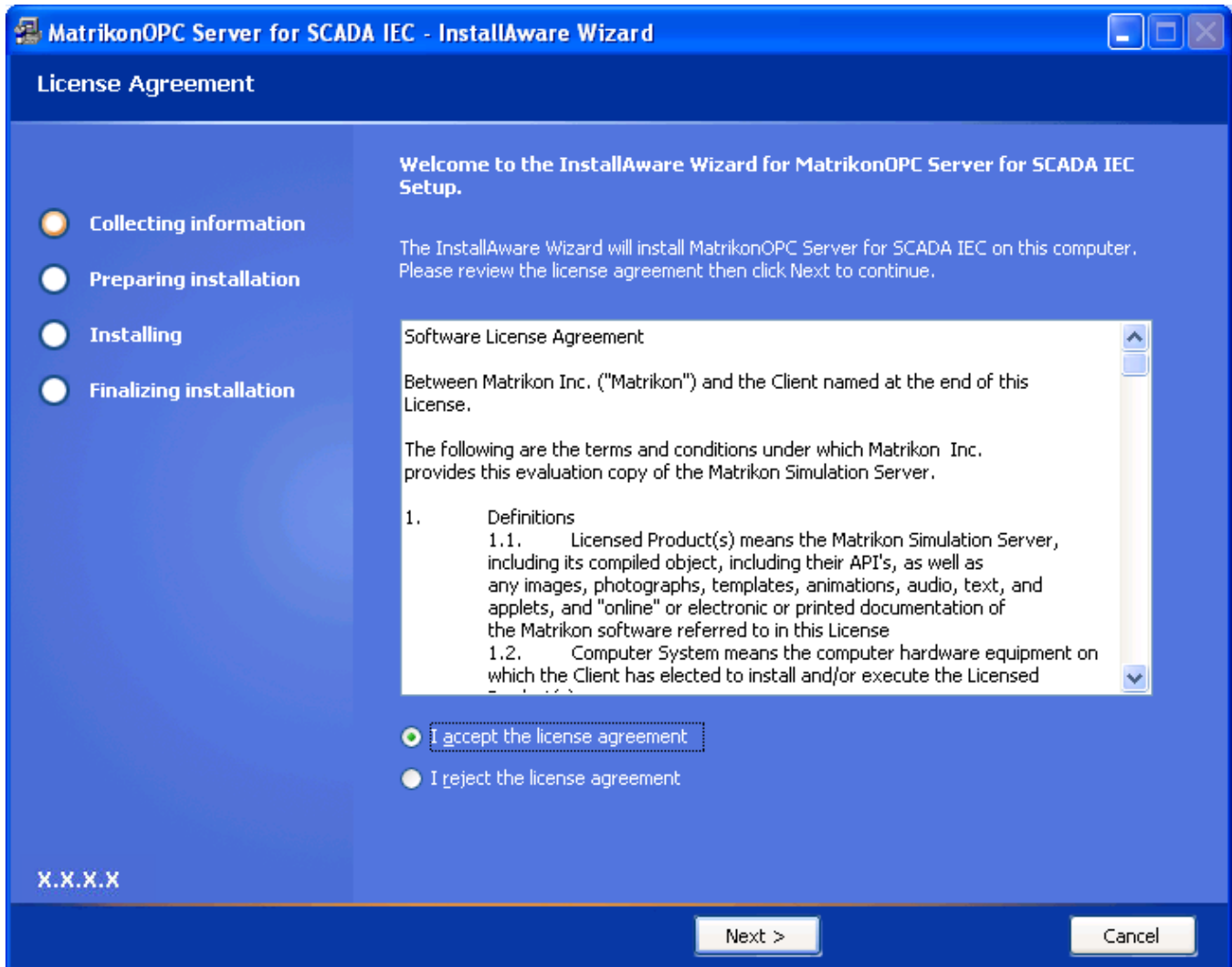


Figure 2 - License Agreement Screen

3. Read the **Software License Agreement**, use 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 **Product Registration** screen (Figure 3) appears.

Note: From this point until the actual installation begins, 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.

Product Registration

Please enter the registration information

☒ **Collecting information**
☐ **Preparing installation**
☐ **Installing**
☐ **Finalizing installation**

User Name: Company:
Address: City:
Country: Postal/Zip Code:
Phone Number: E-mail Address:
Transaction Number: [Note: The license file will be sent to this e-mail address, please ensure that it is valid]
Evaluation:

All fields must be entered before proceeding

X.X.X.X

Figure 3 - Product Registration Screen

6. Enter the required registration information.

Notes:



- The **Next** button is **not** available until all fields have been entered.
- Ensure the **E-mail Address** is valid as that is the address to which the license file is sent.

7. Click on the **Next** button. The **Setup Type** screen (Figure 4) appears.

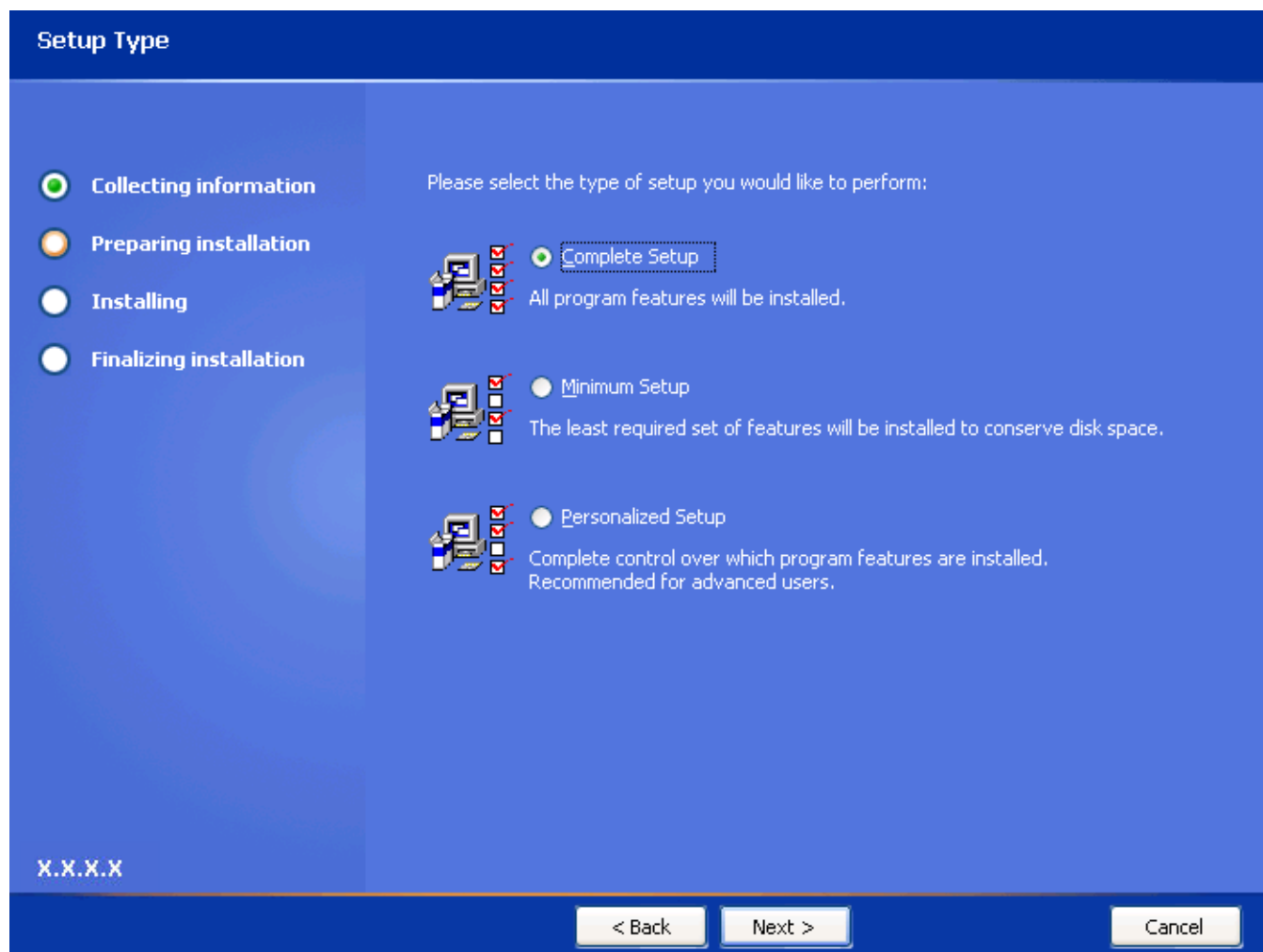


Figure 4 - Setup Type Screen

8. Select the type of setup to be performed.

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

9. Click on the **Next** button. The **Destination Folder** screen (Figure 5) appears.

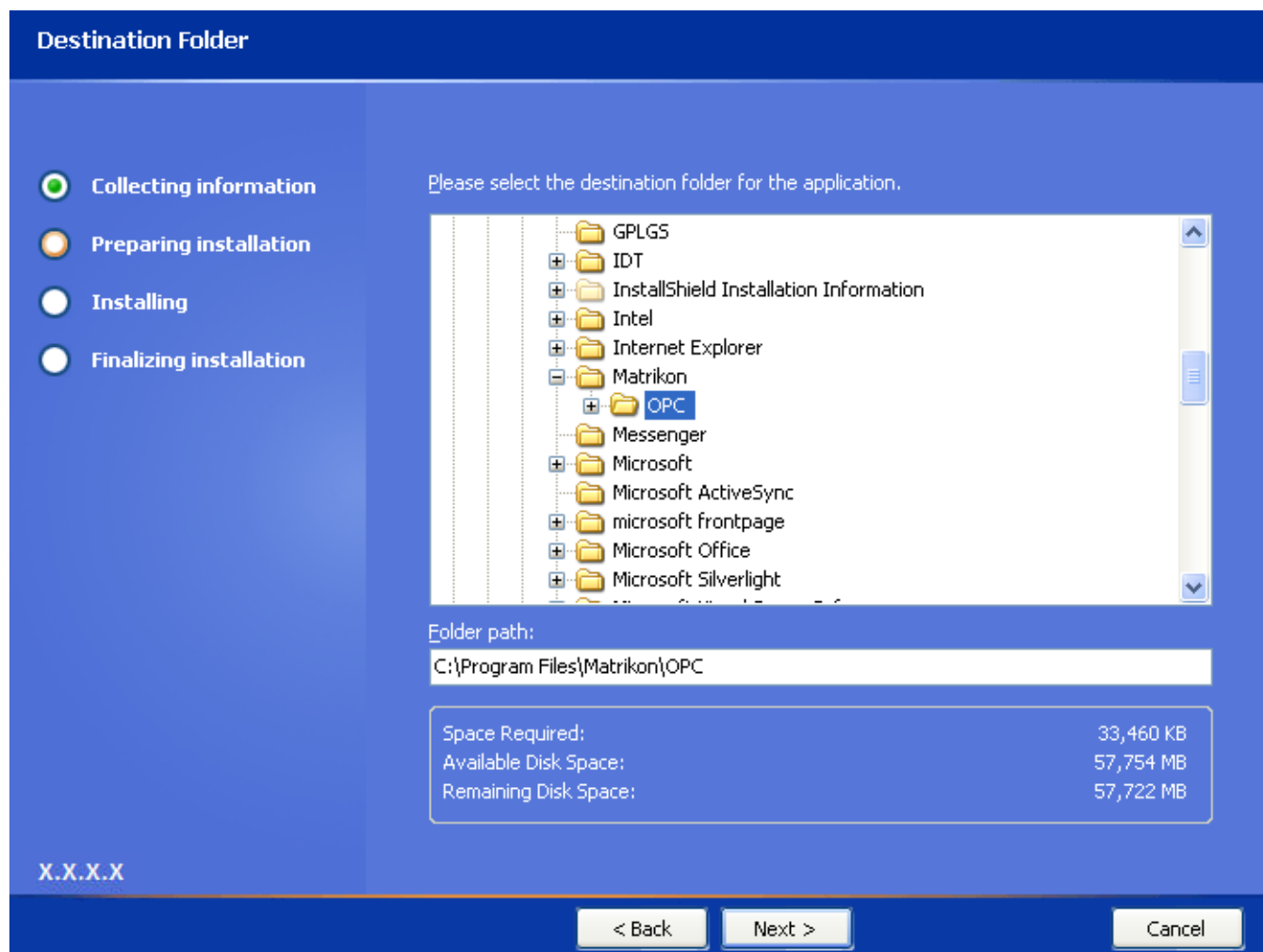


Figure 5 - Destination Folder Screen

10. Select the folder in which to install MatrikonOPC Server for SCADA IEC, or accept the default location displayed in the **Folder path** field.
11. Click on the **Next** button. The **Start Menu** screen (Figure 6) appears.

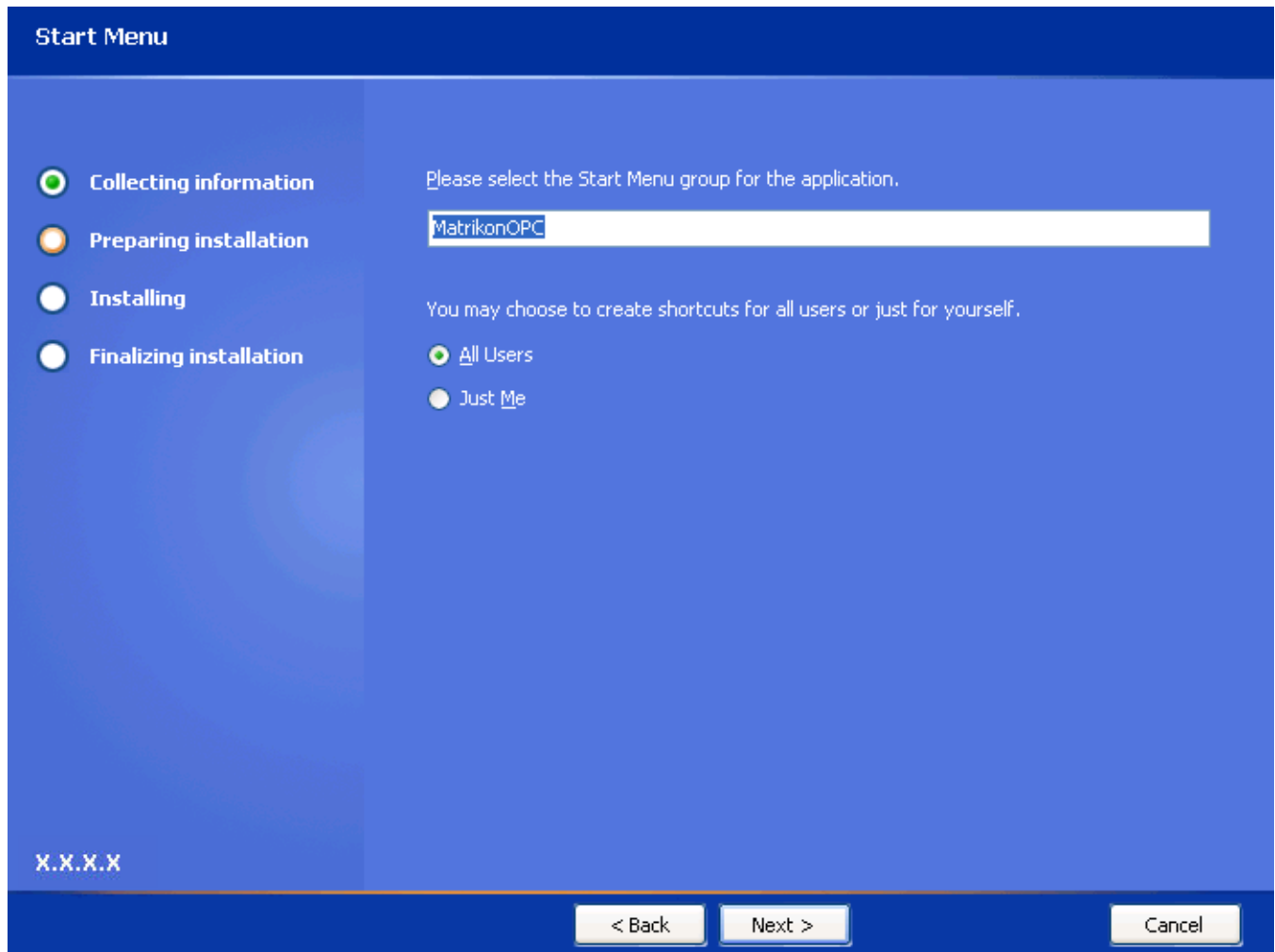
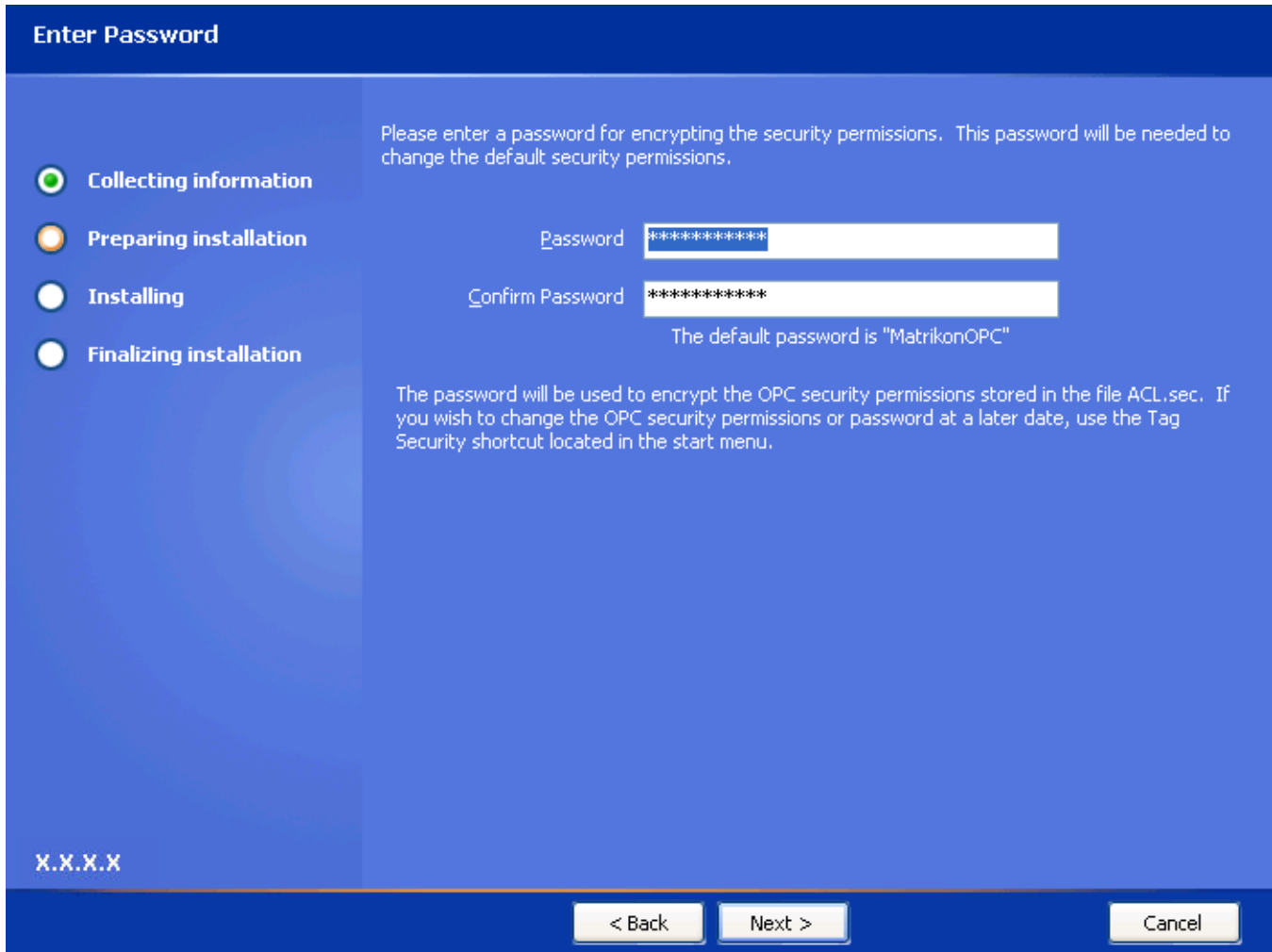


Figure 6 - Start Menu Screen

12. 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.
13. Click on the **Next** button. The **Enter Password** screen (Figure 7) 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 7 - Enter Password Screen

14. 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 F – Security**.

15. Click on the **Next** button to accept the default password. The **Ready to Install** screen (Figure 8) appears.

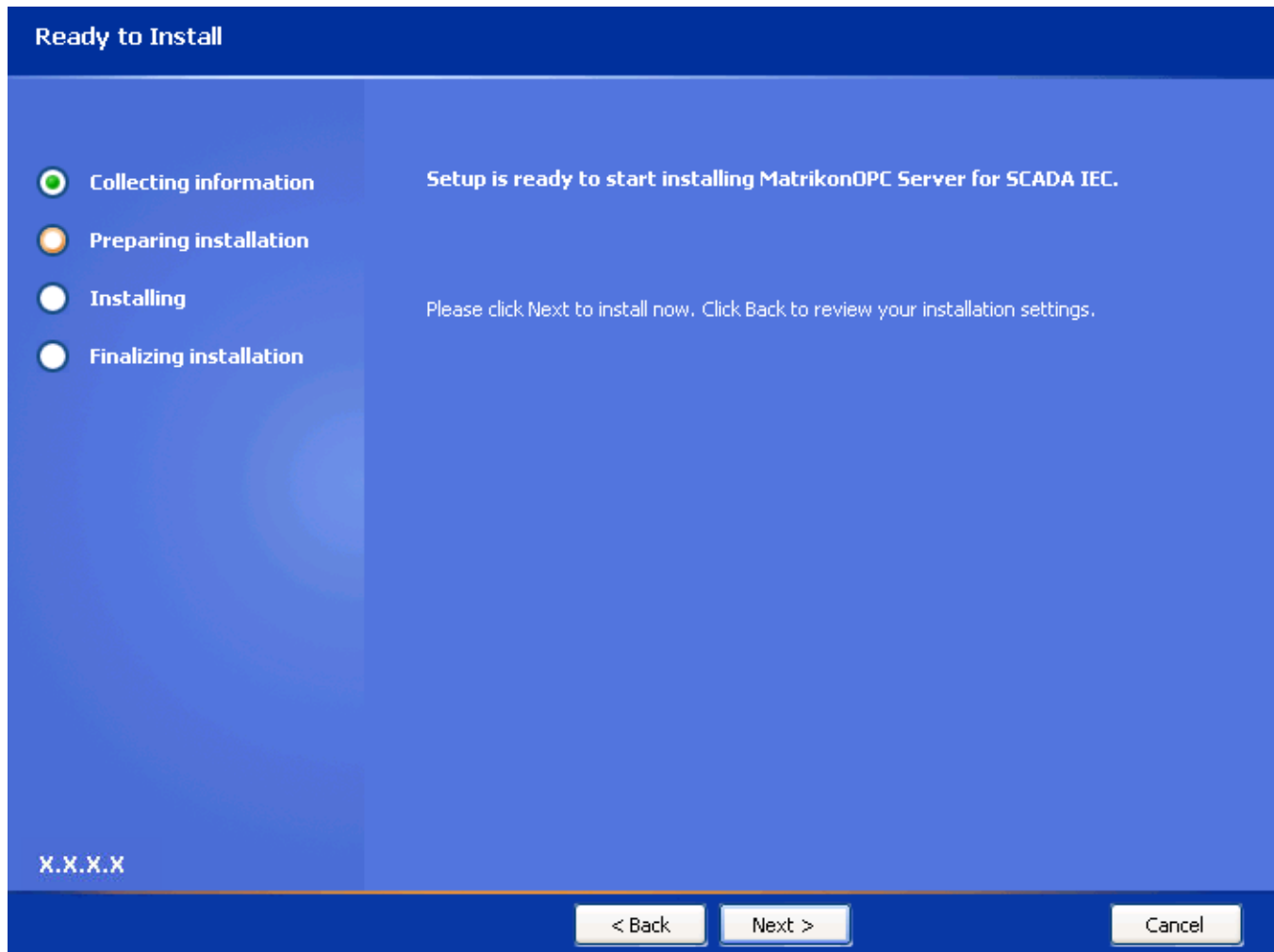


Figure 8 - Ready to Install Screen

16. Click on the **Next** button. The **Installing MatrikonOPC Server for SCADA IEC** 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.

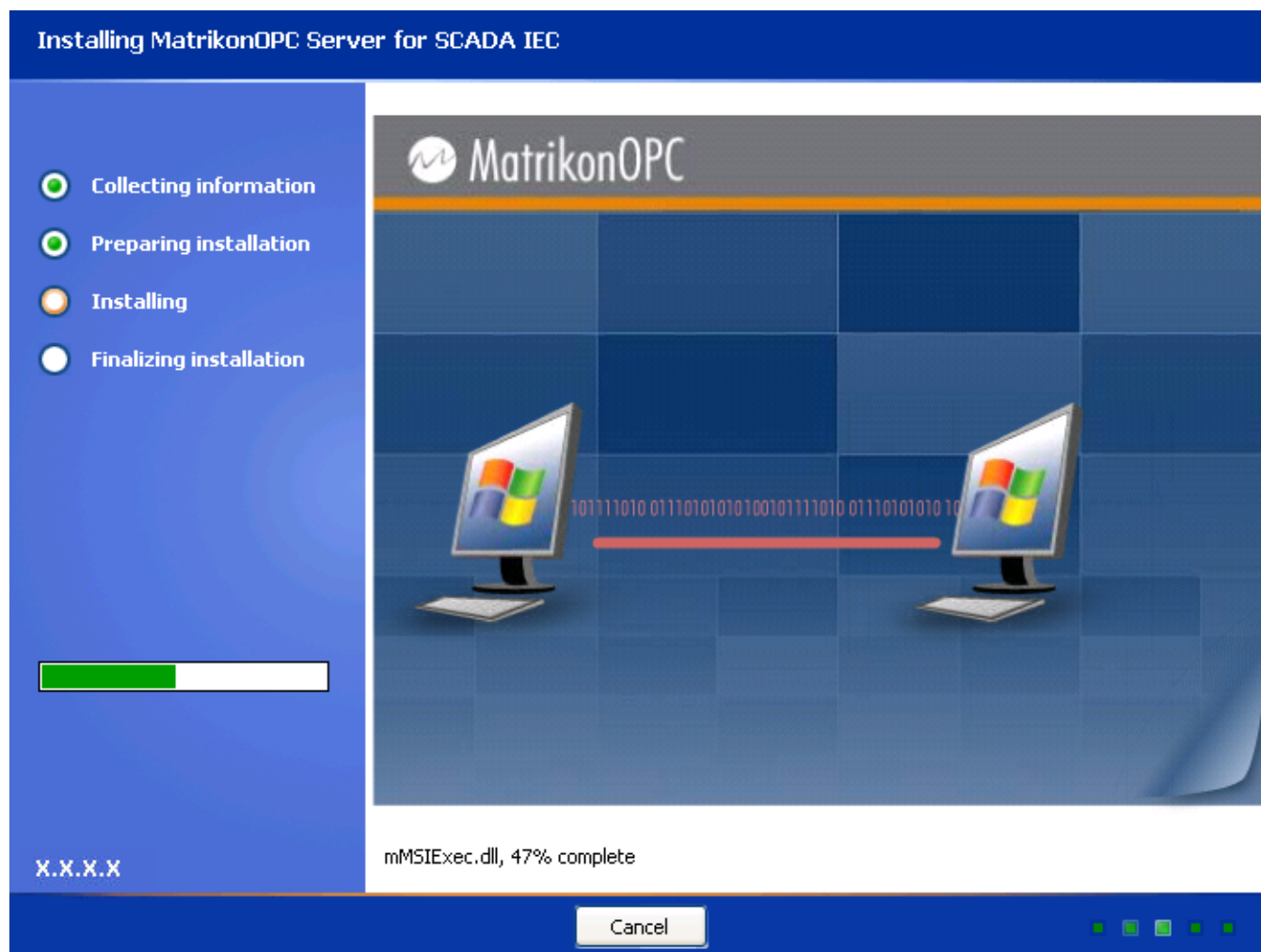


Figure 9 - Installing MatrikonOPC Server for SCADA IEC Screen

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

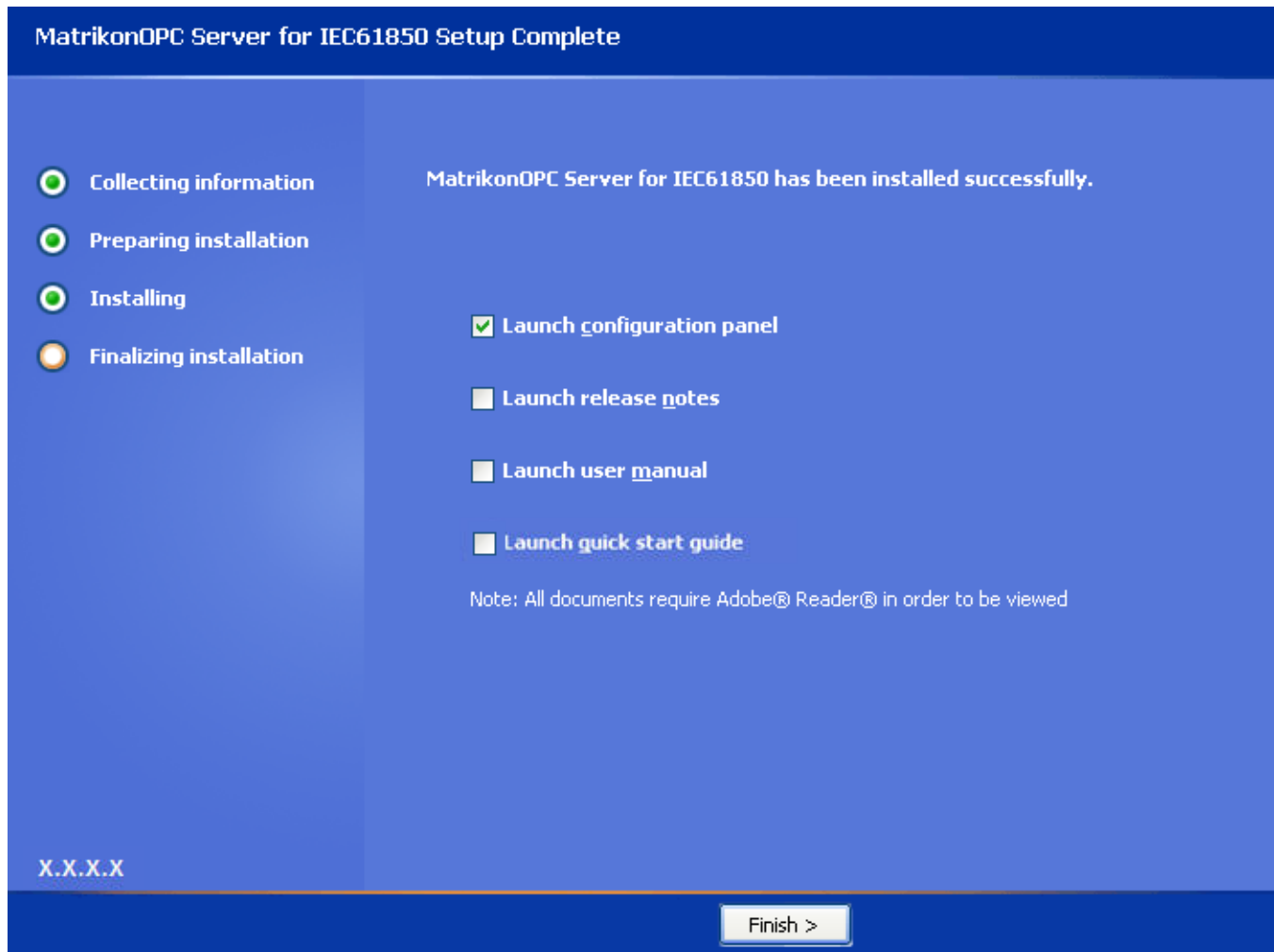


Figure 10 - MatrikonOPC Server for SCADA IEC Setup Complete Screen

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

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

20. The necessary files are 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\IEC60870

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.
AuthorizeRequest.MTK	Licensing request file (please send to Matrikon).
IEC 60870 Release Notes.pdf	Release Notes for this product.
Licensing Procedures.pdf	Licensing procedures document.
MATRIKONOPC IEC 60870 User Manual.pdf	This User's Manual.
OPCIEC60870.EXE	Server executable.
ProgID.txt	Security information file used by the encryption utility.
Project Info.log	Product version information for the current build.
PSTCFGIEC60870Lib.ocx	Server ActiveX configuration panels.
PSTCFGScadaLib.ocx	Server ActiveX configuration panels.
security.cfg	Security configuration file.
ServerOpts.ini	The initialization file for recording the server's initial settings.

Table 2 - Files Installed in "IEC60870" 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	MatrikonOPC Server Security Configuration Tool.
EULA.pdf	License document.
eximg.dll	Component of OPC Explorer.
Hasp.exe	Hardware key checking utility.
haspds_windows.dll	Hardware key licensing library.
HINSTALL.EXE	Hardware key device driver installation utility.
MatrikonOPC Explorer User Manual.pdf	User's manual for the MatrikonOPC Explorer.
MTKAUTHORIZE.EXE	Matrikon product authorization utility.
OEM_MATRIKON_OPC.DLL	MatrikonOPC OEM badge library.

File Name	Description
OPCAuto.dll	Matrikon OPC Automation Component – enables developers to access OPC data from client applications developed using automation tools such as <i>Visual Basics</i> , <i>VBA</i> , and <i>VB Script</i> .
OPCDA20_AUTO.DOC	MatrikonOPC Automation Component interface standard.
OPCDAAUTO.DLL	MatrikonOPC Automation Component – enables developers to access OPC data from client applications developed using automation tools (e.g., <i>Visual Basic</i> , <i>VBA</i> , <i>VB Script</i>).
OPCEXPLORER.EXE	MatrikonOPC Explorer – a general-purpose OPC client useful for testing the capabilities of any OPC server.
opchda_ps.dll	The proxy-stub files to allow OPC clients to make remote connections to an OPC HAD Server.
opchda10_auto.doc	Matrikon OPC Automation Component interface standard.
OPCHDAAuto.dll	Matrikon OPC Automation Component – enables developers to access OPC data from client applications developed using automation tools such as <i>Visual Basics</i> , <i>VBA</i> , and <i>VB Script</i> .
PSTBasicInnerLayerLib.ocx	Additional Server ActiveX configuration panels.
PSTCFG.EXE	Matrikon product configuration utility.
PSTCFGPS.DLL	Matrikon product configuration marshalling library.

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 Equations
opc_aeps.dll	OPC Alarms and Events 1.0 Interfaces Marshalling Library
opccomn_ps.dll	OPC Common Interfaces and Marshalling Library
Opcenum.exe	OPC Server List Component
opcproxy.dll	OPC Data Access 2.0 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 IEC 60870 supports **both** 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 IEC 60870 User's Manual*:



- Requesting a software license.
- Enabling a temporary software authorization.
- Installing a permanent software license.
- Generating a new *AuthorizeRequest.MTK* file.
- De-licensing software.

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)	8:00 am-5:00 pm	+1-877-OPC-4-ALL
Europe / Africa * UTC/GMT +1 hours (CET)	9:00 am-5:00 pm	+49-221-969-77-0 (Request OPC Support)
Middle East * UTC/GMT +3 hours	9:00 am-5:00 pm	+973-174-65363
Australia / Asia * UTC/GMT +10 hours (AEST)	9:00 am-5:00 pm	+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 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 IEC is required for the server to function properly, but users can customize the server's behaviour 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 IEC 60870** section of this manual shows users how to start the software. The next four sub-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. The **Alias Configuration** section explains how to create user-defined aliases in place of regular OPC items, followed by four sub-sections that cover saving, clearing, and loading configuration settings, and shutting down the server.

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 a checkbox (refer to **Advanced Options** for more information about, including the location of, this checkbox).

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 IEC 60870

To launch the MatrikonOPC Server for IEC 60870, choose the appropriate shortcut from the **Start** menu.

To start the MatrikonOPC Server for IEC 60870:

1. Click on the Windows **Start** button and select **Programs -> MatrikonOPC -> IEC60870**, and choose **MatrikonOPC Server for SCADA IEC**.

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).

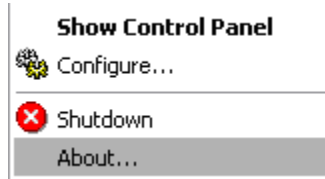


Figure 12 - Tool Tray Menu

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 **Control Panel**.

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 MatrikonOPC IEC 60870 server. It displays the current configuration and allows you 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.

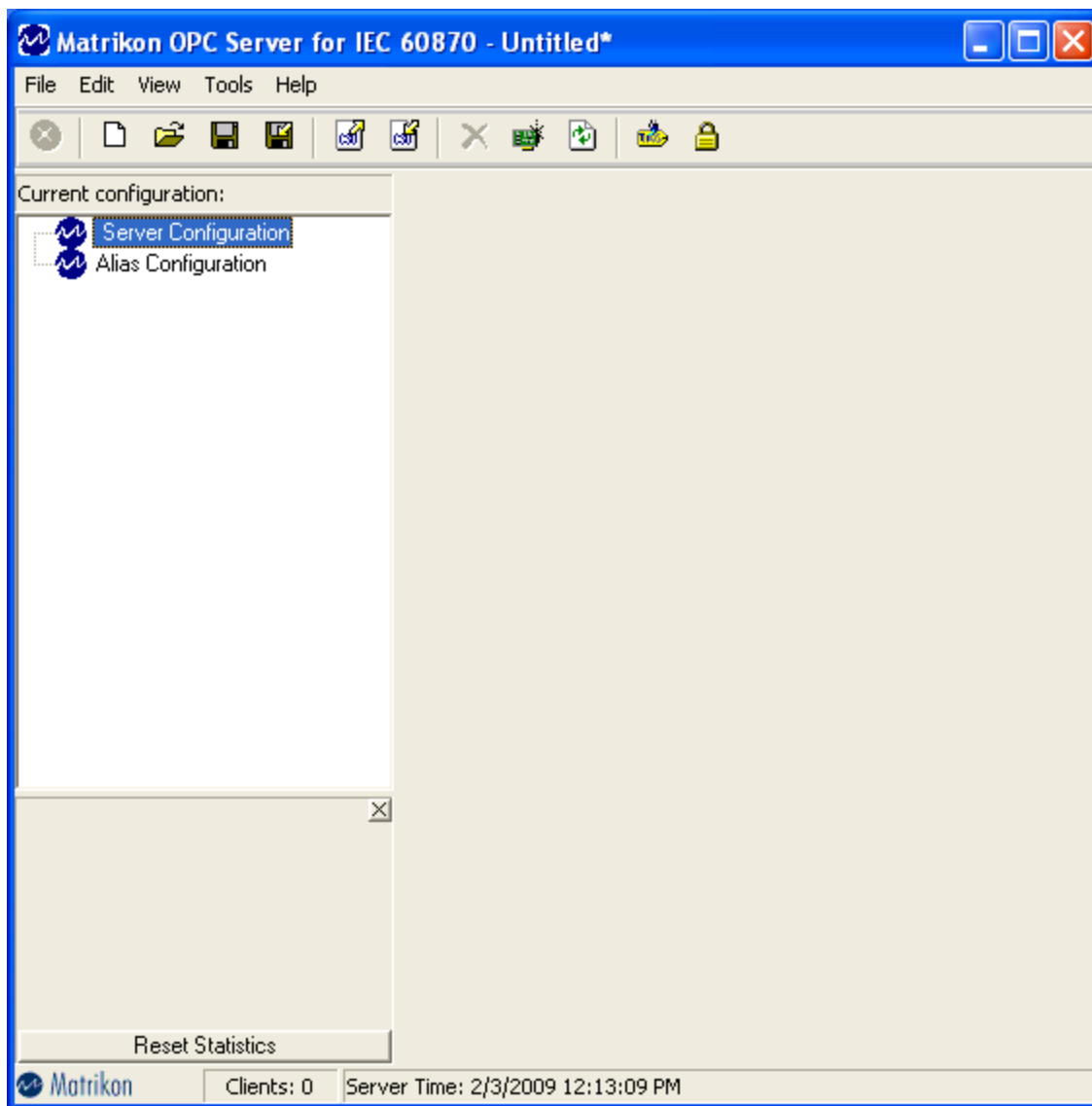


Figure 14 - Configuration Window

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 signalling 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.
 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 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 F – 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 four tabs: **General**, **General Logging**, **Interface Logging**, and **Advanced**.

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).

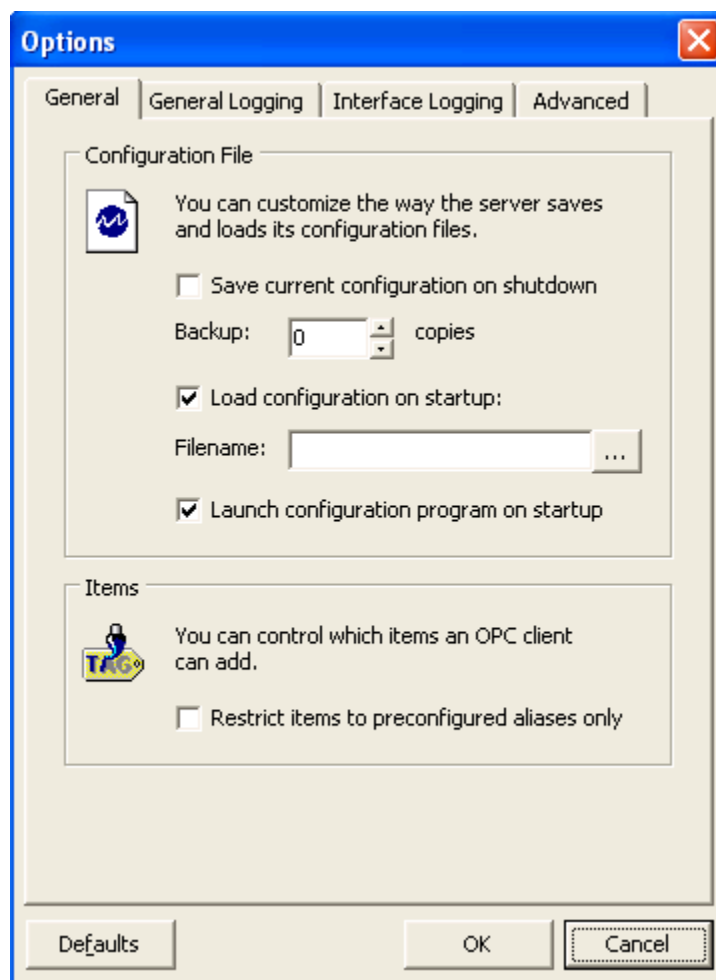


Figure 15 - General Options Tab

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	Prevents OPC clients from adding items other than configured aliases, if selected. Selecting this option will cause clients to see only aliases when

Field	Description
only	browsing this server. Note: As is the case with any changes to General options, if this option is changed you will need to restart the server for the change to take effect.

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).

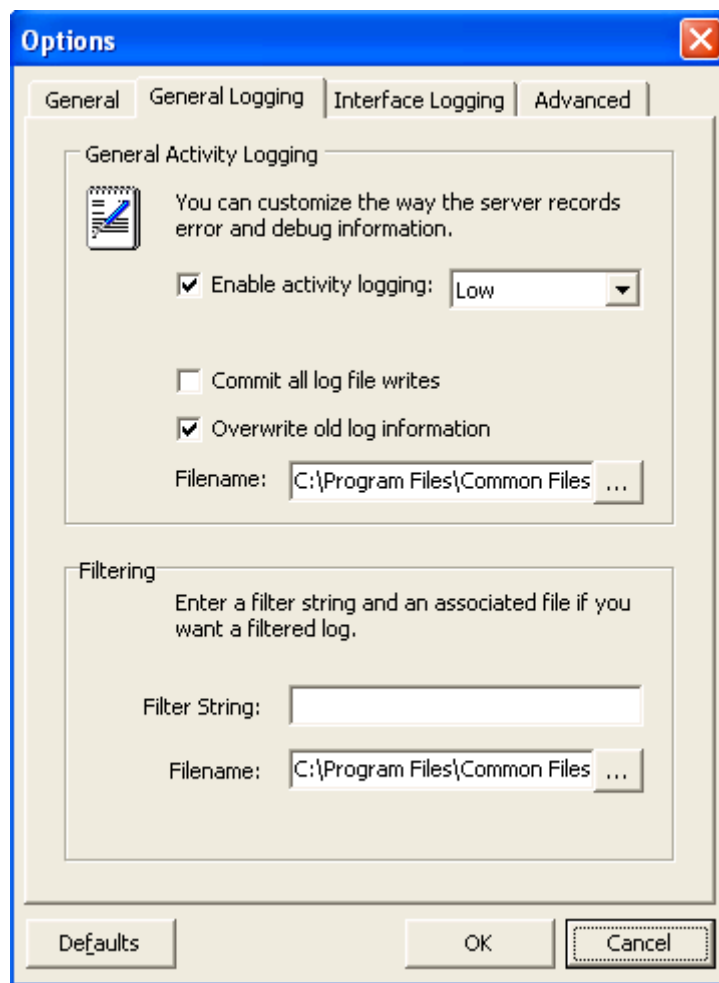


Figure 16 - General Logging Options Tab

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 (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.
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\COMMON FILES\MatrikonOPC\COMMON\PSTCFGMatrikon.OPC.ROCplus. 1.LOG , where X is the server number when multiple installations are present.
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).

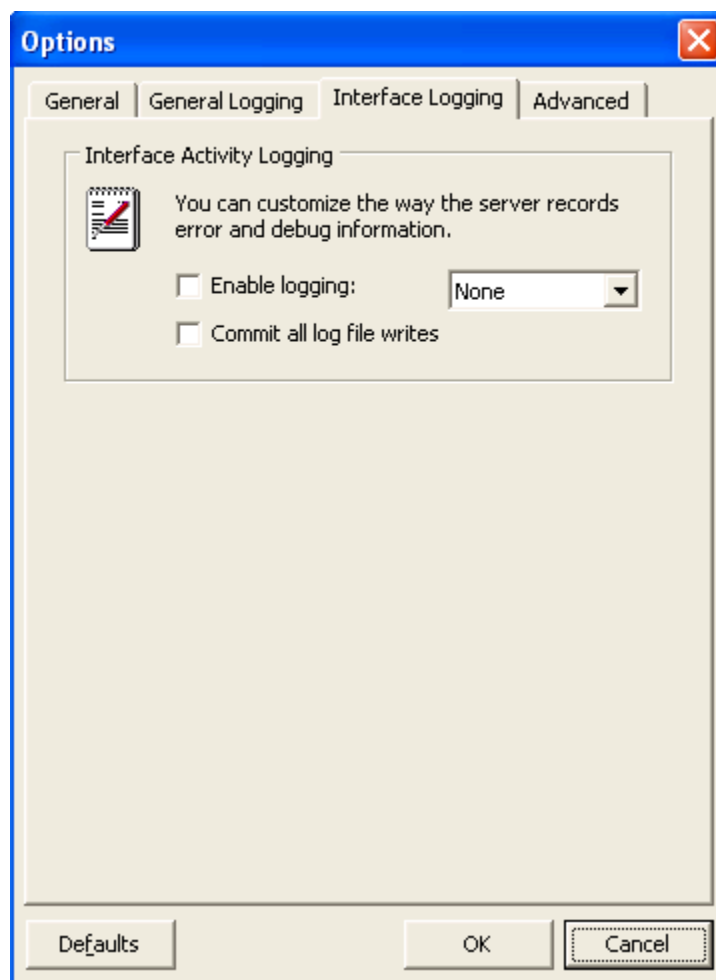


Figure 17 - Interface Logging Options Tab

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, and can also fill up the hard drive.
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 to display the Advanced options (Figure 18).

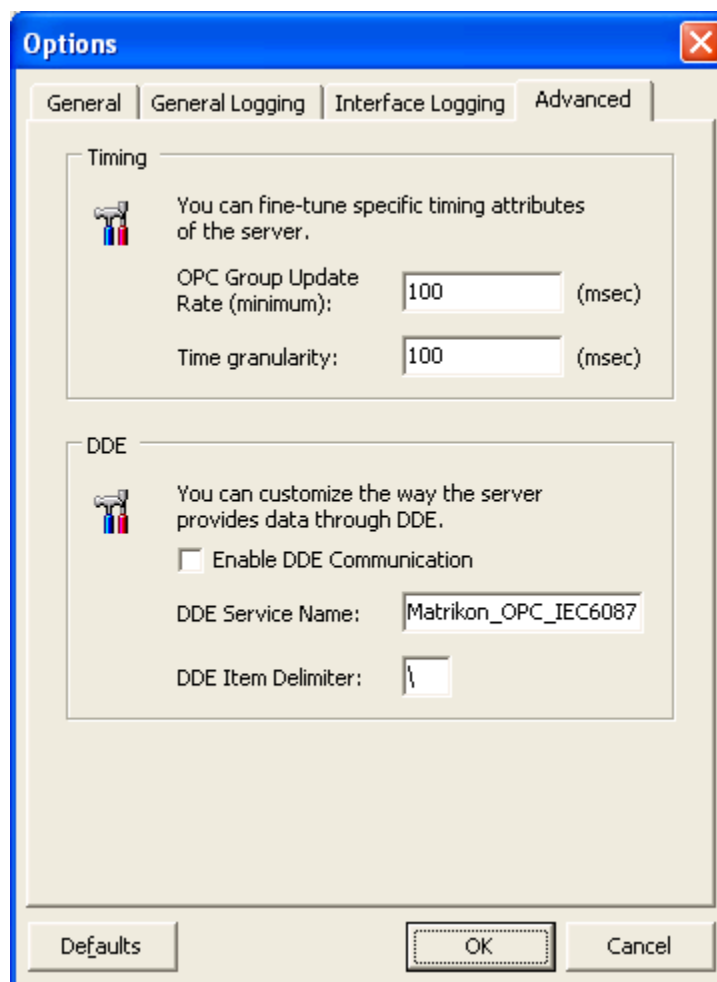


Figure 18 - Advanced Options Tab

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.
Enable DDE Communication	Selecting this checkbox this will allow the server to accept Dynamic

Field	Description
	Data Exchange (DDE) connections.
DDE Service Name	The DDE service name that should be used by clients to connect to this program.
DDE Item Delimiter	The character to be used to indicate the start of a new item in the DDE data request.

Table 19 - Advanced Options Tab Fields

Notes:

- For more information about DDE, refer to the **Dynamic Data Exchange (DDE)** section in this manual.
- 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 MatrikonOPC IEC 60870 server requires some configuration for it to run properly, but you can customize the server's behaviour as required. This section shows you how to create and edit objects using the **Configuration** window.

Creating Objects

The **Insert New Object** and **Create New** windows are used to create MatrikonOPC Server for SCADA IEC 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.

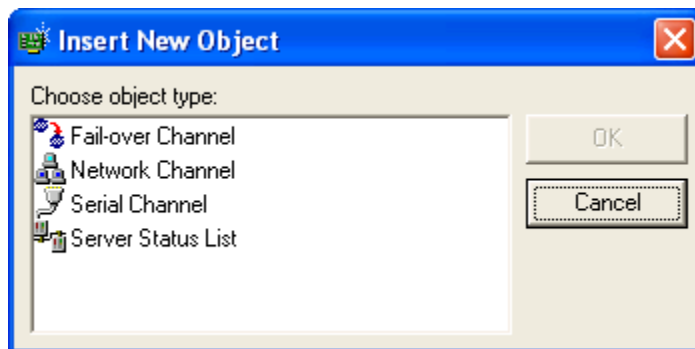


Figure 19 - Insert New Object Window

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 Server Status List
Fail-over Channel	None

Selected Object	Insert New Object Window Options
Network Channel	Network Host
Network Host	Dial-up Connection IEC 60870 Unit
Dial-up Connection	IEC 60870 Unit
IEC 60870 Unit	None
IEC 60870 Unit	None
Serial Channel	Dial-up Connection IEC 60870 Unit Radio
Dial-up Connection	IEC 60870 Unit
IEC 60870 Unit	None
IEC 60870 Unit	None
Radio	IEC 60870 Unit
IEC 60870 Unit	None
Server Status List	None

Table 20 - Insert New Object Window – Available Objects

To insert a new object:

- On the **Configuration** window, select the **Server Configuration** item 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 type of object you want to create.

Note: Different objects may be available depending on which object is currently selected in the tree view.
- Click on the **OK** button.
- The **Create New** window appears.

To create a newly inserted object:

- 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. You may also choose to enter a description of the object.
- Edit the configuration components as desired.
- 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

The **Create New** window (Figure xx) displays the settings available for a new object.

The following sub-sections contain information on the types of objects available and how to configure them.

Creating and Configuring a Fail-Over Channel Object

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

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**

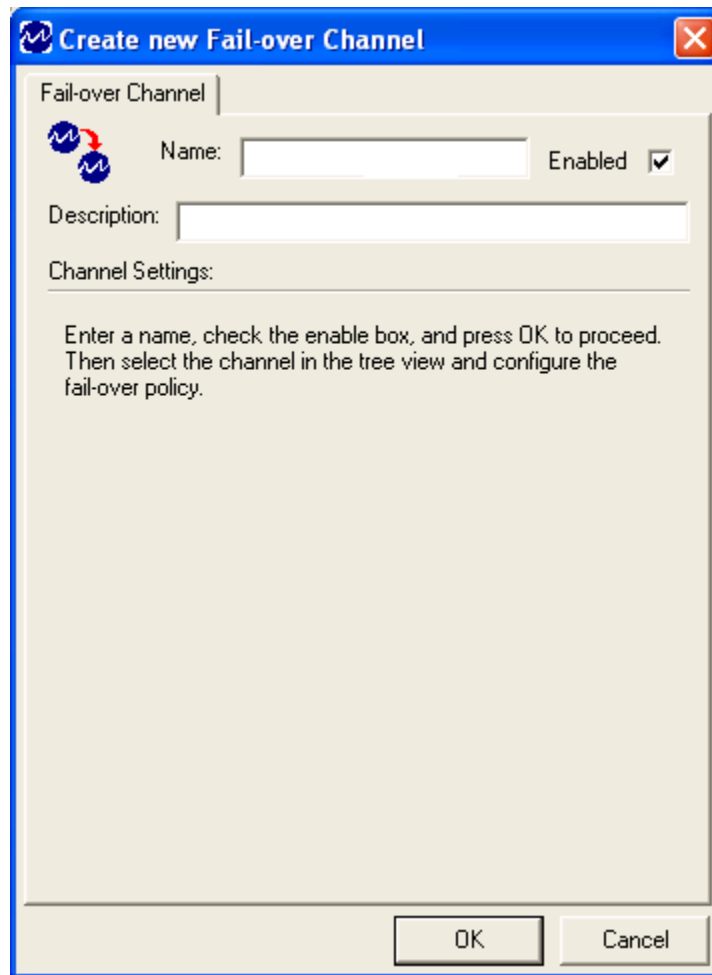


Figure 20 - Create New Fail-Over Channel Window

Neither the **Communication** tab (Figure 21) nor the **Load Distribution** tab (Figure 22) are available until you have already created the Fail-over Channel. To display these tabs, select the Fail-over Channel in the **Current Configuration** list and it will appear in the **Fail-over Channel Settings** window.

Communication Tab

The **Fail-over Channel - Communication** tab (Figure 21) includes settings for primary, secondary, and standby channels.

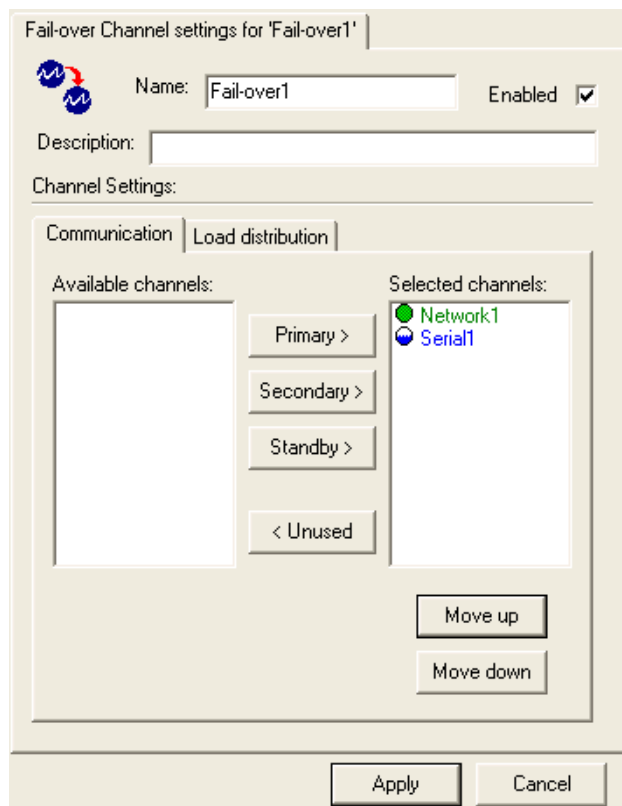


Figure 21 - Fail-Over Channel Settings Communication Tab

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

Note: The configuration fields for the Fail-over Channel are not available at initial creation time.

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. 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	Communication channels not presently used in the fail-over policy.
Selected channels	Communication channels presently used in the fail-over policy: ● primary, ○ standby, or ● secondary/distributed load.

Component	Description
Primary >	Add the selected channel or channels to the fail-over policy as a  primary.
Secondary >	Add the selected channel or channels to the fail-over policy as a  secondary.
Standby >	Add the selected channel or channels to the fail-over policy as a  standby.
< Unused	Remove the selected channel or channels from the fail-over policy.
Move up	Move the selected channel or channels to a higher priority in the fail-over policy.
Move down	Move the selected channel or channels to a higher priority in the fail-over policy.
Apply	Select this button to save any changes and close the window.
Cancel	Select this button to close the window without saving any changes made.

Table 21 - Fail-Over Channel - Communication Tab Components

Load Distribution Tab

The **Fail-over Channel - Load Distribution** tab allows you to specify load distribution.

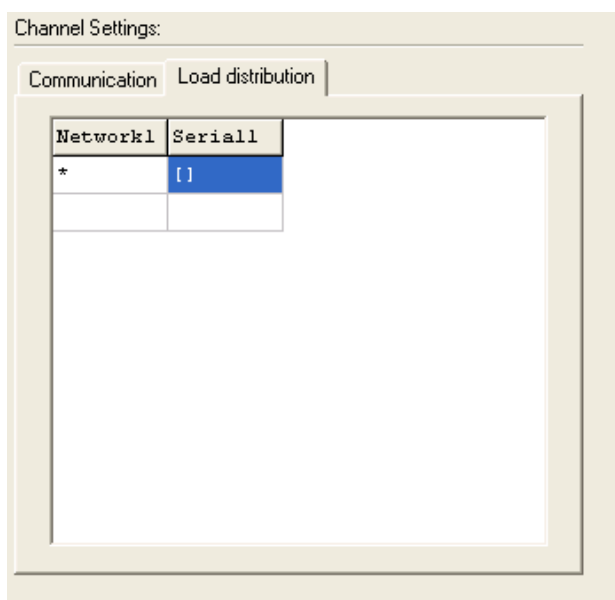


Figure 22 - Fail-Over Channel Settings Load Distribution Tab

The **Load Distribution** tab contains a grid of text entry cells, with a column for each selected communication channel.

To create a Fail-over 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 **Fail-over Channel** object type.
4. Click on the **OK** button.
5. The **Create New** window appears (Figure 19).

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.

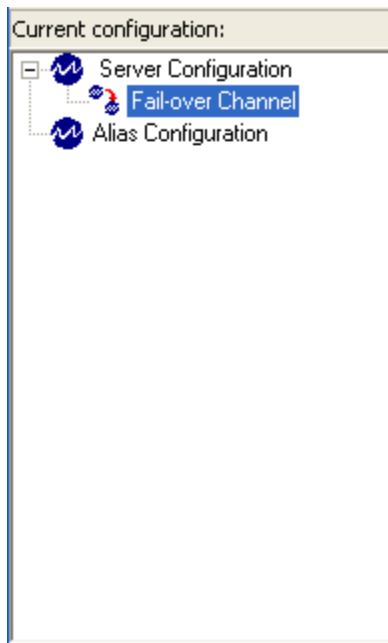


Figure 23 - New Fail-Over Channel Object

To specify load distribution:

1. In the **Configuration** window, under **Server Configuration**, select an existing **Fail-over channel**.
2. The **Fail-over Channel Settings** panel is displayed.
3. Click on the **Load Distribution** tab to view and edit load distribution settings for this fail-over channel.

- For each channel selected on the **Communication** tab, enter a pattern-matching string under the appropriate column to specify the data items to poll or to avoid polling on that channel.

Notes:

- The pattern-matching string must follow the syntax of the *Visual Basic Like* operator and applies to the portion of the **item ID** following the channel name. Prefix the string with an exclamation point (!) to indicate items to avoid scanning on that channel if possible.
 - In general, Primary and Secondary channels each have a single filter string: * (match all) and [] (match none), respectively. A Standby channel has no filter strings at all (this indicates that all items are undesired). The use of Primary, Secondary, and Standby channels is entirely at the user's discretion.
- When you have edited the settings, either click on the **Communication** tab to edit the communications settings, or

Click on the **Apply** button to commit your changes.

Creating and Configuring a Network Channel Object

The **Create New Network Channel** window (Figure 24) displays the settings available for configuring a **Network Channel**. The settings include protocol, inter-device delay, and threshold rate.

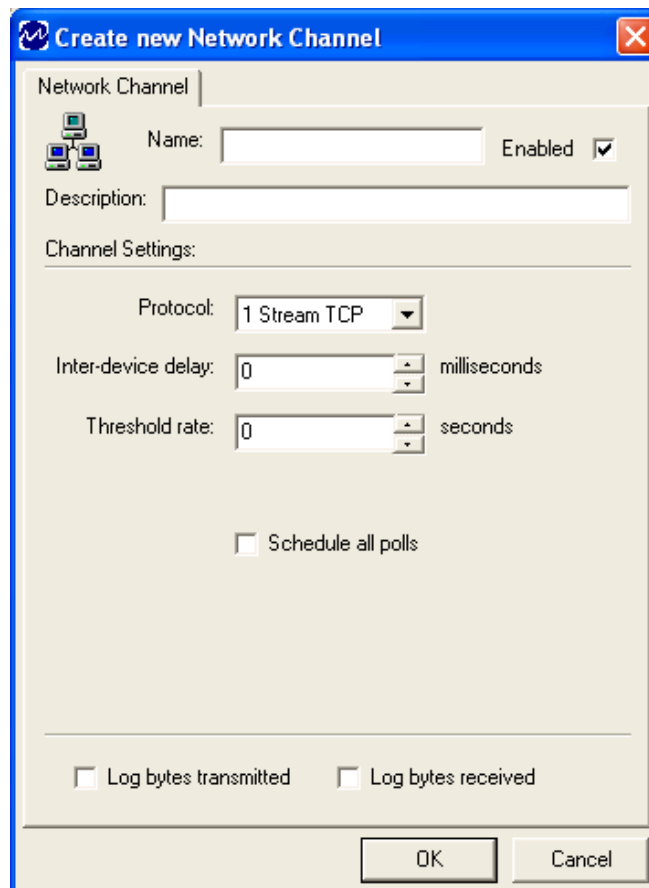


Figure 24 - Create New Network Channel Window

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. 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.
Inter-device delay	Allows you to specify 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. Default = 0
Threshold rate	Maximum achievable scan interval (in seconds) for the channel. The server polls items with update rates faster than this on a continuous basis. Changing this option requires the server to re-optimize communication with all units on this channel. Default = 0 Note: All units on the channel must re-optimize if this parameter changes.
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 cleared. 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.

Component	Description
OK	Select this button to save any changes and close the window.
Cancel	Select this button to close the window without saving any changes made.

Table 22 - Create New Network Channel Window Components

To create a Network 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 **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.

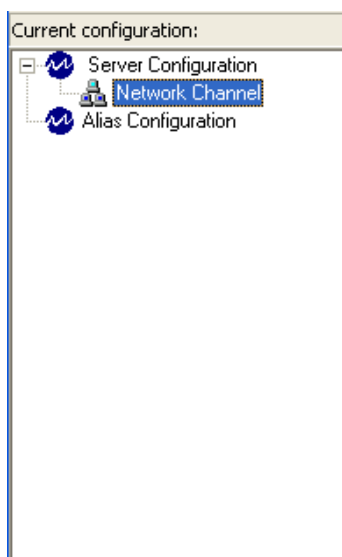


Figure 25 - New Network Channel Object

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

The **Create New Serial Channel – Communication** tab (Figure 26) includes those settings for device, baud rate, parity, etc.

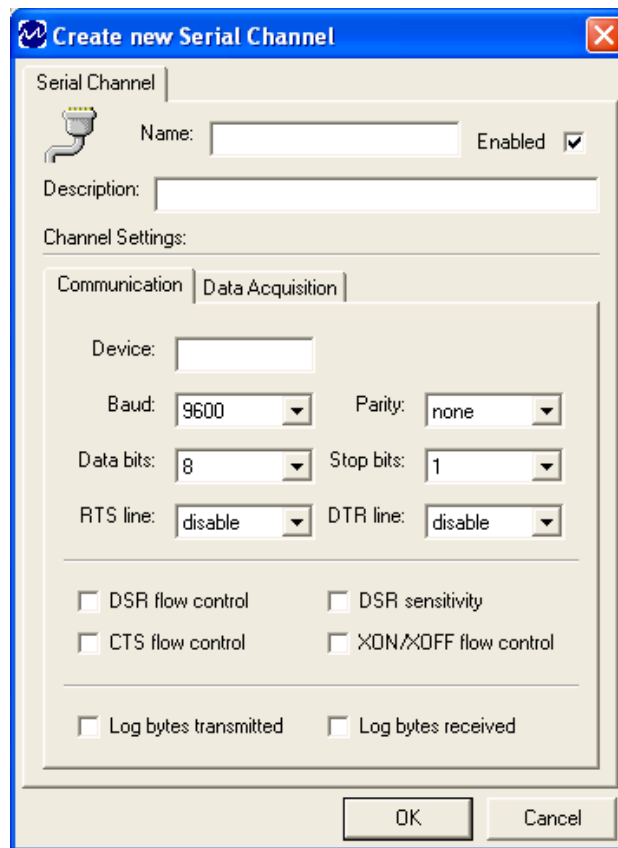


Figure 26 - Create New Serial Channel Window - Communication Tab

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.,

Component	Description
	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. By default, this field is blank. Note: This information stays consistent across both tabs.
Device	Allows you to enter a local communications resource name (i.e., COM port).
Baud	Allows you to define the communication rate by selecting a value from the drop-down list. Values range between 110 and 256000 . Default = 9600
Parity	Allows you to select, from the drop-down list, the type of parity to be used. Options available are none , odd , even , mark , and space . Default = none
Data bits	Allows you to 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	Allows you to select, from the drop-down list, the number of stop bits. Options available are 1 , 1.5 , and 2 . Default = 1
RTS line	Allows you to select, from the drop-down list, a Request To Send (RTS) preset. Available options are disable , enable , handshake , and toggle . Default = disable Note: Must be disabled when working with radio modems that require key up and key down delays.
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. If this option is selected and DSR is turned off, output is suspended until DSR is sent again. 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). If this option is selected, the driver ignores any bytes received, unless the DSR modem input line is high. 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. If this option is selected and CTS is turned off, output is suspended until CTS is sent

Component	Description
	again. 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 during transmission and reception. 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. Note: This information stays consistent across both tabs.
Cancel	Select this button to close 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

The **Create New Serial Channel - Data Acquisition** tab (Figure 27) includes settings for delay times and intervals.

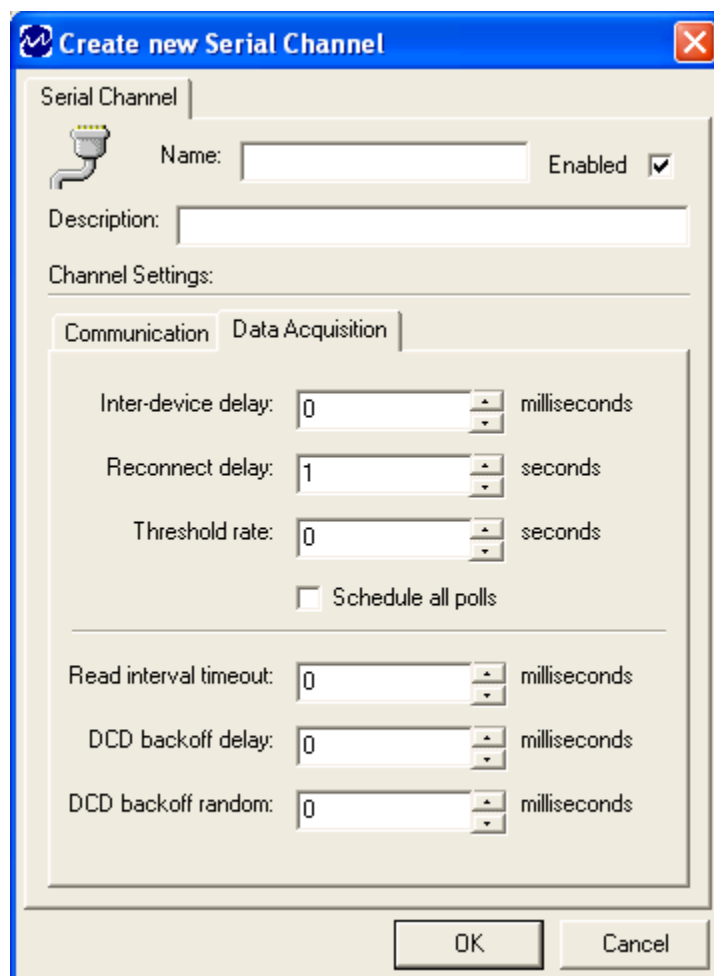


Figure 27 - Create New Serial Channel Window - Data Acquisition Tab

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

Component	Description
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. By default, this field is blank. Note: This information stays consistent across both tabs.
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

Component	Description
	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 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 channel. The server polls items with update rates faster than this on a continuous basis. Changing this option requires the server on this channel to re-optimize communication with all units 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 = checkbox is cleared. Note: All units on the channel must re-optimize if this parameter changes.
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
OK	Select this button to save any changes and close the window. Note: This information stays consistent across both tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across both tabs.

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

To create a Serial 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 **Serial Channel** object type.
 4. Click on the **OK** button.
 5. 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.

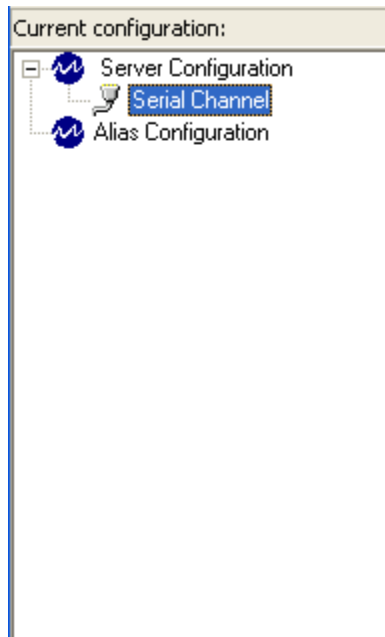


Figure 28 - New Serial Channel Object

Creating and Configuring a Server Status List Object

The **Server Status List** object makes it possible to monitor the status of the OPC server in a customizable way. The Server Status List object contains a list of device links that can exist anywhere in the OPC server hierarchy. The status of the server will be checked at the configured status check period, by examining the status of the subscribed device links. Device links added to

the subscriptions list can be directly monitored, or may be entered as parent device links of subordinates that will be directly monitored.

There are two options for the logic that will determine the server status. For the **Server Status** to be **Running**, the first option requires that there is at least one subscribed device link that is running. In this case, if all subscribed device links enter a failure condition (e.g., become disconnected), the **Server Status** will be **Failed**. The second option is stricter as it is required that all subscribed device links be running. In this case, if any subscribed device links enter a failure condition, the **Server Status** will be **Failed**.

Multiple Server Status Lists can exist and there can be one or more device links contained within a Server Status List. There is no restriction on having a particular device link contained within more than one Server Status List.

The **Create New Server Status List** window (Figure 29) displays the settings available for configuring a Server Status List object.

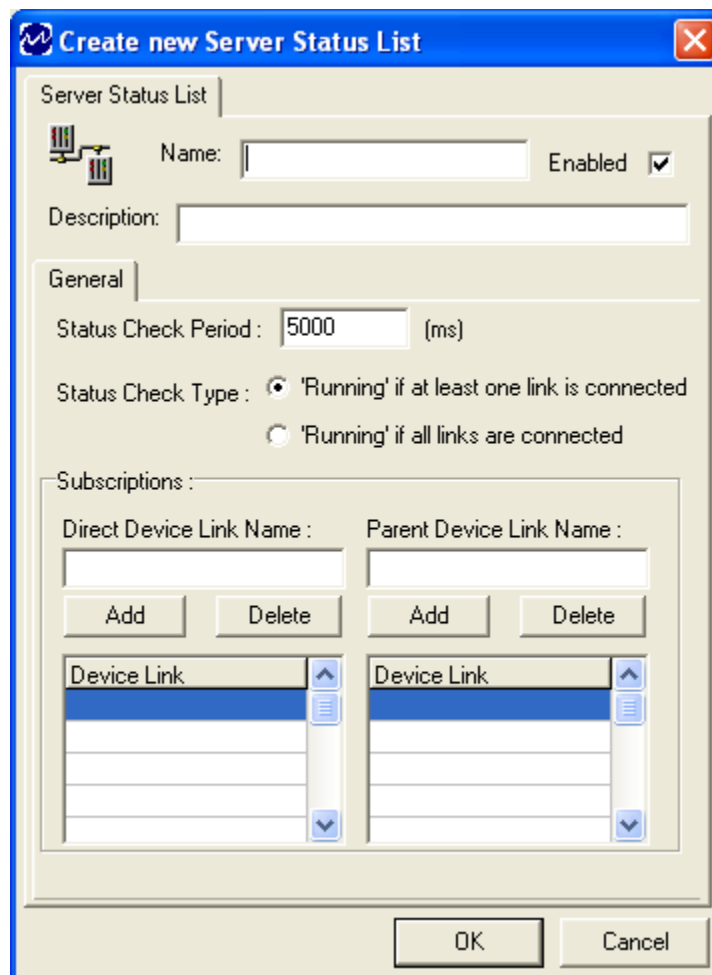


Figure 29 - Create New Server Status List Window

Table 25 describes the components of the **Create New Server Status List** 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.

Component	Description
	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 cleared.
Description	This field is optional and takes any user-defined text (64-character maximum) for documentation purposes. By default, this field is blank.
Status Check Period	Allows you to enter a value to define how often (in milliseconds) to check connected device links to make sure they are still actively communicating with a device. Default = 5000 ms.
Status Check Type	Allows you to select the type of logic used to determine Server Status . Selecting the first option, 'Running' if at least one link is connected , results in a Server Status of Running (rather than Failed) if there are one or more device links with a status of Running . Selecting the second option, 'Running' if all links are connected , results in a Server Status of Failed if there are one or more device links with a status of Failed .
Subscriptions	This section of the General tab displays those device links defined as part of the server status list. The Subscriptions section contains the following fields and buttons which are described below: Direct Device Link Name , Parent Device Link Name , Add , Delete .
Direct Device Link Name	Allows you to enter the name of the device link that is going to be added to the list of Direct Device Links. These device links have their state monitored directly. The full path of the device link must be entered.
Parent Device Link Name	Allows you to enter the name of the device link that is going to be added to the list of Parent Device Links. The subordinates of these device links will have their state monitored directly. The full path of the parent device link must be entered. Note: Only immediate subordinates are monitored. If a parent device link named Parent has a subordinate Child that is the parent of another device link, Grandchild , only the Child device link is monitored. For Grandchild to be monitored, it may be added to the Direct Device Link list, or Child may be added to the Parent Device Link list.
Add	After entering a device link name into either the Direct Device Link Name field, or the Parent Device Link Name field, use the Add button for that particular list to add the device link to the list. Note: Once you have added a device link, you can make changes to it or delete it (see Delete for more information). To update a device link, from the list, highlight the one you want to change. Notice that the Add button now reads Update . Make the necessary changes and click on the Update button.

Component	Description
Delete	Select the device link you want to remove from a particular list (either a Direct Device Link Name, or a Parent Device Link Name) and click on the Delete button.
OK	Select this button to save any changes and close the window.
Cancel	Select this button to close the window without saving any changes made.

Table 25 - Create New Server Status List Window Components

To create a Server Status List 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 **Server Status List**.
- 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 **Server Status List** is selected, then the **Create New Server Status List** 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 **Server Configuration** item as shown in Figure 30.

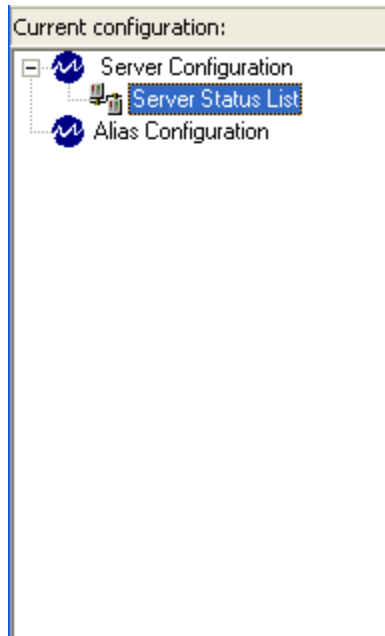
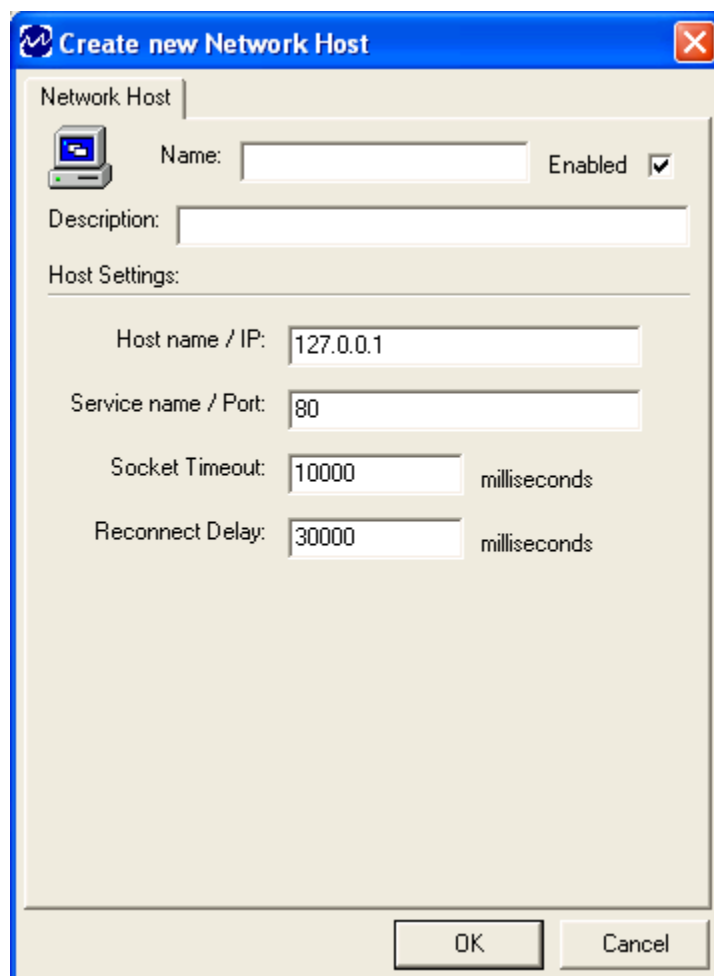


Figure 30 - New Server Status List Object

Creating and Configuring a Network Host Object

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

The **Create New Network Host** window (Figure 31) displays the settings available for configuring a **Network Host**: host and service names, socket timeouts, reconnect delay, ping frequency and attempts.



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 31 - Create New Network Host Window

Table 26 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 DNS host name or "dotted quad" IP address. A blank field indicates that the socket binds to a local address and behaves as a server.
Service name / Port	Allows you to define the IP service name or port number.

Component	Description
Socket Timeout	Allows you to specify the time (in milliseconds) to wait for a response on the socket. Default = 10000
Reconnect Delay	Allows you to specify the time (in milliseconds) to wait before attempting to reconnect. Default = 30000
OK	Select this button to save any changes and close the window.
Cancel	Select this button to close the window without saving any changes made.

Table 26 - 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 32) appears.

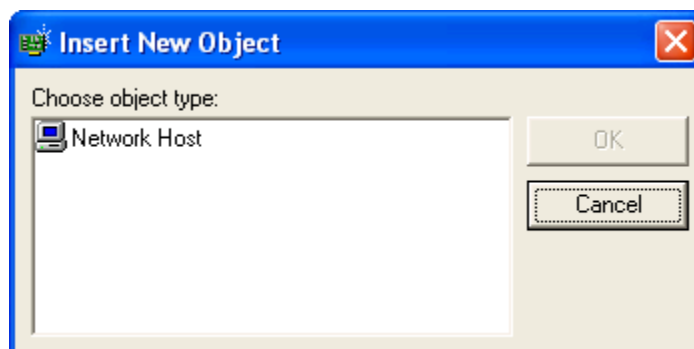


Figure 32 - Insert New Object

- From the displayed list, select **Network Host**.
- Click on the **OK** button.
- The **Create New** window appears (Figure 31).

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.

8. Click on the **OK** button. The object is created and will appear as a child of the **Network Channel** item as shown in Figure 33.

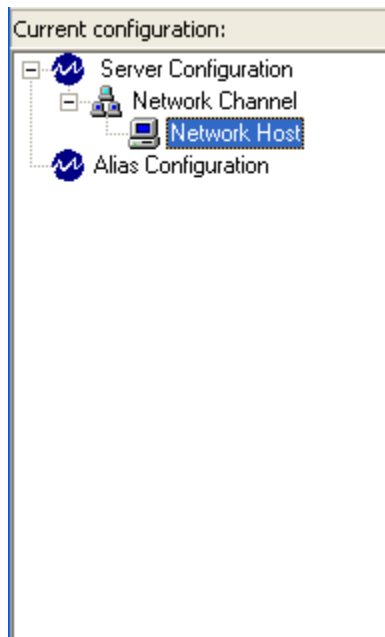


Figure 33 - New Network Host Object

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 Dial-up Connection** window displays the settings available when creating a **Dial-up Connection** object and includes three tabs:

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

Notes:

- When communicating with a dial-up modem on a direct serial connection, you must configure the serial communication channel to employ the appropriate form of flow control for the modem. Typical hardware flow control involves setting the DTR line control to *enable* (see **Serial Channel Settings Communication Tab**). Modems generally do not use parity (set to *none*) and use either **8** data and **1** stop bit, or **7** data and **2** stop bits.
- Ensure that there is enough idle time between dial-outs (polls) for the server to receive incoming calls when the controlled station is configured to dial in spontaneously. Otherwise, the controlled station consistently receives busy signals. Increase the inter-device delay or schedule dial-out operations to leave sufficient time for dial-in connections (see **Serial Channel Settings Data Acquisition Tab**).



Dial-Up Tab

The **Create New Dial-up Connection - Dial-up** tab (Figure 34) includes dial command, delays, and redials settings.

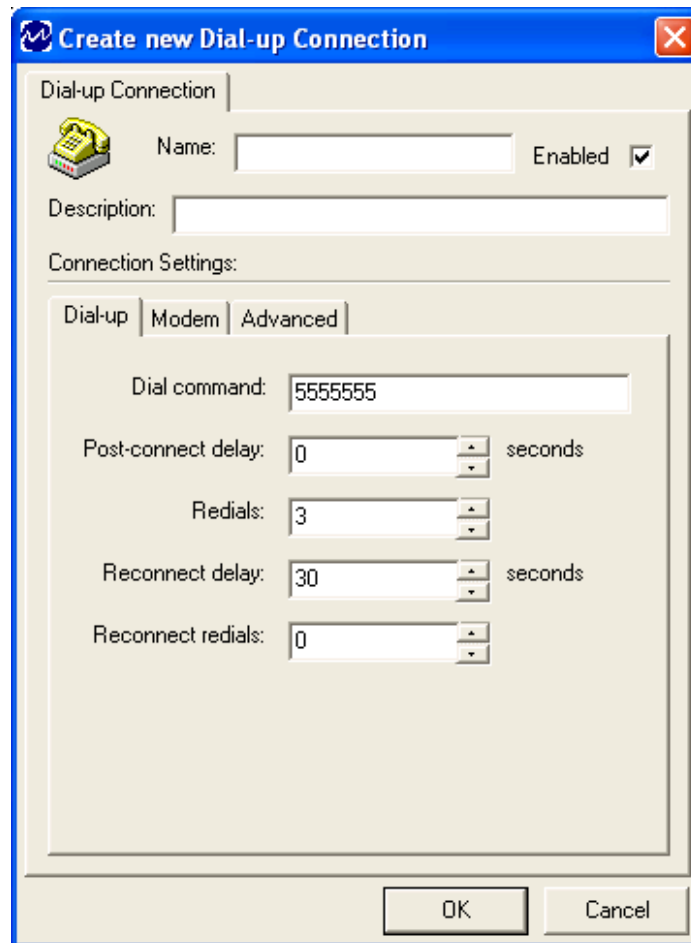


Figure 34 - Create New Dial-Up Connection Window - Dial-Up Tab

Table 27 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 ATD 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	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

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

Modem Tab

The Create New **Dial-up Connection - Modem** tab (Figure 35) includes settings for the modem's reset command and delay, the initialize command, and the number of retries

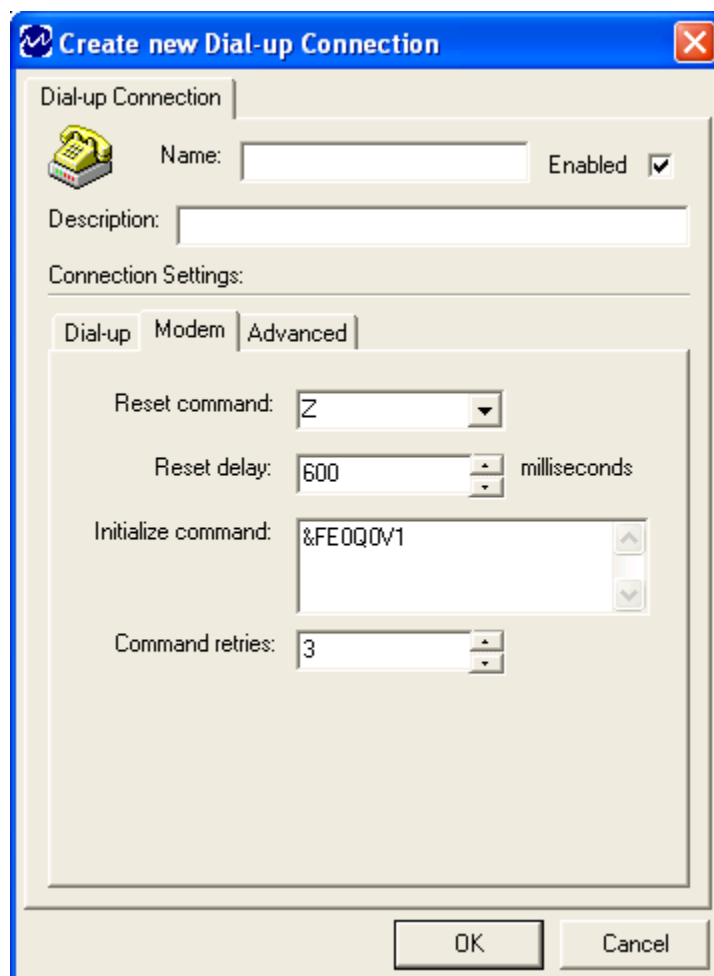


Figure 35 - Create New Dial-Up Connection Window - Modem Tab

Table 28 describes the components of the **Create New Dial-up Connection - Modem** 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.
Reset command	Allows you to select, from the drop-down list, a modem reset command

Component	Description
	(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 EOQ0V1 .
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	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 28 - Create New Dial-up Connection Window - Modem Tab Components

Advanced Tab

The **Create New Dial-up Connection - Advanced** tab (Figure 36) includes settings for timeouts, command terminator, and escape character and guard time.

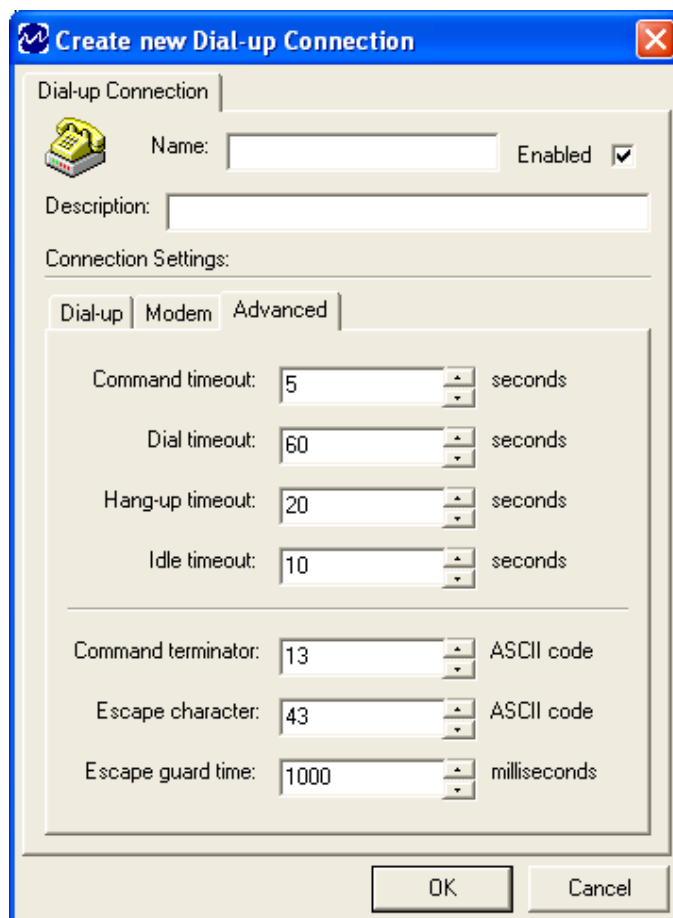


Figure 36 - Create New Dial-up Connection - Advanced Tab

Table 29 describes the components of the **Dial-up Connection Settings Advanced** 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.
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 dialled 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 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.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 29 - Create New Dial-Up Connection Window - Advanced Tab Components

To create a Dial-up Connection object:

Notes:



- When using the communication channel to receive dial-in connections, configure one and only one dial-in connection. Leave the **Dial** command blank (no dial-out), and enable auto-answer in the initialization string (**S0=1**). Alternatively, you can pre-initialize the modem from persistent RAM or dip switches, and omit the dial-up configuration entirely.
- Recommended commands for modem initialization are factory defaults (**&F**), local echo off (**E0**), result codes enabled (**Q0**), result codes displayed as text (**V1**). The server does not recognize results codes displayed as numbers (**V0**) as this too closely resembles RTU communication. The server requires result codes for it to function properly, so do not turn them off (**Q1** or **Q2**). Other possible commands are disable auto-answer (**S0=0**), wait for carrier one minute (**S7=60**), carrier detect timeout 0.6s (**S9=6**), and carrier loss delay 1.4s (**S10=14**).
- On the **Advanced** tab, do not set the escape sequence character (**S2=43**), carriage return character (**S3=13**), or guard time (**S12=20**) with the initialization string. This can prevent the server from putting the modem into command mode properly.

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 (Figure 37) appears.

Note: The available objects displayed in the **Insert New Object** window depends on the selected parent item.

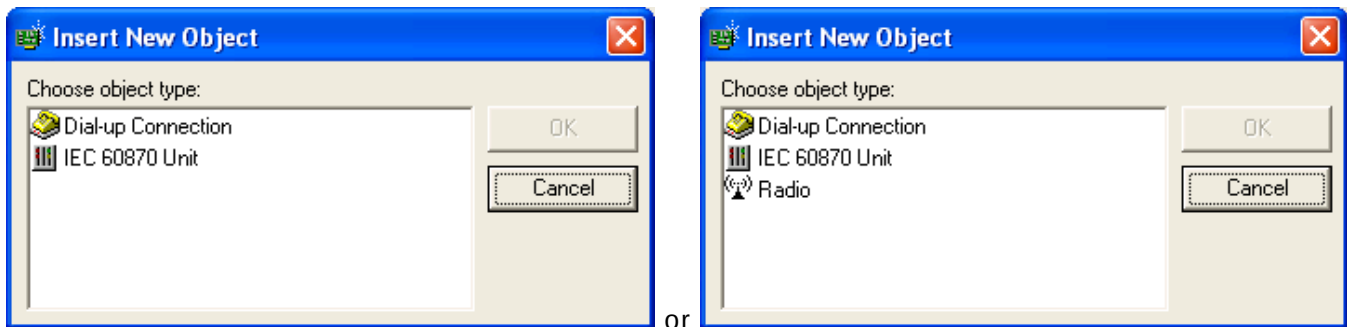


Figure 37 - Insert New Object Window

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 34).

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 38 (depending on what the selected parent item was).

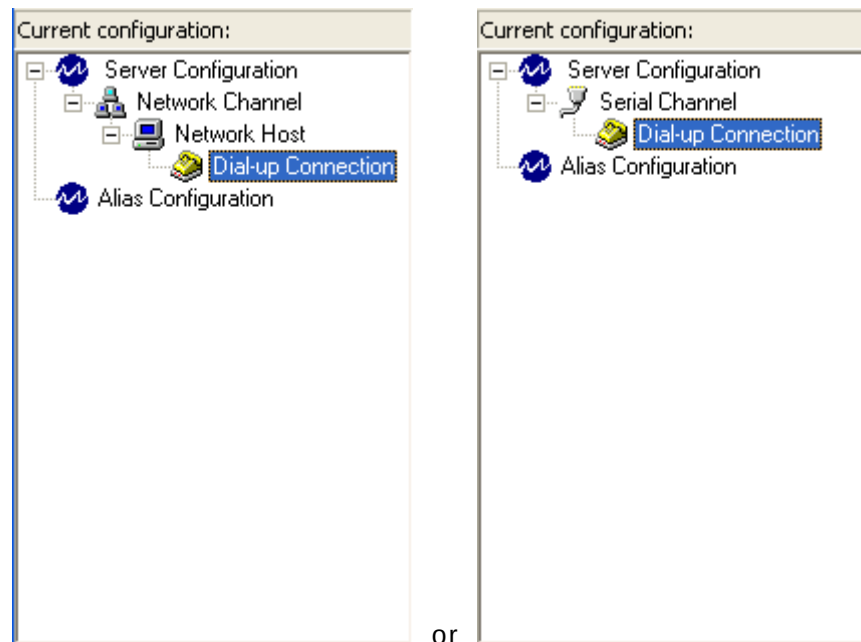


Figure 38 - New Dial-Up Connection Object

Creating and Configuring an IEC 60870 Unit Object

Note: An **IEC 60870 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 **Create New** window (Figure 39) displays the settings available when creating an **IEC 60870 Unit** object.

The **Create New IEC 60870 Unit** window includes four tabs:

- **Communication**

- Data Acquisition
- Parameters
- Advanced

Communication Tab

The Create New **IEC 60870 Unit - Communication** tab (Figure 39) includes settings for the link address, protocol, base poll time, time bias, originator address, and the field sizes for the link address, cause of transmission, common address, and object address.

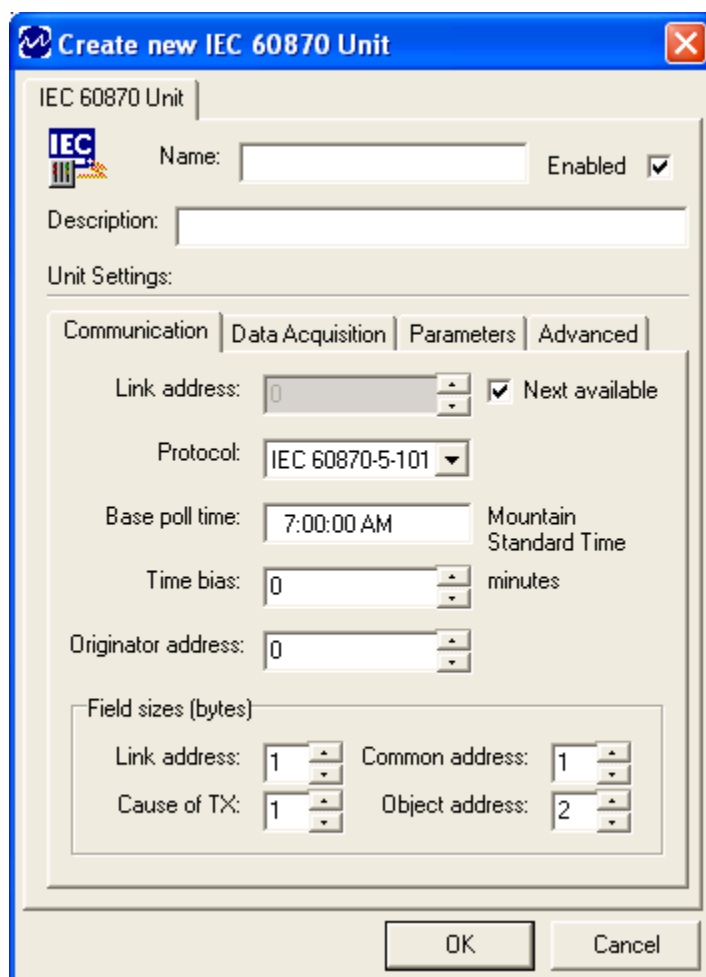


Figure 39 - Create New IEC 60870 Unit Window - Communication Tab

Table 30 describes all of the components of the **Create New IEC 60870 Unit - 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.,

Component	Description
	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.
Link address	Allows you to enter or select a value defining an IEC 60870-5 link address (0-65535). The unit disconnects and reconnects if this parameter changes. Changing this option requires the server to reset communication with this unit. This field is not available (i.e., is greyed out) when the Next available checkbox is selected.
Next available	When this checkbox is selected, the unit will default to the next available IEC 60870-5 link address on this channel. When this checkbox is selected, the Unit address field is disabled (i.e., greyed out).
Protocol	Allows you to select, from the drop-down list, which protocol the unit supports (i.e., IEC 60870-5-101 or IEC 60870-5-104).
Base poll time	Allows you to enter or select a normalization time for scheduling polls, stored as UTC HH:MM:SS. 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 a timestamp from the controlled station, to convert it to UTC.
Originator address	Cause of transmission originator address (if cause size is 2).
Field sizes (bytes)	
Link address	Allows you to enter or select the size (in bytes) of the link address field (0, 1, or 2).
Common address	Allows you to enter or select the size (in bytes) of the common address field (1 or 2).
Cause of TX	Allows you to enter or select the size (in bytes) of the cause of transmission field (1 or 2).
Object address	Allows you to enter or select the size (in bytes) of the information object address fields (1, 2, or 3).
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 30 - Create New IEC 60870 Unit Window - Communication Tab Components

Data Acquisition Tab

The **Create New IEC 60870 Unit - Data Acquisition** tab (Figure 40) includes settings for the inter-message delay, reply timeout, retries, reconnect delay, reconnect retries, max interrogate time, command timeout and reset process delay.

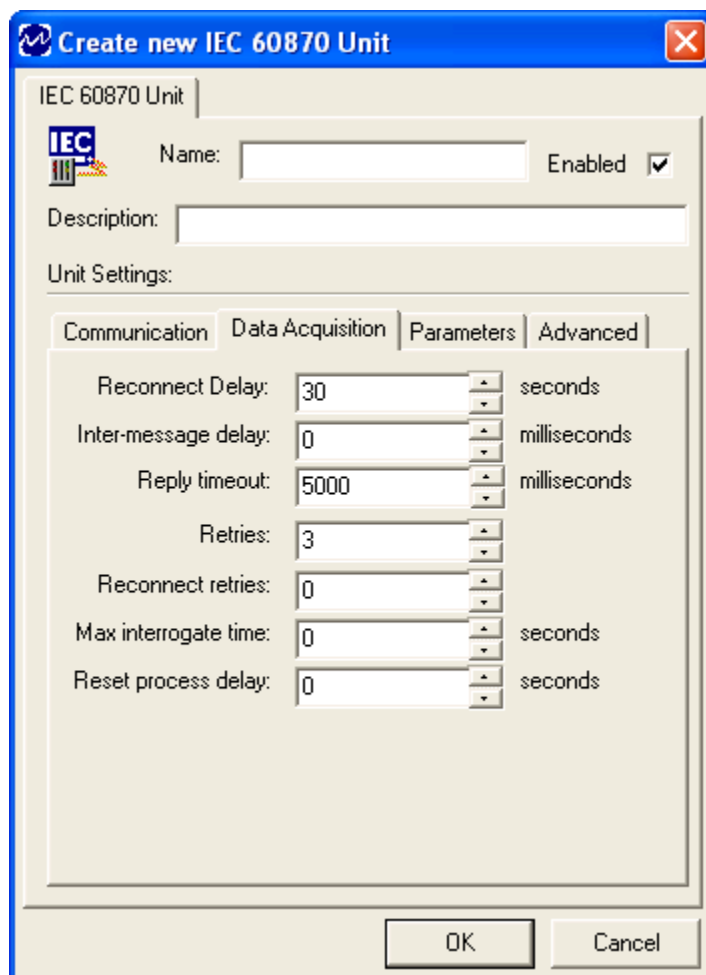


Figure 40 - Create New IEC 60870 Unit Window - Data Acquisition Tab

Table 31 describes all components of the Create New **IEC 60870 Unit - Data Acquisition** 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.

Component	Description
	By default, this field is blank. Note: This information stays consistent across all tabs.
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. Default = 30
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. Note: If this is set to 0 then the setting will be disabled. Default = 0
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. Note: If this setting is too short, communication can become confused. Default = 5000
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. Default = 3
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. Default = 0
Max interrogate time	Allows you to enter or select a value defining the maximum amount of time (in seconds) to allow a unit to be interrogated. A value of 0 indicates that interrogation must be stopped manually. Default = 0
Reset process delay	Allows you to enter or select a value defining the minimum amount of time (in seconds) to wait before attempting to reconnect after receiving a reset process activation confirmation. Default = 0
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 31 - Create New IEC 60870 Unit Window - Data Acquisition Tab Components

Parameters Tab

The **Create New IEC 60870 Unit - Parameters** tab includes settings (Figure 41) for the IEC 60870 timing parameters t_0 , t_1 , t_2 , t_3 and the message sequence parameters k and w .

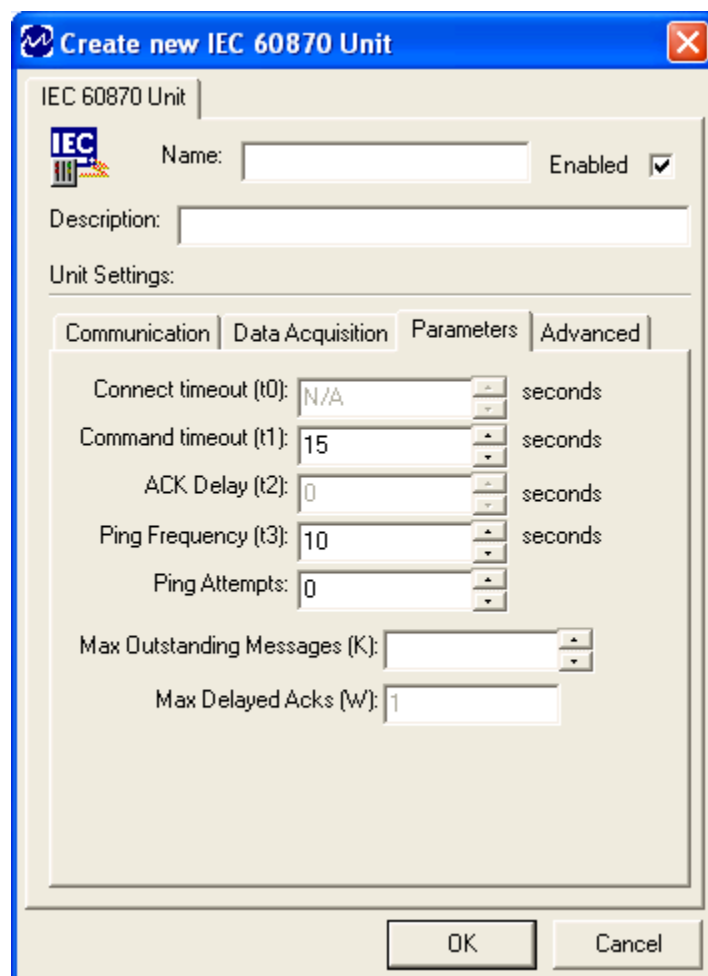


Figure 41 - Create New IEC 60870 Unit Window - Parameters Tab

Table 32 describes the components of the **Create New IEC 60870 Unit - Parameters** 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.
Connect Timeout (t0)	Displays a value defining the amount of time (in seconds) that the OPC server will wait for a response when attempting to connect to a device.

Component	Description
	This option is not configurable on the unit and therefore the field appears disabled (i.e., greyed out). The connect timeout used during communication depends on the protocol selected (60870-5-101 vs. 60870-5-104), and is a combination of the command timeout and in the case of the 60780-5-104 protocol, the TCP/IP socket timeout configured on the Network Host device link.
Command Timeout (t1)	Allows you to enter or select a value to define the amount of time (in seconds) the OPC server should wait for a response to a command sent to the device. If this timeout is exceeded, the server will start retrying the command according to the retry settings on the Data Acquisition tab. This item corresponds to the IEC 60780-defined t₁ parameter.
ACK Delay (t2)	Displays the maximum amount of time (in seconds) the server will delay sending an acknowledgement. This corresponds to the IEC 60870 defined t₂ parameter. This item is not configurable, is set to 0 , and therefore the field appears disabled (i.e., greyed out). The OPC server will acknowledge all received packets immediately.
Ping Frequency (t3)	Allows you to enter or select a value defining the time (in seconds) required for sending test frames in case of a long idle state. This corresponds to the IEC 60870 defined t₃ parameter. The OPC server will send a test frame if no other message has been received for this amount of time.
Ping Attempts	Allows you to enter or select a value defining the number of ping attempts that are to be made. When a test frame is sent, and no response is received in the Command Timeout length of time, the OPC server will attempt to send additional test frames until either the device responds, or the number of Ping Attempts is exhausted. When the number of Ping Attempts is exhausted without a response, the OPC server will report the unit as failed, and will move on in the polling cycle.
Max Outstanding Messages (K)	Allows you to enter or select a value defining the maximum difference between the receive sequence number and the send state variable. The OPC server will continue sending messages to the end device until there is the specified number of outstanding messages awaiting a response. No further messages will be sent until commands time out, or a response is received.
Max Delayed Acks (W)	Displays the latest acknowledgement after receiving the specified number of I-format APDUs. This item is not configurable, is fixed at 1, and therefore the field appears disabled (i.e., greyed out). The OPC server will send an acknowledgement immediately after receiving each I-format APDU.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 32 - Create New IEC 60870 Unit Window - Parameters Tab Components

Advanced Tab

The **Create New IEC 60870 Unit - Advanced** tab (Figure 42) includes settings for balanced transmission, confirm user data, send short ACK, receive short ACK, allow commands, optimistic commands, allow C_RD_NA_1, latch monitor data, require ACTTERM and require GI ACTTERM.

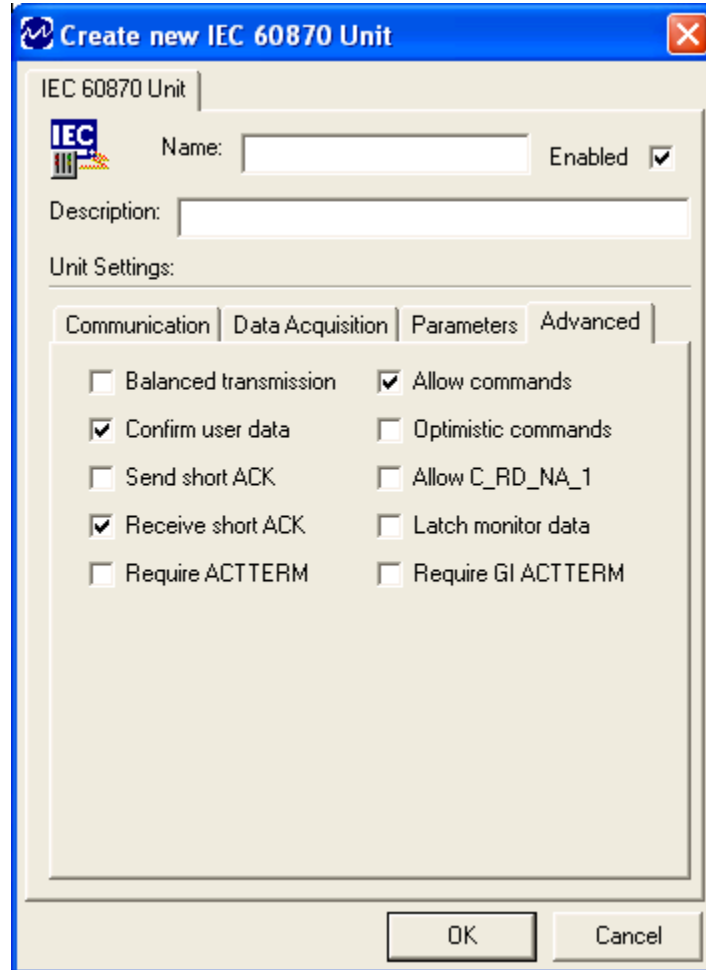


Figure 42 - Create New IEC 60870 Unit Window - Advanced Tab

Table 33 describes the components of the **Create New IEC 60870 Unit - Advanced** 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.

Component	Description
	By default, this field is blank. Note: This information stays consistent across all tabs.
Balanced transmission	This checkbox indicates whether the link is balanced (i.e., any station can transmit spontaneously) as opposed to unbalanced (i.e., only the controlling station can transmit spontaneously). The link is balanced if the checkbox is selected.
Allow commands	This checkbox indicates whether output operations are allowed (i.e., checkbox is selected) to a unit, or disallowed (i.e., checkbox is cleared).
Confirm user data	This checkbox indicates whether to request confirmation of user data transmissions (i.e., checkbox is selected). This has no effect on broadcast units.
Optimistic commands	This checkbox indicates whether to update a command item with the written value and an uncertain (non-specific) quality immediately after issuing the activation/deactivation command and before receiving the confirmation response.
Send short ACK	This checkbox indicates whether to transmit single-character acknowledgements (i.e., checkbox is selected) rather than fixed-length control frames (i.e., checkbox is cleared).
Allow C_RD_NA_1	This checkbox indicates whether to use single-read commands (C_RD) to perform instantaneous polls for monitor items. Otherwise (i.e., checkbox is cleared), a device read does nothing.
Receive short ACK	This checkbox indicates whether to accept single-character acknowledgements from the controlled station (i.e., checkbox is selected) rather than just fixed-length control frames (i.e., checkbox is cleared).
Latch monitor data	When this checkbox is selected, items “freeze” at their last value/quality/timestamp rather than going to bad qualities when the unit is set off scan.
Require ACTTERM	When this checkbox is selected, the OPC server waits for and acknowledges an ACTTERM command from the device following the completion of a command. This option does not apply to the C_IC_NA and C_CI_NA items.
Require GI ACTTERM	When this checkbox is selected, the OPC server waits for and acknowledges an ACTTERM command from the device following the completion of either the C_IC_NA or C_CI_NA command. The IEC 60780 specification states that an ACTTERM for these messages is optional. This option must be configured to match the behaviour of the specific device.
OK	Select this button to save any changes and close the window. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 33 - Create New IEC 60780 Unit Window - Advanced Tab Components

To create an IEC 60870 Unit object:



Note: When creating a new **IEC 60870 Unit** object, on the **Communication** tab, a checkbox labelled **Next Available** appears next to the **Link address** field. If the checkbox is selected, the **Link address** field is disabled. Leave the checkbox selected to have the server automatically choose the next available station address on the channel. The **Next Available** checkbox does not appear on the **Communication** tab when you select an existing unit in the **Current configuration** pane of the **Configuration** window.

1. On the **Configuration** window, select a previously-created **Network Host**, **Dial-up Connection**, **Serial Channel**, or **Radio** link, 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.

Note: The object listed in the **Insert New Object** window will depend on the previously-created object selected in step 1.

3. From the displayed list, select the **IEC 60870 Unit** object type.
4. Click on the **OK** button.

5. 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 **IEC 60870 Unit** is selected, then the **Create New IEC 60870 Unit** 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.

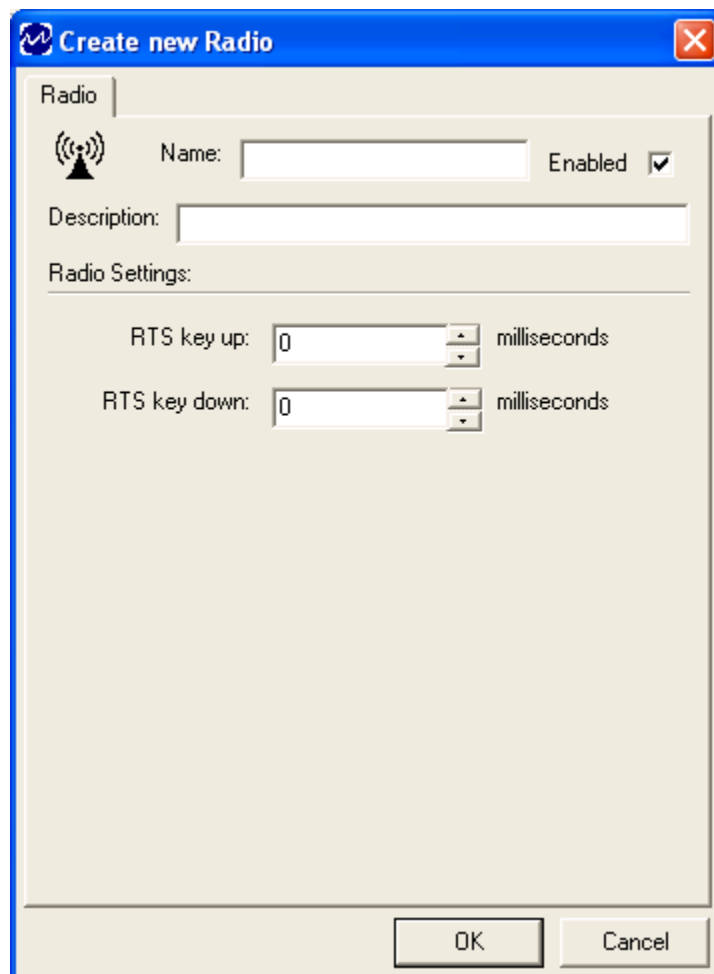
Note: For the object to be used for communication, it must be enabled (i.e., the **Enabled** checkbox is selected). This can be done at any time.

8. Click on the **OK** button. The object is created and will appear either as a child of the selected item.

Creating and Configuring a Radio Object

Note: A **Radio** object is created as a child of a **Serial Channel**.

The **Create New Radio** window (Figure 43) includes setting the RTS key up and key down.



The image shows a Windows-style dialog box titled "Create new Radio". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into sections. At the top, there's a "Radio" tab. Below it, on the left, is a radio icon. To its right is a "Name:" label followed by a text input field. Further right is an "Enabled" label with a checked checkbox. Below these is a "Description:" label followed by a larger text input field. Underneath is a section titled "Radio Settings:". It contains two rows: "RTS key up:" followed by a numeric input field set to "0" and a "milliseconds" label, and "RTS key down:" followed by another numeric input field set to "0" and a "milliseconds" label. At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 43 - Create New Radio Window

Table 34 describes all of 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. Note: This information stays consistent across all tabs.
Cancel	Select this button to close the window without saving any changes made. Note: This information stays consistent across all tabs.

Table 34 - Create New Radio Window Components

To create a Radio object:

- 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 44) appears.

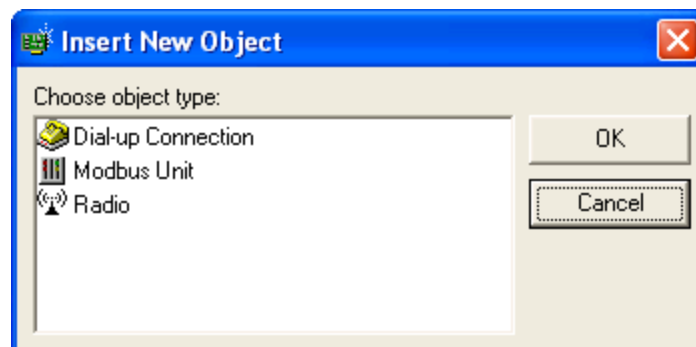


Figure 44 - Insert New Object

- From the displayed list, select **Radio**.
- Click on the **OK** button.
- The **Create New** window appears (Figure 43).
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 45.

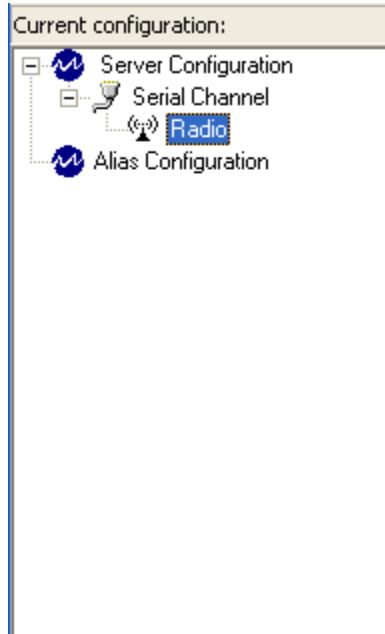


Figure 45 - New Radio Object

Creating and Configuring Server Defaults

The **Server Defaults** window (Figure 46) is used to both view and to edit server default settings, which are used as the initial settings when creating a new object of that type. The **Server Defaults** window includes tabs for each object type:

- **Serial Channel**
- **Network Channel**
- **Fail-over Channel**
- **Server Status List**
- **Dial-up Connection**
- **Radio**
- **IEC 60870 Unit**
- **Network Host**

Clicking on these tabs will take you to the respective server defaults for that object type. Use the scroll buttons (outlined in red in Figure 46) to scroll through the available tabs.

To access the Server Defaults window:

1. From the **Configuration** window, select the **Defaults** menu option from the **View** menu on the toolbar.
2. The **Server Defaults** window is displayed.

To edit server default settings:

1. In the **Server Default** window, click on the tab associated with the type of object for which you want to set server defaults.
2. Change the default configuration settings as required.
3. After changing the settings, either click another tab to edit the more settings, or

Click on the **Apply** button to commit your changes.

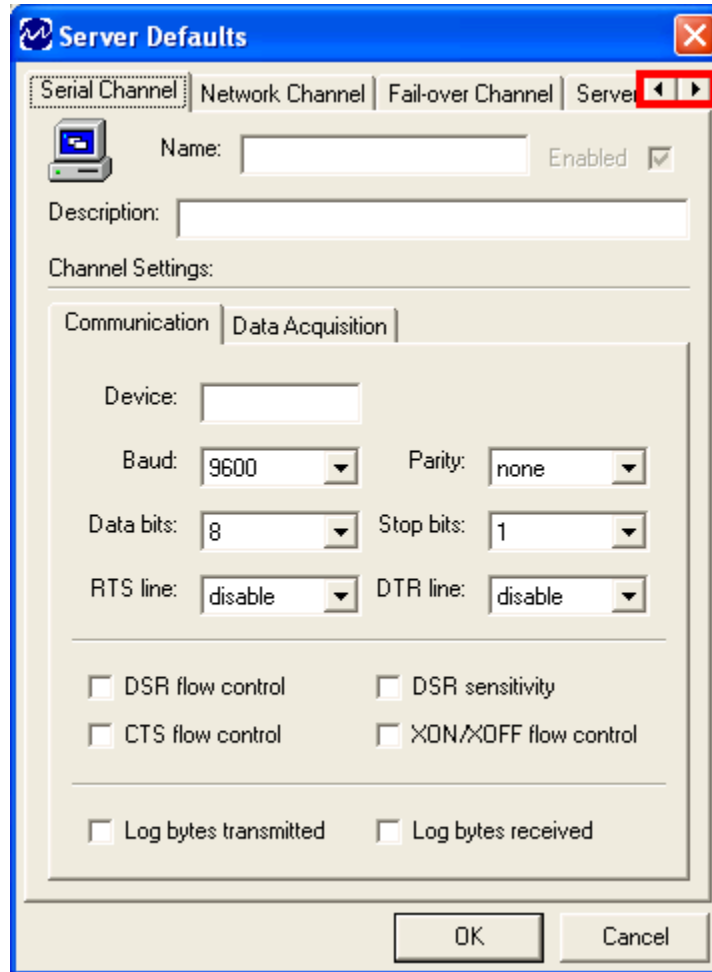


Figure 46 - Server Defaults Window

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 47) will appear when users remove an object that has data items to which one or more OPC clients hold reference.

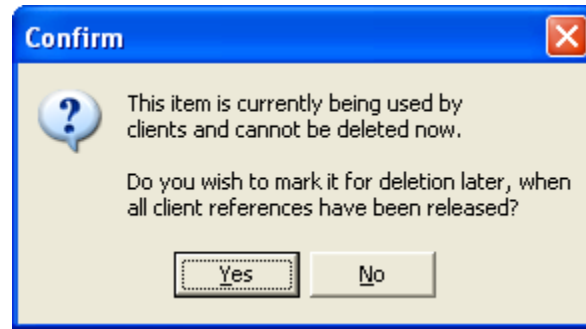


Figure 47 - Client Reference Warning Message

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 47) 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.

The following sub-sections contain information on the types of objects available and how to configure them.

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

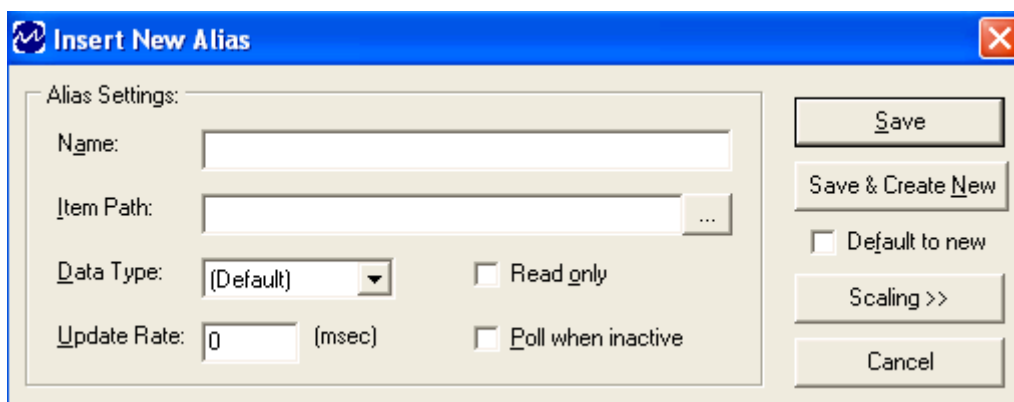
Note: Alias Groups can be renamed after they have been created.

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 48) to insert a new alias into an Alias Group, or insert a new alias on its own directly under the Alias Configuration node.



The **Insert New Alias** window is a dialog box with a blue title bar and a red close button. It contains the following fields and controls:

- Alias Settings:**
 - Name:** A text input field.
 - Item Path:** A text input field with an ellipsis button (three dots) to its right.
 - Data Type:** A dropdown menu currently showing "(Default)".
 - Update Rate:** A text input field showing "0" followed by "(msec)".
- Checkboxes:**
 - ☐ **Read only**
 - ☐ **Poll when inactive**
- Buttons:**
 - Save**
 - Save & Create New**
 - ☐ **Default to new**
 - Scaling >>**
 - Cancel**

Figure 48 - Insert New Alias Window

Table 35 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 (three dots) 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.
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.
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.

Component	Description
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 window.

Table 35 - Insert New Alias Window Options

The **Insert New Alias** window can be expanded to display **Scaling Options** (Figure 49). The available forms of scaling include: **Linear**, **Square Root**, **Gain / Offset**, and simple text **Expressions**.

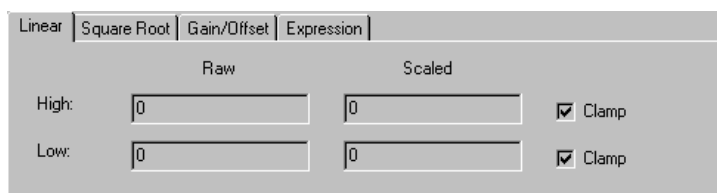


Figure 49 - Insert New Alias Window Scaling Options

Table 36 describes the **Scaling Options** for the **Insert New Alias** window.

Tab	Component	Description
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.
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.
	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.

Table 36 - 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 50), listing the aliases it contains.

Contents of alias group 'New Alias 1':				
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 50 - Contents Table

3. From the **Edit** menu, choose **Insert New Alias**.
4. The **Insert New Alias** window (Figure 48).
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**.
8. The **Scaling Options** are displayed at the bottom of the **Insert New Alias** window (Figure 49).
9. Configure the **Scaling Options** as required (see Table 36 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: **Linear**, **Square Root**, **Gain/Offset**, and **Expression**.

10. Configure the remaining fields as required (see Table 35 for a description of all the components).
11. 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 48), 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 37 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 37 - Expression Wizard Options

Notes:

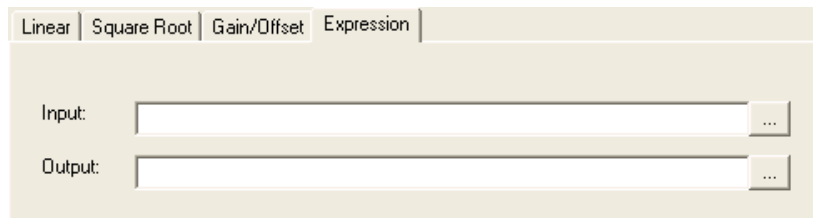
- The **Expression Wizard** appears and functions the same for an input expression as it does for an output expression. The differences being the expression field label: **Input Expression**, **Output Expression**, and that one is for reads and the other for writes.
- If you are expecting to read a particular 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 50 - Contents Table
3.), listing the aliases it contains.
4. 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.
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 49 - Insert New Alias Window Scaling Options
6.) 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.

7. Select the **Expression** tab (Figure 51).



The image shows a window with four tabs: Linear, Square Root, Gain/Offset, and Expression. The Expression tab is selected. Below the tabs, there are two input fields labeled 'Input:' and 'Output:'. Each field has a text box and an ellipsis button to its right.

Figure 51 - Expression Tab

8. Click on the ellipsis button adjacent to the **Input** field (or **Output** field).
9. The **Expression Wizard** (Figure 52) is displayed.



The image shows the Expression Wizard dialog box. It has a title bar with 'Expression Wizard' and a close button. Inside, there is a section labeled 'Input Expression' with a large text area. Below this, there is a section labeled 'Insert at cursor position' with three buttons: 'Database field', 'Function', and 'Variable'. Under these buttons is a row of operators: '+', '-', '*', '/', '=', '<', '>', '<=>', '>=', 'Not', 'And', and 'Or'. At the bottom, there are buttons for 'Clear', 'Validate', 'OK', and 'Cancel'.

Figure 52 - Expression Wizard

10. 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.
11. Click on the **Function** button to go to the **Select function** (Figure 53) window. After selecting the required function, click on the **Continue** button to close the **Select function** window and return to the **Expression Wizard**.



Figure 53 - Select Function Window

12. Click on the **Variable** button to go to the **Select variable** (Figure 54) window. After selecting the required variable, click on the **OK** button to close the **Select variable** window and return to the **Expression Wizard**.

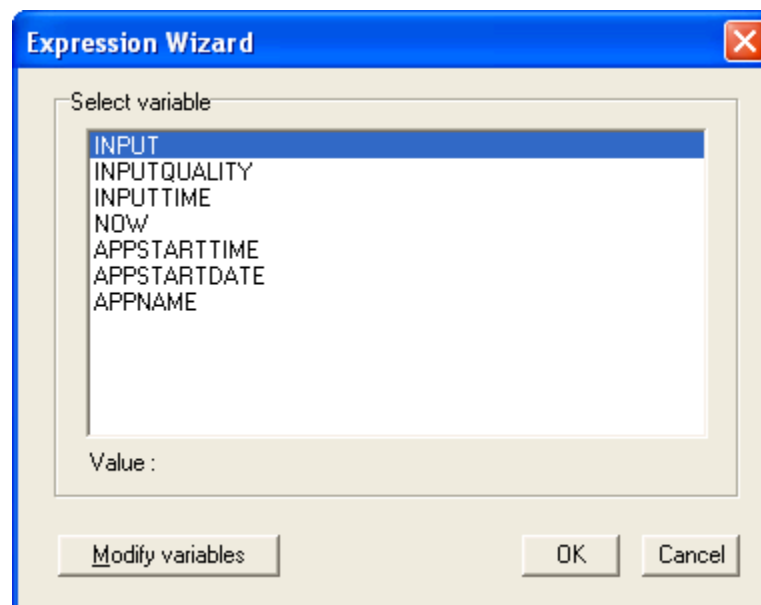


Figure 54 - Select Variable Window

13. If required, from the **Select variable** window, click on the **Modify variables** button to access the **User Defined Functions Editor** (Figure 55) which allows you to add, change, or delete variables.

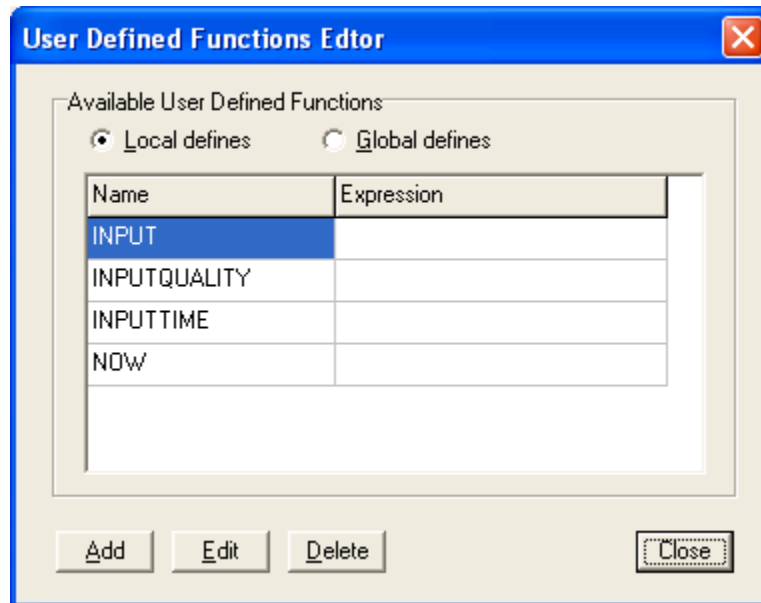


Figure 55 - User Defined Functions Editor

14. The **Operators** buttons (Figure 56) allow you to enter an operation descriptor based on the selected button.



Figure 56 - Operators Buttons

15. Click on the **Validate** button to determine whether or not the expression is valid.
16. 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.
17. 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.
18. From either the **Insert New Alias** or **Edit Alias** window, click on the **Save** button.
19. 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

Note: If you have previously saved a configuration, you can clear the current configuration and then load the saved configuration file.

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

Note: Ordinarily, the server shuts down automatically shortly after the last OPC client disconnects from it. However, if the **Configuration** window is displayed, the configuration utility locks the server so that it will not shut down.

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.

**Notes:**

- 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**.
- If the server is shut down while a client is still connected, the client response is dependent upon that client. Some clients may handle the shutdown gracefully, some will attempt to restart the server, and others will crash. Generally, the client should be disconnected before shutting down the server.

OPC Data Items

This section describes the OPC data items used in the MatrikonOPC IEC 60870 server.

IEC 60870 Items

The server supports **A.T[:Q].X** notation for addressing individual objects on a unit.

- The server tries to extract a valid object address from a given item ID.
- The server accepts any valid integer in the range of **1** to **65535** (as applicable) for the logical station/sector address **A** (the “common address” of the application service data unit).
- The server accepts any valid mnemonic for the type identifier **T** (e.g., **M_ME**, **C_SC_NA**).
- If the mnemonic is for a command or a parameter, the server checks for and accepts any valid integer between **0** and **255** appended to the mnemonic with a colon for the command qualifier **Q** (e.g., **C_IC_NA:20**). The server assumes a value of **0** if the qualifier is not present.
- The server accepts any valid integer in the range of **0** to **16777215** (as applicable) for the information object address **X**.
- The server requires at least the channel and unit names prefixed to the object address, each element separated by a period (e.g., **COM1.RTU1.1.M_SP.1**), to differentiate between objects on different units and different communication channels.

The server accepts communication options 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 server accepts communication options specified in the access path for an item.
- 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. This accommodates clients that do not support access paths. Upon installation, the escape character defaults to the slash (**/**) character. This value can be changed by modifying the following registry key:

\HKEY_CLASSES_ROOT\CLSID\ {189547C8-82A4-48c7-B462-A4BBDB73FDD6} \Options \ItemIDEscapeCharacter

For example, if the escape character is the default **/**, and the Item ID is **NET.GW1.RTU1.1.C_IC_NA:20.0**, and the desired access path is **- +** (which indicates that the item should be polled on connection/reconnection, but never polled cyclically), the following item ID can be used on an OPC client that does not support access paths:

NET.GW1.RTU1.1.C_IC_NA:20.0 / - +

The server supports the following communication options for device items. Changes to the options for an item may require the server to re-optimize the unit where the item is located.

Option	Description
-	Indicates that this item will never be polled cyclically. It may be combined with the + and ! options, but not with the numeric interval option.
+	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. The server may optimize these items separately from other items scheduled at the same scan interval.

Option	Description
interval	Scan interval (milliseconds) for the item. 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 the server uses the fastest one.
!	Indicates that the server polls the item at a high priority (honouring the fastest scan rate). If the same item is requested several times, then the server polls the item at high priority if any of the requested access paths contain this flag.

Table 38 - Communication Options for Device Items

Any combination is valid providing it maintains this order: non-cyclic, initial poll, interval, priority.

Table 39 describes examples of how access path options can be used to control how items are polled.

Item ID / Access Path	Description
NET.GW.RTU.1.C_IC_NA:20.0 / - +	The server will perform a general interrogation command on the selected RTU and CADDR when the OPC server connects to or reconnects to the RTU.
NET.GW.RTU.1.C_IC_NA:20.0 / +120000	The server will perform a general interrogation command on the selected RTU and CADDR when the OPC server connects to or reconnects to the RTU. The server will also perform a cyclic general interrogation command every 120000 milliseconds. The update rate for the OPC group containing this item is overridden by the access path option.
NET.GW.RTU.1.M_SP.0 / 20000	The OPC server will poll the item cyclically every 20000 milliseconds. The update rate for the OPC group containing this item is overridden by the access path option.

Table 39 - Access Path Option Examples

Data Items

The server supplies the following data items with the specified data types and access rights for each IEC 60870 unit (with the common address field omitted for brevity).

Monitor Items

The server supplies the following read-only data items for access to monitored information objects. The server exposes the quality descriptor fields as part of the OPC item data quality word.

Item ID	Data Type	OV	SB	BL	NT	IV	Comments
M_SP.X	VT_BOOL	*	✓	✓	✓	✓	Single-point information (OFF, ON). OV applies only to packed change events (ASDU 20).
M_DP.X	VT_UI1		✓	✓	✓	✓	Double-point information (INTERMEDIATE, OFF, ON, INDETERMINATE).
M_ST.X	VT_I2	✓	✓	✓	✓	✓	Step position with transient state indication.
M_BO.X	VT_UI4	✓	✓	✓	✓	✓	Bit string.

Item ID	Data Type	OV	SB	BL	NT	IV	Comments
M_ME.X	VT_R8	✓	✓	✓	✓	✓	Measurement (normalized/scaled/floating point).
M_IT.X	VT_I4					✓	Integrated total.
M_EI.0	VT_UI1						End of initialization (most recent cause).
P_ME:Q.X	VT_R8						Parameter of measurement. Qualifier (Q): 1-63 = kind of parameter.

Table 40 - Monitor Items

The server issues single-read commands (C_RD) when the client requests an instantaneous poll (read from DEVICE) for these items, with the exception of M_EI, when configured to do so. For more information refer to [Creating and Configuring an IEC 60870 Unit Object](#), in particular, the **Allow C_RD_NA_1** option on the **Advanced** tab.

Command Items

The server supplies the following read-write data items for issuing control commands.

Process Control

The server supplies the following data items for issuing process commands in the control direction.

Item ID	Data Type	Qualifier (Q)	Comments
C_SC_NA:Q.X	VT_UI1	0 = default 4 = short pulse 8 = long pulse 12 = persistent +128 = select	Single command.
C_SC_TA:Q.X	VT_UI1		Single command with time.
C_DC_NA:Q.X	VT_UI1		Double command
C_DC_TA:Q.X	VT_UI1		Double command with time.
C_RC_NA:Q.X	VT_UI1		Regulating step command
C_RC_TA:Q.X	VT_UI1		Regulating step command with time.
C_SE_NA:Q.X	VT_R8	0 = default +128 = select	Set point command – normalized.
C_SE_TA:Q.X	VT_R8		Set point command with time – normalized.
C_SE_NB:Q.X	VT_R8		Set point command – scaled.
C_SE_TB:Q.X	VT_R8		Set point command with time – scaled.
C_SE_NC:Q.X	VT_R8		Set point command – floating-point.
C_SE_TC:Q.X	VT_R8		Set point command with time – floating-point.
C_BO_NA:Q.X	VT_UI4	N/A	Bit string command.
C_BO_TA:Q.X	VT_UI4	N/A	Bit string command with time.

Table 41 - Process Control Items

The server issues the specified activation command when the client writes a control value to one of these items. If the controlled station responds with a positive confirmation, then the server updates the data item with the written value and a good quality, and returns a success result. If the controlled station responds with a negative confirmation or error message, or does not respond at all, then the server updates the data item with a bad quality and returns a failure result.

If the controlled station issues an activation termination for the command (at a later time), then the server updates the data item with the written value, a good quality, and a “constant” limit to indicate that the command is now complete.

For single, double, regulating step, and set-point commands, the server issues a deactivation command for the last control message sent for that item when the client writes an empty value. If the controlled station responds with a positive confirmation, then the server updates the data item with an empty value and a good quality and returns a success result. If the controlled station responds with a negative confirmation or error message, or does not respond at all, then the server updates the data item with a bad quality and returns a failure result.

For single, double, and regulating step commands, the server combines the written value with the qualifier specified in the item ID using a bit-wise OR operation to create the qualifier code actually sent with the activation command. This allows the client to perform different operations on the same information object using a single data item.

The server updates the item with the written value and an uncertain quality after sending the activation/deactivation command and before receiving confirmation when configured to do so.

System Control

The server supplies the following data items for issuing system commands in the control direction.

Item ID	Data Type	Qualifier (Q)	Comments
C_IC_NA:Q.0	VT_BOOL	1-19 = reserved 20 = station 21-36 = group 1-16 37-63 = reserved 64-225 = private	Activate/deactivate general interrogation command.
C_CI_NA:Q.0	VT_BOOL	1-4 = group 1-4 5 = general 6-31 = reserved 32-63 = private +64 = freeze & read +128 = freeze & reset +192 = read 7 reset	Activate/deactivate counter interrogation command.
C_CS_NA.0	VT_DATE	N/A	Clock synchronization command.
C_RP_NA.0	VT_UI1	N/A	Reset process command.
C_CD_NA.0	VT_UI2	N/A	Delay acquisition command. Note: This command is only applicable to IEC 60870-5-101.

Table 42 - System Control Items

With respect to the IEC 60870-5-101 protocol, when the general interrogation, counter interrogation, clock synchronization, and delay acquisition commands are issued, the server sends the corresponding activation command at the specified scan rate (or instantaneously on demand), provided it is greater than the threshold rate for the channel. The user may specify the “-” access option to prevent this from occurring automatically. For more information, refer to the Access Path Option Examples in Table 39.

The same functionality is also present in the IEC 60870-5-104 protocol, with the exception that the user cannot issue a delay acquisition command.

For the general interrogation and counter interrogation commands, the server sends the corresponding activation command when the client writes a TRUE value to the item. For the general interrogation command, the server sends the corresponding deactivation command when the client writes a FALSE value to the item.

The server sends the clock synchronization command with the current time adjusted by the time bias when the client writes any value to that item. For IEC 60870-5-101, the server adds the calculated transmission delay to the current time before sending it if the client is currently reading the corresponding C_CD item and the item has a good quality.

For IEC 60870-5-101, the server sends the delay acquisition spontaneous command with the transmission delay (in milliseconds) specified by the value written by the client to that item. This allows the controlled station to correct clock synchronization commands.

The server sends the reset process command with the qualifier specified by the value written by the client to that item (**1** for general reset, **2** for event buffer reset, and so on).

For the general interrogation and counter interrogation commands, if the controlled station responds with a positive confirmation, then the server updates the data item with the active state and a good quality and returns a success result. If the controlled station issues an activation termination for the command (at a later time), then the server updates the data item with a FALSE value, a good quality, and a constant limit to indicate that the command is now complete.

For the clock synchronization command, if the controlled station responds with a positive confirmation, then the server updates the data item with the sent time and a good quality and returns a success result. If the controlled station issues a spontaneous clock synchronization command, then the server updates the data item with the received clock reading and a good quality and uses this value to qualify short time stamps from that station.

For the reset process command, if the controlled station responds with a positive confirmation, then the server updates the data item with the sent qualifier and a good quality and returns a success result.

For the delay acquisition command (which applies only to the IEC 60870-5-101 protocol when being read), if the controlled station responds with a positive confirmation, then the server calculates the transmission delay as the round-trip time minus the turn-around time (in response), divided by two. Then the server updates the data item with the calculated result and a good quality.

For all of these command items, if the controlled station responds to an activation or deactivation command with a negative confirmation or error message, or does not respond at all, then the server updates the data item with a bad quality and returns a failure result.

The server broadcasts these commands when the data item indicates a link address of 255/65535 and/or a common address of 255/65535. The server allows write-only access to such items and does not wait for confirmation from the controlled station for such commands, as each station/substation will respond independently.

Parameter Control

The server supplies the following data items (Table 43) for issuing parameter commands in the control direction.

Item ID	Data Type	Qualifier (Q)	Comments
P_ME_NA.Q.X	VT_R8	1 = threshold	Parameter of measurement command – normalized value.
P_ME_NB.Q.X	VT_R8	2 = smoothing factor	Parameter of measurement command – scaled value.
P_ME_NC.Q.X	VT_R8	3 = high limit	Parameter of measurement command – floating-point command.
		4 = low limit	
		5-31 = reserved	
		32-63 = private	
P_AC_NA:1.0	VT_BOOL	1	Activate/deactivate previously loaded parameters command.
P_AC_NA:Q.X	VT_BOOL	2 = object parameter	Activate/deactivate parameter command.
		3 = persistent cyclic / periodic transmission	
		4-127 = reserved	
		128-255 = private	

Table 43 - Parameter Control Items

For the parameter of measurement items, the server issues the specified activation command when the client writes a control value to one of these items. If the controlled station responds with a positive confirmation, then the server updates the data item with the written value and a good quality and returns a success result. If the controlled station responds with a negative confirmation or error message, or does not respond at all, then the server updates the data item with a bad quality and returns a failure result.

For the parameter activation/deactivation commands, the server issues the specified activation command when the client writes a TRUE value to the item and the specified deactivation command when the client write a FALSE value. If the controlled station responds with a positive confirmation, then the server updates the data item with the written value and a good quality and returns a success result. If the controlled station responds with a negative confirmation or error message, or does not respond at all, then the server updates the data item with a bad quality and returns a failure result.

The server updates the item with the written value and an uncertain quality after sending the activation/deactivation command and before receiving confirmation when configured to do so.

Configuration Items

The MatrikonOPC IEC 60870 server supplies control items to allow users to view and alter individual configuration parameters at run time, as detailed by the table entries in the following sections. The server ensures that changing individual configuration parameters will have the minimum possible impact on communication at run time. However, the server may re-optimize or disconnect and reconnect individual sections when certain configuration parameters change.

Common Parameters

The MatrikonOPC IEC 60870 server supplies the configuration parameters items listed in Table 44 for all communication objects.

Item ID	Description	Default
Name	Name of the object (element of item ID).	

Item ID	Description	Default
Description	User-defined text string (minimum of 64 characters).	(blank)
Enabled	Enable/disable object. Newly enabled objects are unmarked for deletion.	FALSE
Deleted	Mark/unmark object for deletion. Newly marked objects are disabled.	FALSE
Configuration	Describes all configuration parameters for the object as an XML string. The precise format of the Configuration XML string depends on the type of object to which it belongs. In general, the element name is the object type, and the individual settings are attributes on that element.	

Table 44 - Common Configuration Parameters

Communication Channel Parameters

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 45 for all communication channels (serial and network).

Item ID	Description	Default
Threshold	Maximum achievable scan interval (in milliseconds) for the channel. The server polls items with update rates faster than this on a continuous basis. All units on the channel re-optimize if this parameter changes.	1000
ScheduleAllPolls	Rather than polling them continuously, the server schedules items with update rates faster than the threshold rate to poll at the threshold rate. All units on the channel re-optimize if this parameter changes.	FALSE
InterDeviceDelay	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.	0
ReconnectDelay	Minimum amount of time (in milliseconds) to wait before attempting to reconnect after an attempt to connect to a channel has failed.	0
LogTx	Enable/disable the logging of bytes transmitted at medium level.	FALSE
LogRx	Enable/disable the logging of bytes transmitted at medium level	FALSE

Table 45 - Communication Channel Configuration Parameters

Serial Channel Parameters

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in * Channel and all units on it, disconnect and reconnect if this parameter changes.

Table 46 displays the parameters for all serial channels. Most settings go directly to the serial UART.

Item ID	Description	Default
Device	* Device name (COM1).	
Baud	* Baud rate (110 - 256000).	9600
DataBits	* Number of data bits (4 – 8).	8
Parity	* Parity (none, odd, even, mark, or space).	None

Item ID	Description	Default
StopHalfBits	* Determines the number of stop bits (0 for 1, 1 for 1 ½, or 2 for 2).	0
OutxDsrFlow	*Data Set Ready output flow control (output suspended while DSR is off).	FALSE
OutxCtsFlow	*Clear To Send output flow control (output suspended while CTR is off).	FALSE
DsrSensitivity	* Data Set Ready input sensitivity (input ignored while DSR is off).	FALSE
OutxOnOffFlow	* XON/XOFF software input/output flow control.	FALSE
RtsControl	* Request To Send line/flow control. 0 = RTS off 1 = RTS on 2 = handshake (raise RTS when input buffer less than ½ full, lower when more than ¾ full) 3 = toggle (raise RTS when bytes available for transmission, lower when all buffered bytes have been sent)	0
DtrControl	* Data Terminal Ready line/flow control. 0 = DTR off 1 = DTR on 2 = handshake (raise DTR when input buffer less than ½ full, lower when more than ¾ full)	0
ReadIntervalTimeout	Maximum amount of time (in milliseconds) between the reception of one character and the arrival of the next. 0 = no limit.	0
BackoffDelay	Minimum amount of time (in milliseconds) for DCD (RLSD) to be low before transmitting to avoid collision with spontaneous messages.	0
BackoffRandom	Maximum amount of time (in milliseconds) to randomly wait for DCD to go low. Set both Delay and Random to 0 (zero) to ignore DCD.	0

* Channel and all units on it, disconnect and reconnect if this parameter changes.

Table 46 - Serial Channel Configuration Parameters

Radios

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 47 for all radio modems/repeaters.

Item ID	Description	Default
KeyUp	Minimum amount of time (in milliseconds) to wait after setting the RTS signal before transmitting.	0
KeyDown	Minimum amount of time (in milliseconds) to wait before clearing the RTS signal after transmitting.	0

Table 47 - Radio Configuration Parameters

Network Channels

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 48 for all IP network channels.

Item ID	Description	Default
Protocol	Internet protocol (IP) type. Channel and all hosts and units on it, disconnect and reconnect if this parameter changes. 0 = Datagram TCP (treats the protocol as a series of discrete "packets") 1 = Stream TCP (treats the protocol as a continuous stream of bytes) 2 = Datagram UDP	1

Table 48 - Network Channel Configuration Parameters

Network Hosts

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 49 for all IP network hosts.

Item ID	Description	Default
Host	DNS host name or "dotted-quad" IP address. Blank indicates that the socket binds to a local address and behaves as a server (slave emulation). Host and all units on it, disconnect and reconnect if this parameter changes.	127.0.0.1
Service	Service name or port number. Host and all units on it, disconnect and reconnect if this parameter changes.	80

Table 49 - Network Host Configuration Parameters

Fail-Over Channels

The IEC 60870 OPC Server supplies access to the fail-over policy and load distribution criteria for all fail-over channels via the Configuration item (an XML string). The fail-over policy contains a series of channel elements. Each element has a name attribute that refers to a communication channel, and zero or more load sub-elements. The channel referenced by the name attribute is a sibling of the fail-over channel.

```
<CFailoverDevLink name="Fov1" description="">
  <channel name="Net1"><load>* </load></channel>
  <channel name="Net2"><load>[]</load></channel></CFailoverDevLink>
```

Dial-Up Connections

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 50 for all dial-up connections via Hayes-compatible or CDPD modems that support the AT command set.

Item ID	Description	Default
Reset	Modem reset command (sent following AT). Connection hangs up and redials if this parameter changes.	Z
Initialize	Modem initialization commands (sent following AT). Connections	&FE0Q0V1

Item ID	Description	Default
	hangs up and redials if this parameter changes.	
Dial	Any valid sequence of characters that can follow an ATD (i.e., telephone number) dial command. Blank indicates that units dial in to the server. Connection hangs up and redials if this parameter changes.	5555555
CarriageReturn	ASCII code (0 – 127) for the character that terminates commands/responses.	13
EscapeCharacter	ASCII code (0 – 127) for the character used to escape into command mode.	43
EscapeGuardTime	Amount of time (in milliseconds) to wait before/after the escape sequence.	1000
ResetDelay	Amount of time (in milliseconds) to wait after the reset command completes.	600
CommandTimeout	Maximum amount of time (in milliseconds) to wait for the modem to respond to AT commands with a valid result code (e.g., "OK", "ERROR").	5000
CommandRetries	Maximum number of times to resend a command and wait for a response before concluding that communication has failed with the modem.	3
DialTimeout	Maximum amount of time (in milliseconds) to wait for the modem to receive a carrier ("CONNECT") after dialling before aborting the call.	60000
HangupTimeout	Maximum amount of time (in milliseconds) to wait for the modem to hang up after issuing the ATH0 command.	20000
Redials	The maximum number of times to redial the connection before concluding that communication has failed with the unit or units on that connection.	3
ReconnectDelay	Minimum amount of time (in milliseconds) to wait before attempting to reconnect after an attempt to dial out to the connection has failed.	0
ReconnectRedials	The maximum number of times to redial the connection when trying to reconnect after communication has failed with the connection.	0
PostConnectDelay	Minimum amount of time (in milliseconds) to wait after establishing a dial-out connection before sending message to the unit or units.	0
IdleTimeout	Maximum amount of time (in milliseconds) to allow an idle connection to continue (no communication) before hanging up.	1000

Table 50 - Dial-Up Connection Configuration Parameters

IEC 60870 Units

The MatrikonOPC IEC 60870 server supplies the configuration parameter items listed in Table 51 for all IEC 60870 units.

Item ID	Description	Default
address	IEC 60870-5 link address (0 – 65535). Unit disconnects and reconnects if this parameter changes.	Next available
protocol	Indicates which IEC 60870-5 protocol the unit supports. 1 = IEC 60870-5-101 4 = IEC 60870-5-104	1
mode	Indicates how the unit behaves. 0 = controlling station 1 – controlled station (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 controlled station to convert it to UTC.	0.0
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 when the unit is set off scan.	FALSE
interMessageDelay	Minimum amount of time (in milliseconds) between the last request/response to/from this unit and the next request to this same unit.	0
replyTimeout	Maximum amount of time (in milliseconds) to wait for a response to a link 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 (in 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 connect after communication has failed with a unit.	0
maxInterrogate	Maximum amount of time (in milliseconds) to allow a unit to be interrogated. A value of zero indicates that interrogation must be halted manually.	0
commandTimeout	Maximum amount of time (in milliseconds) to wait for the response to an application command (regardless of link communication). This is equivalent to the IEC 60870-defined t_1 parameter.	15000
resetDelay	Minimum amount of time (in milliseconds) to wait before attempting to reconnect after receiving a reset process activation confirmation.	0

Item ID	Description	Default
balanced	Indicates whether the link is balanced (any station can transmit spontaneously) as opposed to unbalanced (only the controlling station can transmit spontaneously).	FALSE
addressSize	Size (in bytes) of the link address field (0, 1, or 2).	1
causeSize	Size (in bytes) of the cause of transmission field (1 or 2).	1
commonSize	Size (in bytes) of the common address field (1 or 2).	1
objectSize	Size (in bytes) of the information object address fields (1, 2, or 3).	2
originator	Cause of transmission originator address (if causeSize is 2).	0
confirmData	Indicates whether to request confirmation of user data transmissions. No effect on broadcast units.	FALSE
txShortAck	Indicates whether to transmit single-character acknowledgements rather than fixed-length control frames.	FALSE
rxShortAck	Indicates whether to accept single-character acknowledgements from the controlled station rather than just fixed-length control frames.	TRUE
singleRead	Indicates whether to use single-read commands (C_RD) to perform instantaneous polls for monitor items. Otherwise, a device read does nothing.	FALSE
optimisticCommand	Indicates whether to update a command item with the written value and an uncertain (non-specific) quality immediately after issuing the activation/deactivation command and before receiving the confirmation response.	FALSE
requireActerm	Indicates if the OPC server will wait for and acknowledge an ACTTERM command from the device following the completion of a command. This option does not apply to the C_IC_NA and C_CI_NA items.	FALSE
requireGIActterm	Indicates if the OPC server will wait for and acknowledge an ACTTERM command from the device following the completion of either the C_IC_NA or C_CI_NA command. The IEC 60780 specification states that an ACTTERM for these messages is optional. This option must be configured to match the behaviour of the specific device.	FALSE
maxOutstandingMessages	Indicates the maximum difference between the receive sequence number and the send state variable. The OPC server will continue sending messages to the end device until there is the specified number of outstanding messages awaiting a response. No further messages will be sent until commands time out, or a response is received. This value corresponds to the IEC 60870 defined k parameter.	1
DevicePingFrequency	Indicates the time (in milliseconds) required for sending test frames in case of a long idle state. This corresponds to the IEC 60870 defined t₃ parameter. The OPC server will send a	20000

Item ID	Description	Default
	test frame if no other message has been received for this amount of time.	
DevicePingAttempts	Indicates the number of ping attempts that are to be made. When a test frame is sent, and no response is received in the Command Timeout length of time, the OPC server will attempt to send additional test frames until either the device responds, or the number of Ping Attempts is exhausted. When the number of Ping Attempts is exhausted without a response, the OPC server will report the unit as failed, and will move on in the polling cycle.	1

Table 51 - IEC 60870 Unit Communication Configuration Parameters

Dynamic Object Creation

The MatrikonOPC IEC 60870 server dynamically creates certain objects at run-time as the client references them in newly added items. The server automatically creates an object of the appropriate type if the referenced IEC 60870 unit, radio, dial-up connection, or network host does not exist. The server assumes default configuration settings for the new object, disables it, and marks it for deletion.

Once the server creates an object, use the control items to configure it, and then set it enabled to unmark it for deletion and bring it into operation.

To dynamically create a radio or dial-up connection, you must manually create at least one object of that type in the appropriate location. Otherwise, the server assumes that you want to create an IEC 60870 unit in that location. The server does not dynamically create communication channel objects under the root; you must create these manually.

Control Items

The MatrikonOPC IEC 60870 server supplies the control items listed in Table 52 for all communication objects (e.g., channels, units).

Item ID	Description	Default
Connected	Indicates whether the channel, sub-channel, or unit is currently connected. Write a Boolean true to force a connection, or false to force a disconnection (or hang-up). The channel, sub-channel, or unit will automatically try to re-connect as long as it is enabled.	Connected
Scan	Enable/disable polling of unit on a channel or a sub-channel, or on an individual unit. Demand operations such as writes and device reads ignore this setting.	Scan

Table 52 - Communication Object Control Item

The IEC 60870 server supplies the control items listed in Table 53 for each unit.

Item ID	Description	Default
Interrogate	Interleave continuous polls (those with scan rates faster than threshold rate – see below) to a unit with regular polls in the round-robin sequence. For example, when interrogating unit 1 in a field of five units, the poll sequence would be 1, 2, 1, 3, 1, 4, 1, 5, 1, 2, and so on. The	Interrogate

Item ID	Description	Default
	server may interrogate at most, one unit at a time. When an operator commands the server to interrogate a new unit, then the server ceases interrogation of any previous unit on the same channel. The user may configure a maximum interrogation time.	
Link	Read-only. Status of transmission link. 1 = active 0 = unavailable -1 = inactive (test returns NACK) or busy (DFC = 1) On an unbalanced link, the server must query the status of the link (function 9) at the specified scan rate when the client subscribes to this item and no other transactions are occurring on the unit. On a balanced link, the server must test for the link (function 2) at the specified scan rate when the client subscribes to this item and no other transactions are occurring on the unit. On an IEC 60870-5-104 link, the server must activate the test function at the specified scan rate when the client subscribes to this item and no other transactions are occurring on the unit.	Link

Table 53 - Unit Control Item

The IEC 60870 server supplies the control items listed in Table 54 for each dial-up connection.

Item ID	Description	Default
Carrier	Indicates whether the dial-up connection is currently established (carrier present). Write a Boolean false to force a disconnection (hang-up). The dial-up connection will automatically try to re-connect as long as it is enabled.	Carrier

Table 54 - Dial-Up Connection Control Item

Table 55 describes the statistical and control items available for the Server Status List device link.

Field	Description
@Monitor List	A numbered list of the device links being monitored by the Server Status List device link. The full path of the device link is provided, as entered in the Server Status List device link's subscription list.
@Server Status	Indicates the customized status of the server based on the settings for the Server Status List device link. The status options are: Running , Failed , or No Configuration (if the monitor list is empty).

Table 55 - Server Status List Device Link OPC Items

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 G - Offline Mode**.

SCADA Communication

In general, most SCADA applications involve communication with large fields of remote units over a slow medium, such as radio or dial-up modem. As a consequence, it may take a relatively long time to collect/exchange all of the necessary data from/with the field. Such applications require the use of an efficient and orderly transaction exchange mechanism in order to transfer data reliably.

This section describes how the IEC 60870 server implements reliable, optimized communication for supervisory control and data acquisition.

Channels

The MatrikonOPC IEC 60870 server supports the channels of communication described in the following sub-sections.

Serial

The IEC 60870 OPC Server supports direct serial communication via RS232, RS422, RS485, etc. In addition, the server:

- Supports a variety of settings for baud rate, data bits, parity, and stop bits.
- Supports RTS/CTS flow control as well as other common types of flow control (DSR/DTR, software XON/XOFF).
- Supports DCD transmission collision avoidance with random back-off time.
- Allows you to preset control line states (RTS, DTR) to accommodate line converters (RS232/RS485, RS232/RS485, etc.).

Radio

The IEC 60870 server supports serial radio modems with the following additional requirement:

- The server supports key up/down delays for transceiver warm-up and cool-down, with different delays for one or more repeaters on the same channel.

Network

The IEC 60870 server supports network communication via Internet Protocol (IP). In addition, the server:

- Establishes client connections to both TCP/IP and UDP/IP servers.
- Accepts incoming connections and responds to requests from TCP/IP or UDP/IP clients.
- Supports direct network communication with a single device or with multiple devices through a terminal server.
- Supports Point-to-Point Protocol (PPP) and Cellular Digital Packet Data (CDPD) via dial-up networking (externally pre-configured).

Dial-Up

The IEC 60870 OPC Server supports Hayes-compatible dial-up modems via serial or network connection.). In addition, the server:

- Supports any modem that responds to the standard AT command set.
- Tolerates any character case and white space in command responses.
- Issues reset and initialization commands before dialling out and after hanging up.

- Supports communication directly with CDPD modems using the Hayes standard AT command set. These modems must respond normally to the following commands: AT, ATZ, ATO, ATH0, and ATD followed by the user entry.
Note: The server can be configured to avoid using the ATZ command if necessary.
- Supports auto-answer for dial-in connections even while using the same modem to dial out.

Poll Optimization

The IEC 60870 server organizes poll requests as efficiently as possible.

The server provides values for data items in OPC groups at the requested update rate for those groups (fastest rate used when more than one group references the same items). If the requested update rate is too fast for the server to handle, it makes a “best effort” to update as fast as possible. Internally, the server tries to keep the data items at least as fresh as indicated by the update rate. The server will not, however, send updates to the OPC client any faster than the update rate in order to avoid overwhelming it.

Poll optimization involves the destruction and re-creation of communication packets for reading in the most efficient manner. During the optimization process, the server gathers the requested data items into bundles with similar scan rates, and then uses those bundles to generate packets. Optimization is most successful when it generates the fewest number of packets to contain all items with the same scan rate.

Once the server has completed the optimization process and has generated the necessary packets to read the requested data, it then determines whether to queue the packets for transmission. Queued packets are transmitted to the unit at the earliest opportunity. Once all packets have been sent, the queue is emptied and the unit relinquishes control of the circuit to the next unit.

Transactions

The IEC 60870 server employs a robust transaction exchange mechanism for supervisory control and data acquisition. The server completes all same-priority transactions for a particular unit before moving on to the next unit, but interrupts lower-priority transactions in order to carry out higher-priority transactions, (after the current transaction has completed). Demand operations, such as writes and device reads, have the highest priority.

Continuous

The IEC 60870 server polls all units continuously, in a cyclic, round-robin fashion (one after another) in order of the unit station numbers, when configured to do so. The server optimizes together low-priority items with scan times faster than a configured threshold rate and then polls them continually.

Any packet with a scan rate less than the threshold rate is queued immediately following optimization. Also, any packets with a scan rate less than the threshold rate is immediately re-queued when the queue is emptied.

Threshold Rate

In some cases, it may take minutes or even hours for the server to perform all of the communication operations necessary to finish one complete poll of all units on a channel. This has a significant impact on the optimization and scheduling of read operations. The Threshold Rate is used by the server to distinguish between scan rates that are attainable and those that are not.

The Threshold Rate indicates the fastest scan rate (in milliseconds) that the channel can realistically provide. This allows the polling mechanism to generate larger, more efficient packets for items with scan rates faster than the Threshold Rate, to be sent “as fast as possible”. Items

with scan rate equal to or slower than the Threshold Rate are optimized as normal and scheduled to send at their specified rate.

For example, if it takes approximately five minutes to collect all the desired information from a large field of units, then it is not possible for a particular item to receive an update every ten seconds without interrupting the round-robin polling sequence. In such a case, a Threshold Rate of 300,000 milliseconds would be appropriate, as it would allow the driver to optimize all items scanning faster than five-minute intervals into fewer packets.

Configuring the Threshold Rate for best performance may require some experimentation. The Poll Time and Overrun statistics may help to determine the best setting. Alternatively, choose a smaller Threshold Rate and configure all fast items to have scan rates below the Threshold Rate and all slow items to have scan rates well above the chosen rate.

Interrogation

Use the Interrogate control item to place a particular unit on a communication channel into interrogate mode. This has the effect of interleaving high-priority polls for that unit into the round-robin sequence. The interleaved polls only request items with scan rates less than the Threshold Rate; scheduled reads continue in the normal fashion (unaffected).

For example, in a field of ten units, if unit 3 is placed into interrogate mode, all of its continuous polls will be sent after unit 1 has finished sending, and again after unit 2 has finished sending, and again after unit 4, and so on. In other words, the polling sequence changes from 1...2...3...4...etc. to 1...3...2...3...4...3...etc.

This option might be used when activity on a specific unit is of particular interest for a period of time, and operators are not able to wait for the complete round-robin sequence to finish. Only one unit on a channel may be placed into interrogate mode at a time. Naturally, the interleaved polls increase the total amount of time required to poll all units on the channel.

Scheduled

The polling mechanism manages the schedule during idle processing. Whenever a packet becomes due, it is placed on a queue for transmission at the earliest opportunity. The packet's next scheduled time is then calculated, usually just by adding the scan interval to the last scheduled time.

When scheduling packets, the IEC 60870 server calculates the absolute time at which that packet should be sent first (aside from the initial queuing). This first scheduled time is normalized to the base poll time configured for the unit. The server handles scheduled polls due for a unit first before handling continuous polls.

Scheduled packets with the initial poll option are queued immediately. The server always performs optimization when initially establishing or re-establishing communication with a unit. Therefore, the aforementioned packets are queued immediately at these times. The schedule all polls option transforms all continuous polls on a channel into scheduled polls with a scan rate equal to the Threshold Rate. This allows for finer control over precisely when these polls occur.

Priority

Certain types of operations may need to interrupt the regular round-robin polling sequence in order to carry out important tasks. To facilitate this, the "due" queue is sorted, first by the priority level of the packet, and then by the order in which they are queued. Thus, the packet at the front of the queue is also the highest-priority packet to be sent.

When a unit queries the channel to find out whether it is its turn to communicate, it also indicates the priority level of its next packet to be sent. If this level is higher than the level presently being used by any other unit, the requesting unit is granted priority override and takes over

communicating on the channel. The unit will retain priority override as long as it continues sending packets at the same priority level, and no other unit requests to send at a higher level.

Once a unit has finished sending all the packets at a certain level, those packets are immediately removed from the queue, allowing them to become due again before lower-priority packets are finished, if necessary. The channel keeps track of the last unit sending at lower levels so that polling continues where it left off when a unit finishes priority override.

Overruns

Whenever it becomes a particular unit's turn to communicate, it services all of the messages in its own queue until they have all been sent. During this time, duplicate packets cannot be entered into the queue. If a packet becomes due again before it has been removed from the queue, then this constitutes an overrun providing this occurs while communication is still good. Overruns are a symptom that there are communication problems, or that the Threshold Rate needs to be tuned.

Instantaneous

Demand (i.e., user-initiated) operations, such as reading from a device or writing control values, bypass the schedule and priority queue and execute immediately, in the order indicated by the client application. These types of operations force the driver to attempt to re-establish communication with failed devices immediately, regardless of the configured reconnection delay.

Integrity

The IEC 60870 server uses specialized communication algorithms to maintain communication integrity as much as possible. This section describes how the server deals with communication integrity with regard to Transmission, Reception, Failure and Recovery, and Redundancy and Fail-over.

Transmission

Before transmitting a packet, the server may impose a short delay, based on configured settings for the port and the unit. This delay can be used to help slower devices keep up with polling, to avoid overloading the circuit, and, sometimes, to allow unsolicited messages to be received from field devices.

Inter-message delay is configured on a per-unit basis, and indicates the amount of quiet time that must be allowed to pass between receiving a response from and transmitting the next request to the same unit. Inter-device delay is configured on a per-port basis, and indicates the delay that must pass between receiving a response from one unit and transmitting a request to another unit on the same circuit. It is also used whenever a broadcast occurs on the circuit.

Reception

The IEC 60870 server employs a sliding window algorithm in order to filter out line noise on incoming messages without always having to wait for one entire timeout interval.

The server attempts to read sufficient bytes for a fixed-size response header. If the header is not valid, then the server discards the first byte of the header and repeats the process until the timeout interval passes. If the header is valid, then the server attempts to read sufficient bytes for the remainder of the message (length in header) including the CRC. If the CRC is not valid, then the server discards the first byte of the header and repeats the process until the timeout interval passes. If the CRC is valid, then the server considers the response valid and processes the content.

Failure and Recovery

The IEC 60870 server uses the Reply Timeout and Retry settings in order to determine when communication has failed with a particular unit.

Whenever a request sent to a unit fails to receive a valid response within the timeout period, the polling mechanism repeats the request up to the specified number of Retries. If the proper response is still not received, the unit is considered to be in communication failure mode. The server also concludes that communication has failed with a particular unit when the number of consecutive failed demand operations is greater than the Retries setting for that unit.

The server polls units experiencing communication failure at a slower rate, based on the Reconnect Delay, using the configured number of Reconnect Retries for each attempt. However, the server attempts to re-establish communication with failed units immediately when it executes demand operations for that unit.

In addition, the server uses the reconnect delay for the channel when it cannot connect to the communication medium (for example, when it is unable to open the COMM port) to avoid pinning the CPU.

Redundancy and Fail-Over

The IEC 60870 server supports redundant channels of communication to the same physical unit. The fail-over mechanism used by the server is flexible, making it easy to use regular fail-over scenarios.

Those operators who have used older versions of SCADA software are likely accustomed to configuring each RTU first and the channels of communication afterwards. With the IEC 60870 server, it is the other way around.

You begin by configuring the path of communication from the host computer out to the field, exactly as you would if you were not using fail-over. The only difference is that a given RTU will appear more than once in the configuration, probably once for each communication channel. Each object in the configuration represents a link in the path of communication from the server to a source of real-time data.

For example, you might want to configure the scenario shown in Figure 57.

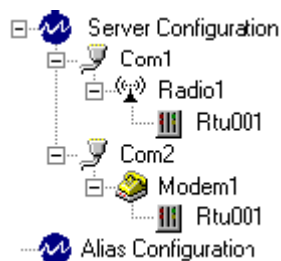


Figure 57 - Server Configuration Scenario

COM1.RADIO1.RTU001 and **COM1.MODEM1.RTU001** both reference the same physical unit, but using two different (independent) paths of communication.

If you want to use fail-over with this configuration, you need to add a fail-over object, called **FOV1**, as shown in Figure 58.

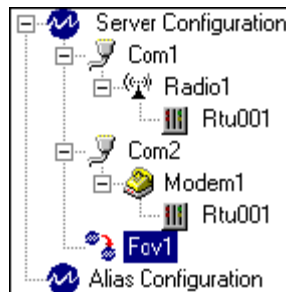


Figure 58 - F0V1 Server Configuration Scenario

In the configuration panel for FOV1 (Figure 59), a list of available communication channels that have already been configured is displayed, in this case **COM1** and **COM2**. For a simple example, you could assign COM1 as a Primary fail-over channel and COM2 as either a Secondary or Standby fail-over channel (these are interchangeable when there is only one non-Primary fail-over channel).

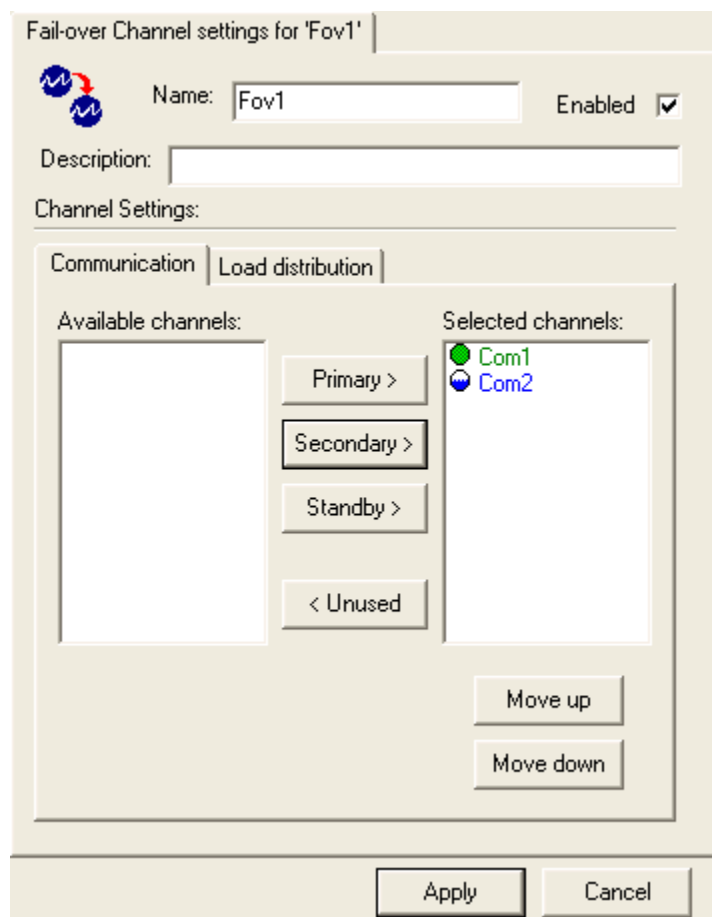


Figure 59 - Fail-Over Channel Settings for F0V1

This tells FOV1 to always continually poll for data using COM1, and only use COM2 if communications fail on COM1. When communications recover on COM1, FOV1 stops using COM2 and returns to using COM1.

Fail-over is employed on an item-by-item basis. If you want the server to fail-over data collection for a particular item from one communication channel to another, you must address that item via the fail-over object rather than one of the configured communication channels. You may still

address the object via the configured communication channels if you have other reasons for doing so, but the server will not use fail-over with that item.

Primary, Secondary, and Standby Channels

To address an item via the fail-over object, you must prefix the portion of the Item ID that is common to all communication channels with the name of the fail-over object (**FOV1** in our example). So, **FOV1.RTU001.1.M_SP.1**, using the settings in our example, would create and start scanning **COM1.RADIO1.RTU001.1.M_SP.1** (Primary) and then create and start scanning **COM2.MODEM1.RTU001.1.M_SP.1** (Standby or Secondary) if the Primary ever receives a bad quality (due to communication failure or other problems). The server does not change the qualities of fail-over items to bad until communication has failed with on all channels.

Secondary and Standby are only differentiated when you have more than two communication channels. Secondary is an auxiliary fail-over channel, whereas Standby is only used in an emergency as a last resort. When more than one Secondary channel exists, the channels have an order or preference: when communication is recovered with a higher-priority channel, it ceases communication with lower-priority channels. There is no order for Standby channels: if communication is recovered with just one, it ceases communication with all the others.

The IEC 60870 server attempts to communicate with each unit on the Primary channel first (i.e. on start-up) before failing over to a Standby channel. The server fails over communications from the Primary channel to a Standby channel if communications with the unit fail on the Primary channel. The server attempts to re-establish communication with the unit on the Primary channel using the reconnect delay and reconnect retry settings, if configured to do so. Otherwise, the server does not attempt to restore communication with the unit on the Primary channel unless communications fail on the Standby channel (fail-back).

The IEC 60870 server supports both “hot” and “cold” Standby channels. The server keeps all hot Standby channels polling at all times. The server keeps all cold Standby channels disconnected so long as they are not required for failed-over communication. The server determines which Standby channel to use for failed over communications based on the order assigned to the channels by the user. The server determines the Primary communication channel to be the first channel. The server allows the client to disable a specific communication channel in order to force the server to fail communications on that channel.

Another example would be if you add several other paths of communication, such as another modem on COM3, and a satellite uplink on COM4. The modem on COM3 is a slower model, so you would prefer to use the one on COM2 if possible. The uplink may be expensive and you may want to avoid using it except as a last resort. You would configure the fail-over policy as follows:

- COM1: *Primary*
- COM2: *Secondary* (at a **higher** priority than COM3)
- COM3: *Secondary* (at a **lower** priority than COM2)
- COM4: *Standby*

There is nothing to prevent users from adding multiple Primary channels, which would result in a fully redundant communication with the server simultaneously polling the same points on both channels. Sites with very stringent data integrity requirements may choose to do this, but would likely use load distribution instead.

Load Balancing

Load balancing involves configuring Primary - Secondary - Standby on an item-by-item basis using filter strings. The Load Distribution tab contains a string grid that allows you to specify which items are to be polled on the respective communication channels. Rather than specifying individual items,

however, you would enter pattern strings that allow the server to match the items to their appropriate channels. The server uses *Visual Basic*-like syntax for these strings.

The syntax is described in detail at:

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/vblr7/html/vaoprLike.asp>

For example, to have all single-point information objects polled on channel 1 and all analog measurements polled on channel 2, enter ***.M_SP.*** under the channel 1 column and ***.M_ME.*** under the channel 2 column.

The grid grows automatically as you add pattern strings. The pattern string applies to the portion of the Item ID following the fail-over channel name (so, for **FOV1.RTU001.1.M_SP.1**, **RTU001.1.M_SP.1** matches the filter ***.M_SP.***).

You can prefix a pattern-matching string with an exclamation point (!) to indicate items that you would like to avoid scanning on a particular channel, if possible. The server will only poll those items on that channel as a last resort, such as when communications have failed on every other channel. The server would stop polling such items on the non-preferred channel as soon as communication is recovered on a preferred channel.

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. Contact the MatrikonOPC Sales department for further information about this product.

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.

The server includes an option on each communication channel to log all bytes transmitted and/or received for that channel at a medium detail level (see **Communication Channel Parameters**). In combination with output to a console window this may serve as a protocol analyzer. The server also logs communication events such as communication recovery, invalid CRCs, error responses, incomplete responses, and timeouts.

Additionally, the server logs the number of bytes of leading noise (squellch head) and trailing noise (squellch tail) distinctively. This helps operators to correctly tune the key up and key down settings on radio-equipped field devices.

Statistical Items

The server supplies statistical information pertaining to communication in the form of real-time data items (for each individual unit and summary items for the channel). The server allows users to

reset individual statistics by writing a zero value (as applicable). If a summary statistic is reset, then the server resets corresponding statistics at all subordinate levels.

The IEC 60870 server supplies a control item at each level to allow users to reset all statistics simultaneously. This is described in Table 56.

Item ID	Description	Default
ResetStatus	Simultaneously resets all statistics at the selected level and all subordinate levels (if any).	ResetStats

Table 56 - Reset Statistics Control Item

In addition, statistical items are supplied for all communication objects, as listed in Table 57.

Item ID	Description	Default
CommFail	Read-only. True if communication with the object has failed. Once in this mode, the item changes to "false" only when a response is received from the unit or at least one unit on the communication path.	CommFail
Sent	Total number of messages sent initially.	Sent
Retried	Total number of messages sent again as a retry.	Retried
TotalSent	Total number of messages sent (Sent + Retried).	TotalSent
NoResponse	Total number of messages that failed to receive any kind of response.	NoResponse
Incomplete	Total number of messages that received only a partial response.	Incomplete
ChecksumError	Total number of responses with checksum errors.	ChecksumError
Invalid	Total number of invalid responses received (Incomplete + ChecksumError).	Invalid
ErrorResponse	Total number of valid error responses received.	ErrorResponse
Received	Total number of expected responses received.	Received
TotalReceived	Total number of valid responses received (ErrorResponse + Received).	TotalReceived
Failure	Total number of times communication has failed (i.e., has run out of retries).	Failure
Timeout	Total number of communication timeouts that have occurred.	Timeout
Overrun	Total number of times that a scheduled poll has come due a second time before it has yet been sent and cleared from the "due" list.	Overrun
Unsolicited	Total number of unsolicited messages received.	Unsolicited
PollComplete	Total number of times that the "due" list has been completely cleared.	PollComplete
LastSent	Read-only. The time at which the last request was transmitted.	LastSent
LastResponse	Read-only. The time at which the last valid response was	LastResponse

Item ID	Description	Default
	received.	
PercentValid	Read-only. Proportion of Total Received to Total Sent as a percentage.	PercentValid
PercentReturn	Read-only. Proportion of Received to Sent as a percentage.	PercentReturn

Table 57 - Communication Objects Statistical Items

Additional statistical items are supplied for all communication channels, as listed in Table 58.

Item ID	Description
Broadcasts	Total number of broadcasts sent.
BytesIn	Total number of bytes received.
BytesOut	Total number of bytes transmitted.
BpsIn	Read-only. Bytes received per second.
BpsOut	Read-only. Bytes transmitted per second.
CurrentUnit	Read-only. Name of the unit presently communicating on the circuit, or else the name of the circuit itself in the case of a broadcast.

Table 58 - Communication Channels Statistical Items

Additional statistical items are supplied for all IEC 60870 units, as listed in Table 59.

Item ID	Description
PollTime	Read-only. Total amount of time (in milliseconds) between when the unit last emptied its "due" queue (completed sending all poll messages) and the time previous to that. Indicates the approximate round-robin poll interval.

Table 59 - IEC 60870 Unit Statistical Item

Additional statistical items are supplied for all dial-up connections, as listed in Table 60.

Item ID	Description
LastDialout	Read-only. The time at which the last dial-out was attempted.
LastAnswered	Read-only. The time at which the last dial-up connection was established.
Busy	Total number of times a busy signal was received ("BUSY").
Dialout	Total number of dial-out attempts ("ATD...").
NoAnswer	Total number of times that there was no answer ("NO ANSWER").
NoCarrier	Total number of times that there was no carrier signal ("NO CARRIER").
NoDialTone	Total number of times there was no dial tone ("NO DIALTONE").
Answered	Total number of success dial-outs ("CONNECT").
PercentAnswered	Read-only. Proportion of successful dial-outs (Answered) to dial-out attempts (Dialout) as a percentage.

Table 60 - Dial-Up Connection Statistical Items

Data Qualities and Timestamps

The MatrikonOPC IEC 60870 server uses standard OPC quality codes to indicate the status of each item, as described in Table 61.

Hex	Dec	Quality	Description
DB	219	Good, local override (constant)	Information objects blocked (BL = 1).
D8	216	Good, local override	Information object substituted (SB = 1).
C3	195	Good, non-specific (constant)	Command activation terminated (completed successfully).
C0	192	Good, non-specific	Normal.
58	88	Uncertain, sub-normal	Information object time tag invalid (IV = 1) or unsynchronized.
54	84	Uncertain, EU exceeded	Information object overflow (OV = 1).
50	80	Uncertain, sensor inaccurate	Not used.
44	68	Uncertain, last usable value	Information object not topical (NT = 1).
40	64	Uncertain, non-specific	Information object (step position) transient (T = 1). Optimistic command executing.
1C	28	Bad, out of service	OPC group or item inactive, or unit or channel disabled (perhaps due to expired software license).
18	24	Bad, communication failure	Communications have failed with the unit or channel. The last good value is unknown.
14	20	Bad, last known value	Communications have failed with the unit or channel. The last good value is known. The server retains the last known "good" value in the real-time cache for each data item during communication failure whenever possible.
10	16	Bad, sensor failure	Information object invalid (IV = 1).
0C	12	Bad, device failure	Not used.
08	8	Bad, not connected	Unit deleted in server configuration (or new configuration loaded).
04	4	Bad, configuration error	Monitor data returned for a type other than specified, information object not available, negative confirmation or error for command.
00	0	Bad, non-specific	No initial data.

Table 61 - OPC Quality Codes

The server copies the quality descriptor byte (OV, BL, SB, NT, IV) into the vendor-specific byte of the quality word when they are returned with an information object. When the quality descriptor is unknown due to communication problems, the server sets the vendor-specific byte to zero.

The server copies the time field into the item timestamp when it is returned with a valid data object, adjusting it by the bias setting. When the time field is not returned or its value is unknown due to communication problems, the server sets the timestamp to the time at which the problem is detected.

Result Codes

The server uses the standard OPC result codes to indicate the outcome of a read or write operation for a particular item. These codes are listed in Table 62.

Code (Hex)	Result	Description
00000000	S_OK	The operation completed successfully.
0004000E	OPC_S_CLAMP	The server accepted the data value but the output was clamped.
80004001	E_NOTIMPL	The output function is not implemented.
80004005	E_FAIL	The operation failed.
80070057	E_INVALIDARG	One or more arguments are invalid in the output message.
C0040002	OPC_E_BADTYPE	The server cannot convert the data to/from the specified data type.
C0040006	OPC_E_BADRIGHTS	The client does not have the necessary rights to perform the operation.
C0040007	OPC_E_UNKNOWNITEMID	The specified item is no longer available in the server's address space.
C004000B	OPC_E_RANGE	The data value is out of range.

Table 62 - OPC Result Codes

Limitations

MatrikonOPC Server for IEC 60870 has no known or expected limitations.

Refer to the *MatrikonOPC Server for IEC 60870 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/Solutions** and **Questions/Answers** sections 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, or the software license has expired.

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.

Check that the correct HASP hardware key is securely fastened to the parallel port. If it is, run the HINSTALL program that is located in the **Program Files\Common Files\MatrikonOPC\Common** directory.

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 behaviour for COM servers. However, this behaviour 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 60) is launched.
3. In the **Registry Editor**, under **HKEY_CLASSES_ROOT**, look for the required program ID (e.g., *Matrikon.OPC.Simulation.1*).

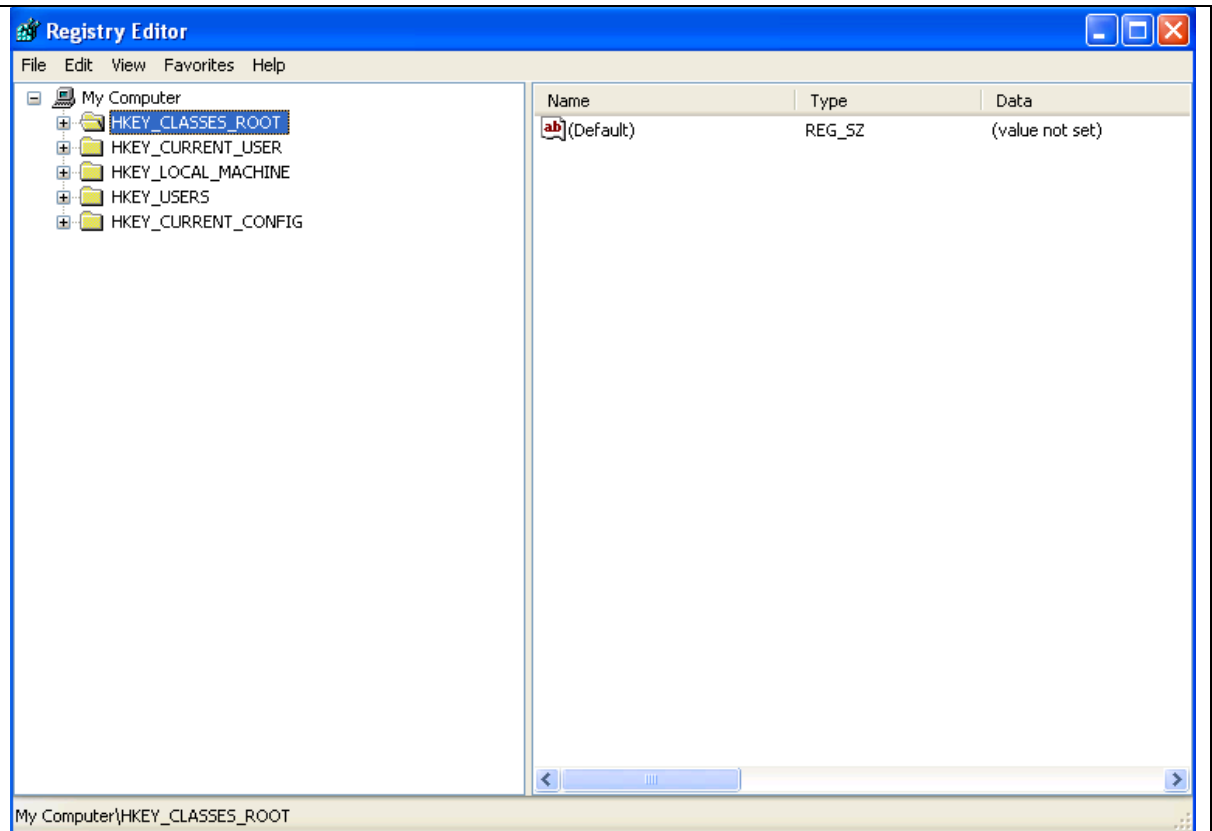


Figure 60 - Registry Editor

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

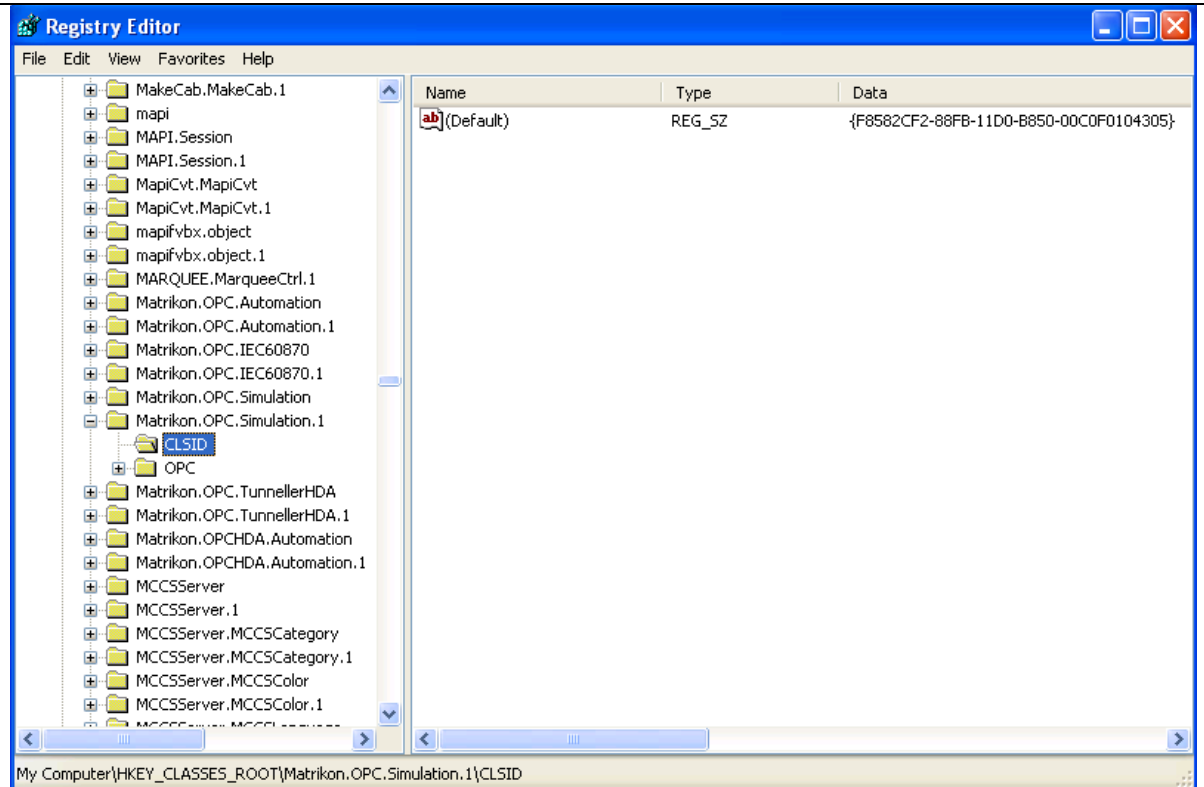


Figure 61 - Program ID Branch

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 Matrikon logo in Tool Tray

Problem: The server cannot be configured because there is no Matrikon logo  in the **Tool Tray**.

Solution: If the Server is running as a service, the Matrikon 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 (device).

Solution: Check the object configuration (refer to the **Server Configuration** section in this manual). Ensure that the **Enabled** checkbox is selected.

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 format

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 remote program in OPC client application

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

Solution: Follow the steps outlined in **Appendix A - Distributed COM (DCOM)** to copy the program ID from the server machine to the client machine.

Access denied 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 **Appendix A – Distributed COM (DCOM)**.

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 **Appendix A – Distributed COM (DCOM)**.

About screen and Configuration window do not show up

Problem: The **About** screen and **Configuration** window do not show up when a remotely connecting 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 consider running the server as an NT service. For more information, refer to **Appendix A – Distributed COM (DCOM)**.

DA 2.05 asynchronous I/O does not work

Problem: After installing an older OPC server, DA 2.05 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).

Server cannot find hardware key

Problem: The server cannot find my hardware key. (Providing hardware key is in use.)

Solution: Try running the **hasp.exe** utility under:

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

When this is run, a window appears. With the hardware key plugged into the printer port on the back of the computer, select **Check key** from the **Utilities** menu. If an error message appears (e.g., “*There is a problem with the hardware key set-up.*”), then there is a problem reading the hardware key. You should see **IEC 60870 OPC Server**, or something similar, in the window.

Questions and Answers

How do I remove the server as a service?

Problem: How do I remove the server as a service?

Solution: Re-register the OPC server executable using the **/REGSERVER** command-line switch.

Does the server need to be started 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.

How can I get OPC data into other applications?

Problem: How can I get OPC data into *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 **Support** for examples of how to do this in *Excel*, *Visual Basic*, or an *HTML* document.

Does the server support the IEC 60870-5-102 protocol?

Problem: Does the server support the IEC 60870-5-102 protocol?

Solution: The server does not support IEC 60870-5-102 at this time. Although it shares many design elements in common with IEC 60870-5-101, 102 is essentially a separate application protocol for the transmission of integrated totals representing the amount of electrical energy transferred between power utilities (etc.).

Does the server support the IEC 60870-103 protocol?

Problem: Does the server support the IEC 607870-5-103 protocol?

Solution: The server does not support IEC 60870-5-103 at this time. Although it shares many design elements in common with IEC 60870-5-101, 103 is essentially a separate application protocol for the informative interface of protection equipment.

Can I treat an unsigned integer value as a Boolean?

Problem: I want my client software to treat an OPC unsigned integer value as a Boolean.

Solution: Conversion from an OPC Boolean type to an unsigned integer cannot be done directly since the Boolean true value is defined as **-1** in OPC. However, this functionality can be supported indirectly on your MatrikonOPC server using an alias for the unsigned integer (for more information on aliases, please refer to the **Alias Configuration** section of this manual). This configuration for the **Bucket Brigade.UInt2** item from **Matrikon.OPC.Simulation.1** is shown in Figure 62, but this technique should work for any unsigned integer type.

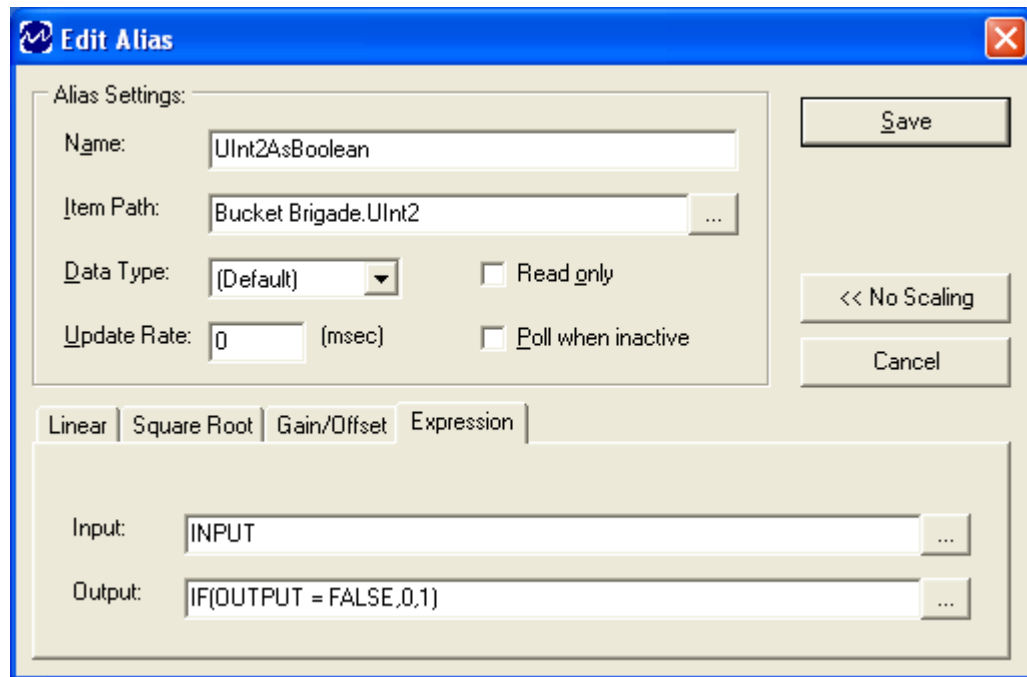


Figure 62 - Edit Alias Window

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

Un-Installation

To successfully un-install MatrikonOPC IEC 60870, using the **Add or Remove Programs** from the Microsoft Windows **Control Panel** is recommended.

To un-install MatrikonOPC IEC 60870:

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 is displayed.
4. Scroll through the list of currently installed programs and updates to find and select **MatrikonOPC Server for SCADA IEC**.

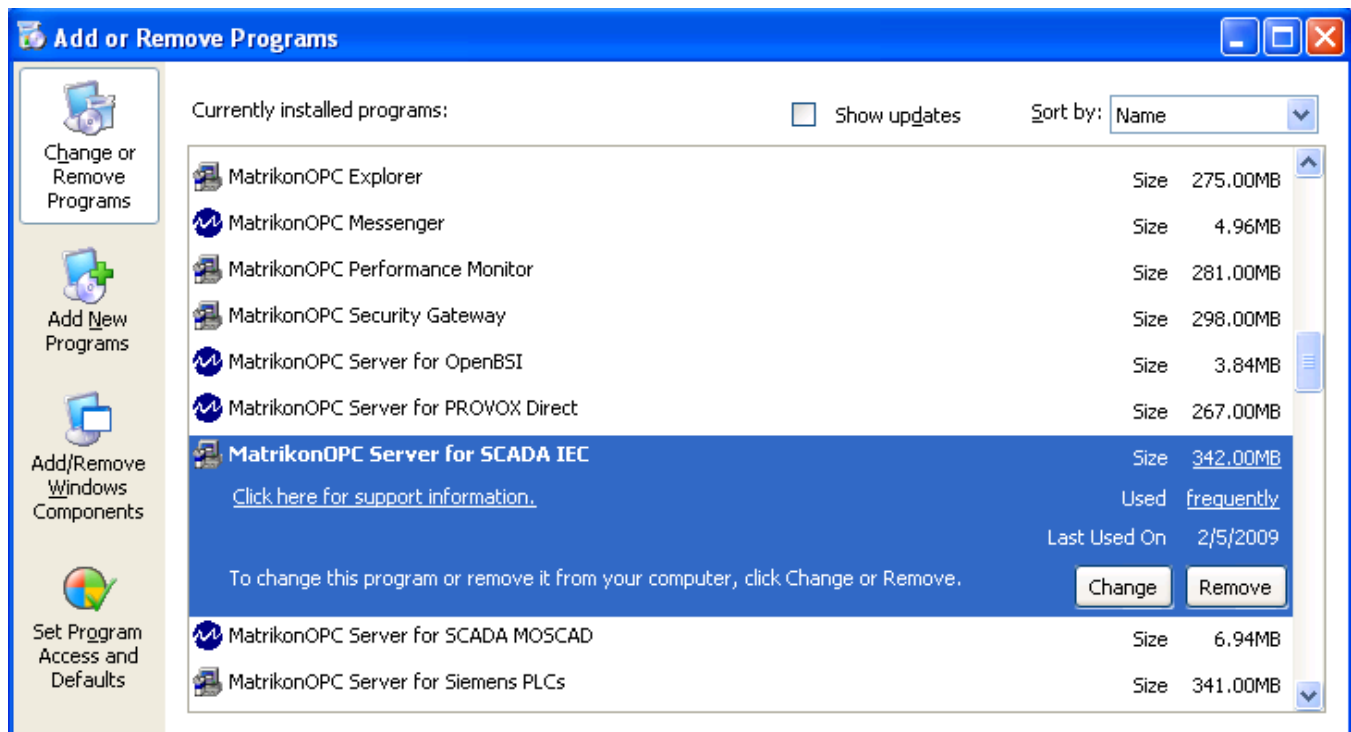


Figure 63 - Add/Remove Programs

5. Click on the **Remove** button associated with the MatrikonOPC Server for IEC 60870 program to initiate the un-install process.
6. The **MatrikonOPC Server for SCADA IEC – InstallAware Wizard** window appears, and the **Welcome to MatrikonOPC Server for SCADA IEC Maintenance** screen (Figure 64) is displayed.

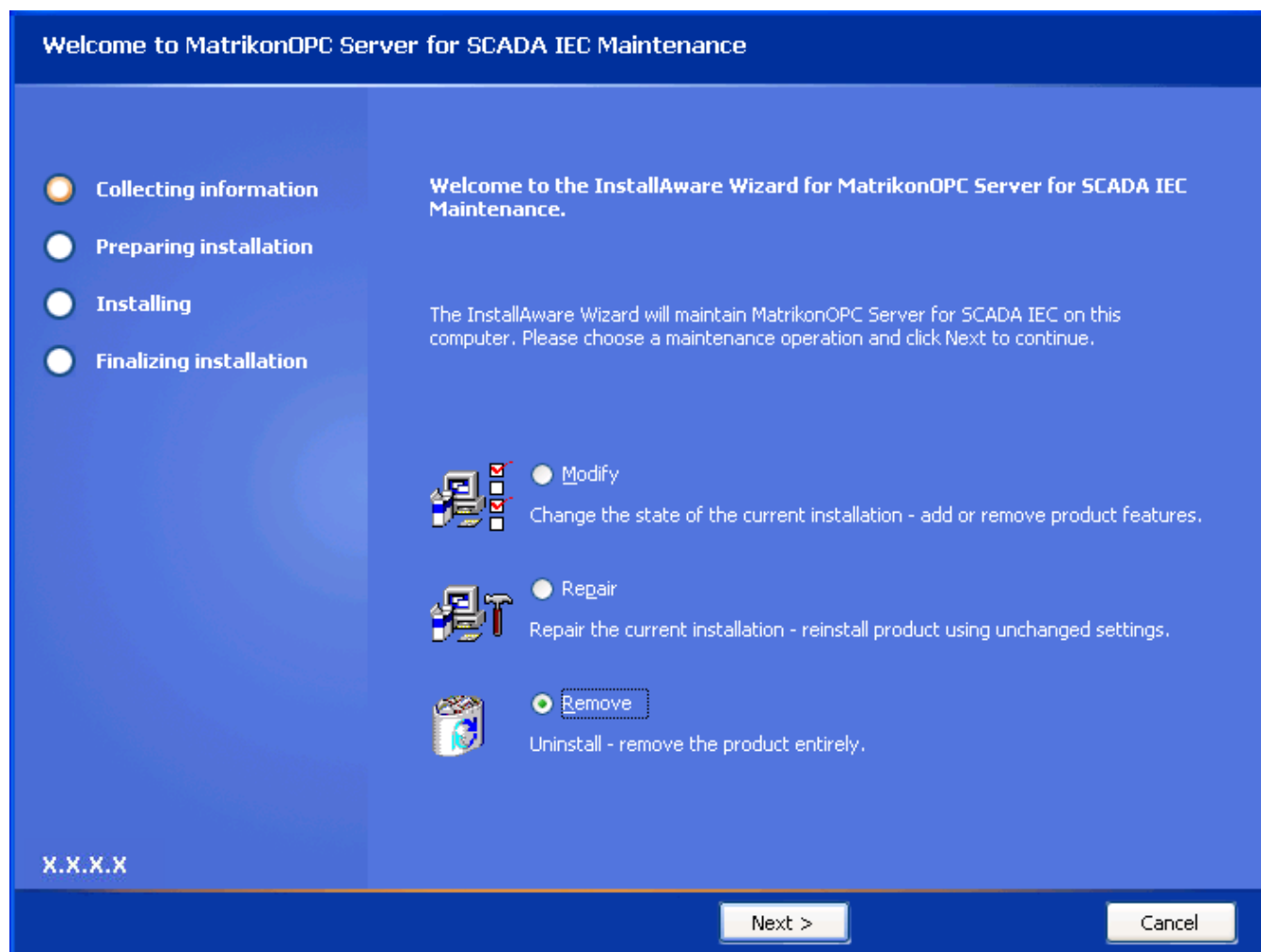


Figure 64 - Welcome to the MatrikonOPC Server for SCADA IEC Maintenance Screen

7. Select the **Remove** option button to un-install MatrikonOPC Server for IEC 60870 entirely.
8. Click on the **Next** button. The **Ready to Uninstall** screen (Figure 65) is displayed.

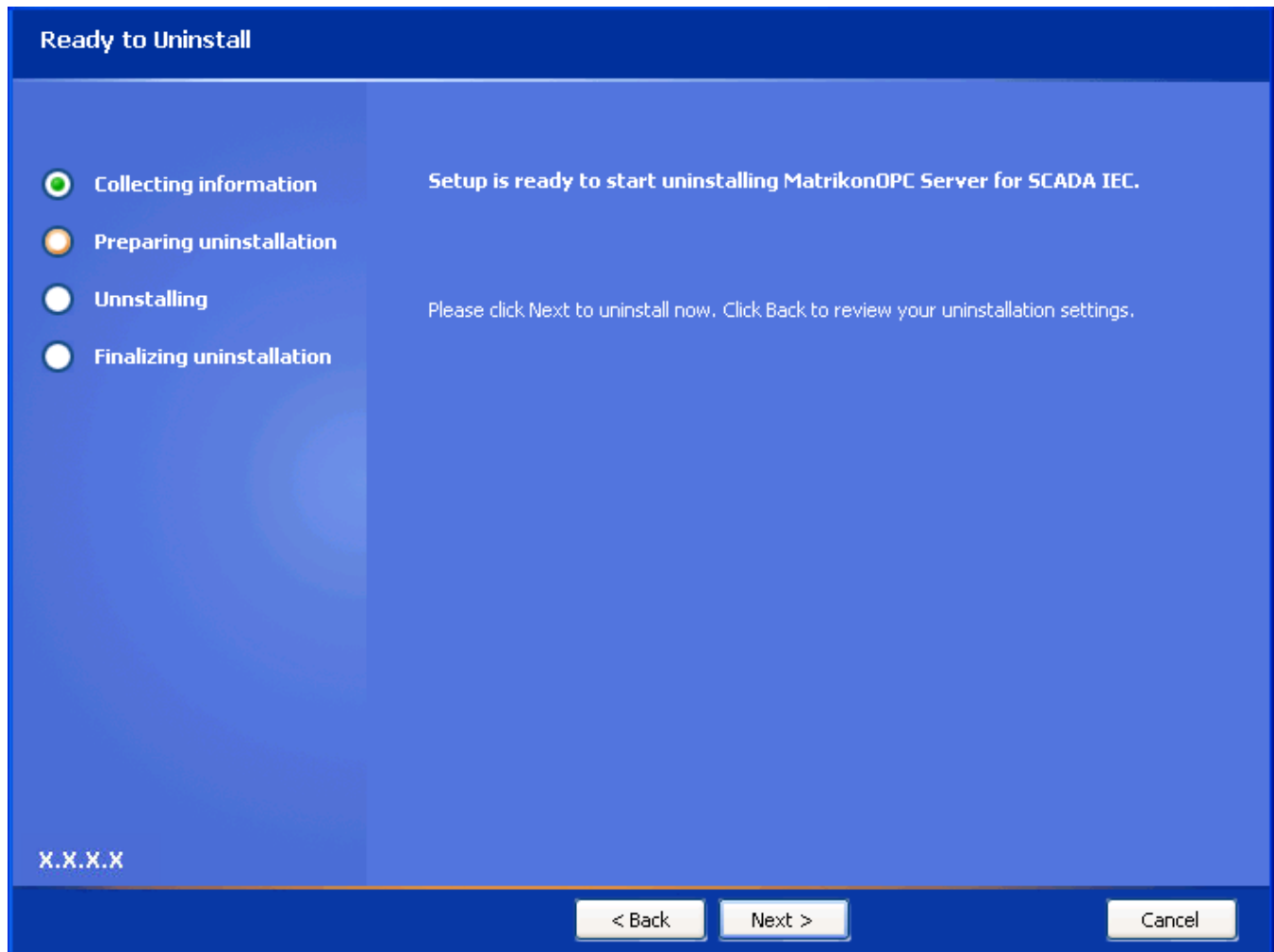


Figure 65 - Ready to Uninstall Screen

9. Click on the **Next** button.
10. The **Uninstalling MatrikonOPC Server for SCADA IEC** screen (Figure 66) appears and the un-install takes place.

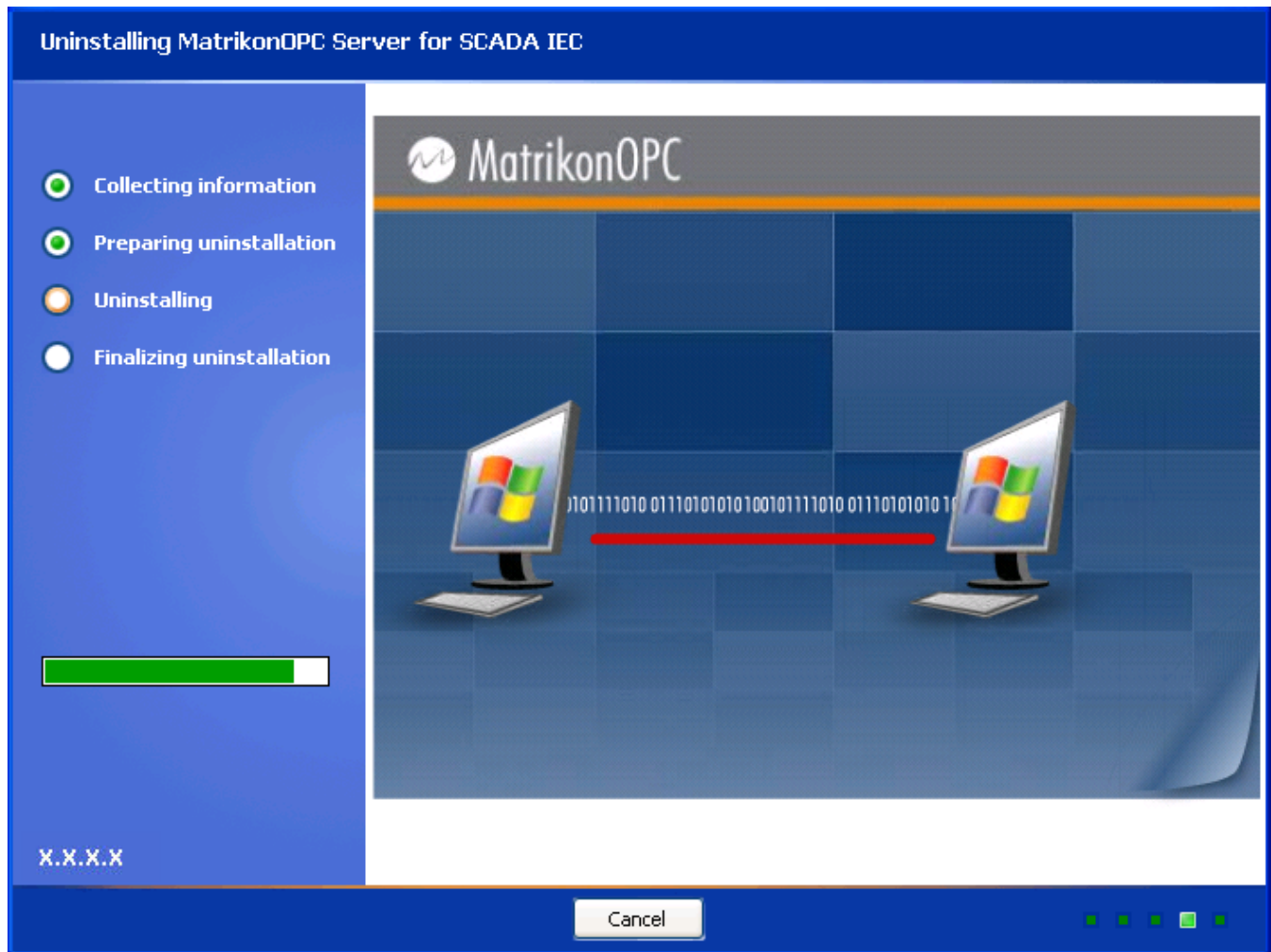


Figure 66 - Uninstalling MatrikonOPC Server for SCADA IEC Screen

11. When the un-install has finished, the **MatrikonOPC Server for SCADA IEC Setup Complete** screen (Figure 67) appears stating that MatrikonOPC Server for SCADA IEC was successfully un-installed.

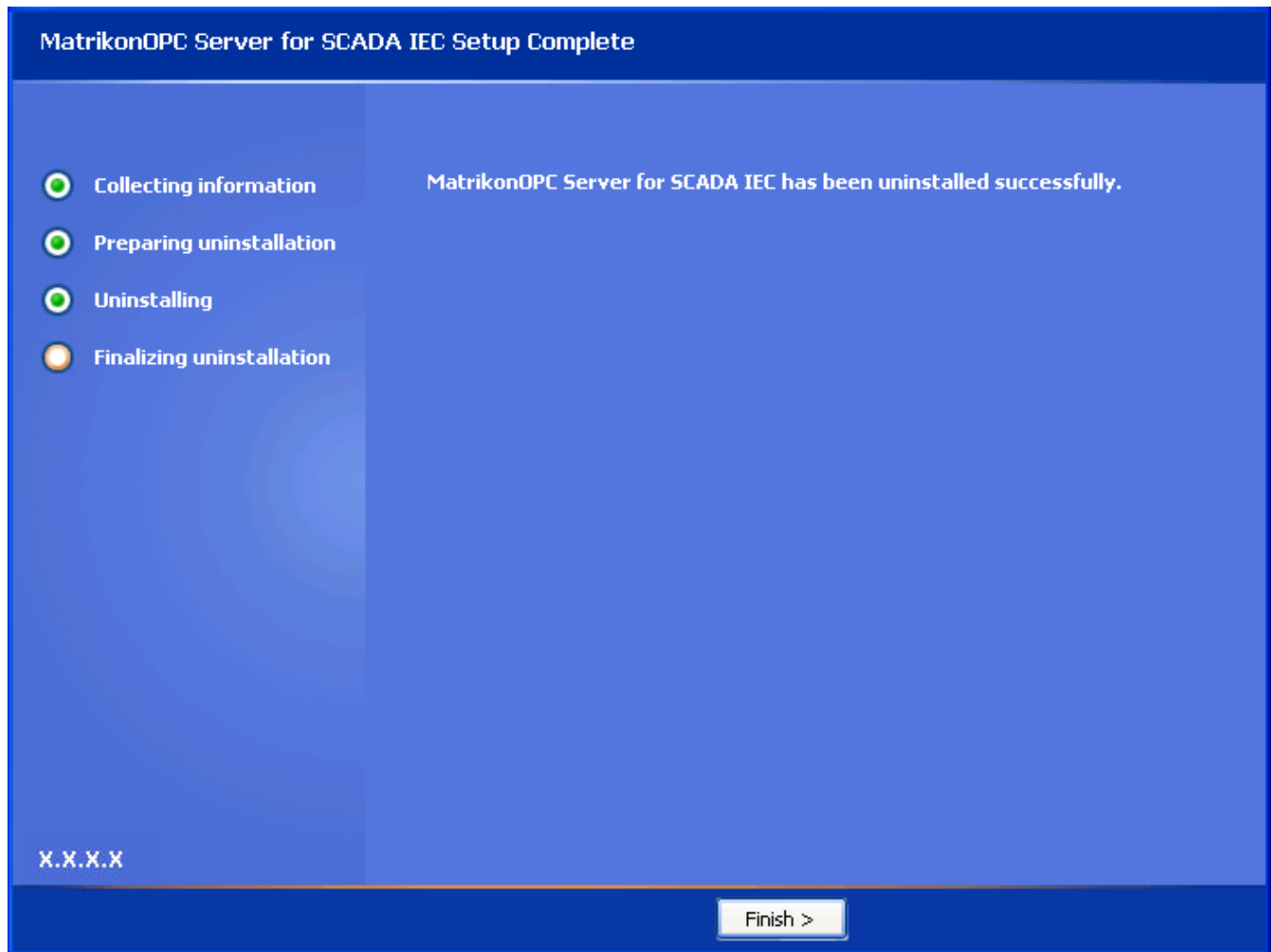


Figure 67 - MatrikonOPC Server for SCADA IEC Setup Complete Screen

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>.

- *OPC Overview 1.0*
- *OPC Common Definitions and Interfaces 1.0*
- *OPC Security Custom Interface 1.0*
- *OPC Data Access Custom Interface Standard 2.05*

The server passes the automated certification test with the **OPC Foundation Compliance Test** utility.

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.IEC60870**.
- Version-specific program ID is **Matrikon.OPC.IEC60870.1**.
- OPC sub-key and vendor information string.
- Globally unique application ID (e.g., **9FA8E7F7-3610-4FEA-91E5-E0F8A3D8C866**).
- Globally unique class ID number (e.g., **189547C8-82A4-48C7-B462-A4BBDB73FDD6**).
- Full path of 32-bit local server executable.
- OPC Data Access Server 1.0 and 2.0 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

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.
- Write control values to items (on device).

The server supports asynchronous I/O operations as defined for **DA 2.0**.

- Read items value 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 2.0**.

- 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 1.0a**.

- 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 1.0a**.

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

IEC 80670 Interoperability

For more information on IEC 60870, view the documents listed below (as well as others) at <http://www.iec.org>:

- IEC 60870-5 Telecontrol equipment and systems – Part 5: Transmission protocols
 - o Section 1 – Transmission frame formats
 - o Section 2 – Link transmission procedures
 - o Section 3 – General structure of application data
 - o Section 4 – Definition and coding of application information elements
 - o Section 5 – Basic application functions
 - o Section 101 – Companion standard for basic telecontrol tasks (amendments 1 and 2).
 - o Section 104 – Network access for IEC 60870-5-101 using standard transport profiles.
- Norwegian IEC 60870-5-101 User Conventions (Revision 2.0)
- Norwegian IEC 60870-5-104 User Conventions

IEC 60870-5-101 Interoperability Profile

The following section outlines the interoperability profile for the IEC 60870-5-101 protocol.



Note: The full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

Legend:

- ☐ Not Implemented
- ☒ Implemented

System or Device

System-specific parameter.

- ☐ System definition
- ☒ Controlling station definition (Master)
- ☐ Controlled station definition (Slave)

Network Configuration

Network-specific parameter.

- ☒ Point-to-point
- ☒ Multiple point-to-point
- ☒ Multi-point-partyline
- ☒ Multi-point-star

Physical Layer

Network-specific parameter.

Transmission Speed (Control Direction)

Unbalanced interchange
Circuit V.24/V.28
Standard

Unbalanced interchange
Circuit V.24/V.28
Recommended if >1 200 bit/s

Balanced interchange
Circuit X.24/X.27

☒ 100 bit/s
☒ 200 bit/s
☒ 300 bit/s
☒ 600 bit/s
☒ 1 200 bit/s

☒ 2 400 bit/s
☒ 4 800 bit/s
☒ 9 600 bit/s

☒ 2 400 bit/s
☒ 4 800 bit/s
☒ 9 600 bit/s
☒ 19 200 bit/s
☒ 38 400 bit/s

☒ 56 000 bit/s
☒ 64 000 bit/s

Transmission Speed (Monitor Direction)

Unbalanced interchange
Circuit V.24/V.28
Standard

Unbalanced interchange
Circuit V.24/V.28
Recommended if >1 200 bit/s

Balanced interchange
Circuit X.24/X.27

☒ 100 bit/s
☒ 200 bit/s
☒ 300 bit/s
☒ 600 bit/s
☒ 1 200 bit/s

☒ 2 400 bit/s
☒ 4 800 bit/s
☒ 9 600 bit/s

☒ 2 400 bit/s
☒ 4 800 bit/s
☒ 9 600 bit/s
☒ 19 200 bit/s
☒ 38 400 bit/s

☒ 56 000 bit/s
☒ 64 000 bit/s

Link Layer

Network-specific parameter.

Frame format FT 1.2, single character 1 and the fixed time-out interval are used exclusively in this companion standard.

Link Transmission Procedure

☒ Balanced transmission
☒ Unbalanced transmission

Frame Length

Maximum length L

Link Address Field

☒ Not present (balanced transmission only)
☒ One octet
☐ Two octets

- ☒ Structured
- ☒ Unstructured

Application Layer

Transmission Mode for Application Data

Mode 1 (least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Transmission Mode for Application Data

System-specific parameter.

- ☒ One octet
- ☒ Two octets

Information Object Address

System-specific parameter.

- ☒ One octet
- ☒ Two octets
- ☒ Three octets
- ☐ Structured
- ☒ Unstructured

Selection of Standard ASDUs

Process Information in Monitor Direction

Station-specific parameter.

☒	<1>	:=	Single-point information	M_SP_NA_1
☒	<2>	:=	Single-point information with time tag	M_SP_TA_1
☒	<3>	:=	Double-point information	M_DP_NA_1
☒	<4>	:=	Double-point information with time tag	M_DP_TA_1
☒	<5>	:=	Step position information	M_ST_NA_1
☒	<6>	:=	Step position information with time tag	M_ST_TA_1
☒	<7>	:=	Bitstring of 32 bit	M_BO_NA_1
☒	<8>	:=	Bitstring of 32 bit with time tag	M_BO_TA_1
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
☒	<10>	:=	Measured value, normalized value with time tag	M_ME_TA_1
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
☒	<12>	:=	Measured value, scaled value with time tag	M_ME_TB_1
☒	<13>	:=	Measured value, short floating point value	M_ME_NC_1
☒	<14>	:=	Measured value, short floating point value with time tag	M_ME_TC_1

☒	<15> :=	Integrated totals	M_IT_NA_1
☒	<16> :=	Integrated totals with time tag	M_IT_TA_1
☐	<17> :=	Event of protection equipment with time tag	M_EP_TA_1
☐	<18> :=	Packed start events of protection equipment with time tag	M_EP_TB_1
☐	<19> :=	Packed output circuit information of protection equipment with time tag	M_EP_TC_1
☒	<20> :=	Packed single-point information with status change detection	M_PS_NA_1
☒	<21> :=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30> :=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31> :=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32> :=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33> :=	Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
☒	<34> :=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35> :=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36> :=	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
☒	<37> :=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38> :=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39> :=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40> :=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either ASDUs of the set <2>, <4>, <6>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30 – 40> are used.

Process Information in Control Direction

Station-specific parameter.

☒	<45> :=	Single command	C_SC_NA_1
☒	<46> :=	Double command	C_DC_NA_1
☒	<47> :=	Regulating step command	C_RC_NA_1
☒	<48> :=	Set point command, normalized value	C_SE_NA_1
☒	<49> :=	Set point command, scaled value	C_SE_NB_1
☒	<50> :=	Set point command, short floating point value	C_SE_NC_1
☒	<51> :=	Bitstring of 32 bit	C_BO_NA_1

System Information in Monitor Direction

Station-specific parameter.

☒	<70> :=	End of initialization	M_EI_NA_1
-------------------------------------	---------	-----------------------	-----------

System Information in Control Direction

Station-specific parameter.

☒	<100> :=	Interrogation command	C_IC_NA_1
☒	<101> :=	Counter interrogation command	C_CI_NA_1
☒	<102> :=	Read command	C_RD_NA_1
☒	<103> :=	Clock synchronization command	C_CS_NA_1
☐	<104> :=	Test command	C_TS_NA_1
☒	<105> :=	Reset process command	C_RP_NA_1
☒	<106> :=	Delay acquisition command	C_CD_NA_1

Parameter in Control Direction

Station-specific parameter.

☒	<110> :=	Parameter of measured value, normalized value	P_ME_NA_1
☒	<111> :=	Parameter of measured value, scaled value	P_ME_NB_1
☒	<112> :=	Parameter of measured value, short floating point value	P_ME_NC_1
☒	<113> :=	Parameter activation	P_AC_NA_1

File Transfer

Station-specific parameter.

☐	<120> :=	File ready	F_FR_NA_1
☐	<121> :=	Section ready	F_SR_NA_1
☐	<122> :=	Call directory, select file, call file, call section	F_SC_NA_1
☐	<123> :=	Last section, last segment	F_LS_NA_1
☐	<124> :=	ACK file, ACK section	F_AF_NA_1
☐	<125> :=	Segment	F_SG_NA_1
☐	<126> :=	Directory {blank or X, only available in monitor (standard) direction}	F_DR_NA_1

Type Identifier and Cause of Transmission Assignments

Station-specific parameter.

Shaded boxes: Option not required.

Blank: Functions or ASDI not used.

Mark Type Identification/Cause of Transmission Combinations: "X" is only used in the standard direction.

Type Identification		Cause of Transmission																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47	
<1>	M_SP_NA_1		X	X		X						X	X		X						
<2>	M_SP_TA_1			X		X						X	X								
<3>	M_DP_NA_1		X	X		X						X	X		X						
<4>	M_DP_TA_1			X		X						X	X								
<5>	M_ST_NA_1		X	X		X						X	X		X						
<6>	M_ST_TA_1			X		X						X	X								
<7>	M_BO_NA_1		X	X		X									X						
<8>	M_BO_TA_1			X		X															
<9>	M_ME_NA_1	X	X	X		X									X						
<10>	M_ME_TA_1			X		X															
<11>	M_ME_NB_1	X	X	X		X									X						
<12>	M_ME_TB_1			X		X															
<13>	M_ME_NC_1	X	X	X		X									X						
<14>	M_ME_TC_1			X		X															
<15>	M_IT_NA_1			X												X					
<16>	M_IT_TA_1			X												X					
<17>	M_EP_TA_1																				
<18>	M_EP_TB_1																				
<19>	M_EP_TC_1																				
<20>	M_PS_NA_1		X	X		X						X	X		X						
<21>	M_ME_ND_1	X	X	X		X									X						
<30>	M_SP_TB_1			X		X						X	X								
<31>	M_DP_TB_1			X		X						X	X								
<32>	M_ST_TB_1			X		X						X	X								
<33>	M_BO_TB_1			X		X															
<34>	M_ME_TD_1			X		X															
<35>	M_ME_TE_1			X		X															
<36>	M_ME_TF_1			X		X															
<37>	M_IT_TB_1			X												X					
<38>	M_EP_TD_1																				
<39>	M_EP_TE_1																				
<40>	M_EP_TF_1																				
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X	
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X	
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X	
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X	
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X	
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X	
<51>	C_BO_NA_1						X	X	X	X	X						X	X	X	X	
<70>	M_EI_NA_1				X																
<100>	C_IC_NA_1						X	X	X	X	X						X	X	X	X	
<101>	C_CI_NA_1						X	X			X						X	X	X	X	
<102>	C_RD_NA_1					X											X	X	X	X	
<103>	C_CS_NA_1			X			X	X									X	X	X	X	
<104>	C TS NA 1																				

Type Identification		Cause of Transmission																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47	
<105>	C_RP_NA_1						X	X									X	X	X	X	
<106>	C_CD_NA_1			X			X	X									X	X	X	X	
<110>	P_ME_NA_1						X	X							X		X	X	X	X	
<111>	P_ME_NB_1						X	X							X		X	X	X	X	
<112>	P_ME_NC_1						X	X							X		X	X	X	X	
<113>	P_AC_NA_1						X	X	X	X							X	X	X	X	
<120>	F_FR_NA_1																				
<121>	F_SR_NA_1																				
<122>	F_SC_NA_1																				
<123>	F_LS_NA_1																				
<124>	F_AF_NA_1																				
<125>	F_SG_NA_1																				
<126>	F_DR_TA_1*																				
* Blank or X only.																					

* Blank or X only.

Basic Application Functions

Station Initialization

Station-specific parameter.

X Remote initialization

Cyclic Data Transmission

Station-specific parameter.

X Cyclic data transmission

Read Procedure

Station-specific parameter.

X Read procedure

Spontaneous Transmission

Station-specific parameter.

X Spontaneous transmission

Station Interrogation

Station-specific parameter.

X global

X group 1

X group 7

X group 13

☒ group 2	☒ group 8	☒ group 14
☒ group 3	☒ group 9	☒ group 15
☒ group 4	☒ group 10	☒ group 16
☒ group 5	☒ group 11	
☒ group 6	☒ group 12	

Note: Information object addresses assigned to each group must be shown in a separate table.

Clock Synchronization

Station-specific parameter.

- ☒ Clock synchronization

Command Transmission

Object-specific parameter.

- ☒ Direct command transmission
- ☒ Direct set-point command transmission
- ☒ Select and execute command
- ☒ Select and execute set-point command
- ☒ C_SE ACTTERM used
- ☒ No additional definition
- ☒ Short-pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Long-pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Persistent output

Transmission of Integrated Totals

Station or object-specific parameter.

- ☒ Counter read
- ☒ Counter freeze without reset
- ☒ Counter freeze with reset
- ☒ Counter reset
- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Object-specific parameter.

- ☒ Threshold value

- ☒ Smoothing factor
- ☒ Low limit for transmission of measured value
- ☒ High limit for transmission of measured value

t-specific parameter.

- ☒ Activation/deactivation of persistent cyclic or periodic transmission of the addressed object.

Test Procedure

Station-specific parameter.

- ☐ Test procedure

File Transfer

Station-specific parameter.

File transfer in monitor direction

- ☐ Transparent file
- ☐ Transmission of disturbance data of protection equipment
- ☐ Transmission of sequences of events
- ☐ Transmission of sequences of recorded analogue values

File transfer in control direction

- ☐ Transparent file

Background Scan

Station-specific parameter.

- ☒ Background scan

Acquisition of Transmission Delay

Station-specific parameter.

- ☒ Acquisition of transmission delay

IEC 60870-5-104 Interoperability Profile

The following section outlines the interoperability profile for the IEC 60870-5-104 protocol.



Note: The full specification of a system may require individual selection of certain parameters for certain parts of the system, such as the individual selection of scaling factors for individually addressable measured values.

Legend:

- ☐ Not Implemented
- ☒ Implemented

System or Device

System-specific parameter.

- ☐ System definition
- ☒ Controlling station definition (Master)
- ☐ Controlled station definition (Slave)

Application Layer

Transmission Mode for Application Data

Mode 1 (least significant octet first), as defined in 4.10 of IEC 60870-5-4, is used exclusively in this companion standard.

Common Address of ASDU

System-specific parameter.

- ☒ Two octets

Information Object Address

System-specific parameter.

- ☐ Structured
- ☒ Unstructured
- ☒ Three octets

Cause of Transmission

System-specific parameter.

- ☒ Two octets (with originator address). Originator address is set to zero if not used.

Length of APDU

System-specific parameter.

The maximum length of the APDU is 254 (default). The maximum length may be reduced by the system.

- ☐ 255 Maximum length of APDU per system

Selection of Standard ASDUs

Process Information in Monitor Direction

Station-specific parameter.

☒	<1>	:=	Single-point information	M_SP_NA_1
☒	<3>	:=	Double-point information	M_DP_NA_1
☒	<5>	:=	Step position information	M_ST_NA_1
☒	<7>	:=	Bitstring of 32 bit	M_BO_NA_1
☒	<9>	:=	Measured value, normalized value	M_ME_NA_1
☒	<11>	:=	Measured value, scaled value	M_ME_NB_1
☒	<13>	:=	Measured value, short floating point value	M_ME_NC_1
☒	<15>	:=	Integrated totals	M_IT_NA_1
☒	<20>	:=	Packed single-point information with status change detection	M_SP_NA_1
☒	<21>	:=	Measured value, normalized value without quality descriptor	M_ME_ND_1
☒	<30>	:=	Single-point information with time tag CP56Time2a	M_SP_TB_1
☒	<31>	:=	Double-point information with time tag CP56Time2a	M_DP_TB_1
☒	<32>	:=	Step position information with time tag CP56Time2a	M_ST_TB_1
☒	<33>	:=	Bitstring of 32 bit with time tag CP56Time2a	M_BO_TB_1
☒	<34>	:=	Measured value, normalized value with time tag CP56Time2a	M_ME_TD_1
☒	<35>	:=	Measured value, scaled value with time tag CP56Time2a	M_ME_TE_1
☒	<36>	:=	Measured value, short floating point value with time tag CP56Time2a	M_ME_TF_1
☒	<37>	:=	Integrated totals with time tag CP56Time2a	M_IT_TB_1
☐	<38>	:=	Event of protection equipment with time tag CP56Time2a	M_EP_TD_1
☐	<39>	:=	Packed start events of protection equipment with time tag CP56Time2a	M_EP_TE_1
☐	<40>	:=	Packed output circuit information of protection equipment with time tag CP56Time2a	M_EP_TF_1

Either the ASDUs of the set <2>, <4>, <6>, <10>, <12>, <14>, <16>, <17>, <18>, <19> or of the set <30 – 40> are used.

Process Information in Control Direction

Station-specific parameter.

☒	<45>	:=	Single command	C_SC_NA_1
☒	<46>	:=	Double command	C_DC_NA_1
☒	<47>	:=	Regulating step command	C_RC_NA_1
☒	<48>	:=	Set point command, normalized value	C_SE_NA_1
☒	<49>	:=	Set point command, scaled value	C_SE_NB_1
☒	<50>	:=	Set point command, short floating point value	C_SE_NC_1

☒	<51> :=	Bitstring of 32 bit	C_BO_NA_1
☒	<58> :=	Single command with time tag CP56Time2a	C_SC_TA_1
☒	<59> :=	Double command with time tag CP56Time2a	C_DC_TA_1
☒	<60> :=	Regulating step command with time tag CP56Time2a	C_RC_TA_1
☒	<61> :=	Set point command, normalized value with time tag CP56Time2a	C_SE_TA_1
☒	<62> :=	Set point command, scaled value with time tag CP56Time2a	C_SE_TB_1
☒	<63> :=	Set point command, short floating point value with time tag CP56Time2a	C_SE_TC_1
☒	<64> :=	Bitstring of 32 bit with time tag CP56Time2a	C_BO_TA_1

Either the ASDUs of the set <45> - <51> , or of the set <58> - <64> are used.

System Information in Monitor Direction

Station-specific parameter.

☒	<70> :=	End of initialization	M_EI_NA_1
-------------------------------------	---------	-----------------------	-----------

System Information in Control Direction

Station-specific parameter.

☒	<100> :=	Interrogation command	C_IC_NA_1
☒	<101> :=	Counter interrogation command	C_CI_NA_1
☒	<102> :=	Read command	C_RD_NA_1
☒	<103> :=	Clock synchronization command	C_CS_NA_1
☒	<105> :=	Reset process command	C_RP_NA_1
☐	<107> :=	Test command with time tag CP56Time2a	C_TS_TA_1

Parameter in Control Direction

Station-specific parameter.

☒	<110> :=	Parameter of measured value, normalized value	P_ME_NA_1
☒	<111> :=	Parameter of measured value, scaled value	P_ME_NB_1
☒	<112> :=	Parameter of measured value, short floating point value	P_ME_NC_1
☒	<113> :=	Parameter activation	P_AC_NA_1

File Transfer

Station-specific parameter.

☐	<120> :=	File ready	F_FR_NA_1
☐	<121> :=	Section ready	F_SR_NA_1
☐	<122> :=	Call directory, select file, call file, call section	F_SC_NA_1

☐	<123> :=	Last section, last segment	F_LS_NA_1
☐	<124> :=	ACK file, ACK section	F_AF_NA_1
☐	<125> :=	Segment	F_SG_NA_1
☐	<126> :=	Directory {blank or X, only available in monitor (standard) direction}	F_DR_NA_1

Type Identifier and Cause of Transmission Assignments

Station-specific parameter.

Shaded boxes: Option not required.

Blank: Functions or ASDI not used.

Mark Type Identification /Cause of Transmission Combinations: "X" is only used in the standard direction.

Type Identification		Cause of Transmission																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47	
<1>	M_SP_NA_1		X	X		X						X	X		X						
<3>	M_DP_NA_1		X	X		X						X	X		X						
<5>	M_ST_NA_1		X	X		X						X	X		X						
<7>	M_BO_NA_1		X	X		X									X						
<9>	M_ME_NA_1	X	X	X		X									X						
<11>	M_ME_NB_1	X	X	X		X									X						
<13>	M_ME_NC_1	X	X	X		X									X						
<15>	M_IT_NA_1			X												X					
<20>	M_PS_NA_1		X	X		X						X	X		X						
<21>	M_ME_ND_1	X	X	X		X									X						
<30>	M_SP_TB_1			X		X						X	X								
<31>	M_DP_TB_1			X		X						X	X								
<32>	M_ST_TB_1			X		X						X	X								
<33>	M_BO_TB_1			X		X															
<34>	M_ME_TD_1			X		X															
<35>	M_ME_TE_1			X		X															
<36>	M_ME_TF_1			X		X															
<37>	M_IT_TB_1			X												X					
<38>	M_EP_TD_1																				
<39>	M_EP_TE_1																				
<40>	M_EP_TF_1																				
<45>	C_SC_NA_1						X	X	X	X	X						X	X	X	X	
<46>	C_DC_NA_1						X	X	X	X	X						X	X	X	X	
<47>	C_RC_NA_1						X	X	X	X	X						X	X	X	X	
<48>	C_SE_NA_1						X	X	X	X	X						X	X	X	X	
<49>	C_SE_NB_1						X	X	X	X	X						X	X	X	X	
<50>	C_SE_NC_1						X	X	X	X	X						X	X	X	X	
<51>	C_BO_NA_1						X	X	X	X	X						X	X	X	X	
<58>	C SC TA 1						X	X	X	X	X						X	X	X	X	

Type Identification		Cause of Transmission																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	20 to 36	37 to 41	44	45	46	47	
<59>	C_DC_TA_1						X	X	X	X	X							X	X	X	X
<60>	C_RC_TA_1						X	X	X	X	X							X	X	X	X
<61>	C_SE_TA_1						X	X	X	X	X							X	X	X	X
<62>	C_SE_TB_1						X	X	X	X	X							X	X	X	X
<63>	C_SE_TC_1						X	X	X	X	X							X	X	X	X
<64>	C_BO_TA_1						X	X	X	X	X							X	X	X	X
<70>	M_EI_NA_1*				X																
<100>	C_IC_NA_1						X	X	X	X	X							X	X	X	X
<101>	C_CI_NA_1						X	X			X							X	X	X	X
<102>	C_RD_NA_1					X												X	X	X	X
<103>	C_CS_NA_1			X			X	X										X	X	X	X
<105>	C_RP_NA_1						X	X										X	X	X	X
<107>	C_TS_TA_1																				
<110>	P_ME_NA_1						X	X							X			X	X	X	X
<111>	P_ME_NB_1						X	X							X			X	X	X	X
<112>	P_ME_NC_1						X	X							X			X	X	X	X
<113>	P_AC_NA_1						X	X	X	X								X	X	X	X
<120>	F_FR_NA_1																				
<121>	F_SR_NA_1																				
<122>	F_SC_NA_1																				
<123>	F_LS_NA_1																				
<124>	F_AF_NA_1																				
<125>	F_SG_NA_1																				
<126>	F_DR_TA_1*																				
* Blank or X only.																					

Basic Application Functions

Station Initialization

Station-specific parameter.

X Remote initialization

Cyclic Data Transmission

Station-specific parameter.

- X** Cyclic data transmission

Read Procedure

Station-specific parameter.

X Read procedure

Spontaneous Transmission

Station-specific parameter.

- ☒ Spontaneous transmission

Station Interrogation

Station-specific parameter.

- | | | |
|---|--|--|
| ☒ global | | |
| ☒ group 1 | ☒ group 7 | ☒ group 13 |
| ☒ group 2 | ☒ group 8 | ☒ group 14 |
| ☒ group 3 | ☒ group 9 | ☒ group 15 |
| ☒ group 4 | ☒ group 10 | ☒ group 16 |
| ☒ group 5 | ☒ group 11 | |
| ☒ group 6 | ☒ group 12 | |

Note: Information object addresses assigned to each group must be shown in a separate table.

Clock Synchronization

Station-specific parameter.

- ☒ Clock synchronization

Command Transmission

Object-specific parameter.

- ☒ Direct command transmission
- ☒ Direct set-point command transmission
- ☒ Select and execute command
- ☒ Select and execute set-point command
- ☒ C_SE ACTTERM used
- ☒ No additional definition
- ☒ Short-pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Long-pulse duration (duration determined by a system parameter in the controlled station)
- ☒ Persistent output

Transmission of Integrated Totals

Station or object-specific parameter.

- ☒ Counter read
- ☒ Counter freeze without reset

- ☒ Counter freeze with reset
- ☒ Counter reset
- ☒ General request counter
- ☒ Request counter group 1
- ☒ Request counter group 2
- ☒ Request counter group 3
- ☒ Request counter group 4

Parameter Loading

Object-specific parameter.

- ☒ Threshold value
- ☒ Smoothing factor
- ☒ Low limit for transmission of measured value
- ☒ High limit for transmission of measured value

Parameter Activation

Object-specific parameter.

- ☒ Activation/deactivation of persistent cyclic or periodic transmission of the addressed object.

Test Procedure

Station-specific parameter.

- ☐ Test procedure

File Transfer

Station-specific parameter.

File transfer in monitor direction

- ☐ Transparent file
- ☐ Transmission of disturbance data of protection equipment
- ☐ Transmission of sequences of events
- ☐ Transmission of sequences of recorded analogue values

File transfer in control direction

- ☐ Transparent file

Background Scan

Station-specific parameter.

X Background scan

Acquisition of Transmission Delay

Station-specific parameter.

Definition of Timeouts

For more information refer to **Creating and Configuring an IEC 60870 Unit Object**, in particular, the **Parameters** tab.

Parameter	Default Value	Remarks	Selected Value
t_0	30 s	Timeout of connection establishment.	Not Configurable.
t_1	15 s	Timeout of send or test APDUs	Configurable
t_2	10 s	Timeout for acknowledges in the case of not data messages $t_2 < t_1$.	Always acknowledges – effectively set at 0.
t_3	20 s	Timeout for sending test frames in the case of a long idle state.	configurable

Maximum range of values for all timeouts: 1 to 255 s, accuracy 1 s.

Maximum Number of Outstanding I Format APDUs (k) and Latest Acknowledge APDUs (w)

For more information refer to **Creating and Configuring an IEC 60870 Unit Object**, in particular, the **Parameters** tab.

Parameter	Default Value	Remarks	Selected Value
k	12 APDUs	Maximum difference between received sequence numbers to send the state variable.	1 APDU. Configurable.
w	8 APDUs	Latest acknowledge after receiving w I format APDUs	1 APDU. Not configurable.

Maximum range of values (k): 1 to 32767 ($2^{15} - 1$) APDUs, accuracy 1 APDU.

Maximum range of values (w): 1 to 32767 APDUs, accuracy 1 APDU. **Recommendation:** w should not exceed two-thirds of k .

Portnumber

This parameter is server-configurable. For more information refer to **Creating and Configuring a Network Host Object**, in particular, the **Service name / Port** option.

Parameter	Value	Remarks
Portnumber	2404	May be configured on the Host channel.

RFC 2200 Suite

RFC 2200 is an official Internet standard which describes the state of standardization of protocols used in the Internet as determined by the Internet Architecture Board (IAB). It offers a broad spectrum of actual standards used in the Internet. The suitable selection of documents from RFC 2200 defined in this standard for given projects has to be chosen by the user of this standard.

- ☒ Ethernet 802.3
- ☒ Serial X.21 interface
- ☐ Other selection from RFC 2200

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, specs, etc, can be found at <http://www.microsoft.com/com/default.mspx>.

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.



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 68) appears.

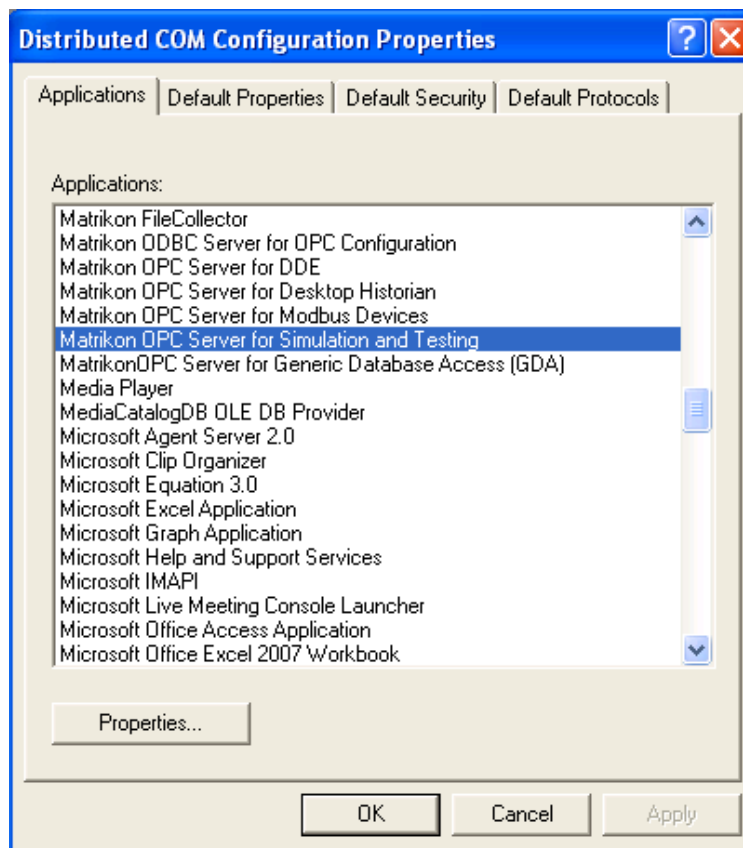


Figure 68 - Distributed COM Configuration Properties Window

4. Click on the **Security** tab to set the security for the server.
5. The **Distributed COM Configuration Security** tab (Figure 69) appears.

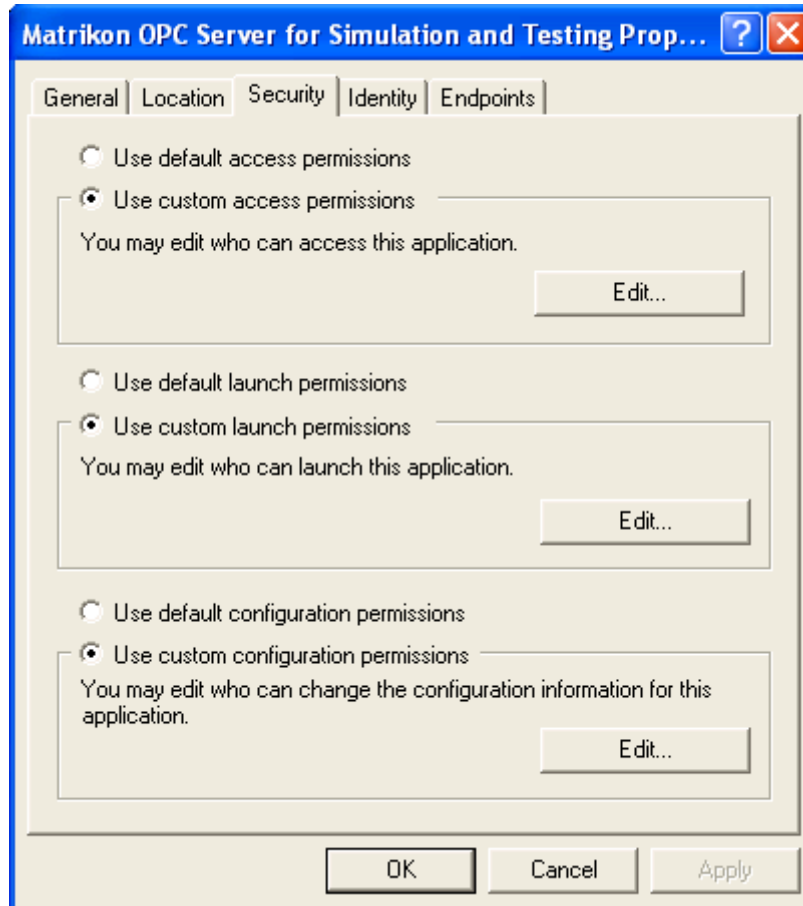


Figure 69 - Distributed COM Configuration Security Tab

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 70) appears.

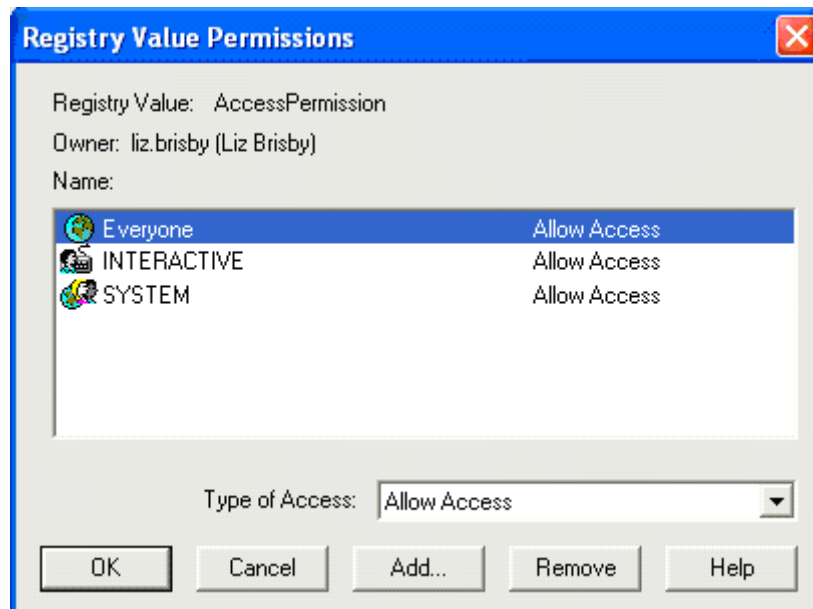


Figure 70 - Registry Value Permissions Window

9. To add users to the list click **Add**.
10. The **Add Users and Groups** window (Figure 71) appears.

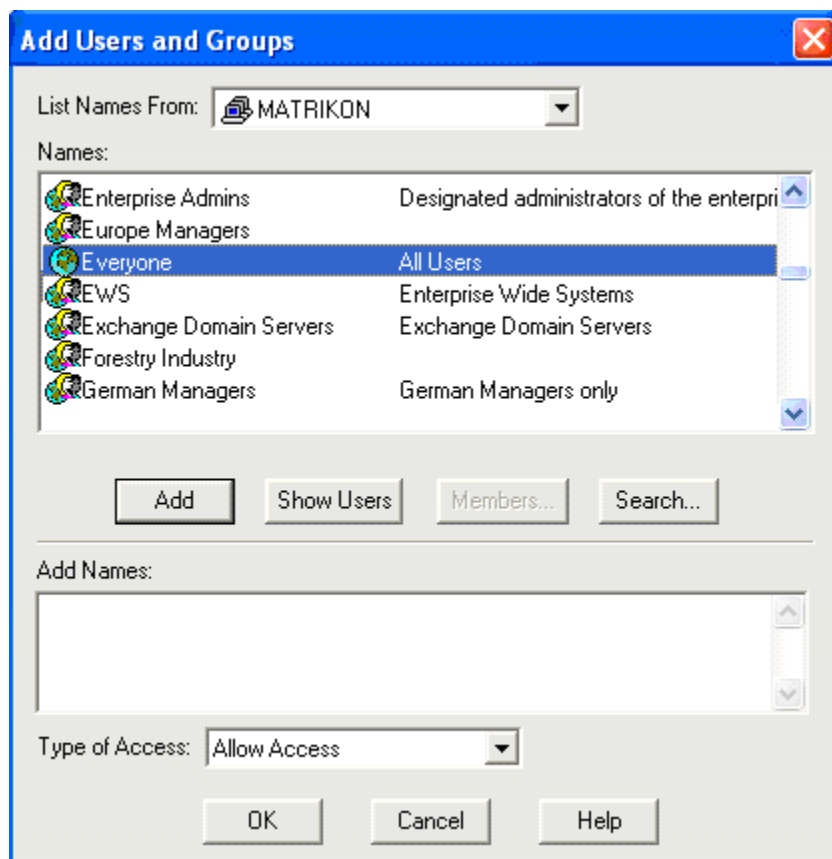


Figure 71 - Add Users and Groups Window

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.



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.



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 Matrikon OPC 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 63.

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 63 - Expressions Constructs 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 64.

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 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

Table 64 - 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 65.

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

Field	Description
	2 = clamp high value 3 = clamp both high and low values

Table 65 - 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 66.

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

Table 66 - 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 67.

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 67 - Additional File Import/Export Field Descriptions - Expression Scaling

Scaling Algorithms

For each type of scaling, a different algorithm (Table 68) 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	$SQRT(INPUT) + 5$	$(OUTPUT - 5) * (OUTPUT - 5)$

Table 68 - Scaling Algorithms

Appendix C Standard Data Types

The Standard data types and their descriptions are listed in Table 69.

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 69 - 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/behaviour.

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.

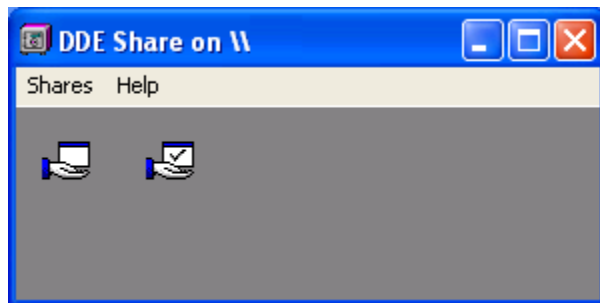


Figure 72 - DDE Share

NetDDE must first be configured using the DDEShare application (*DDEShare.exe*) as shown in Figure 72. Each SERVICE and TOPIC pair, or "NetDDE Share", that is to be available through NetDDE must be assigned a unique name.

Appendix E Common IEC 60870 Item Configurations

There are several common uses of the access path options combined with specific IEC 60870 items to configure

Configuring an Access Path Option

Access path options can be used two ways:

1. If the OPC client used supports an access path field, the option string may be entered there.
2. If the OPC client does not support configuring access paths, or if the following option is more convenient to configure with the client, then append the desired option string to the end of the item ID following the escape character. The default escape character is `/`. For example, subscribe the OPC client to the item ID **Net.Gw.Rtu1.1.M_SP.0/ACCESSPATH**.

Non-Polled Items

A non-polled item is one that has an OPC subscription configured, but that the OPC server will never poll cyclically. This is frequently used for write-only items, or items which the OPC client will read only when a demand read request is made to the OPC server. This option is enabled with the `-` access path option. The `-` option must be the first item in an access path option string.

Initial Interrogation

An initial interrogation occurs when a connection or reconnection is made to the unit. Initial interrogations are used for filling in values that do not change frequently, and for getting all of the qualities of the items to reflect the device values rather than the quality caused by loss of connection. Initial interrogation of any point is configured using the `+` access path option. For example, **Net.Gw.Rtu1.1.M_SP.0/+** will poll the item as per the OPC update rate, and will perform an additional poll on connection or reconnection to the unit. This option can be combined with the poll rate option **Net.Gw.Rtu1.1.M_SP.0/-+** which will only poll the item when a connection or reconnection occurs.

OPC Group Subscription Update Rate vs. Access Path Poll Rate

The OPC specification for a group subscription states that the OPC server may send updated data no more often than the update rate. When no access path poll rate is used, the OPC update rate is also used as the polling rate for data that is unchanged. This can cause unnecessary extra communication to the end device.

When an access path poll rate is specified, the OPC group update rate continues to limit how often the OPC server can send updated data to the OPC client. However, the access path poll rate controls how often the OPC server will query the device for more data. This is useful primarily when devices can send data when it changes, and the device does not need to be polled regularly to get this data. For example, if a value changes once an hour on average, it does not need to be polled every second. However, if the value does occasionally change more often, the client should not have to wait up to an hour to see that change.

To configure this type of polling:

1. Determine the maximum amount of delay between the OPC server receiving a new value for the item, and passing it on to the OPC client.
2. Create an OPC group using the delay (in milliseconds) for the update rate.

3. Add the items to the group, configuring the item with an access path with an update rate -. For example, **Net.Gw.Rtu1.1.M_SP.0/3600000** for a one-hour poll rate. Note that this can be combined with the initial interrogation option. For example, **Net.Gw.Rtu1.1.M_SP.0/+3600000** for a one-hour poll rate with a poll on connection or reconnection. The non-pollled item option -, may not be combined with a poll rate.

IEC 60870 Interrogation Commands

The C_IC_NA and C_CI_NA control items for IEC 60870 devices are read-triggered commands to execute interrogations on the device. The C_IC_NA command is a general interrogation command. The C_CI_NA command is a counter interrogation command. When these commands are issued for a specific ASDU on the device, the device responds by sending the current value of all general or counter items in the ASDU.

An interrogation item for each ASDU on the device must be configured separately. The access path options described above should be used with these command items to configure initial and cyclic interrogation commands. For the following examples, it is assumed that there is a Network device link named **Net**, with a host named **GW**, connected to an RTU named **RTU1**.

For an initial interrogation only of ASDUs 1, 2 and 3, subscribe to:

Net.GW.RTU1.1.C_IC_NA:20.0/-+

Net.GW.RTU1.2.C_IC_NA:20.0/-+

Net.GW.RTU1.3.C_IC_NA:20.0/-+

For a cyclic interrogation of ASDU 4 at 30-minute intervals:

Net.GW.RTU1.4.C_IC_NA:20.0/1800000

For a cyclic interrogation of ASDU 5 at 30-minute intervals with an initial interrogation:

Net.GW.RTU1.5.C_IC_NA:20.0/+1800000

Appendix F 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**.

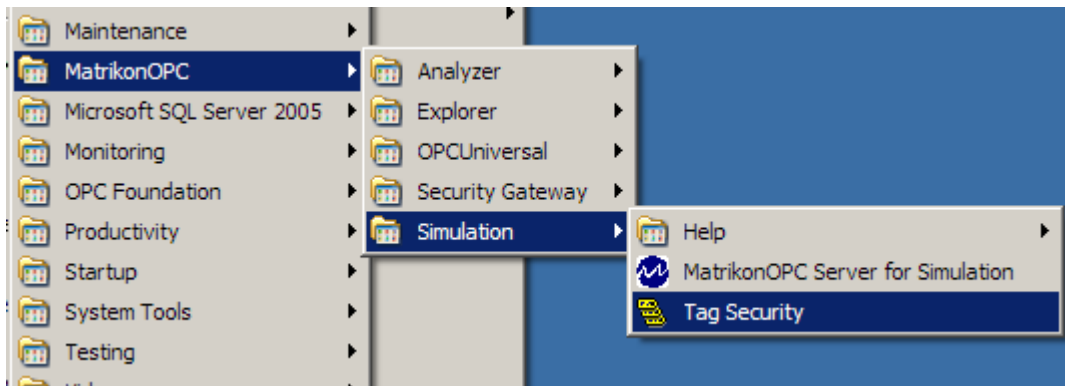


Figure 73 - Start Menu Navigation

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 74) appears.



Figure 74 - Enter Server Password Window

2. Enter the password that was created during the installation of the OPC server.
 3. Click on the **OK** button.
- Note:** During installation, if the user did not enter a password for encryption, then steps 1 through 3 are skipped.
4. The **MatrikonOPC Tag Security Configuration Utility** screen (Figure 75) appears.

Layout

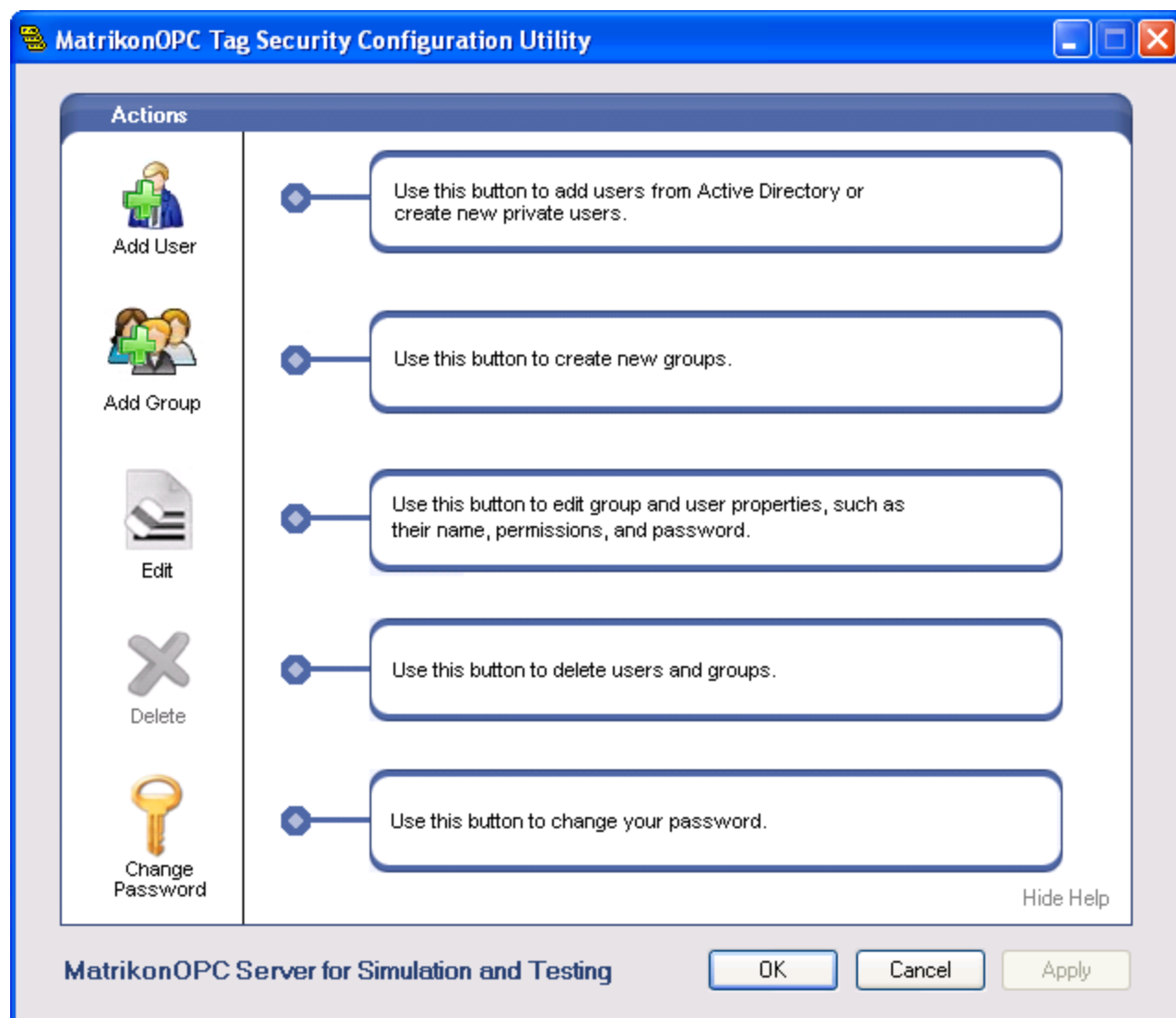


Figure 75 - MatrikonOPC Tag Security Configuration Utility Main Screen

The **MatrikonOPC Tag Security Configuration Utility** screen displays the name of the OPC server that is being configured for tag security. In Figure 75 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 greyed-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 76). 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.

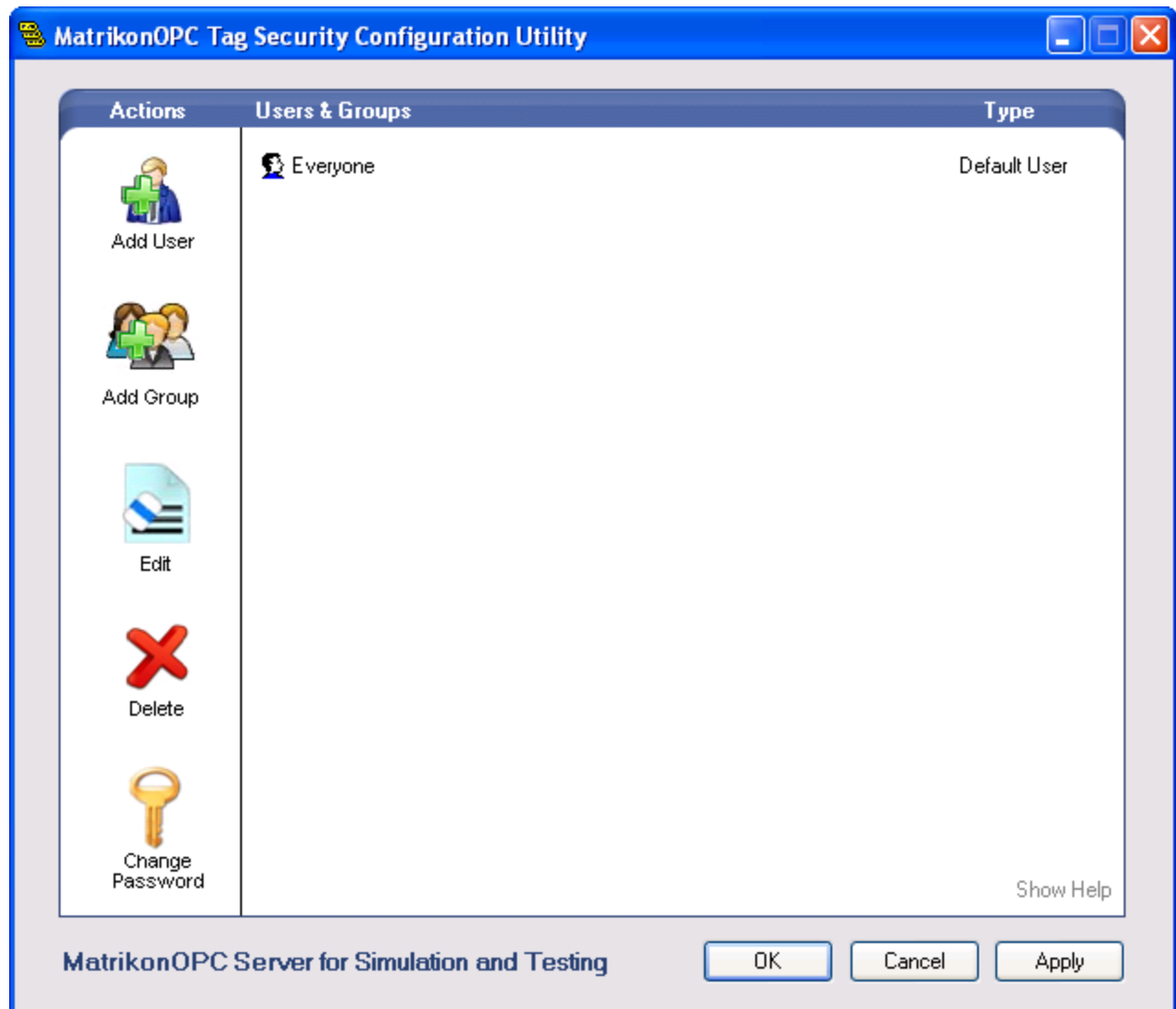


Figure 76 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups

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 77) appears. The **NT User** option button is selected by default. This will allow the addition of a user from a Windows NT Domain.

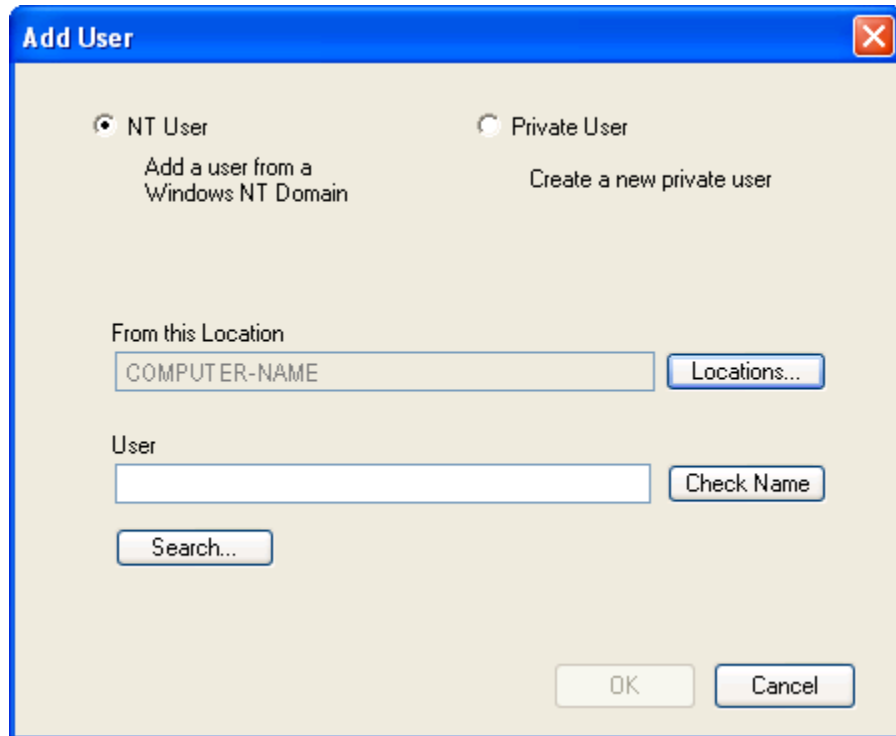


Figure 77 - Add User Window (NT)

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 78 for a sample list of defined users and groups).
6. The **Edit <Username>** window (Figure 83) appears. Follow the instructions in the **Edit User** section for adding permissions.

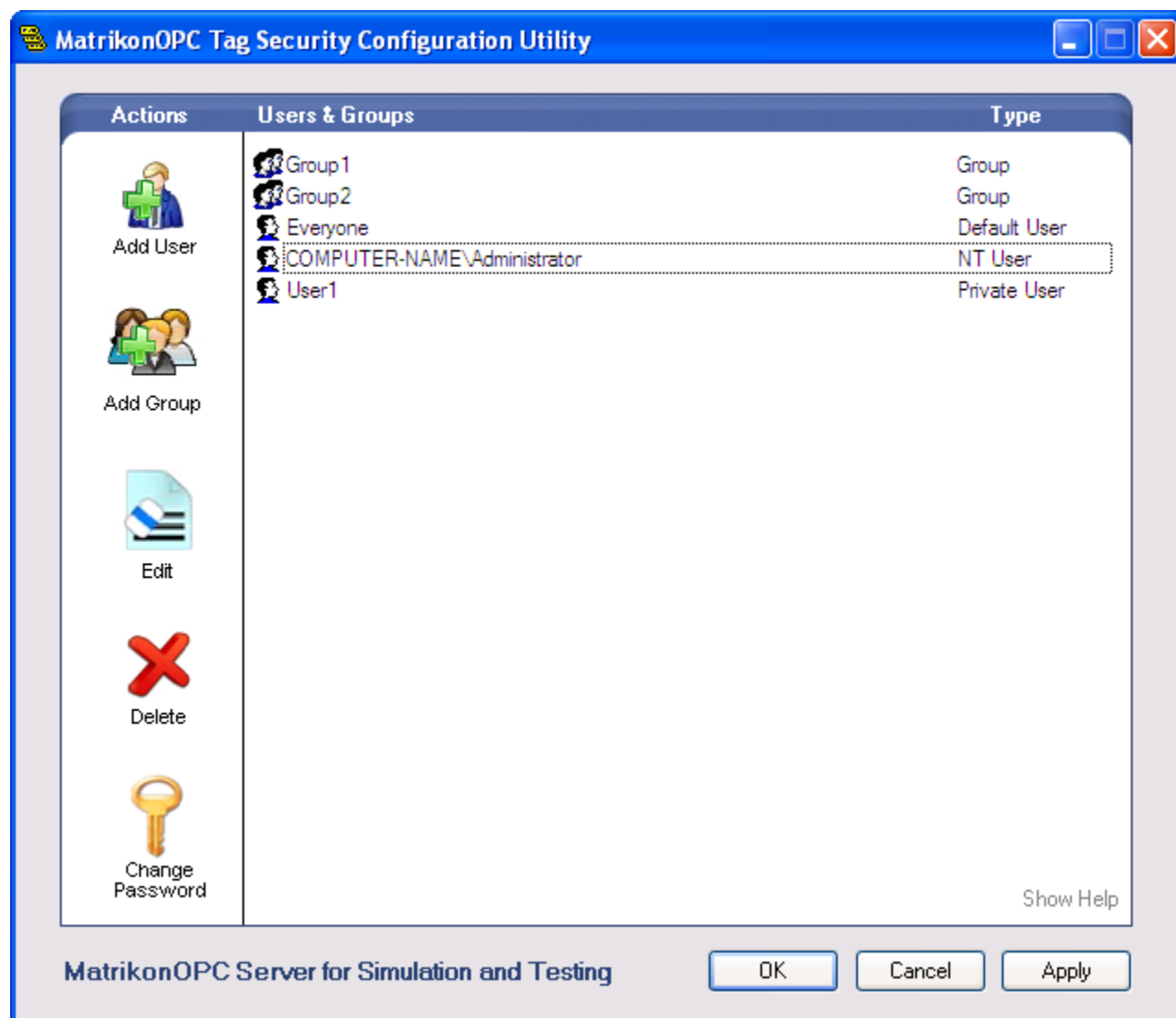


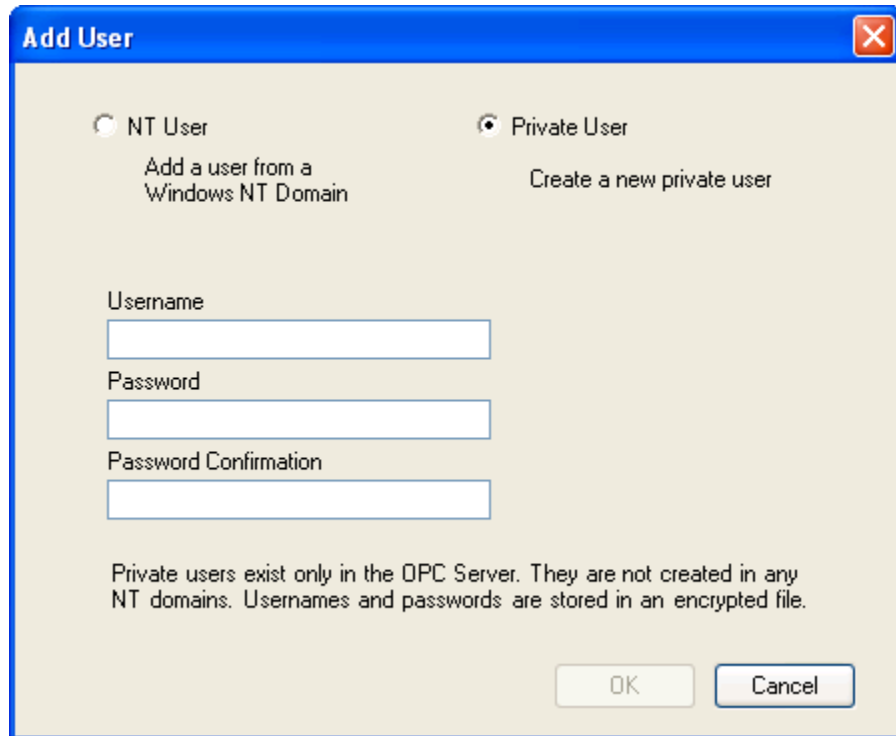
Figure 78 - Defined Users and Groups

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 77) appears.
3. Select the **Private User** option button (Figure 79).



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 labeled '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 79 - 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 78 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.

2. The **Add Group** window (Figure 80) appears. The **NT Group** option button is selected by default. This will allow the addition of an NT group from a Windows NT Domain.

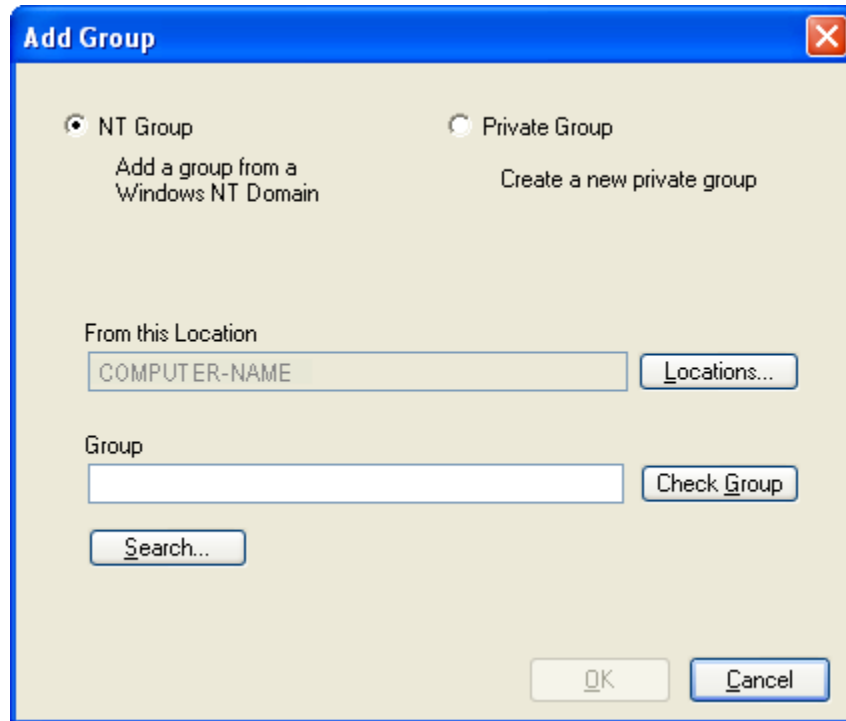


Figure 80 - Add Group Window (NT)

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 **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.
5. 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 78 for a sample list of defined users and groups).
6. The **Edit <Groupname>** window (Figure 90) 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:

1. From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add Group** button.
2. The **Add Group** window (Figure 80) appears.
3. Select the **Private Group** option button (Figure 81).

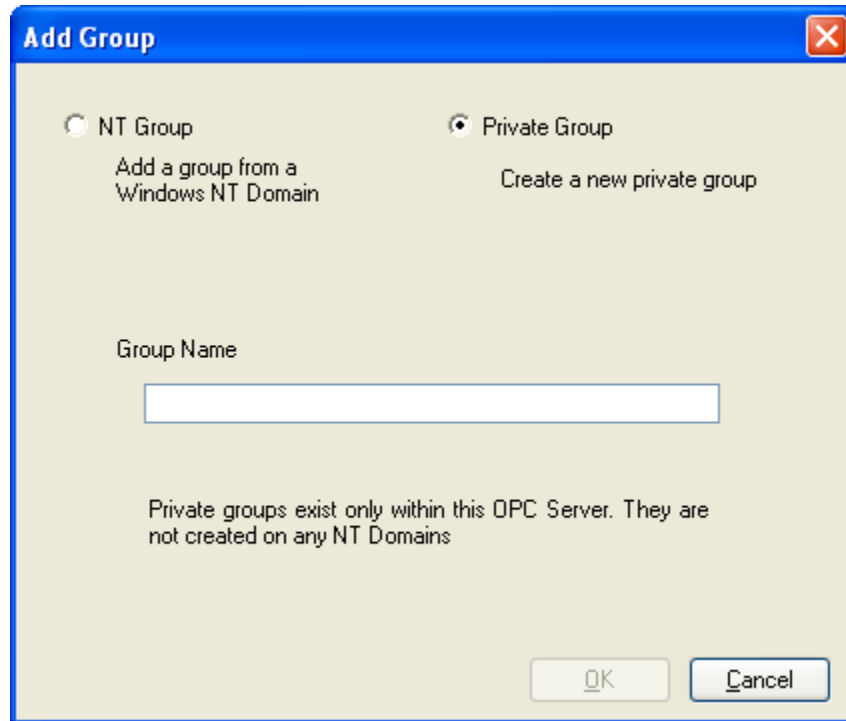


Figure 81 - Add Group Window (Private)

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 78 for a sample list of defined users and groups).
6. The **Edit <Groupname>** window (Figure 90) 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 82) appears.

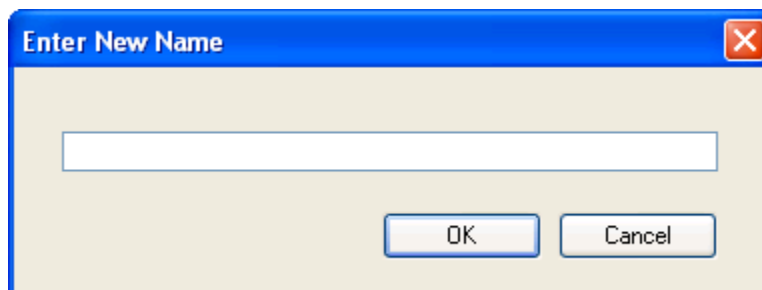


Figure 82 - Enter New Name Window

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 83) 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.

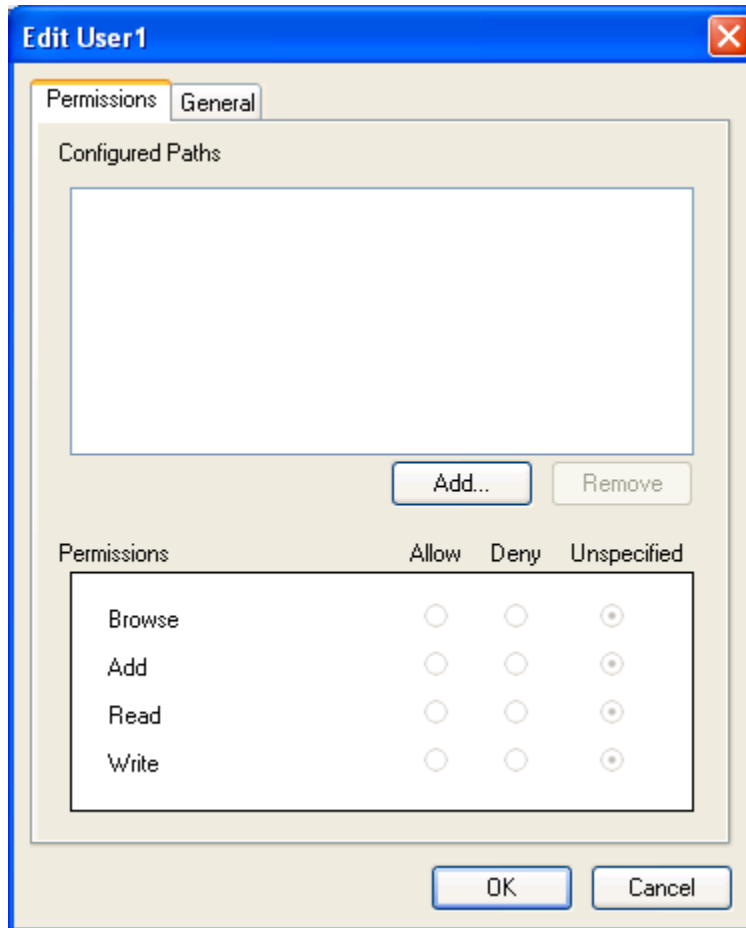


Figure 83 - Edit <Username> Window (Permissions Tab)

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

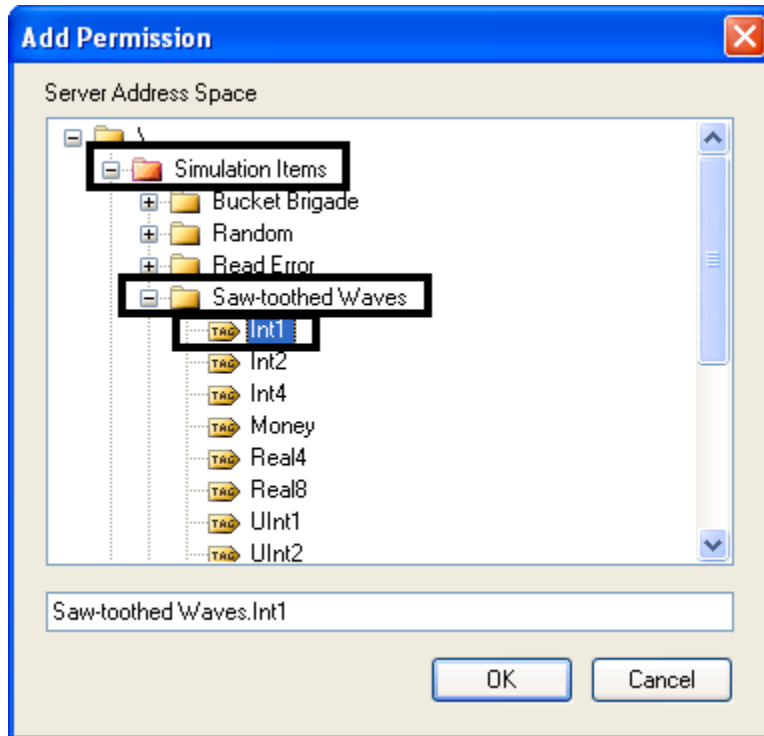


Figure 84 - Add Permission Screen (Server Address Space)

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.<item ID>**), 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 85) 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.

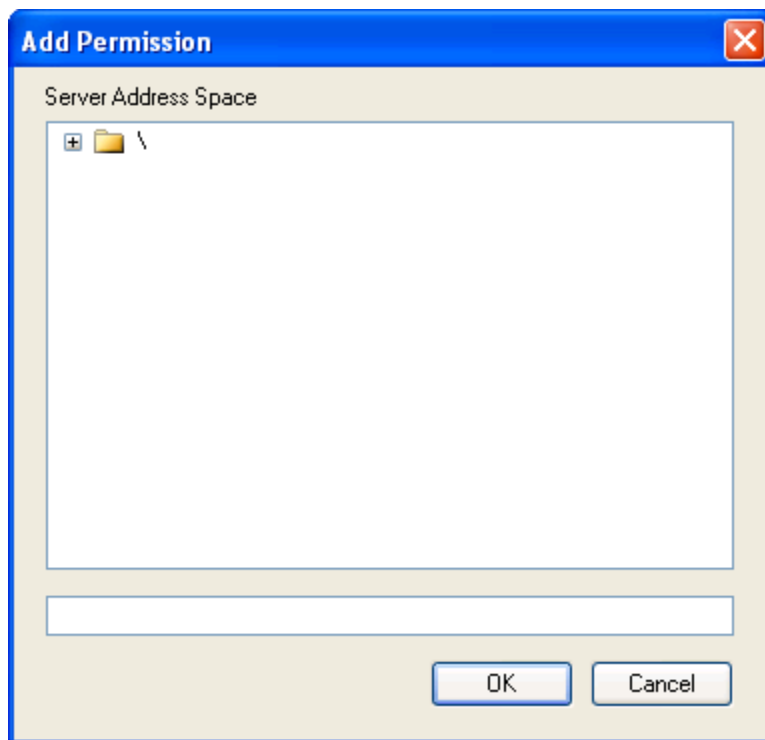


Figure 85 - Add User Permission Window

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 86) 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](#).

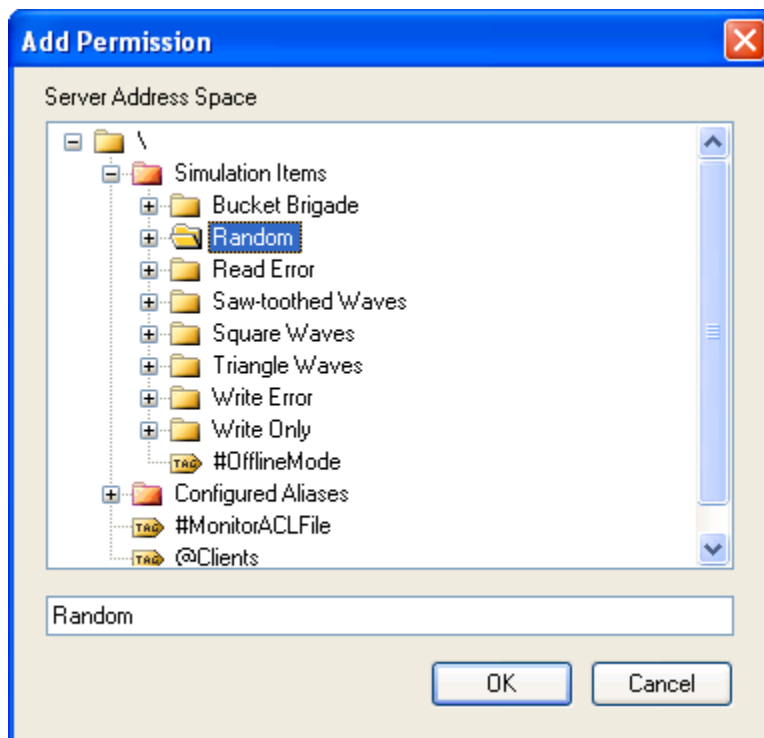


Figure 86 - Add Permission Window: Browsing Server Address Space

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 87.

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.

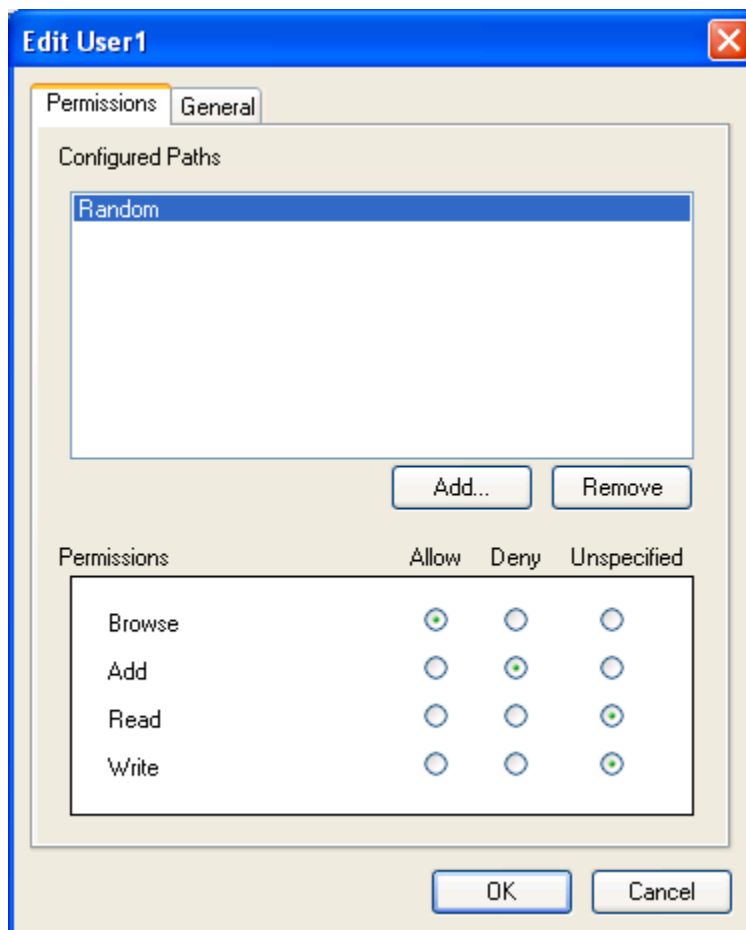


Figure 87 - Edit <Username>: Example

On the **General** tab (Figure 88) 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.

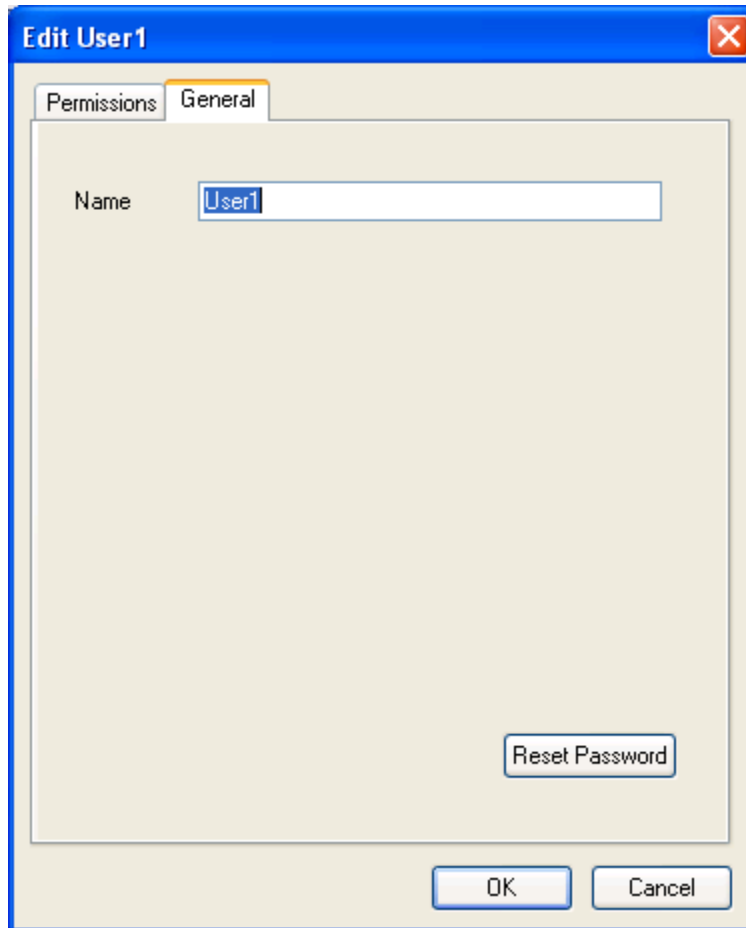


Figure 88 - Edit <Username> Window (General Tab)

To change the user's password:

1. Click on the **Reset Password** button. The **Reset Password** window (Figure 89) appears.

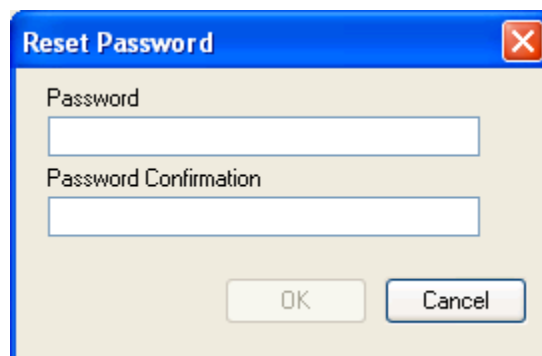


Figure 89 - Reset Password Window

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 90) 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.

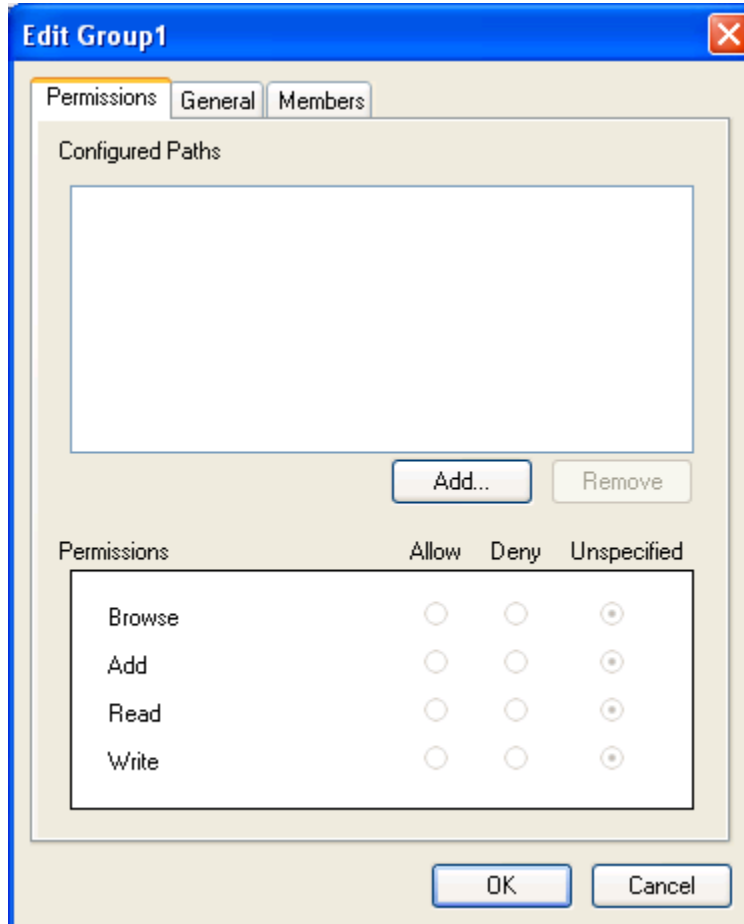


Figure 90 - Edit <Groupname> Window (Permissions Tab)

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 91) 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.

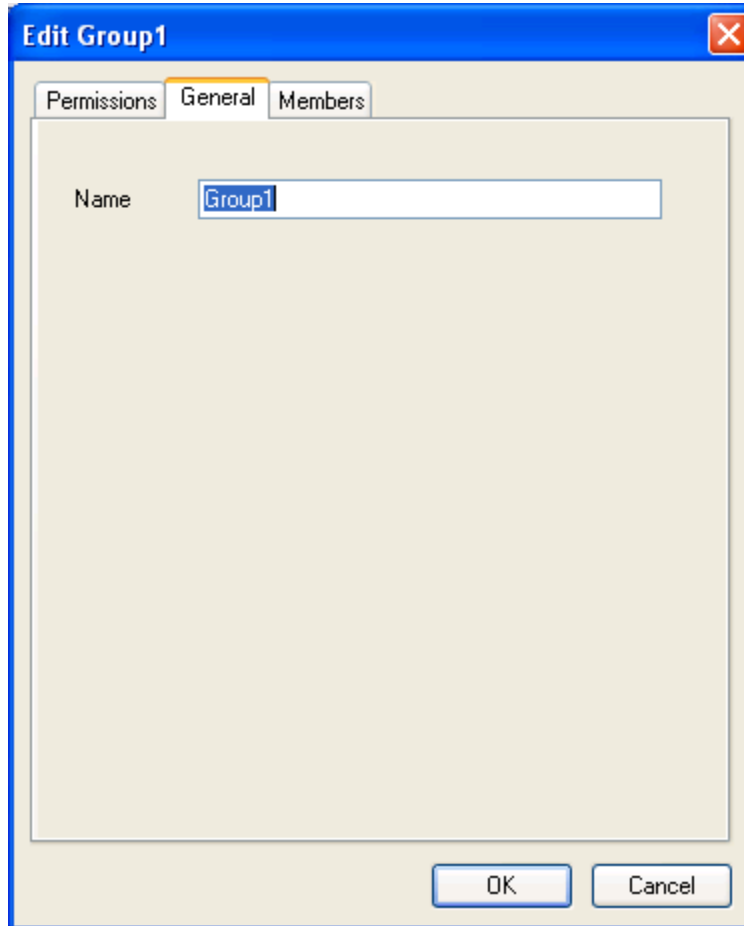


Figure 91 - Edit <Groupname> Window (General Tab)

On the **Members** tab (Figure 92), the users that are part of the current group are defined. By default, the **Group Members** screen section is empty. In Figure 92, **User1** has been added to **Group1**.

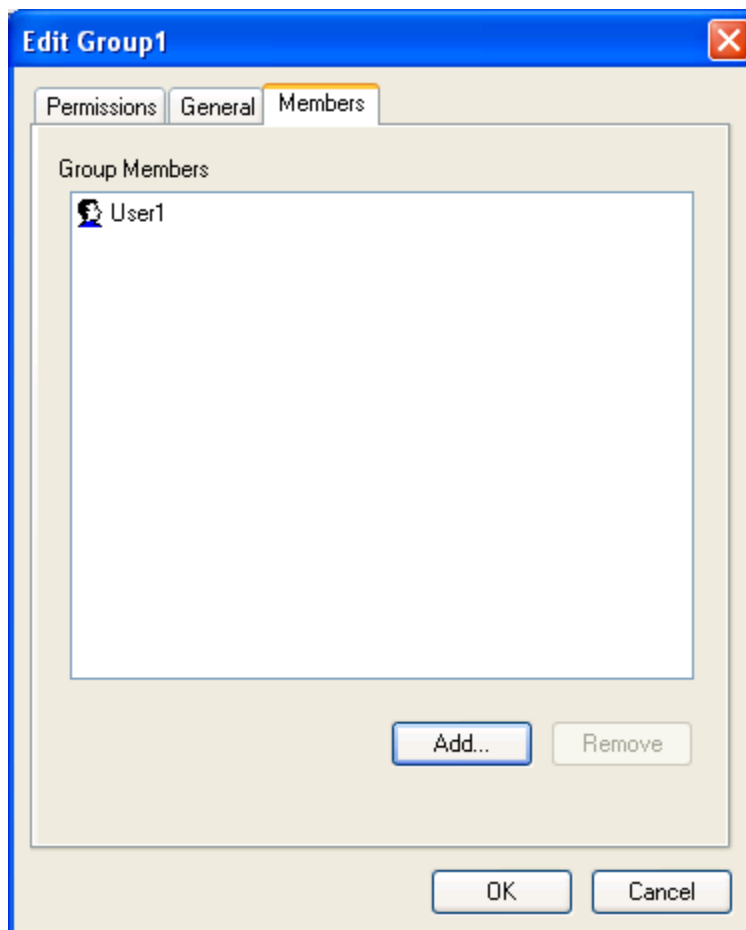


Figure 92 - Edit <Groupname> Window (Members Tab)

To add one or more members to the group:

1. Click on the **Add** button. The **Add Existing User** window (Figure 93) appears.

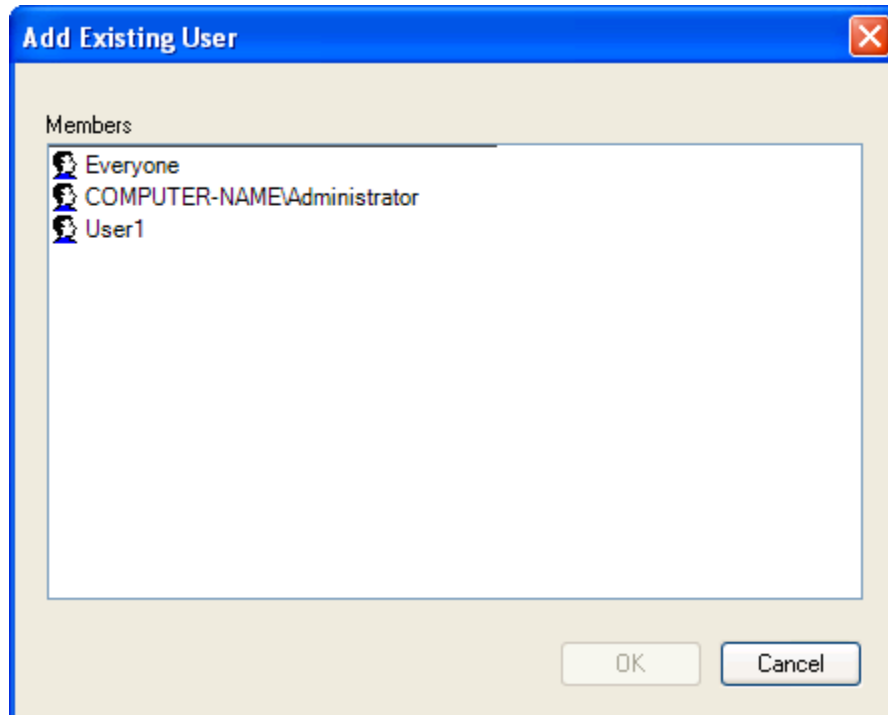


Figure 93 - Add Existing User Window

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 92).

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 78), 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 75).
2. The **Change Password** window (Figure 94) 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 an icon of a padlock. At the bottom right are "OK" and "Cancel" buttons.

Figure 94 - 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 70:

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

Table 70 - 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 71 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 71 - 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 72 lists all defined users and groups and their associated permissions. Table 73 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 72 - Example 2: Permissions

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

Table 73 - 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 78), 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 78). 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, and the user name has not been defined in the **Users & Groups** list, 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 87). 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 74 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 74 - 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 G 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 75 shows the value behaviour for each data type:

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

Table 75 - 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 H 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 fail 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 IEC, 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.

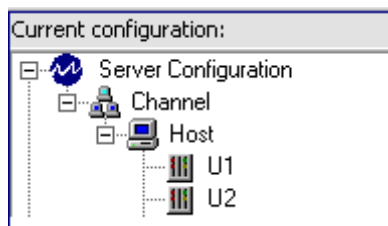


Figure 95 - Example

Appendix I Features and Examples

Introduction

This appendix describes the common features and newest enhancements added for the server, complete with examples.

Round-Robin Example

As explained in **Appendix H – SCADA Servers Connection Logic**, all of the MatrikonOPC SCADA servers poll in a round-robin mechanism. This server 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

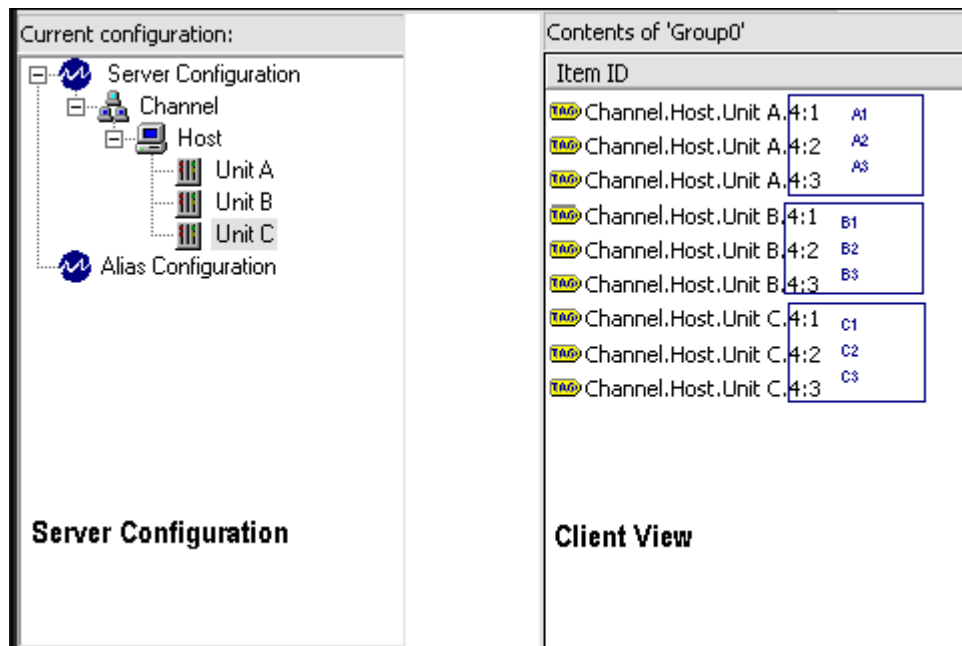


Figure 96 - Example 1

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.

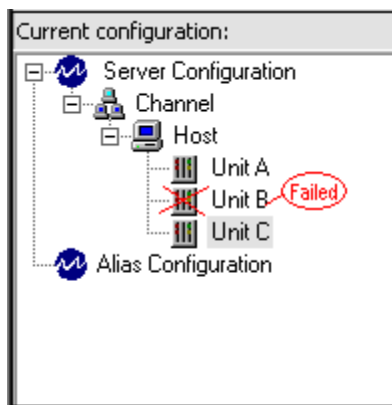


Figure 97 - Unit B Fails

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 98 - Retry Applied on Unit B Items

3. After the **Failed Polls Allowed** counter has been exceeded, the **Quality** of 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

Client View

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.

Figure 99 - 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 100 - 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 101 - Reconnect Retries

Note: The reconnection logic applied depends on which type of device link failed to connect. For example, if what fails is the IEC 60870 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.

Scanning and Stay Connected Option

In the normal operation any unit device link that is currently not being scanned from an OPC client, will disconnect until a client requests items that belong to that unit device link. To force the unit device link to be connected at all times even if none of its items are being currently scanned, the **Stay Connected** option must be selected.

Note: This option needs to be used when the unit device link is used as a redundant link in a Redundancy Group.

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 102 - 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.

Appendix J 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 that 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 76 - 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.
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 77 - 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 I – 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 78 - 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 79 - 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 80 - 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

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.
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.
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

OPC Item	Description
	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 = 0 .
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 81 - 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 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

OPC Item	Description
	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 82 - 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>E0Q0V1</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 dialled 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 83 - Dial-Up Object OPC Items