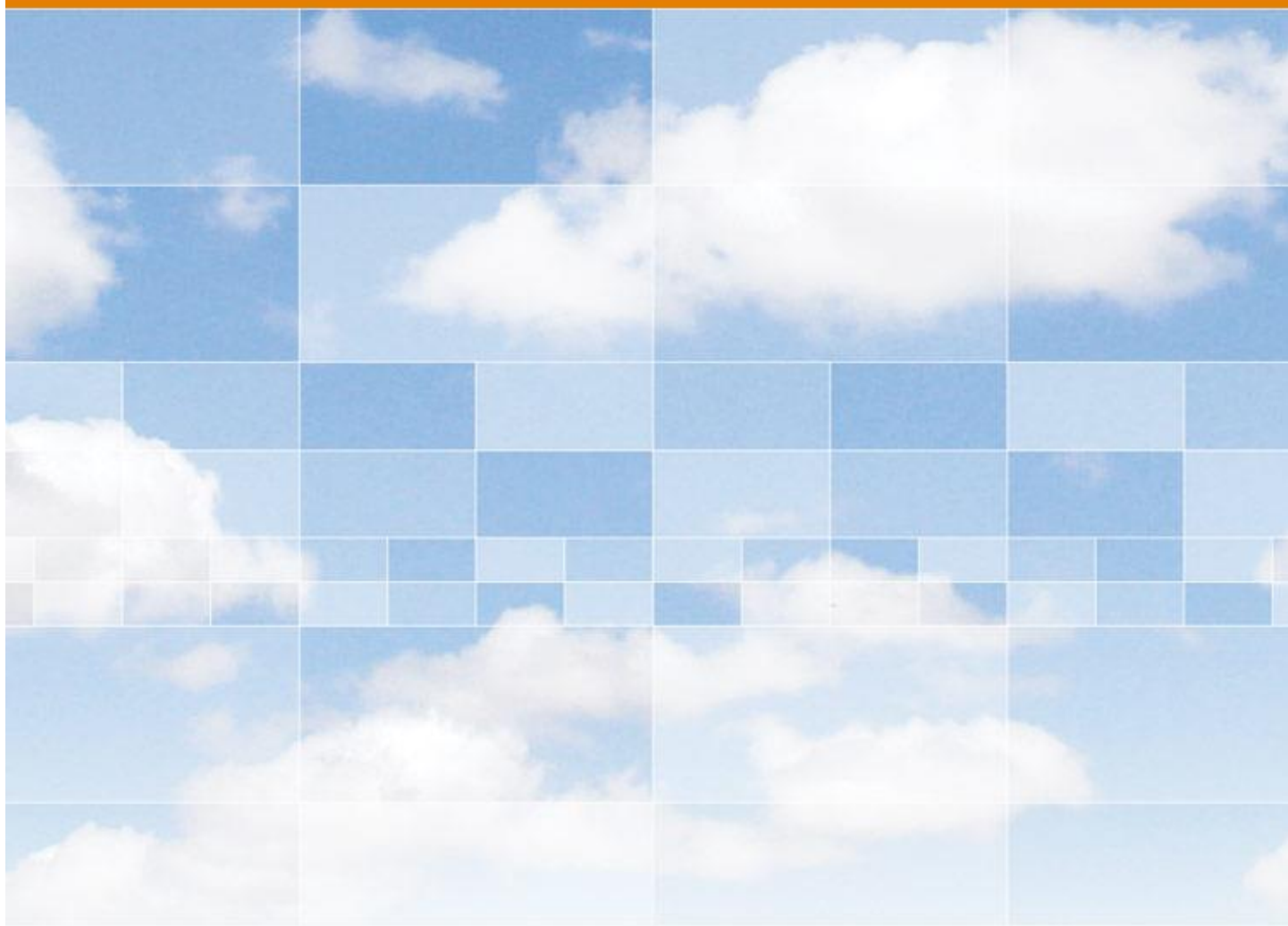




MatrikonOPC Server for IEC 61850/61400-25

User's Manual

MatrikonOPC Server for IEC 61850/61400-25

User's Manual

This manual is a product of Matrikon International

Matrikon International.
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
2009-11-10	1.0	Initial document.	CGAP, LB
2009-12-16	1.1	Revised panel information and added details about optimization.	CGAP
2010-01-13	2.0	Updated for panel changes.	CGAP
2010-01-18	2.1	Added supported features to Introduction section. Updated screenshot and components for Browse tab (Figure 4). Updated OPC Data Items and Limitations sections.	CGAP, LB
2010-01-22	2.2	Updated product name references for consistency.	CGAP, LB
2010-01-25	2.3	Updated Software Requirements.	LB
2010-04-16	3.0	Updated for UCS use. Updated to software version 1.1.0. Converted document to standard plug-in template.	CGAP, LB
2010-05-03	4.0	Added support for 61400-25 and OPC A&E Protocol Logging.	CGAP, CN
2010-08-17	5.0	Added configuration for Authentication and ASCE Calling parameters. Updated Software Requirements.	CGAP, LB
2010-08-25	6.0	Converted to standard template.	LB
2010-09-27	7.0	Updated: software version to 1.3.0, New IED Device Link (Optimization tab) window screenshot and field descriptions, File Menu/Shutdown Server description, shutting down the server note, General Logging Options Tab/Enable activity logging description.	MA, LB

2010-09-30	7.1	Updated OPC Data Item section: added IED level statistical and control items table, added control operations section. Updated Limitations section.	LW, MA, LB
2010-10-05	7.2	Updated server configuration section: added Control tab screen shot and table, updated Control Operations section. Appendix I – Installed Files, Common folder updated. Added Redundancy Failover Conditions section.	LW, LB
2010-10-15	7.3	Updated OrIdent description. Updated IEC 61850 Control Operations (Select/Operate) section.	LW, LB
2010-10-18	7.4	Added Windows 7 to Software Requirements section.	LB
2012-01-23	8.0	Updated software version to 1.3.1.	LB
2012-06-17	8.1	Updated OPC Data Items, Software Requirements, and after-hours contact numbers.	LB
2012-07-19	8.2	Updated note in Appendix B – Aliases – CSV File Format. Updated install directory in Appendix I – Installed Files.	LB
2014-01-08	8.3	Removed LB refs; updated to software v 1.3.2	MJL
2016-05-31	8.4	v.1.3.3	MJL
2016-12-13	8.5	v. 1.4.0. OS list and screenshots updated. Broken links fixed.	MJL

SOFTWARE VERSION

Version: 1.4.0

DOCUMENT VERSION

Version: 8.5

COPYRIGHT INFORMATION

© **Copyright 1997 - 2017**, Matrikon International, a business unit of Honeywell Limited ("Matrikon International" or "Matrikon"). 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 International.

CONFIDENTIAL

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

IMPORTANT NOTICE

Although every endeavor has been made to ensure that the information contained within this document is up to date and accurate, Matrikon cannot be held responsible for any inaccuracy or error in the information contained within this document. Matrikon makes no warranty of any kind with regard to the information contained within this document and Matrikon shall not be liable for any direct, indirect, incidental or consequential damages which may arise in connection with the furnishing, reliance, or use of the information contained within this document.

Specifications and statements as to performance in this document are Matrikon estimates, intended for general guidance. Matrikon reserves the right to change the information contained within this document and any product specification without notice.

Statements in this document are not part of a contract or program product license insofar as they are incorporated into a contract or license by express preference. Issue of this document does not entitle the recipient to access or use of the products described, and such access or use shall be subject to separate contracts or licenses.

The receiving party shall not disclose, publish, report, communicate, or otherwise transfer any information in this document to any third party, and shall protect all information contained herein from unauthorized disclosure. The receiving party shall permit access to this document only to its employees, agents, subcontractors, and affiliates who reasonably require access to such information contained herein, have been made aware of the confidential nature of this document and have executed a written employment or other confidentiality agreement party to maintain the confidential status of this document.

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 Honeywell International Inc.

Table of Contents

Introduction	11
Who Should Use This Manual	11
Overview of Manual	11
References	12
Document Terminology	13
Getting Started.....	15
System Requirements	15
<i>Software Requirements</i>	<i>15</i>
<i>Hardware Requirements</i>	<i>15</i>
Configuration	16
Starting the MatrikonOPC Server for IEC 61850/61400-25.....	16
Tool Tray Menu	17
Control Panel	17
Configuration Window	18
<i>File Menu.....</i>	<i>20</i>
<i>Edit Menu</i>	<i>20</i>
<i>View Menu.....</i>	<i>21</i>
<i>Tools Menu</i>	<i>22</i>
<i>Help Menu</i>	<i>22</i>
Options Window	22
<i>General Options</i>	<i>22</i>
<i>General Logging Options.....</i>	<i>24</i>
<i>Interface Logging Options.....</i>	<i>25</i>
<i>Advanced Options.....</i>	<i>27</i>
Server Configuration.....	28
<i>Creating Objects.....</i>	<i>28</i>
<i>Creating and Configuring an IED Device Link.....</i>	<i>29</i>
<i>Creating and Configuring a Redundancy Group Object.....</i>	<i>39</i>
<i>Creating and Configuring a Server Status List Object</i>	<i>43</i>
<i>Changing Objects</i>	<i>47</i>
<i>Removing Objects.....</i>	<i>47</i>
Alias Configuration	48
<i>Inserting Alias Groups.....</i>	<i>48</i>
<i>Renaming Alias Groups.....</i>	<i>48</i>
<i>Inserting New Aliases.....</i>	<i>48</i>
<i>Editing Aliases.....</i>	<i>51</i>
<i>Removing Aliases</i>	<i>51</i>
<i>Removing Alias Groups.....</i>	<i>52</i>
<i>Exporting Aliases</i>	<i>52</i>
<i>Importing Aliases.....</i>	<i>52</i>
<i>Configure Alias Scaling</i>	<i>52</i>
<i>Configure Alias Events.....</i>	<i>54</i>
<i>Configure Categories.....</i>	<i>56</i>
Expression Wizard	57
<i>Examples.....</i>	<i>57</i>
Item Path Browser.....	61
Saving a Configuration	62
Clearing a Configuration	62
Loading an Existing Configuration	62
Shutting Down the Server	63

OPC A&E Protocol Logging	64
OPC Data Items	65
IED Items.....	65
IEC 61850 Data Type Mapping	65
IED Level Statistical and Control Items.....	66
IEC 61850 Control Operations (Select/Operate).....	66
Standard Data Items.....	69
Getting Data without Being Connected to a Device	70
Diagnostics	71
Logging.....	71
Limitations	72
Troubleshooting	73
Problems and Solutions.....	73
Questions and Answers	79
Licensing.....	80
Contacting Support.....	80
OPC Compliance	82
Installation	82
Common Interfaces	82
Data Access.....	82
Groups.....	83
Items.....	83
Browsing and Item Properties	83
I/O Operations	83

Table of Appendices

Appendix A Distributed COM (DCOM)	85
DCOM Configuration Utility	85
Default Properties.....	85
Security Permissions.....	86
Server Identity.....	90
Default Protocols	90
Remote Program ID.....	91
Appendix B Aliases	92
Scaling Expressions	92
Advanced Calculations	93
CSV File Format	95
Scaling Algorithms.....	97
Appendix C Standard Data Types.....	98
Appendix D Microsoft Excel as a DDE Client.....	99
DDE Read.....	99
DDE Write	99
Net DDE.....	100
Appendix E Configuring Dynamic Data Exchange (DDE)	101
Appendix F Security	102
Introduction.....	102
OPC Security Implementation	102
MatrikonOPC Tag Security Configuration Utility	103
Security Details.....	125

Appendix G	Offline Mode	128
	Introduction.....	128
	Offline Mode Toggling	128
	Offline Mode Item Values.....	128
	Operational Effects	129
Appendix H	Installation	130
Appendix I	Installed Files	141
Appendix J	Un-Installation	144

Table of Figures

Figure 1 - Tool Tray	16
Figure 2 - Tool Tray Menu.....	17
Figure 3 - Control Panel	18
Figure 4 - Configuration Window.....	19
Figure 5 - General Options Tab.....	23
Figure 6 - General Logging Options Tab	24
Figure 7 - Interface Logging Options Tab	26
Figure 8 - Advanced Options Tab.....	27
Figure 9 - Insert New Object Window	28
Figure 10 - Create New IED Device Link Window (Communications Tab).....	30
Figure 11 - Import Configuration Window.....	32
Figure 12 - Create New IED Device Link Window (Browse Tab)	33
Figure 13 - Create New IED Device Link Window (Control Tab)	34
Figure 14 - New IED Device Link Window (Optimization Tab with Unbuffered Reports Enabled).....	35
Figure 15 - Create New IED Device Link (RCB Tab) Components.....	36
Figure 16 - Create New IED Device Link Window (Advanced Tab).....	37
Figure 17 - New IEC 61850 IED Device Link Object.....	39
Figure 18 - Create New Redundancy Group Window	41
Figure 19 - New Redundancy Group Object	43
Figure 20 - Create New Server Status List Window	44
Figure 21 - New Server Status List Object.....	47
Figure 22 - Client Reference Warning Message	47
Figure 23 - Insert New Alias Window – Alias Type	49
Figure 24 - Contents Table	51
Figure 25 - Configure Scaling Window	53
Figure 26 - Generate Events Options.....	55
Figure 27 - New Category Window	56
Figure 28 - Edit Categories Window	57
Figure 29 - Expression Engine Configuration.....	59
Figure 30 - Expression Wizard.....	59
Figure 31 - Select Function Window	60
Figure 32 - Select Variable Window.....	60
Figure 33 - User Defined Functions Editor	61
Figure 34 - Operators Buttons.....	61
Figure 35 - Structured Block Write Without Caching Enabled	67
Figure 36 - Structured Block Write with caching enabled	68
Figure 37 - Registry Editor	74
Figure 38 - Program ID Branch	75
Figure 39 - Distributed COM Configuration Properties Window	87

Figure 40 - Distributed COM Configuration Security Tab	88
Figure 41 - Registry Value Permissions Window	89
Figure 42 - Add Users and Groups Window	89
Figure 43 - DDE Share	100
Figure 44 - Start Menu Navigation.....	104
Figure 45 - Enter Server Password Window	104
Figure 46 - MatrikonOPC Tag Security Configuration Utility Main Screen	105
Figure 47 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups	106
Figure 48 - Add User Window (NT).....	107
Figure 49 - Defined Users and Groups	108
Figure 50 - Add User Window (Private).....	109
Figure 51 - Add Group Window (NT)	110
Figure 52 - Add Group Window (Private)	111
Figure 53 - Enter New Name Window.....	111
Figure 54 - Edit <Username> Window (Permissions Tab).....	113
Figure 55 - Add Permission Screen (Server Address Space).....	114
Figure 56 - Add User Permission Window.....	115
Figure 57 - Add Permission Window: Browsing Server Address Space	116
Figure 58 - Edit <Username>: Example.....	117
Figure 59 - Edit <Username> Window (General Tab).....	118
Figure 60 - Reset Password Window	118
Figure 61 - Edit <Groupname> Window (Permissions Tab)	119
Figure 62 - Edit <Groupname> Window (General Tab)	120
Figure 63 - Edit <Groupname> Window (Members Tab)	121
Figure 64 - Add Existing User Window	122
Figure 65 - Change Password Window	123
Figure 66 - InstallAware Wizard Verification Window	130
Figure 67 - Pre-Requisites Screen	131
Figure 68 - License Agreement Screen	132
Figure 69 - Setup Type Screen	133
Figure 70 - Destination Folder Screen	134
Figure 71 - Start Menu Screen	135
Figure 72 - Enter Password Screen	136
Figure 73 - Licensing Screen	137
Figure 74 - Ready to Install Screen	138
Figure 75 - Installing MatrikonOPC Server Screen	139
Figure 76 - MatrikonOPC Server Setup Complete Screen	140
Figure 77 - Add or Remove Programs	144
Figure 78 - Welcome to MatrikonOPC Server for IEC 61850/61400-25 Maintenance Screen.....	145
Figure 79 - Ready to Uninstall Screen	146
Figure 80 - Uninstalling MatrikonOPC Server for IEC 61850/61400-25 Screen	147
Figure 81 - MatrikonOPC Server for IEC 61850/61400-25 Setup Complete Screen	148

Table of Tables

Table 1 - Terms and Definitions.....	14
Table 2 - Tool Tray Menu Commands.....	17
Table 3 - Control Panel Commands.....	18
Table 4 - Configuration Window Commands	20

Table 5 - File Menu Commands.....	20
Table 6 - Edit Menu Commands (Server Configuration)	21
Table 7 - Edit Menu Commands (Alias Configuration).....	21
Table 8 - View Menu Commands.....	21
Table 9 - Tools Menu Commands	22
Table 10 - Help Menu Commands	22
Table 11 - General Options Tab Components.....	24
Table 12 - General Logging Options Tab Components	25
Table 13 - Interface Logging Options Tab Components	26
Table 14 - Advanced Options Tab Components.....	28
Table 15 - Insert New Object Window Options.....	29
Table 16 - Create New IED Device Link Window (Communications Tab) Components....	31
Table 17 - Import Configuration Window Components.....	32
Table 18 - Create New IED Device Link Window (Browse Tab) Components	33
Table 19 - Create New IED Device Link Window (Control Tab) Components	34
Table 20 - Create New IED Device Link Window (Optimization Tab) Components.....	35
Table 21 - Create New IED Device Link (RCB Tab) Components	36
Table 22 - Create New IED Device Link Window (Advanced Tab) Components.....	38
Table 23 - Redundancy Modes	40
Table 24 - Create New Redundancy Group Window Components	42
Table 25 - Create New Server Status List Window Components	46
Table 26 - Insert New Alias Window – Alias Type Options	50
Table 27 - Insert New Alias Window – Alias Properties Options.....	51
Table 28 - Configure Scaling Window Options	53
Table 29 - Generate Events Window Options.....	56
Table 30 - New Category Window Options	56
Table 31 - Expression Wizard Options	58
Table 32 – Item Path Browser Options.....	62
Table 33 - Item ID Field Descriptions.....	65
Table 34 - Data Type Mapping	66
Table 35 - IED Level Statistical and Control Items	66
Table 36 - Standard Data Items	69
Table 37 - Server Data Items	69
Table 38 - Redundancy Device Link OPC Items	70
Table 39 - Server Status List Device Link OPC Items.....	70
Table 40 - MatrikonOPC Support Regional Contact Information	80
Table 41 - After-Hours Support	81
Table 42 - Expressions Constructs for Alias Scaling	93
Table 43 - Calculation Operators for Alias Scaling	94
Table 44 - Calculation Functions for Alias Scaling	95
Table 45 - File Import/Export Field Descriptions	96
Table 46 - Additional File Import/Export Field Descriptions - Linear/Square Root Scaling	96
Table 47 - Additional File Import/Export Field Descriptions - Offset Scaling.....	96
Table 48 - Additional File Import/Export Field Descriptions - Expression Scaling	96
Table 49 - Additional File Import/Export Field Descriptions - Calculation Scaling.....	97
Table 50 - Scaling Algorithms.....	97
Table 51 - Standard Data Types	98
Table 52 - Default Tag Security	123
Table 53 - Example 1.....	124
Table 54 - Example 2: Permissions.....	124
Table 55 - Example 2: Groups and Members.....	124
Table 56 - Example 2: Permissions.....	127

Table 57 - Offline Mode Item Values	129
Table 58 - Files Installed in "IEC61850" Folder	141
Table 59 - Files Installed in "Common" Folder	142
Table 60 - Files Installed in "system32" Folder	143

Introduction

This manual is designed to teach you how to configure the MatrikonOPC™ Server for IEC 61850/61400-25.

This MatrikonOPC Server for IEC 61850/61400-25 provides connectivity to any Intelligent Electronic Device (IED) compatible with the IEC 61850 and 61400-25 protocols.

The MatrikonOPC Server for IEC 61850/61400-25 includes support for:

- IEC 61850 Communications over TCP/IP – IEC 61850-8-1 T Profile, MMS over TCP/IP.
- IEC 61400-25-1 Communications for monitoring and control of wind power plants
- IEC 61400-25-4 Annex C: IEC61400 over MMS per IEC 61850-8-1
- Browsing: Cached from device, or polled from device as needed.
- Import communications parameters from SCL files (SCD, CID, and ICD).
- Control blocks supported: Buffered Report Control Block, and Unbuffered report Control Block.
- Data Transfer Modes: Polling Items, Polling Nodes, Polling Data Sets, Data Sets by Report.
- Optimization.
- Device-sourced time stamps and quality.
- Redundancy, including channel redundancy, and fail-over and fail-back.
- Runs as a Windows service.
- Protocol byte streams for the IEC 61850/61400-25 protocols are available as OPC A&E Simple Events.

The purpose of the MatrikonOPC Server for IEC 61850/61400-25 is to maintain a robust connection to substation equipment operating on the IEC 61850 or IEC 61400-25 protocol over a TCP/IP connection using the ISO 9506-1/9506-2 Manufacturing Message Specification (MMS).

Who Should Use This Manual

This manual is intended for use by all users of the MatrikonOPC Server for IEC 61850/61400-25.

This manual explains how to install and configure the software, and how to perform common tasks. In addition, technical information about OPC data items is included, along with sections on diagnostics and troubleshooting.

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 document, or if applicable, any external sources.

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

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

- **Introduction** – this introductory chapter.
- **Getting Started** – provides system requirements 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 A&E Protocol Logging** – describes how to enable and use the protocol logging using the OPC A&E interface.
- **OPC Data Items** – describes the server's items.
- **Diagnostics** – explains how to use logging, statistical items, data qualities, timestamps, and result codes to get the most efficiency from the user's system.
- **Limitations** – provides information on specific performance and operational limitations of the software.
- **Troubleshooting** – provides licensing, MatrikonOPC Support contact information, solutions for common problems that may be encountered, and answers to frequently asked questions.
- **OPC Compliance** – details supported interfaces with regard to installation, common interfaces, and data access.
- **Appendices:**
 - **A** - DCOM
 - **B** – Aliases
 - **C** – Standard Data Types
 - **D** – Microsoft Excel as a DDE Client
 - **E** – Configuring Dynamic Data Exchange (DDE)
 - **F** – Security
 - **G** – Offline Mode
 - **H** – Installation
 - **I** – Installed Files
 - **J** – Un-Installation

References

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

- www.opcfoundation.org
- www.matrikonopc.com
- www.opcsupport.com
- *OPC Overview 1.0*

- *OPC Common Definitions and Interfaces 1.0*
- *OPC Data Access Specification 2.05a*
- *OPC Data Access Specification 3.00*
- *OPC Historical Data Access Specification 1.2*
- *OPC Alarms and Events Specification 1.10*
- *OPC Security 1.00*

Document Terminology

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

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

Term/Abbreviation	Description
A&E	OPC Alarms and Events. Provides access to process alarm and event 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. Provides access to historical process data.
HMI	Human Machine Interface. Device that allows interaction between the user and machine. Typically used in process control applications.
Matrikon	Matrikon Inc.
MatrikonOPC	Matrikon's brand name for its OPC servers and clients.
OPC	A communication standard. Refer to www.opcfoundation.org for more information.
PLC	Programmable Logic Controller.
LN	Logical Node.
LD	Logical Device.
ACSI	Abstract Communication Service Interface – the object model used to represent the services and data points available from a wide range of IEC 61850 hardware.
IEC	International Electrotechnical Commission – an international standards body responsible for the IEC 61850 specification.
IED	Intelligent Electronic Device.
SCL	Substation Configuration Language. An XML-based language that describes the capabilities and configuration of IEC 61850 devices.
ICD	IED Capability Description File. This file is written in SCL and describes the capabilities of a type of IED.

Term/Abbreviation	Description
CID	Configured IED Description. This file is written in SCL and describes the configuration of a specific IED.
SCD	Substation Configuration Description. This is a file written in SCL and describes multiple configured IEDs and their relationship within a substation.
GOOSE	Generic Object Oriented Substation Event. Part of the IEC 61850 standard dealing with broadcast messages from and between IEDs.
GSE	Generic Substation Event. Part of the IEC 61850 standard dealing with broadcast messages from and between IEDs.
GSSE	Generic Substation Status Event. Part of the IEC 61850 standard dealing with broadcast messages from and between IEDs.
RCB	Report Control Block. The IEC 61850 uses Report Control Blocks to manage unsolicited communication between the device and a client.
BRCB	Buffered Report Control Block. The IEC 61850 specification uses Buffered Report Control Blocks to ensure that data is transferred to the client from the device, even when there is a temporary connection failure. The data set and conditions for reporting must be pre-configured on the device. Data is sent by a report-by-exception mechanism rather than polling.
URCB	Unbuffered Report Control Block. The IEC 61850 specification uses Unbuffered Report Control Block for the basic transfer of data on a report-by-exception basis.

Table 1 - Terms and Definitions

Getting Started

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 **Appendix H - Installation** walks you through the installation process. **Appendix I – Installed Files** lists the files that are installed during this process.

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

System Requirements

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



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

Software Requirements

At the minimum, the server requires the following software:

- Microsoft Windows 7, or
- Microsoft Windows Server 2008 (SP1, SP2), or
- Microsoft Windows 10, or
- Microsoft Windows Server 2012, or
- Microsoft Windows Server 2016
- Microsoft .NET 2.0 Framework (included with this install program)



Note: It is recommended that the most current service packs are installed. Service packs levels listed above indicate the versions that have been tested for compatibility.

Hardware Requirements

The server requires the following hardware:

- Intel® CORE i5 Processor
- 4 GB RAM
- 80 GB 7200 RPM Hard Drive

Configuration

The server's Graphical User Interface (GUI) allows users to view and alter configuration parameters at run time. When you view 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 61850/61400-25 is required for it to function properly, but users can customize the server's behavior as required. This chapter shows you how to configure the server and describes each component in detail, including the windows, panels, and menu commands.

The **Starting the MatrikonOPC Server for IEC 61850/61400-25** section of this manual shows you 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. Instructions for configuring the MatrikonOPC Server for IEC 61850/61400-25 as a DDE service appear in **Appendix D - Microsoft Excel as a DDE Client**. 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.

Starting the MatrikonOPC Server for IEC 61850/61400-25

To launch the MatrikonOPC Server for IEC 61850/61400-25, choose the appropriate shortcut from the **Start** menu.

To start the MatrikonOPC Server for IEC 61850/61400-25:

1. Click on the Windows **Start** button and select **Programs** -> **MatrikonOPC** -> **IEC 61850 and 61400-25**, and choose **MatrikonOPC Server for IEC 61850 and 61400-25**.

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 1), located by default in the system tray.



Figure 1 - 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 2).

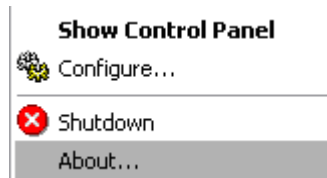


Figure 2 - Tool Tray Menu

Table 2 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 2 - 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 3) appears.



Figure 3 - 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 3 describes the commands in the **Tool Tray Menu**.

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

Table 3 - 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 displays a tree view of objects configured in the server. Select an object to display its current configuration, which appears on the right-hand side of the window.

If the server runs as a local executable, it will remain running even after the main configuration window is closed, even if no clients are connected. Displaying the control panel or main configuration window for the server will “lock” it so that it will not shut down while configuration is being performed.

If the server runs as an NT service, it will remain running so long as there are clients connected to it. Closing the main configuration window will shut down the configuration utility, but will not interfere with the normal operation of the server.

To view the Configuration window:

1. From the **Tool Tray Menu** or the **Control Panel**, select **Configure**.
2. The **Configuration** window (Figure 4) appears.

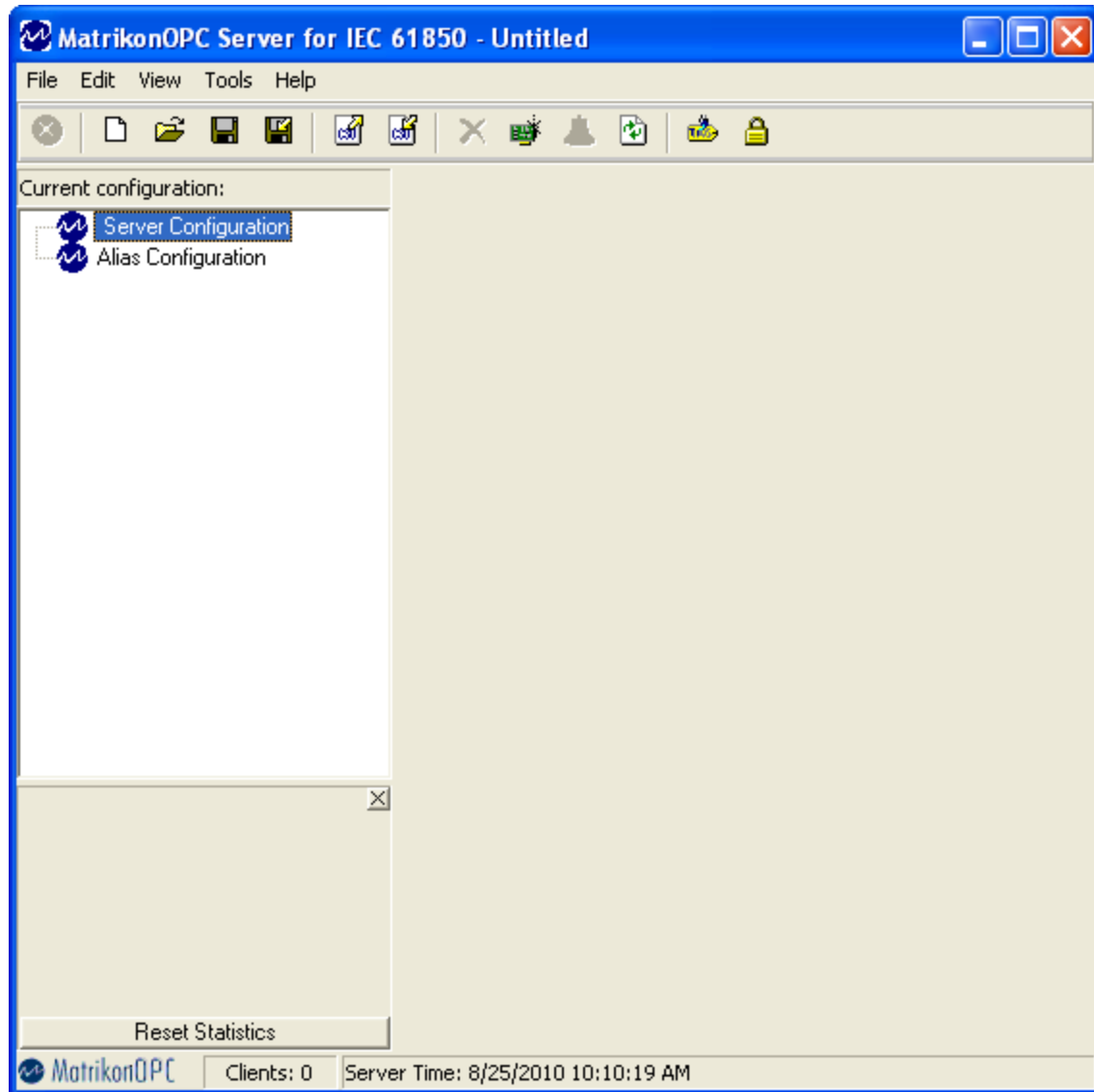


Figure 4 - Configuration Window

Table 4 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
	<i>Sent, Received, Timed Out, Retried, Failed, Overrun.</i>
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 4 - Configuration Window Commands

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

File Menu

Table 5 describes the **File** menu commands.

Command	Description
 New	Clears the current configuration and starts a new one. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing.
 Open	Clears the current configuration and loads a new one from an existing file. Displays the Open Configuration window to prompt for the file name. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing.
 Save	Saves the current configuration to an XML file. Displays the Save Configuration window to prompt for a new file name if the configuration is new and has not been saved before.
 Save As	Saves the current configuration to an XML file. Displays the Save Configuration window to prompt for a new file name.
 Export Aliases	Exports all currently configured aliases to a CSV file. Displays the Export Aliases window to prompt for a file name.
 Import Aliases	Clears all aliases and imports new ones from a CSV file. Displays the Import Aliases window to prompt for an existing file name.
 Shutdown Server	Closes the current configuration and shuts down the server after signaling the shutdown event to all connected clients. If OPC clients are still connected to the server, the user is prompted for confirmation before continuing. Note: This command is available (i.e., enabled) only when you are running the server as an application; it 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 .
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 5 - File Menu Commands

Edit Menu

Table 6 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 6 - Edit Menu Commands (Server Configuration)

Table 7 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 7 - Edit Menu Commands (Alias Configuration)

View Menu

Table 8 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 8 - View Menu Commands

Tools Menu

Table 9 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 9 - Tools Menu Commands

Help Menu

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

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

Table 10 - 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 5).

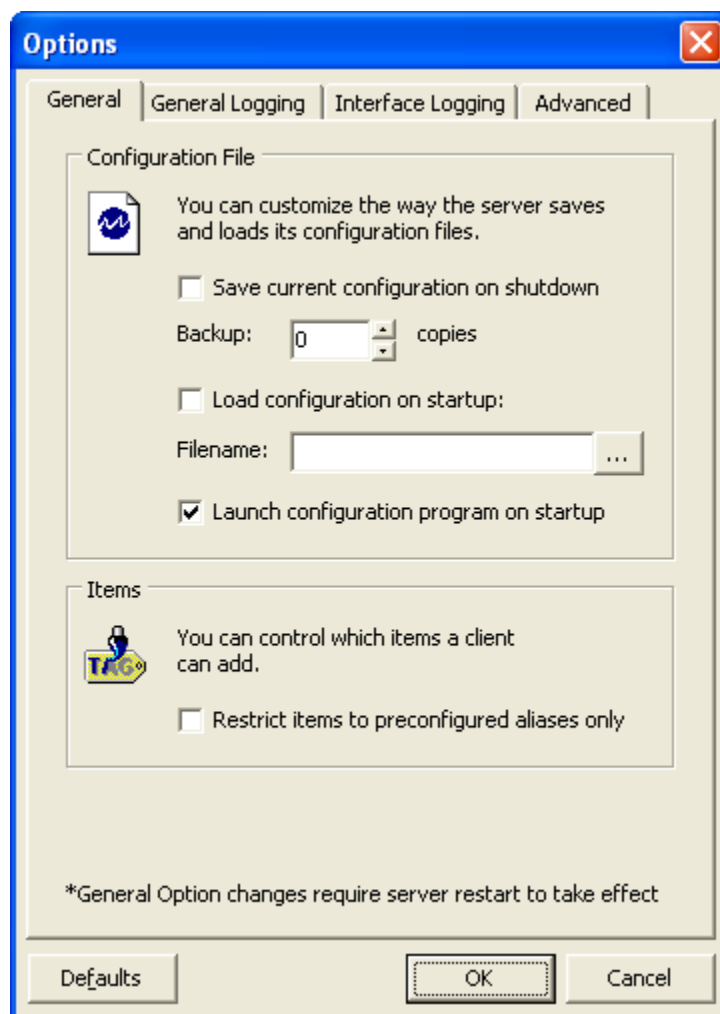


Figure 5 - General Options Tab

Table 11 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 setup	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 11 - General Options Tab Components

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 6).

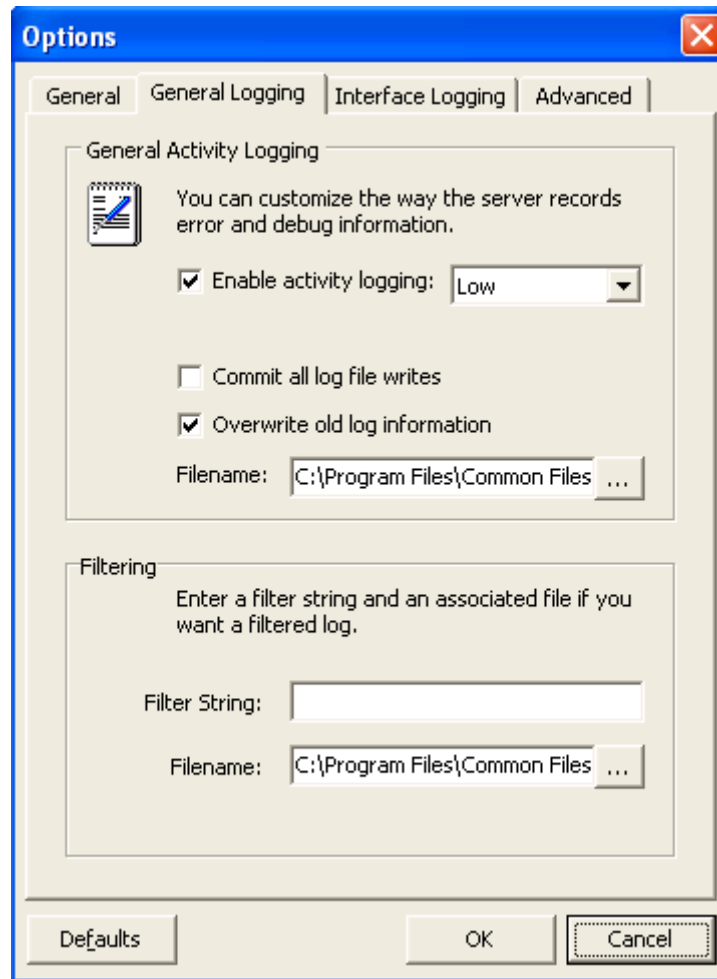


Figure 6 - General Logging Options Tab

Table 12 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: If performance is a concern, to improve it you may want to disable this function (i.e., clear the checkbox).
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.IEC61850.1.LOG .
Filter String	Match string for filtered log is displayed.
Filtering Filename	Displays the full path for the filtered log file. Click on the ellipsis button (...) to display the Open window used to select an existing file name.

Table 12 - General Logging Options Tab Components

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 7).

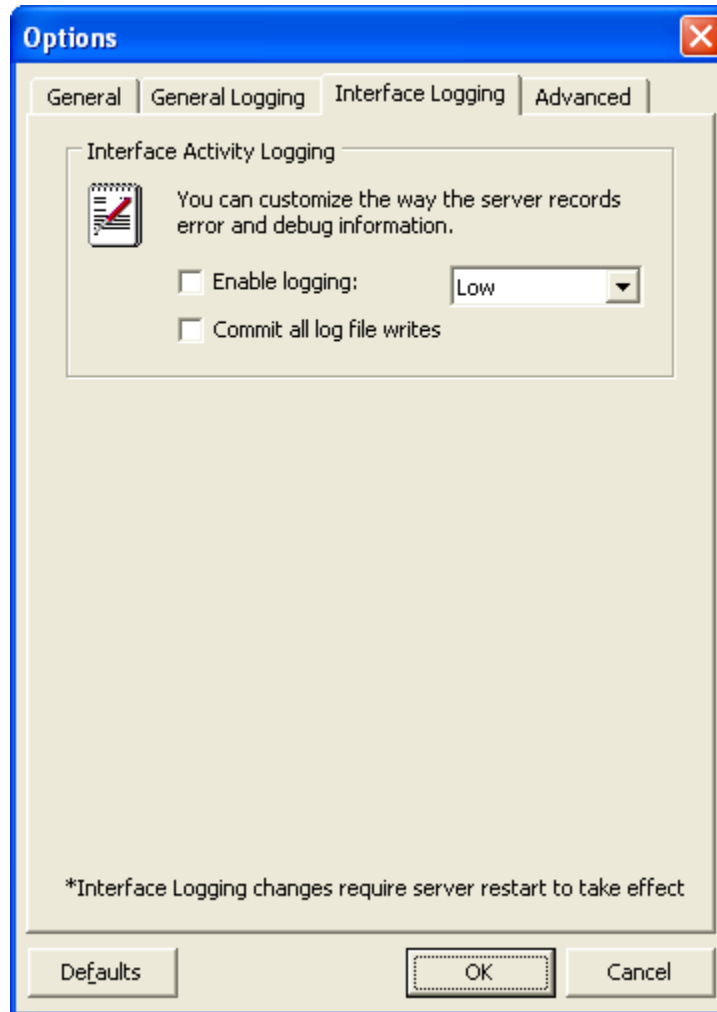


Figure 7 - Interface Logging Options Tab

Table 13 describes the fields available on the **Interface Logging** tab.

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

Table 13 - Interface Logging Options Tab Components

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

Advanced Options

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

To view the Advanced options:

1. On the **Configuration** window, from the **View** menu, select the **Options** menu item.
2. The **Options** window appears.
3. From the **Options** window, select the **Advanced** tab (Figure 8).

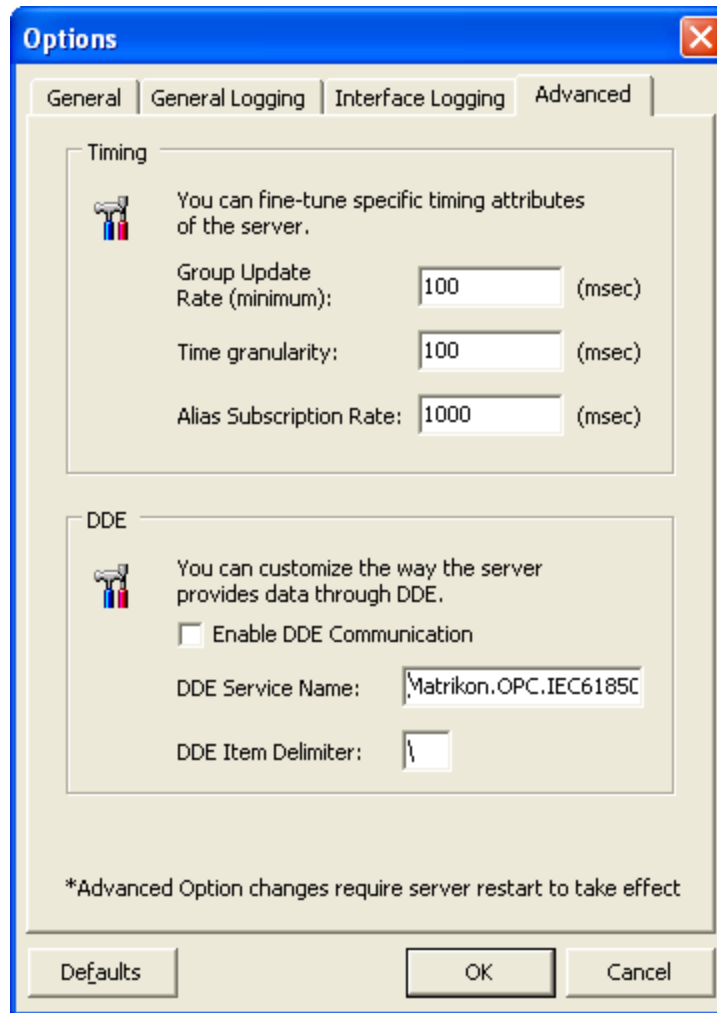


Figure 8 - Advanced Options Tab

Table 14 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

Field	Description
	rate.
Alias Subscription Rate	This is the rate (in milliseconds) at which the Alias features subscribe to underlying data items. This rate is used by the Alias Events features and by the Expression and Calculation engines when other tags are referenced in the expressions. Default = 1000 .
Enable DDE Communication	Selecting this checkbox this will allow the server to accept Dynamic 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 14 - Advanced Options Tab Components

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

Server Configuration

The server requires minimal configuration for it to run properly. You can customize the server's behavior 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 IED device link objects.

Insert New Object Window

The **Insert New Object** window (Figure 9) displays a different set of options depending on the type of object selected and the types of objects already configured under it.

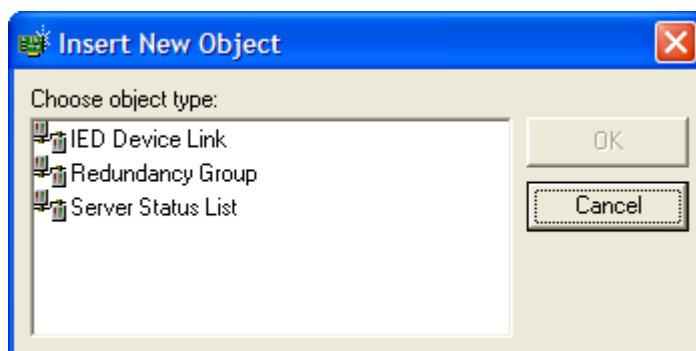


Figure 9 - Insert New Object Window

Table 15 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)	IED Device Link Redundancy Group

Selected Object	Insert New Object Window Options
	Server Status List
IED Device Link	<None>
Redundancy Group	<None>
Server Status List	<None>

Table 15 - Insert New Object Window Options

To insert a new object:

1. On the **Configuration** window, either select the **Define New** menu option from the **Edit** menu, or click on the  icon.
2. The **Insert New Object** window (Figure 9) appears.
3. From the displayed list, select the type of object to be created.
Note: Different objects may be available depending on which object is currently selected in the tree view.
4. Click on the **OK** button.
5. The **Create New** window appears.

To create a newly inserted object:

1. From the **Create New** window, enter a name for the object. This name is part of the item ID that globally identifies data items from under the object. You may also choose to enter a description of the object.
2. Edit the configuration components as desired.
3. Click on the **OK** button. The object is created.
Note: For the object to be used for communication, it must be enabled (i.e., **Enabled** checkbox is selected). This can be done at any time.

Create New Window

The **Create New** window (Figure 10) 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 an IED Device Link

Figure 10 displays the **Create New IED Device Link** window. The **IED Device Link** window divides the configuration options into six categories (i.e., tabs):

- **Communications**
- **Browse**
- **Control**
- **Optimization**
- **RCB**
- **Advanced**

Communications Tab

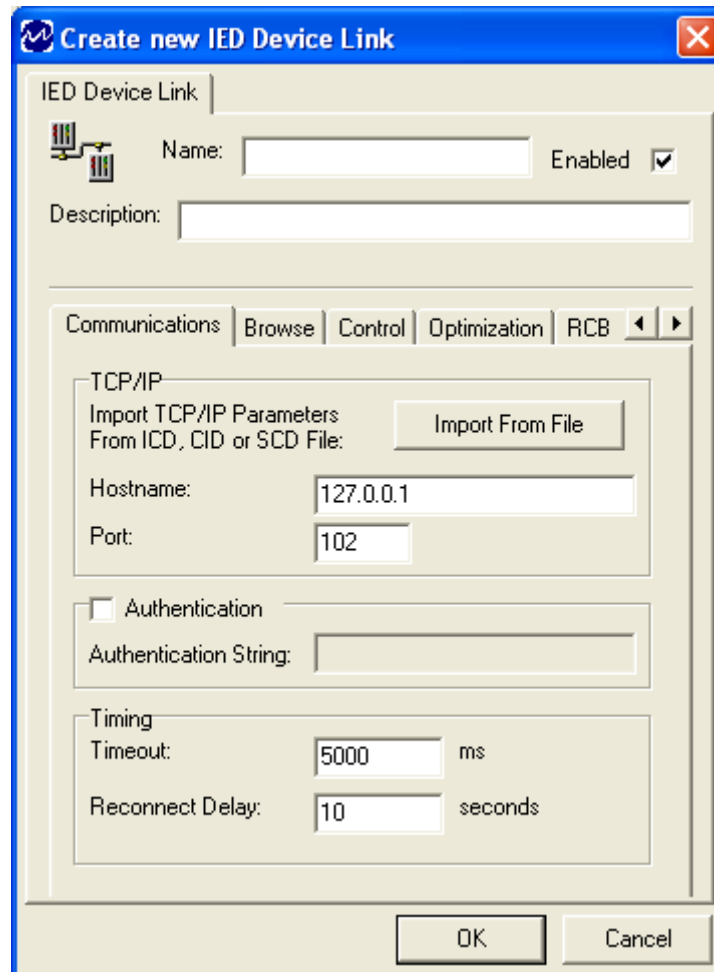


Figure 10 - Create New IED Device Link Window (Communications Tab)

Table 16 describes the components of **Communications** tab on the **Create New IED Device Link** window.

Component	Description
Name	Name of the object, which becomes an element of the item ID for data items under the object. 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, 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.

Component	Description
Import From File	Select this button to access the Import Configuration window which allows you to select an ICD , CID , or SCD file from which to import communications parameters.
Hostname	The hostname or IP Address of the IED.
Port Number	The TCP/IP Port number for the IED. Default = 102 .
Authentication	Select this checkbox to enable authentication while connecting to the IED. Default = Not Selected
Authentication String	Enter the authentication string to be sent to the IED while negotiating a connection. The format and contents of this string are determined by the IED. To enter text in this field, the Authentication option must be selected. Default = Blank
Timeout	Allows you to enter the amount of time, in milliseconds, that the IED Device Link should wait for a response from the device. Default = 5000 .
Reconnect Delay	Allows you to enter the amount of time, in seconds, for the IED Device Link to wait after dropping a connection from the device before attempting to establish a new connection. Default = 10 .
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 this window without saving any changes made. Note: This information stays consistent across all tabs.

Table 16 - Create New IED Device Link Window (Communications Tab) Components

Import Configuration Window

Figure 11 shows the **Import Configuration** window. This window is accessed via the **Import From File** button on the **Communications** tab.

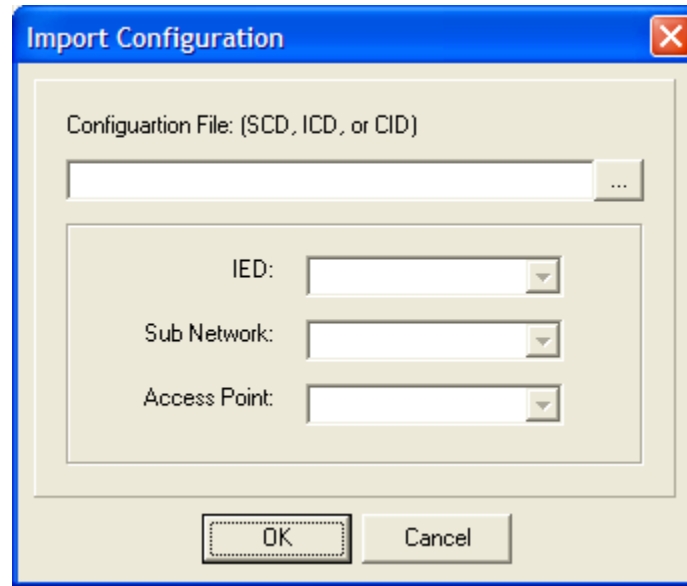


Figure 11 - Import Configuration Window

Component	Description
Configuration File	Allows you to either enter a full path to an SCD , CID , or ICD file, or use the browse (i.e., ellipsis) button to browse the file system to select a file.
IED	Allows you to select, from the drop-down list, which IED from the selected configuration file to gather configuration information. If the selected configuration file contains only a single IED, then that one is selected by default.
Sub Network	Allows you to select, from the drop-down list, which sub-network from the configuration file should be used to gather configuration information from.
Access Point	Allows you to select, from the drop-down list, which access point from the selected configuration file should be used to communicate with the device.
OK	Select this button to accept the selections and update the IEC 61850 Device Link Settings with configuration information from the configuration file. The following settings can be configured if they are available from the selected configuration file: • Hostname (or IP Address) • Port • ACSE Called Parameters
Cancel	Select this button to close the Import Configuration window without changing the settings.

Table 17 - Import Configuration Window Components

Browse Tab

Figure 12 shows the **Browse** tab on the **Create New IED Device Link** window.

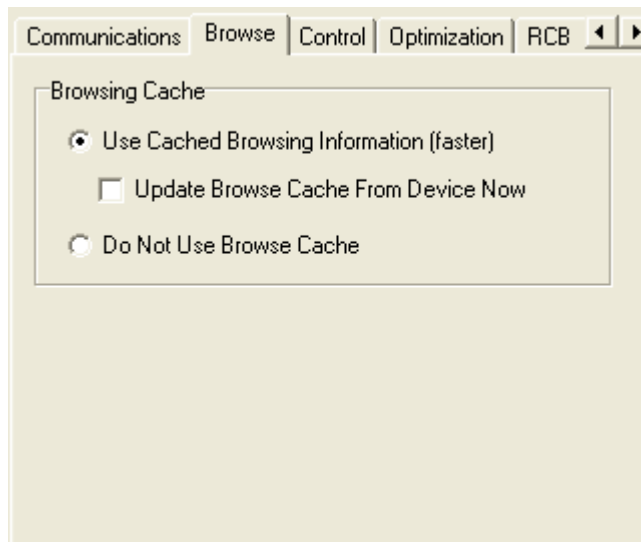


Figure 12 - Create New IED Device Link Window (Browse Tab)

Table 18 describes the **Browse** tab components of the **Create New IED Device Link** window.

Component	Description
Use Cached Browsing Information (faster)	Select this option to cache and store the browsing structure of the OPC server from the device. By default, this option is selected.
Update Browse Cache From Device Now	When Cached Browse Information is being stored, selecting this option causes the OPC server to refresh its cache from the device when the Apply button is clicked. This option automatically resets to un-checked (i.e., cleared) when the refresh is completed.
Do Not Use Browse Cache	Select this option to disable the use of a browsing cache. When an OPC client browses for points on a device connected to this server, the OPC server loads the browsing information straight from the device.

Table 18 - Create New IED Device Link Window (Browse Tab) Components



Note: If an OPC client is using Flat Browsing to get the list of points from the server, it is recommended that the **Use Cached Browsing Information** option is selected to avoid unnecessary communication load on the device.

Control Tab

Figure 12 shows the **Browse** tab on the **Create New IED Device Link** window.

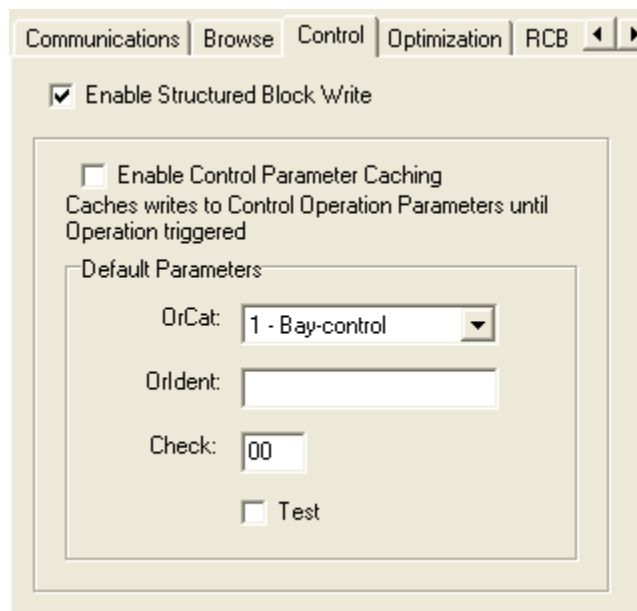


Figure 13 - Create New IED Device Link Window (Control Tab)

Table 19 describes the **Control** tab components of the **Create New IED Device Link** window.

Component	Description
Enable Structured Block Write	Select this checkbox to allow the server to handle control operation while an OPC write is made to the <i>Oper.ctIVal</i> or SBOW.ctIVal if the Enable Control Parameter Caching checkbox is (i.e., not selected). By default, this option is selected.
Enable Control Parameter Caching	Select this checkbox to cache writes for control parameters OPC items to be used for control operations at a later time. By default, this option is cleared (i.e., not selected). Note: Values for the control parameters must be written to the corresponding OPC items. Following that, any value written to the oper , SBOW , or Cancel OPC tags will trigger the control operation command to be sent to the device.
OrCat	Allows you to select, from the drop-down list, the default value of the originator category which is used for control operations. Default = 1 – Bay-control .
OrIdent	Allows you to define the default value of the originator identification which is used for control operations. It is an octString64. The format of this field looks like, 68,96,255 ...etc., where `,` is the delimiter between the elements. Default = Blank .
Check	Allows you to define the default value of the check conditions used for control operations. Default = 00 .
Test	The default value of this checkbox is used for control operations. By default, this option is cleared.

Table 19 - Create New IED Device Link Window (Control Tab) Components

Optimization Tab

Figure 14 show the **Optimization** tab on the **Create New Device Link** window.

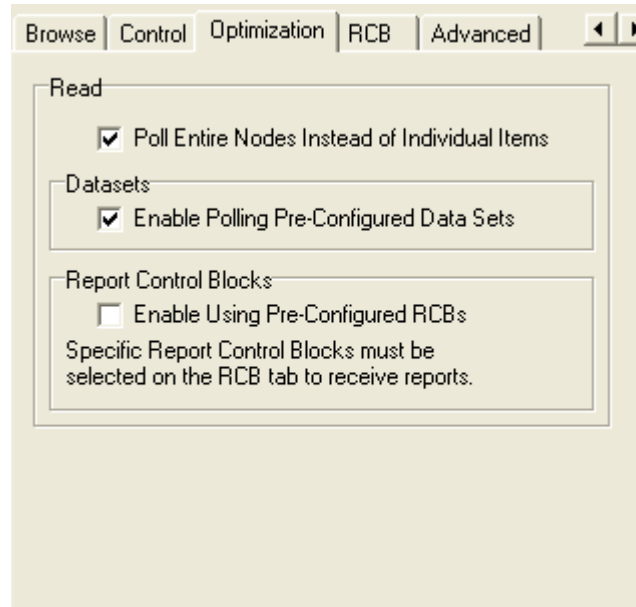


Figure 14 - New IED Device Link Window (Optimization Tab with Unbuffered Reports Enabled)

Component	Description
Poll Entire Nodes Instead of Individual Items	Select this checkbox to poll entire nodes instead of individual values. This decreases the amount of data sent between the OPC server and the device when several values in a node are being read at the same update rate.
Enable Polling Pre-Configured Data Set	Select this checkbox to enable polling data sets which are available on the device when items in those data sets are subscribed to by an OPC client. Note: This checkbox must be enabled to use Report Control Blocks .
Enable Using Pre-Configured RCBs	Select this checkbox to allow the OPC server to receive value updates from the device by unsolicited reports instead of polling. The Report Control Blocks on the device must be pre-configured with valid data sets and related settings. When this checkbox is selected, and specific RCBs are selected on the RCB tab, those reports are automatically enabled by the OPC server when points in the data set associated with the report control block, are subscribed to.

Table 20 - Create New IED Device Link Window (Optimization Tab) Components

RCB Tab

The **RCB** tab controls the use of Unbuffered Report Control Blocks is as shown in Figure 15. This tab is disabled and cannot be configured unless the **Enable Monitoring Configured Reports** and **Enable Using Unbuffered Reports** checkboxes are selected on the **Optimization** tab.

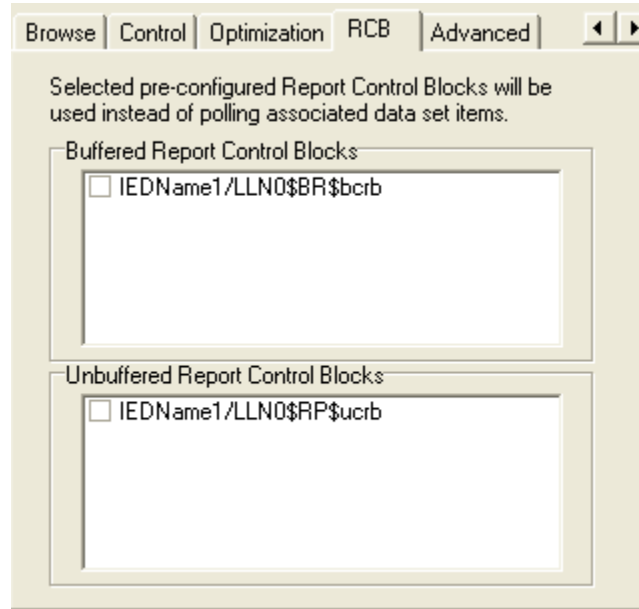


Figure 15 - Create New IED Device Link (RCB Tab) Components

Component	Description
Buffered Report Control Blocks	Each Buffered Report Control Block found on the server are listed here. BRCB's that have been selected are enabled by the OPC server and reports from those blocks used to update data values.
Unbuffered Report Control Blocks	Each Unbuffered Report Control Block found on the server will be listed here. URCB's that have been selected are enabled by the OPC server and reports from those blocks used to update data values.

Table 21 - Create New IED Device Link (RCB Tab) Components



Note: The list of Buffered and Unbuffered Report Control blocks is emptied after the new IED Device Link is created, and communication is established with the device. After the device link is created, return to the **RCB** tab to select which **RCBs** are to be used.

Advanced Tab

Figure 16 shows the **Advanced** tab on the **Create New IED Device Link** window.

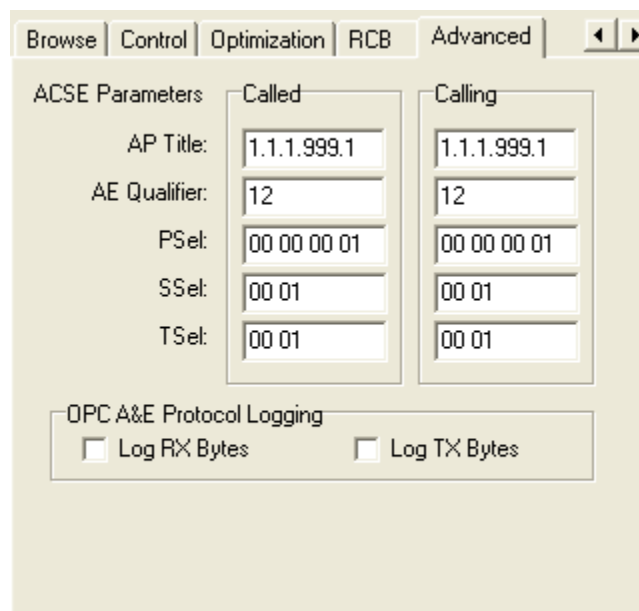


Figure 16 - Create New IED Device Link Window (Advanced Tab)

Table 22 describes the **Advanced** tab components of the **Create New IED Device Link** window.

Component	Description
ACSE Called Parameters: AP Title	This field provides the identity of the application process for which the connection request is intended. This field is used when the device requires more detailed connection and routing information. By default, this field is blank. The value must be in the format of an object identifier such as x.y[.z1[.z2[...]]] where x, y, and z1-zn are numbers. For example, 1.2 or 1.2.7.5. Default = 1.1.1.999.1.
ACSE Called Parameters: AE Qualifier	This field provides the identity of the specific application entity for which the connection request is intended. This field is used when the device requires more detailed connection and routing information. The value must be an integer. Default = 12.
ACSE Called Parameters: PSet	This field is the presentation selector for the connected device, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For example, a0 66, 12, a7 df ff, etc. Default = 00 00 00 01.
ACSE Called Parameters: SSet	This field is the session selector for the connected device, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For example, a0 66, 12, a7 df ff, etc. Default = 00 01.
ACSE Called Parameters: TSet	This field is the transport selector for the connected device, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For

Component	Description
	example, a0 66, 12, a7 df ff , etc. Default = 00 01 .
ACSE Calling Parameters: AP Title	This field provides the identity of the application process that the connection request is originating from. This field is used when the device requires more detailed connection and routing information. By default, this field is blank. The value must be in the format of an object identifier such as x.y[.z1[.z2[...]]] where x , y , and z1-zn are numbers. For example, 1.2 or 1.2.7.5 . Default = 1.1.1.999.1 .
ACSE Calling Parameters: AE Qualifier	This field provides the identity of the specific application entity that the connection request is originating from. This field is used when the device requires more detailed connection and routing information. The value must be an integer. Default = 12 .
ACSE Calling Parameters: PSel	This field is the presentation selector for the device that the connection request is originating from, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For example, a0 66, 12, a7 df ff , etc. Default = 00 00 00 01 .
ACSE Calling Parameters: SSel	This field is the session selector for the device that the connection request is originating from, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For example, a0 66, 12, a7 df ff , etc. Default = 00 01 .
ACSE Calling Parameters: TSel	This field is the transport selector for the device that the connection request is originating from, an optional hexadecimal value of between 1 and 16 octets. Values in this field must be entered as hexadecimal strings with one space between each octet. For example, a0 66, 12, a7 df ff , etc. Default = 00 01 .
OPC A&E Protocol Logging: Log RX Bytes	Select this checkbox to enable A&E Protocol logging of bytes received by the OPC server from the device. By default, this checkbox is cleared.
OPC A&E Protocol Logging: Log TX Bytes	Select this checkbox to enable A&E Protocol logging of bytes transmitted by the OPC server to the device. By default, this checkbox is cleared.

Table 22 - Create New IED Device Link Window (Advanced Tab) Components



Note: All of the parameters on the **Advanced** tab are optional and device dependent. Default values are provided, based on the specifications. Check the configuration information for the IED device to determine values for these options.

To create an IED Device Link:

1. 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.
2. The **Insert New Object** window (Figure 9) appears.
 3. From the displayed list, select **IED Device Link**.
 4. Click on the **OK** button.
 5. The **Create New** window appears (Figure 10).

Note: The item selected in the **Insert New Object** window determines which **Create New** window is displayed. For example, when **IED Device Link** is selected, then the **Create New IED Device Link** 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 is not 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 appears as a child of the **Server Configuration** item as shown in Figure 17.

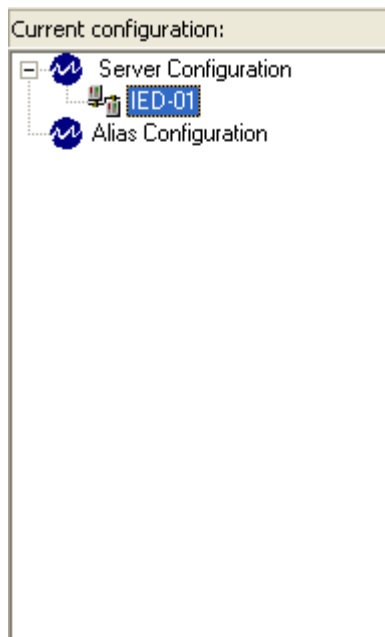


Figure 17 - New IEC 61850 IED Device Link Object

Creating and Configuring a Redundancy Group Object

The Redundancy Group contains a list of device links that can exist anywhere in the OPC server hierarchy. The Redundancy Group assigns one of the device links in the list as the active device link. Depending on the selected redundancy mode (see Table 23), the non-active device links are placed in communicating, standby or disabled states. As operations (e.g., adding items,

reading/writing) are performed on the Redundancy Group, these actions are forwarded through to the active device link. If the active device link enters a failure condition (e.g., becomes disconnected), the Redundancy Group assigns a new active device link by iterating through its list until it can find a device link that is connected.

Multiple Redundancy Groups can exist, and there can be one or more device links contained within a Redundancy Group. A particular device link may only be a member of one redundancy group at a time. The group tries to make one of the device links within itself, the active device link (i.e., the device link that the Redundancy Group is reading/writing data from/to).

Each device link within a Redundancy Group will have an assigned priority. When deciding which device link to make active, the Redundancy Group goes through the list of its device links in order of priority, from highest to lowest. When not in **Cold** redundancy mode, if a device link that has a higher priority than the active device links becomes connected, the Redundancy Group makes that particular device link active.

Items within the Redundancy Group are added with the same item ID as those in its redundant device links with the name of the redundant device link being replaced with the name of the Redundancy Group. Therefore, redundant device links should have identical hierarchy layout and naming conventions below their level. The success of a redundancy item addition depends on whether the Redundancy Group can add the mapped item to the active device link. OPC reads and writes performed on the redundancy item are forwarded to the mapped item in the active device link.

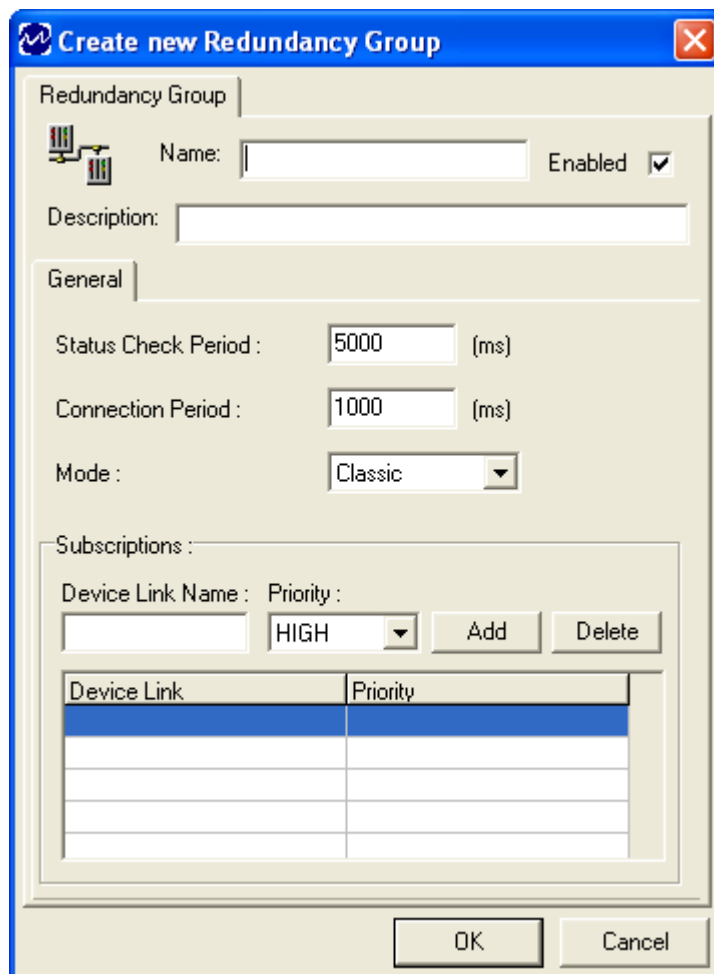
The **Create New Redundancy Group** window (Figure 18) displays the settings available for configuring a Redundancy Group object.

Mode	Description
Classic	All device links are connected. Items are added only to the active device link, but are not removed when a fail over occurs. As failovers occur and cause multiple device links to become active, the collection state becomes the same as Hot .
Hot	All device links are connected. When items are added they are added to all device links in the redundancy group. This means that all device links are actively collecting all the time.
Warm	All device links are connected. When items are added they are added to the active device link. When a failover occurs the items will be removed from the formerly active device link.
Cold	Only the active device link is connected. When items are added they are added to the active device link. When a failover occurs the items will be removed from the formerly active device link. Note: When a device link is a member of a Cold mode redundancy group and not the active device link, then all communication through that device link is disabled.

Table 23 - Redundancy Modes

Redundancy Group Failover Conditions

The MatrikonOPC Server for IEC 61850/61400-25 triggers a redundancy group failover when it detects an association abortion (@**Connected** = **FALSE**) between the server and the IED device.



Create new Redundancy Group

Redundancy Group

Name: Enabled ☒

Description:

General

Status Check Period : (ms)

Connection Period : (ms)

Mode :

Subscriptions :

Device Link Name : Priority :

Device Link	Priority

Figure 18 - Create New Redundancy Group Window

Table 24 describes the components of the **Create New Redundancy Group** 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.
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.

Component	Description
Connection Period	Allows you to enter a value to define how often (in milliseconds) to check connections that have failed (i.e., communication is down) to determine if connections have been restored. Default = 1000 ms.
Mode	Allows you to select, from the drop-down list, the style (Classic , Hot , Warm , Cold) of redundancy management that should be used by this group.
Subscriptions	This section of the General tab displays those device links defined as part of this particular redundant set, and the priorities of the device links. The Subscriptions section contains the following fields and buttons which are described below: Device Link Name , Priority , Add , Delete .
Device Link Name	Allows you to enter the name of the device link that is going to be added as a member of the redundant group of device links. The full path of the device link must be entered.
Priority	Allows you to select a priority (High , Medium , or Low) for the current device link from the drop-down list. Device links of higher priority are preferred to lower priority device links.
Add	After entering a Device Link Name and selecting a Priority , use the Add button to add the device link to the list of redundant device links that appears at the bottom of the General tab. 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.
Delete	From the list of redundant device links that appears at the bottom of the General tab, select the device link you want to remove and click on the Delete button to delete it from the list.
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 24 - Create New Redundancy Group Window Components

To create a Redundancy Group 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 9) appears.
- From the displayed list, select **Redundancy Group**.
- Click on the **OK** button.
- The **Create New** window appears (Figure 10).

Note: The item selected in the **Insert New Object** window determines which **Create New** window is displayed. For example, when **Redundancy Group** is selected, then the **Create New Redundancy Group** 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 is not 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 appears as a child of the **Server Configuration** item as shown in Figure 19.

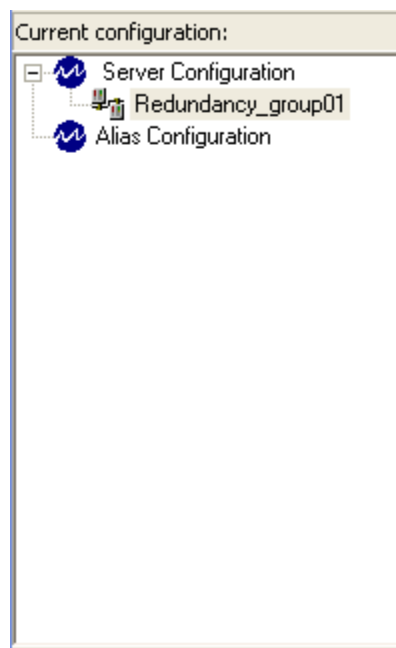


Figure 19 - New Redundancy Group Object

Creating and Configuring a Server Status List Object

Some OPC clients use the OPC call, **GetServerStatus()**, to monitor the state of an OPC server. MatrikonOPC's Server Status List object makes it possible to monitor an OPC server status in a customizable way.

The Server Status List object contains a list of subscribed device links that can exist anywhere in the OPC server hierarchy. The status of the server is checked every configured status check period by examining the status of the subscribed device links. Device links can be added to the Server Status List in one of two ways:

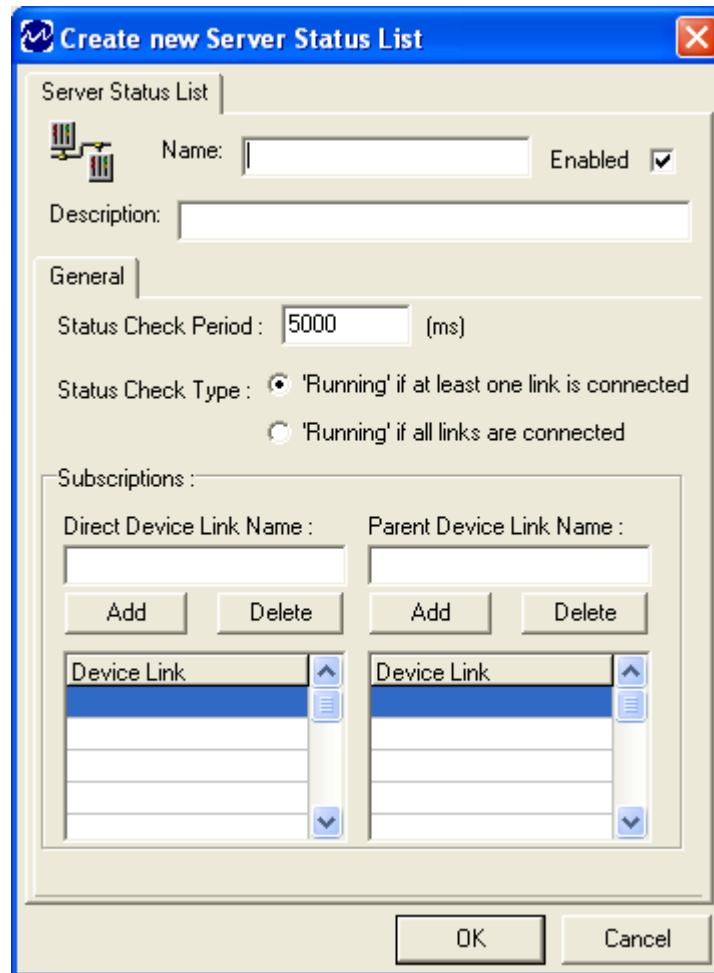
1. **Direct** – the device link is added directly to the subscription list.
2. **Parent** – the device link's sub-ordinates are added to the subscription list.

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 20) displays the settings available for configuring a Server Status List object.



The image shows a Windows-style dialog box titled "Create new Server Status List". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into two tabs: "Server Status List" (selected) and "General".

In the "Server Status List" tab, there is a "Name:" text box, an "Enabled" checkbox (checked), and a "Description:" text box. Below these is the "General" tab, which contains a "Status Check Period:" text box with "5000" and "(ms)" next to it. Below that is a "Status Check Type:" section with two radio buttons: "'Running' if at least one link is connected" (selected) and "'Running' if all links are connected".

Below the status check type is a "Subscriptions:" section. It contains two columns of input fields. The first column is labeled "Direct Device Link Name:" and the second is labeled "Parent Device Link Name:". Each column has an "Add" button and a "Delete" button. Below these are two list boxes, each labeled "Device Link", with up and down arrows on the right side of each list.

At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 20 - 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. 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.

Component	Description
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.
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.

Component	Description
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:

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 9) appears.

3. From the displayed list, select **Server Status List**.

4. Click on the **OK** button.

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

Note: The item selected in the **Insert New Object** window determines which **Create New** window is displayed. For example, when **Server Status List** is selected, then the **Create New Server Status List** 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 is not 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 appears as a child of the **Server Configuration** item as shown in Figure 21.



Figure 21 - New Server Status List Object

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., pane 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 22) will appear when users remove an object that has data items to which one or more OPC clients hold reference.

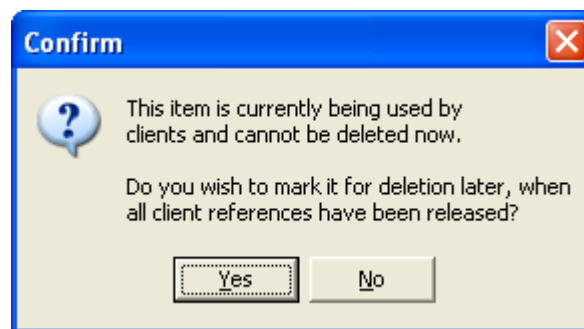


Figure 22 - Client Reference Warning Message

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 22) appears.

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

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

Alias Configuration

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

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

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

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

Inserting Alias Groups

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

To insert an Alias Group:

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

Renaming Alias Groups

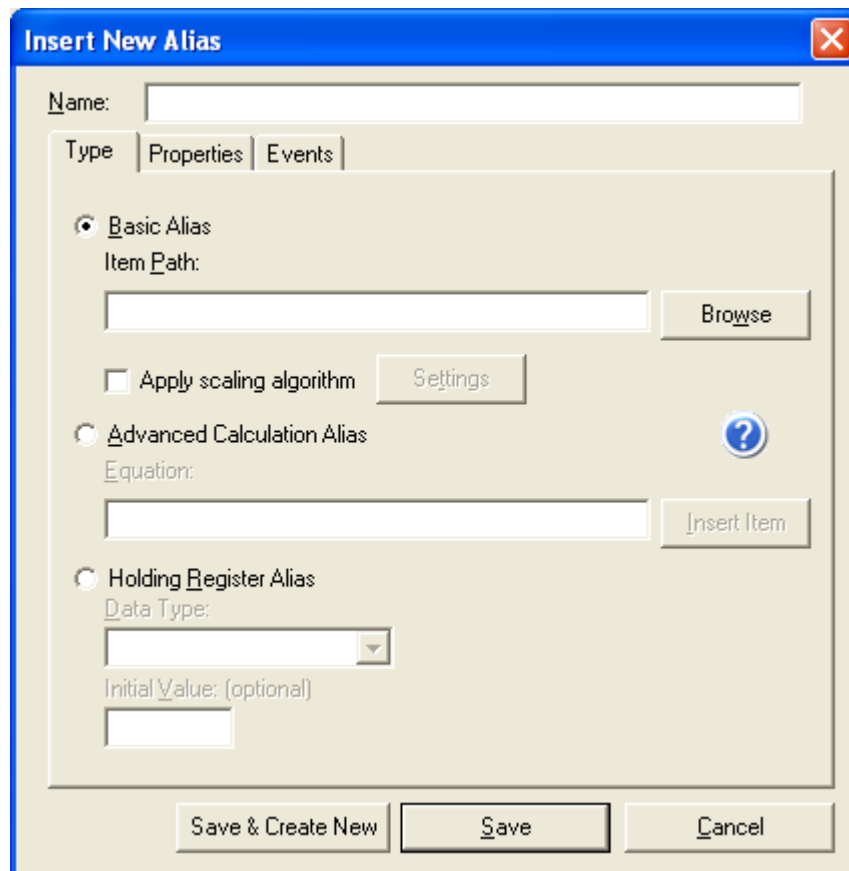
Note: Alias Groups can be renamed after they have been created.

To rename an Alias Group:

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

Inserting New Aliases

Use the **Insert New Alias** window (Figure 23) to insert a new alias into an Alias Group, or insert a new alias on its own directly under the Alias Configuration node.



The dialog box is titled "Insert New Alias" and has a close button (X) in the top right corner. It features three tabs: "Type", "Properties", and "Events". The "Type" tab is currently selected. Inside this tab, there are three radio button options: "Basic Alias" (which is selected), "Advanced Calculation Alias", and "Holding Register Alias".

- Under "Basic Alias", there is an "Item Path" text field followed by a "Browse" button. Below this is an unchecked checkbox labeled "Apply scaling algorithm" with a "Settings" button next to it.
- Under "Advanced Calculation Alias", there is an "Equation" text field followed by an "Insert Item" button. A blue question mark icon is located to the right of this section.
- Under "Holding Register Alias", there is a "Data Type" dropdown menu and an "Initial Value: (optional)" text field.

At the bottom of the dialog, there are three buttons: "Save & Create New", "Save", and "Cancel".

Figure 23 - Insert New Alias Window – Alias Type

Table 26 describes the components of the **Insert New Alias** window.

Component	Description
Name	Allows you to enter a name for the alias (which must be unique within the alias group).
Basic Alias	A basic alias is an alias that renames a data item in the server and optionally allows the configuration of simple scaling. This Alias type is typically used when trying to simplify a servers address space.
Item Path	Fully-qualified item ID for the OPC item to which the alias refers. Click on the Browse button to display the Item Path Browser window used to select an existing OPC item on the server. Note: If Events are enabled, the alias creates a data subscription to the configured item at the Alias Subscription Rate . This rate is configured in the Advanced Options window.
Apply Scaling Algorithm	Basic Aliases can be configured to have scaling calculations applied to the value of the mapped item ID configured under Item Path . To enable the use of a scaling algorithm, check the Apply scaling algorithm checkbox. Click on the Settings button to display the Configure Scaling window used to configured the scaling algorithm used.
Advanced Calculation Alias	An Advanced Calculation Alias allows the user to configuration a data

Component	Description
	point whose value is the result of a mathematical equation that can involve values from multiple data items in the server. See Appendix B – Aliases – Advanced Calculations or click on the Help icon for information on how to write equations and the functions available.
Equation	The equation to apply to calculate the data value of the alias. Use the Insert Item button to display the Item Path Browser window used to select an existing OPC item on the server and insert a reference into the equation.
Holding Register Alias	A Holding Register Alias is a data item that is not associated with any data items in the server. These registers can be read from and written to like any other data item. Typically Holding Register Aliases are used as temporary data locations or for configuration testing during system deployment.
Data Type	The canonical data type of the holding register. All values written to this alias will be converted to this data type. By default, clients will be sent data as this data type.
Initial Value	By default, a holding register will initially contain a value of 0 or the closest value to zero that applies to the data type. If this value requires a different initial value it can be entered here. Note: Not all data types support the configuration of an initial value. This field may be disabled depending on the data type chosen for the holding register.
Save	Save changes to the alias and close the window.
Save & Create New	Save changes to the alias and begin configuring a new one.
Cancel	Discards changes to (abandon creation of) the alias and closes the window.

Table 26 - Insert New Alias Window – Alias Type Options

Component	Description
Data Type	Allows you to select, from the drop-down list, the value of the OPC item to the specified type unless Default is selected. Also serves as the “canonical” data type for the alias. Default = (Default) .
Update Rate	Allows you to enter a value defining the update rate (in milliseconds) to use with the Poll when inactive option. Default = 0 .
Read only	When this checkbox is selected, it prevents OPC clients from writing values to the alias. Note: This option is not available for Calculation aliases, as they are read-only. By default, this checkbox is cleared.
Poll when inactive	If selected, continues updating the value for the alias at the specified

Component	Description
	update rate even if there are no OPC clients currently accessing the alias.

Table 27 - Insert New Alias Window – Alias Properties Options

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 24), 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 24 - Contents Table

3. From the **Edit** menu, choose **Insert New Alias**.
4. The **Insert New Alias** window (Figure 23) appears.
5. Enter a name for the alias in the **Name** field.
6. Select **Basic Alias**.
7. 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.
8. If scaling is desired, check the **Apply scaling algorithm** checkbox and click on the **Settings** button to **Configure Scaling**.
9. From the **Insert New Alias** window, 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 23) 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. The CSV file format does not support event generation settings. All imported aliases will be configured to **not** generate events.

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.

Configure Alias Scaling

An alias can be configured to apply a scaling algorithm to the data. Below is a description of how to configure the scaling algorithms.

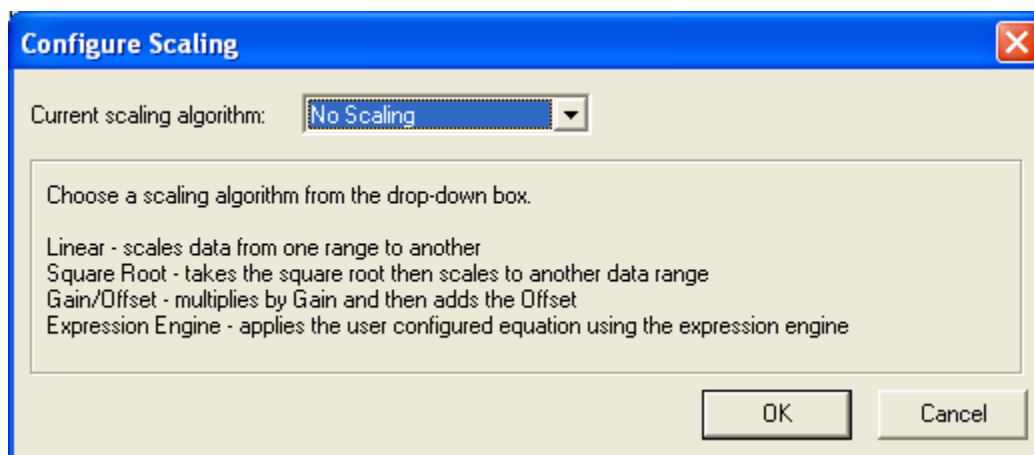


Figure 25 - Configure Scaling Window

Table 28 describes the **Scaling Options** for the **Configure Scaling** window.

Selection	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. For more information, refer to the Expression Wizard section in this manual.
	Output	Simple text equation to apply to outgoing values (writes). Click on the ellipsis button () to display the Expression Wizard screen used to help build a formula. For more information, refer to the Expression Wizard section in this manual.

Table 28 - Configure Scaling Window Options

Notes:

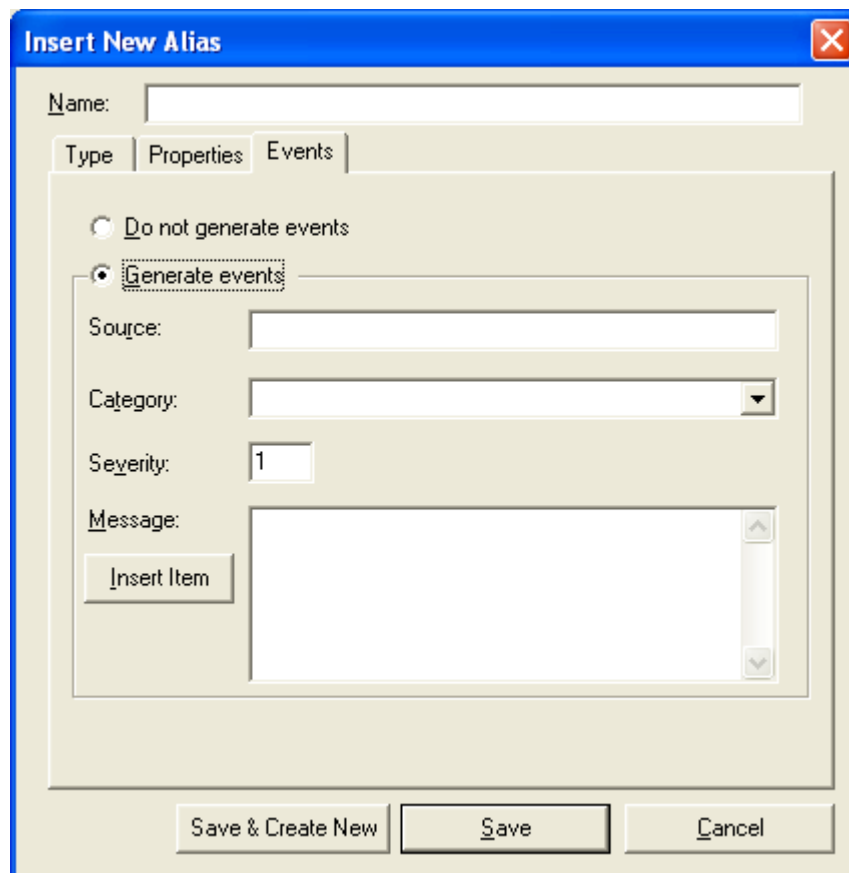


- The data type for scaled values is double-precision real unless the alias data type is specified.
- Using invalid settings, such as **zero-zero** for the high-low range in **Linear** scaling, may be fatal to the server, OPC clients, and communications.
- The OPC item values must be numeric for **Linear**, **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.

Configure Alias Events

Note: Alias Events needs to be licensed separately, and by default, is delivered with only a 30-day demo. To purchase a full Alias Events license, please contact your MatrikonOPC Account Manager.

Use the **Generate Events** (Figure 26) window to configure whether or not aliases generate OPC A&E events when their value changes. Access the **Generate Events** tab through the **Insert New Aliases** window (Figure 26).



The dialog box is titled "Insert New Alias" and has a close button (X) in the top right corner. It features three tabs: "Type", "Properties", and "Events", with the "Events" tab currently selected. Below the tabs, there are two radio buttons: "Do not generate events" (unselected) and "Generate events" (selected). Under the "Generate events" option, there are four input fields: "Source" (a text box), "Category" (a drop-down menu), "Severity" (a text box containing the value "1"), and "Message" (a large text area). An "Insert Item" button is located to the left of the "Message" text area. At the bottom of the dialog, there are three buttons: "Save & Create New", "Save", and "Cancel".

Figure 26 - Generate Events Options

Table 29 describes the **Events** tab fields.

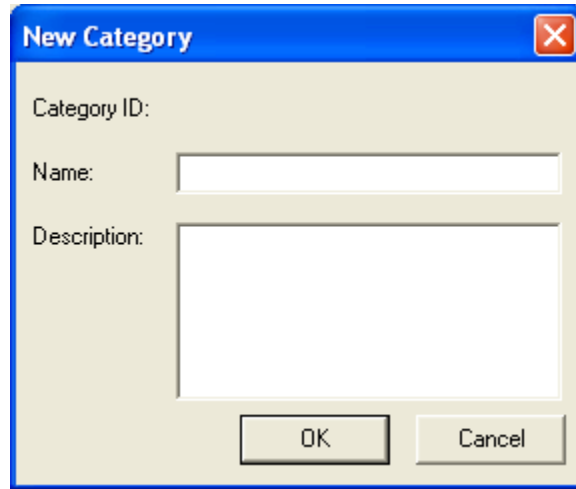
Component	Description
Source	Allows you to enter the name of the source of the event. By default, this field is the Alias Group name, or if there is no Alias Group then the Alias name.
Category	Allows you to select from the drop-down list, the event category under which the event is to be registered. Select either the New Category or Edit Category option to configure the registered categories in the server. For more information, refer to the Configure Categories section for more information.
Severity	Allows you to enter a value defining the severity of the alarm. The allowable range is 1 through 1000 .
Message	Allows you to enter a message that is to appear in the posted event. This message can contain references to data item in the server. These references are replaced with the values of those items at the time the event was generated. Click the Insert Item button to display the Item Path Browser screen used to add item paths to this field. For more information, refer to the Item Path Browser section in this manual. Note: If items are referenced, the alias creates a data subscription to the referenced items at the Alias Subscription Rate. This rate is

Component	Description
	configured in the Advanced Options window.

Table 29 - Generate Events Window Options

Configure Categories

The **New Category** window (Figure 27) is presented when you choose to add a new category to the server from the **Generate Events** window (Figure 26).



The screenshot shows a 'New Category' dialog box with a blue title bar and a close button (X). It contains three input fields: 'Category ID:' (a text box), 'Name:' (a text box), and 'Description:' (a larger text area). At the bottom, there are 'OK' and 'Cancel' buttons.

Figure 27 - New Category Window

Table 30 describes the **New Category** window fields.

Component	Description
Category ID	Displays the ID number that appears in the event that is registered under this category. This numbered field is blank until the category is created. Once the category is created the server assigns a unique ID.
Name	Allows you to enter the name that is to be used to refer to the category.
Description	Allows you to enter a description of what the category represents in the system. The name and the description appear together as the category description in OPC clients that support retrieving category information.

Table 30 - New Category Window Options

The **Edit Categories** window is displayed when you choose to edit categories from the **Generate Events** window (Figure 26).

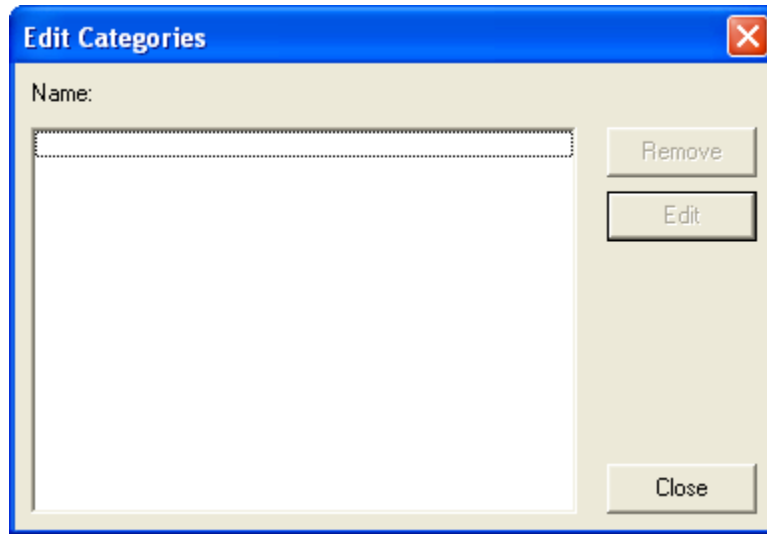


Figure 28 - Edit Categories Window

When presented with the **Edit Categories** window, select the category to edit and click the **Edit** button. This causes the **Edit Category** window to appear which is virtually identical to the **New Category** window.

Note: Some categories cannot be edited. These categories are marked as *Read Only* and can be viewed, but not edited. From the **Edit Categories** window, if you wish to view existing category details, select the required category. Click on the **View** button. The **View Category** window is displayed, which again, is virtually identical to the **New Category** window.

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).

Examples

Example 1:

The following turns any number into a Boolean value. Any non-zero value shows up as a **1**.

IF(INPUT = 0,0,1)

OUTPUT

Example 2:

The following takes the text out of **SAMPLE** and converts it to **ON**. All other values show as **OFF**. If **OUTPUT** is specified in the **Output** field, then the value is transferred to the end OPC item. Using this alias, you can write **SAMPLE** or any other value to the alias to get the display to change from **OFF** to **ON**.

String comparisons are case-sensitive.

IF(INPUT = 'SAMPLE','ON','OFF')

OUTPUT

Table 31 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 31 - 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, listing the aliases it contains.
3. Either create a new alias (for instructions, refer to **Inserting New Aliases**), or Double-click your mouse on an existing alias, or
Click on the **Edit the selected alias item** () button.
4. The **Edit Alias** window appears.
5. Check the **Apply scaling algorithm** checkbox and then click the **Settings** button.
6. Select the **Expression Engine** option (Figure 29).

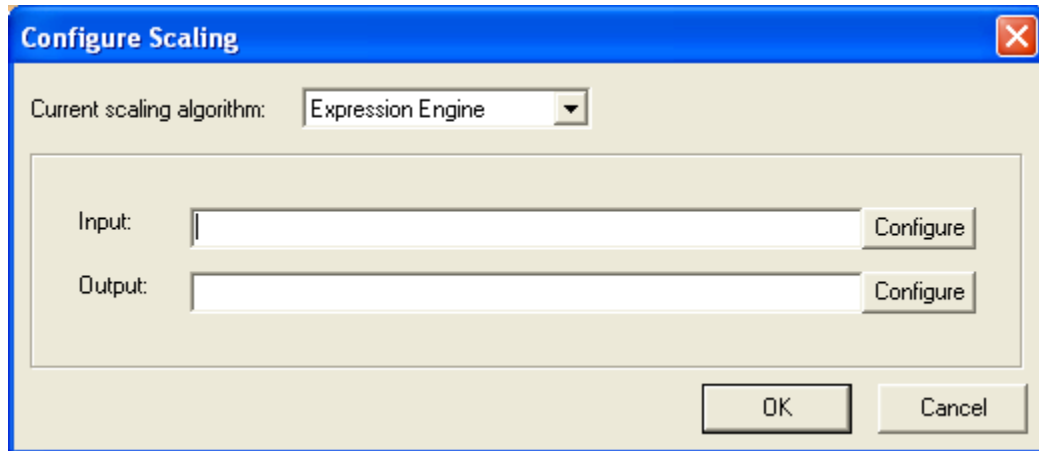


Figure 29 - Expression Engine Configuration

7. Click on the **Configure** button adjacent to the **Input** field (or **Output** field).
8. The **Expression Wizard** (Figure 30) is displayed.

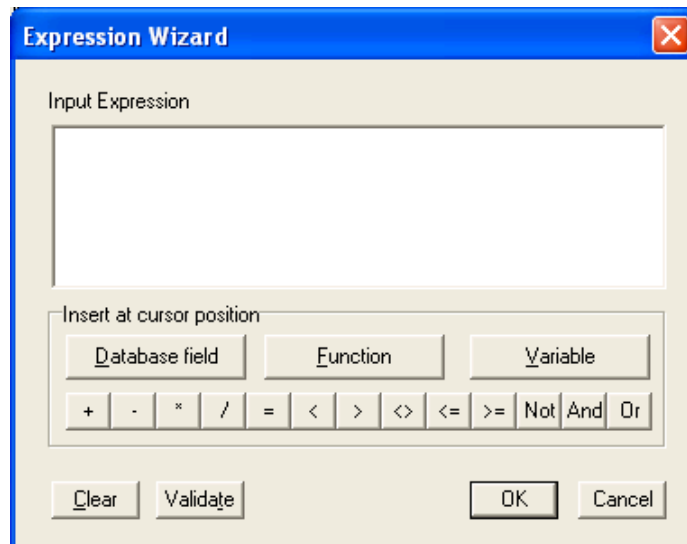


Figure 30 - Expression Wizard

9. Manually enter your new expression in the **Input/Output Expression** field and proceed to step 14.
Or,
Perform steps 9 through 13 using a combination of the **Function**, **Variable**, and **Operators** buttons to create your expression, which will be displayed in the **Input/Output Expression** field as you build it.
10. Click on the **Function** button to go to the **Select function** (Figure 31) window. After selecting the required function, click on the **Continue** button to close the **Select function** window and return to the **Expression Wizard**.

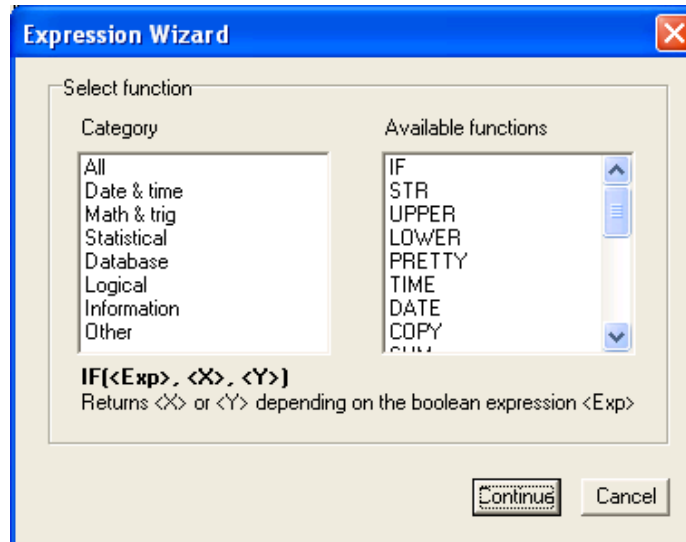


Figure 31 - Select Function Window

11. Click on the **Variable** button to go to the **Select variable** (Figure 32) window. After selecting the required variable, click on the **OK** button to close the **Select variable** window and return to the **Expression Wizard**.

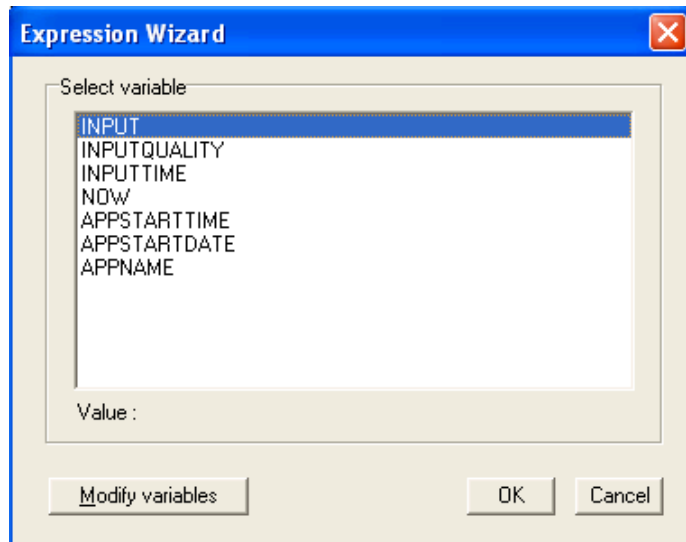


Figure 32 - Select Variable Window

12. If required, from the **Select variable** window, click on the **Modify variables** button to access the **User Defined Functions Editor** (Figure 33) which allows you to add, change, or delete variables.

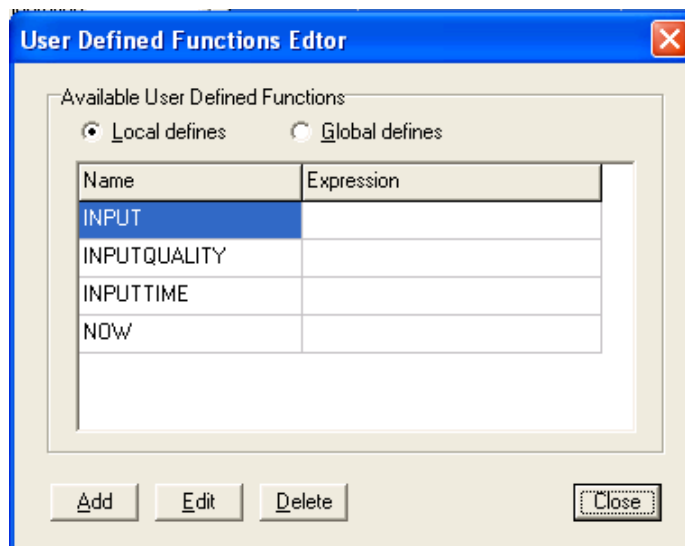


Figure 33 - User Defined Functions Editor

13. The **Operators** buttons (Figure 34) allow you to enter an operation descriptor based on the selected button.

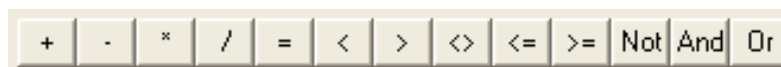


Figure 34 - Operators Buttons

14. Click on the **Validate** button to determine whether or not the expression is valid.
15. If the expression is valid (i.e., a confirmation message is displayed), click on the **OK** button to close the message window and return to the **Expression Wizard** screen.
16. Click on **OK** button on the **Expression Wizard** screen to close the wizard and display the expression in either the **Input** or **Output** field, depending on which expression you defined.
17. From the **Edit Alias** window, click on the **Save** button.
18. The **Edit Alias** window closes and you are returned to the **Configuration** window.

Item Path Browser

The **Basic Alias** and **Advanced Calculation Alias** configuration uses the **Item Path Browser** to add item paths.

Table 32 describes the **Item Path Browser** fields.

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

Component	Description
	item paths.
Refresh	Select this button to refresh the browsing hierarchy in the Branch Hierarchy component.

Table 32 – Item Path Browser Options

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.



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

OPC A&E Protocol Logging

The MatrikonOPC Server for IEC 61850/61400-25 provides OPC A&E simple events to log the data stream as it is transmitted by and received by the OPC server.

To enable this feature, the appropriate check boxes for **Log RX Bytes** and **Log TX Bytes** on the **Advanced** tab of the **IED Device Link** configuration panel.

To use this feature, an OPC A&E client program such as MatrikonOPC Explorer must be used to subscribe to the events.

OPC Data Items

This section describes the OPC data items used in the MatrikonOPC Server for IEC 61850/61400-25.

IED Items

The OPC item ID syntax of this server is as follows with field descriptions defined in Table 33:

IED:LogicalDevice/LogicalNode\$FC\$Data.Attribute[\$]

IED:LogicalDevice.LogicalNode.FC.Data.Attribute[\$]

IED.LogicalDevice.LogicalNode.FC.Data.Attribute[\$]

IED:LogicalDevice/LogicalNode\$DataSet\$Name.RefID

IED.ServerTagName

Field	Description
IED	The name assigned to the IED Device Link during OPC server configuration.
LogicalDevice	The logical device name portion of the fully qualified IEC/61400-25 tag name.
LogicalNode	The logical node name portion of the fully qualified IEC 61850/61400-25 tag name.
FC	The functional Constraint for the fully qualified IEC 61850/61400-25 tag name. This is a two letter code such as ST or MX , or others as defined by the IEC 61850/61400-25 specifications.
Data	The name of the data item from the fully qualified IEC 61850/61400-25 tag name.
Attribute	The name of the specific attribute of the data item from the fully qualified IEC 61850/61400-25 tag name.
ServerTagName	The name of the control or statistical tag defined by the OPC server.
DataSet	The functional constraint for the fully-qualified IEC 61850/61400-25 Data Set tag name. The alternative option is NVL .
Name	The name of a data set object.
RefID	The fully-qualified IEC 61850/61400-25 reference ID of a data set member.
[\$]	This is an optional field. Appending a single \$ symbol to the end of the item's ID means that this is a VT_BSTR type OPC item and its value should be in string format.

Table 33 - Item ID Field Descriptions

IEC 61850 Data Type Mapping

The OPC server maps the data type defined by IEC 61850 specifications to a corresponding OPC data type. Table 34 shows the mapping between the IEC 61850 data types and the OPC types.

IEC 61850 Data Type	OPC Data Type
INT8	VT_I1
INT16	VT_I2

IEC 61850 Data Type	OPC Data Type
INT24	VT_I4
INT32	VT_I4
INT128	VT_DECIMAL
INT8U	VT_UI1
INT16U	VT_UI2
INT32U	VT_UI4
FLOAT32	VT_R4
FLOAT64	VT_R8
ENUMERATED	VT_UI1, UI2, or UI4
CODED ENUM	VT_UI1, UI2, or UI4
OCTET STRING	Vt_ARRAY VT_UI1
VISIBLE STRING	VT_BSTR
UNICODE STRING	VT_BSTR
BOOL	VT_BOOL
ENTRYID	VT_ARRAY VT_UI1
TIMESTAMP	VT_DATE or VT_BSTR
ENTRYTIME	VT_UI8 or VT_BSTR
TRIGGERCONDITIONS	VT_BSTR
QUALITY	VT_BSTR
ARRAY	VT_ARRAY VT_VARIANT
STRUCTURE	VT_ARRAY VT_VARIANT or VT_BSTR

Table 34 - Data Type Mapping

IED Level Statistical and Control Items

The MatrikonOPC Server for IEC 61850/61400-25 supplies statistical and control items listed in Table 35.

Item ID	Description	Default
lastApplErr	The last application error code received from the IED device.	0
lastApplErrDesc	A short description of last application error.	NULL
ctlNum	The value of control sequence number is used for control operations.	0

Table 35 - IED Level Statistical and Control Items

IEC 61850 Control Operations (Select/Operate)

There are four control models defined in IEC 61850. The MatrikonOPC Server for IEC 61850/61400-25 supports these control operations by mapping all control objects and arguments to a corresponding OPC item. The control operation is triggered by a sequence of OPC writes to the

proper OPC items. The server provides three modes to accomplish this. The following section outlines the modes in detail.

1. **OPC Server does a Structured Block Write** – to have the OPC server build the structure, the **Enabled Structured Block Write** option in the OPC server is enabled by default. The following figures illustrate how the server handles direct operate model in block write mode.
 - a) Structured Block Write without caching enabled (caching is disabled by default):

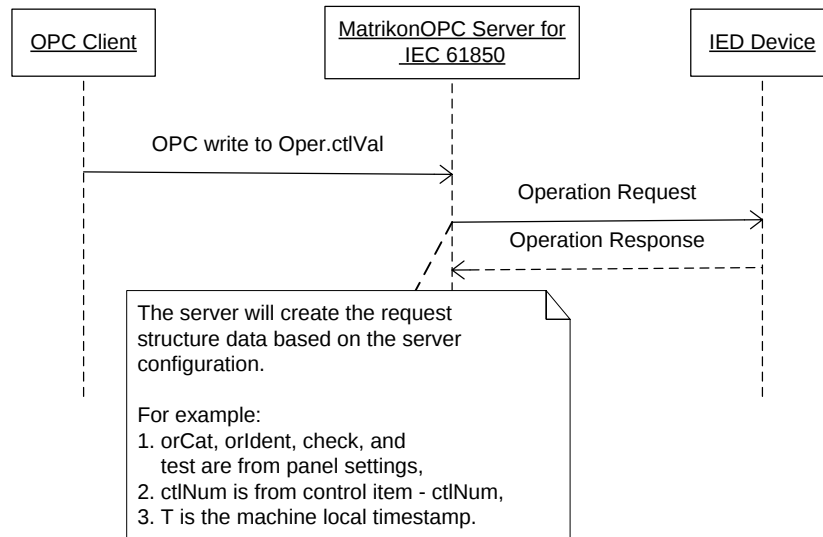


Figure 35 - Structured Block Write Without Caching Enabled

With the **enable control parameter caching** option disabled, the OPC server ignores any OPC write to those control parameter tags, except the **ctlVal** tag. When an OPC write is called on the **ctlVal** tag, the server creates the required data structure for control operations based on default values configured in the configuration panel and sends the request to the device.

b) Structure Block Write with caching enabled:

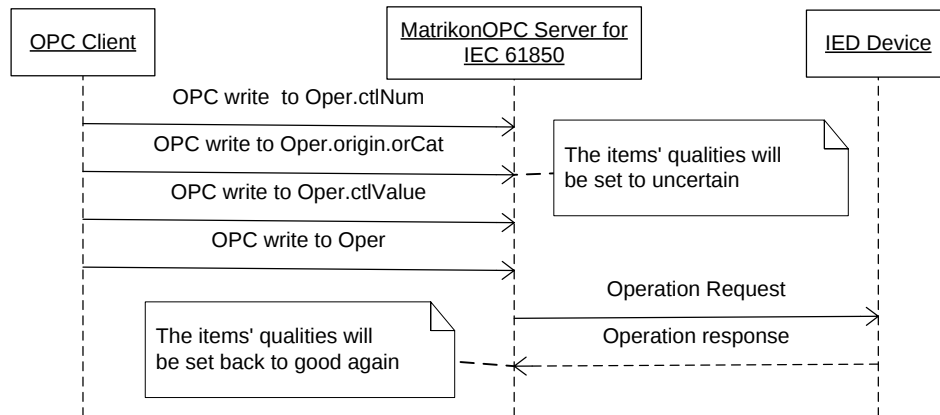
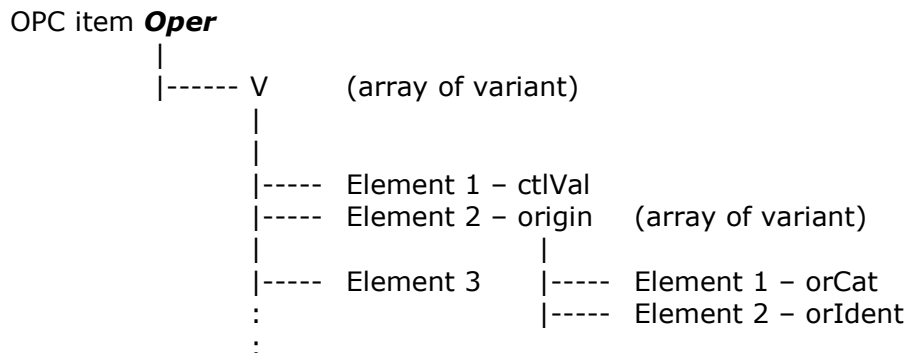


Figure 36 - Structured Block Write with caching enabled

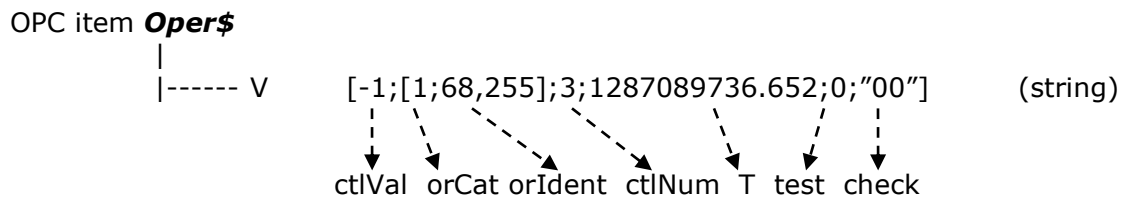
With the **enable control parameter caching** option enabled, the server caches all the OPC writes to the items of those control arguments without sending any requests to the device. The request is sent when an OPC write is made on a proper control tag, such as **Oper**. This feature allows OPC clients that do not support structure writes to set up control arguments one item at a time, and trigger the control operations by writing to the proper control tag, without constructing a complex structure data.

2. **OPC Client performs a Structure Write** – to use this feature the option for **Enabled Structured Block Write** in the OPC server is turned off. The OPC client will handle the structure write in this case, instead of having the OPC server build the structure for it. In the MatrikonOPC Server for IEC 61850/61400-25, all of the control tags are mapped to OPC items which have a data type of ARRAY of Variant. This array represents the proper data structure required by the IEC 61850 control operations. An OPC write with correct arguments to one of these items triggers the corresponding control operations. Shown below is the mapping between control arguments and the OPC item's value for tag **Oper**.



3. **OPC Client performs a String Formatted Structure Write** – this mode does the same as mode 2 (i.e., **Structure Write**). The option for **Enabled Structured Block Write** in the OPC server is turned off. The difference is that it uses string formatted control tag items, for example, using item **Oper\$** instead of item **Oper**. The principle is that the control operation structure data is serialized to this item in a string format while reading and de-serialized

from this item while writing. This allows the OPC clients to complete the control operation with an OPC write on a simple string type instead of a complex array type. Shown below is a typical format for tag **Oper\$**.



- `;` is the delimiter between the control parameters.
- `[`` and `']` are for the structure type.
- `,` is the delimiter between the array elements.

Standard Data Items

The MatrikonOPC Server Framework creates a number of standard data items which can be used for monitoring and controlling certain behavior.

Table 36 describes the standard items available for most device links.

Field	Description
#Enabled	This is a Boolean OPC tag which indicates whether or not the Device Link to which it belongs is enabled. If the value is True or a value of True is written to this item then the Device Link is enabled.
#OfflineMode	Adding this item allows 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. For more information, refer to Appendix G - Offline Mode .
@Connected	This is a Boolean OPC tag which indicates whether or not the Device Link is connected to its resources. Typically True indicates that a connection of an end device has been established.

Table 36 - Standard Data Items

Table 37 describes the standard items available for at the root branch of the server browse tree.

Field	Description
#MonitorACLFile	This 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. For more information, refer to Appendix F - Security .
@Clients	This is a read-only string item which lists the name of every client currently connected to the OPC server.

Table 37 - Server Data Items

Table 38 describes the statistical and control items available for the Redundancy Group device link.

Field	Description
#Manual Device Link	Write to this control item to indicate which device link, of the device links to which the Redundancy Group is subscribed, is forced to be active, whether or not it is available. Clear the value of this control item in order to allow the OPC server to decide which of the subscribed device links should be active, according to their configured priorities and availabilities.
@Active Device Link	The current active device link, which will be the highest-priority of the available device links on the Redundancy Group device link's subscription list.
#Redundancy Group	A numbered list of device links to which the Redundancy Group device link is subscribed. They are ordered from highest to lowest priority. Writing a numbered list of device links will modify the subscribed device links for the Redundancy Group. Note: Writing to this item is not supported if the device link name contains colon ":" or bracket "(" characters. If device link names contain these characters, the Redundancy Group must be configured using the PSTConfig tool .

Table 38 - Redundancy Device Link OPC Items

Table 39 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 39 - 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**.

Diagnostics

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

Logging

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

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

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

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

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

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



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

Limitations

MatrikonOPC Server for IEC 61850/61400-25 has the following limitations:

1. **Does not support GSE** – at this time, the MatrikonOPC Server for IEC 61850/61400-25 does not support GSE (GOOSE/GSSE) messages broadcast by the device.
2. **Does not support several control blocks** – currently, the MatrikonOPC Server for IEC 61850/61400-25 does not support the following control blocks: Substitution Control Block, Setting Group Control Block, Log Control Block.
3. **Does not support all IEC 61850/61400-25 services** – currently, the MatrikonOPC Server for IEC 61850/61400-25 does not support the following IEC 61850/61400-25 services: Logging, File Transfer, Substitution, Time.
4. **Does not support IEC 61400-25 communications mappings other than IEC 61850** – the MatrikonOPC Server for IEC 61850/61400 does not support the other communications service mappings specified by IEC 61400-25-4. Web services, OPC XML-DA, IEC 60870-5-104 and DNP3 protocol mappings are not supported.
5. **Does not support the IEC 61850/61400-25 Server/Publisher model** – currently, the MatrikonOPC Server for IEC 61850/61400-25 does not support acting as a server or a publisher. IEC 61850/61400-25 clients cannot connect to the MatrikonOPC Server for IEC 61850/61400-25 for any purpose.
6. **INT128 Mapping to OPC Data Types** – the largest numeric data type available to OPC servers is the VT_DECIMAL type that allows for 96 bits of precision. The full range of ACSE INT128 values cannot be represented by an OPC server.
7. **Does not support *TimeActivatedOperate*** – currently, the MatrikonOPC Server for IEC 61850/61400-25 does not support the *TimeActivateOperate* operation.

Refer to the MatrikonOPC Server for IEC 61850/61400-25 Release Notes for known issues.

Troubleshooting

This section is intended to assist you by providing **licensing** information and **MatrikonOPC Support** contact information. Also addressed here are 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

Logged in as Administrator to run install

Problem:	Why do I need to be logged in as an Administrator to run the install?
Solution:	For MatrikonOPC software to install correctly, you must be logged in as a user with access to the registry. If you are not an Administrator on the system, the installation will not be able to register the software correctly.

PSTCFG error

Problem:	After my OPC server died, I tried to access the Configuration screen and now I am experiencing access violations and PSTCFG errors.
Solution:	If your OPC server process stops and you leave the PSTCFG running, when you attempt to access the Configuration screen to do anything to your configuration items (add, change, delete, and so on), you will experience access violations. You will need to kill the configuration and restart the server.

Server stops updating client with item values after 30 days

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

Server shuts down after five minutes when no clients connected

Problem:	The server automatically shuts down after five minutes when there are no clients connected.
Solution:	This is standard behavior for COM servers. However, this behavior can be overridden as shown in the following example:  Note: Microsoft highly recommends that you back up the registry before editing it or making changes to it. 1. From the Run command, enter REGEDIT. 2. The Registry Editor (Figure 37) is launched. 3. In the Registry Editor, under HKEY_CLASSES_ROOT, look for the required program ID (e.g., <i>Matrikon.OPC.Simulation.1</i>).

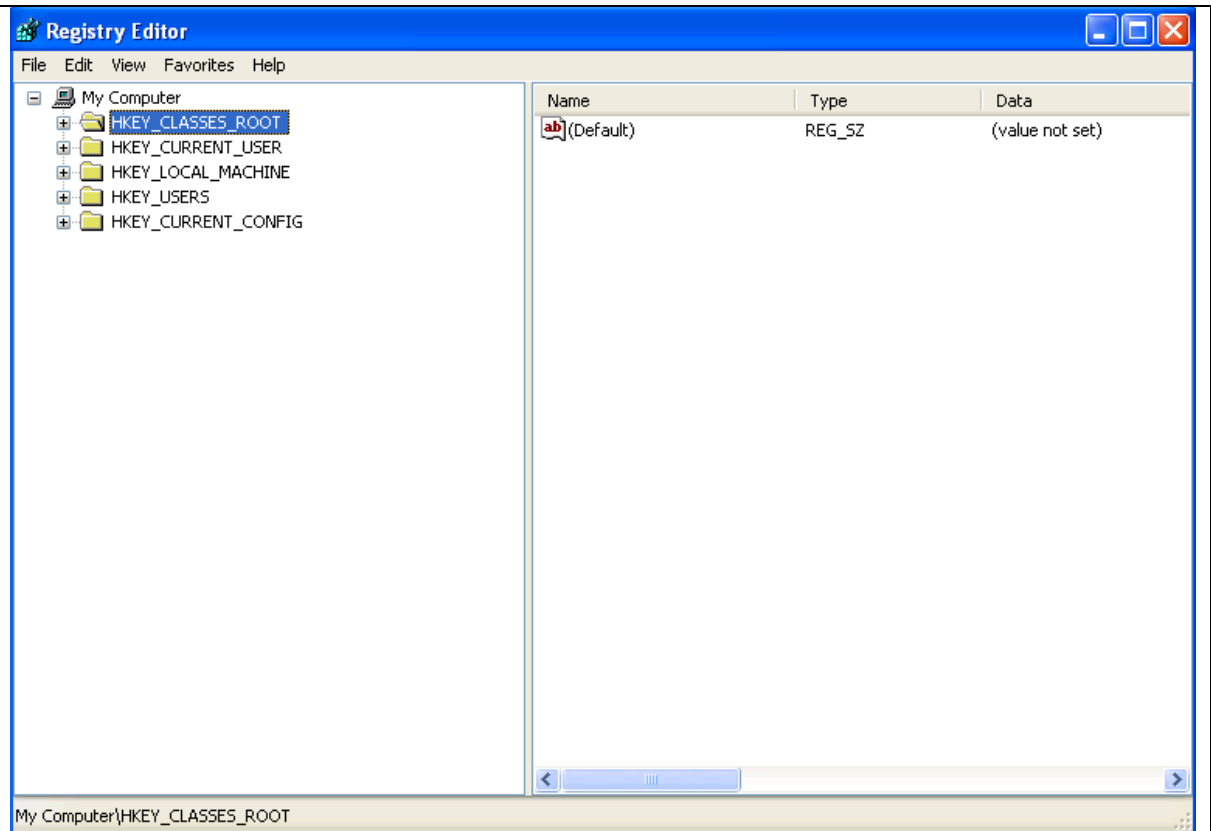


Figure 37 - Registry Editor

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

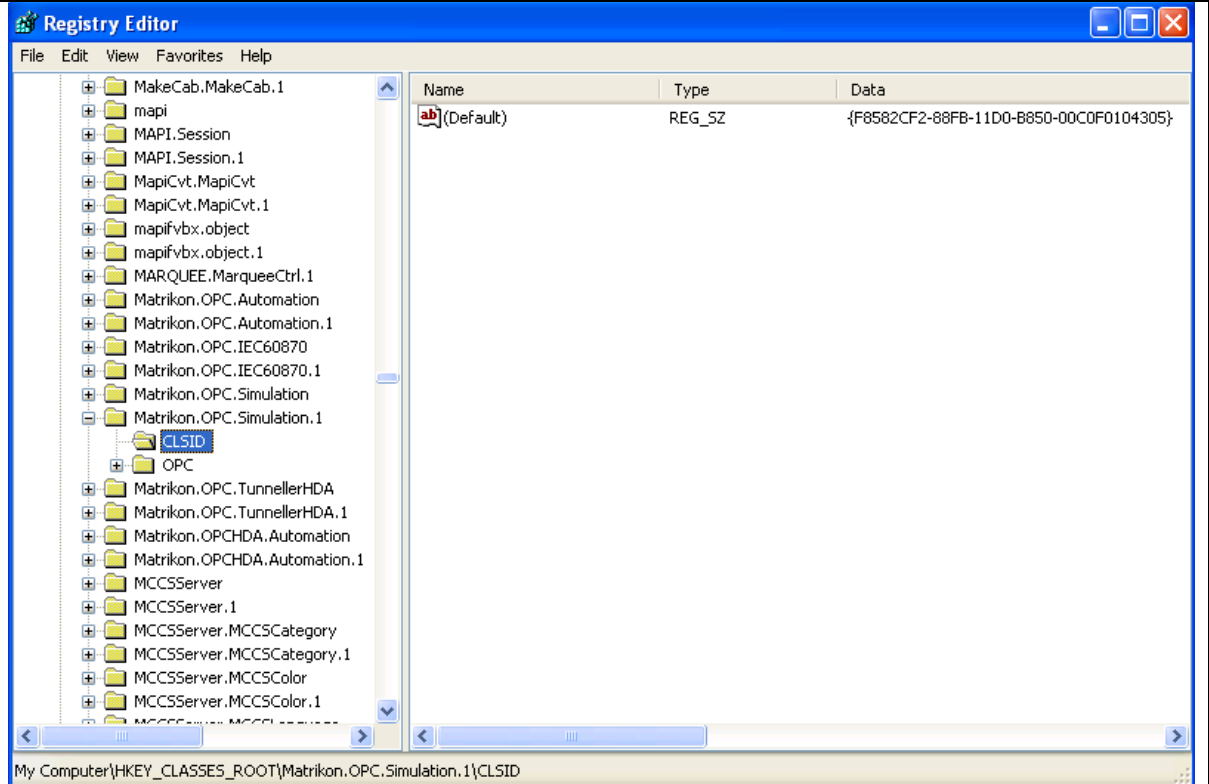


Figure 38 - Program ID Branch

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**).

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 (for more information, refer to **Server Configuration**). Ensure 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 found 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 a service (such as the *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 a 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 is using a large portion of CPU resources

Problem: Server is using 99% of CPU resources.

Solution: Check the server's Time Granularity settings in the servers **Advanced Options**. Ensure the granularity is not set to 0. It is recommended that you not set the value lower than 100.

Trouble communicating through a network

Problem: Experiencing problems communicating to the product's device through a network.

Solution: Make sure users can ping the device. Use the **Start -> Run** with command **CMD** to bring up a command window and type:

```
Ping ipaddress ( e.g., C:\temp>ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms)
```

Where ipaddress is the IP address of the user's <System X> device. If it says "no response", then there are likely network issues between user's computer and the product.

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

Events are not being generated

Problem: Aliases have been configured to generate events, but a subscribed A&E client is not receiving events as expected.

Solution: It is possible to disable event generation at the Alias Group level. Make sure that all of the Alias Groups are set to have events enabled.

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.

How can I access individual bits from an integer item?

Problem: How can I access individual bits from an integer item?

Solution: In order to do this, users will have to apply a mask to the value, which will null all of the bits in the integer value except the one that users want to keep.

For example, if the user wanted to isolate the third bit, they would have to apply a mask that is in binary which will only have the third bit present. In binary, this is the number 4 (0100).

To apply the mask, users must use the AND operator, which will leave a 1, if and only if, both the bits in that position are 1.

$$\begin{array}{r}
 0110 \ 1\mathbf{1}00 \\
 + \ 0000 \ 0\mathbf{1}00 \quad = \ 0000 \ 0\mathbf{1}00 \\
 \quad \quad \quad \nearrow \\
 \quad \quad \text{Data bit we want to access}
 \end{array}$$

In decimal notation, this would be expressed as $108 \text{ AND } 4 = 4$.

To do this in an OPC server, users would configure an alias to use the IF operator. With the example above, where the user wishes to access the third bit in the integer, the statement would appear as:

IF (INPUT AND 4 = 4, 1, 0)

Therefore, if the bit in position 3 is a 1, since $1 \text{ AND } 1 = 1$, the IF statement would be true and would return a 1. If the bit in position is 0, $0 \text{ AND } 1 = 0$, the IF statement would return a false value, which is a 0.

Search the *MatrikonOPC Support Knowledge Base* at www.opcsupport.com to find the answers to other commonly-asked MatrikonOPC Server for IEC 61850/61400-25 questions.

Licensing

Most MatrikonOPC products require that some form of licensing criteria be met for it to function correctly.

The MatrikonOPC Server for IEC 61850/61400-25 supports software licensing **only**.

Note: Alias Events needs to be licensed separately, and by default, is delivered with only a 30-day demo. To purchase a full Alias Events license, please contact your MatrikonOPC Account Manager.

IMPORTANT TO NOTE:

The following licensing information is described in detail within the *Licensing Procedures* document which accompanies the MatrikonOPC Server for IEC 61850/61400-25 software and *User's Manual*:



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

Contacting Support

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

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

For Monday to Friday **daytime support** requests, contact MatrikonOPC Support using the regional phone numbers provided in Table 40.

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)
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 40 - MatrikonOPC Support Regional Contact Information

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

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

Table 41 - After-Hours Support

OPC Compliance

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

- *OPC Overview 1.0*
- *OPC Common Definitions and Interfaces 1.0*
- *OPC Data Access Specification 2.05a*
- *OPC Data Access Specification 3.00*
- *OPC Historical Data Access Specification 1.2*
- *OPC Alarms and Events Specification 1.10*
- *OPC Security 1.00*

Installation

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

- Version-independent program ID is **Matrikon.OPC.IEC61850**.
- Version-specific program ID is **Matrikon.OPC.IEC61850.1**.
- OPC sub-key and vendor information string.
- Globally unique application ID (e.g., **D7CA0556-C317-4512-8B8C-7543DD7F1626**).
- Globally unique class ID number (e.g., **C33ABAC0-15F9-44bb-B303-1424B2C13C7C**).
- Full path of 32-bit local server executable.
- OPC Data Access Server 2.05a and 3.00 implemented component categories.

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

Common Interfaces

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

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

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

Data Access

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

Groups

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

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

Items

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

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

Browsing and Item Properties

The server supports address space browsing.

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

The server supports the following mandatory item properties.

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

I/O Operations

The server supports synchronous I/O operations.

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

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

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

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

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

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

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

- Read items 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 2.05a**.

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

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

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

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

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

Appendix A Distributed COM (DCOM)

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

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

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

Notes:



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

DCOM Configuration Utility

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

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



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

Default Properties

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

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

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

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

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

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

Security Permissions

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

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

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

Setting Security Permissions

To set the security permissions for an OPC Server:

1. Open the DCOM configuration utility.
2. Select the OPC server, and then click **Properties**.
3. The **Distributed COM Configuration Properties** window (Figure 39) appears.

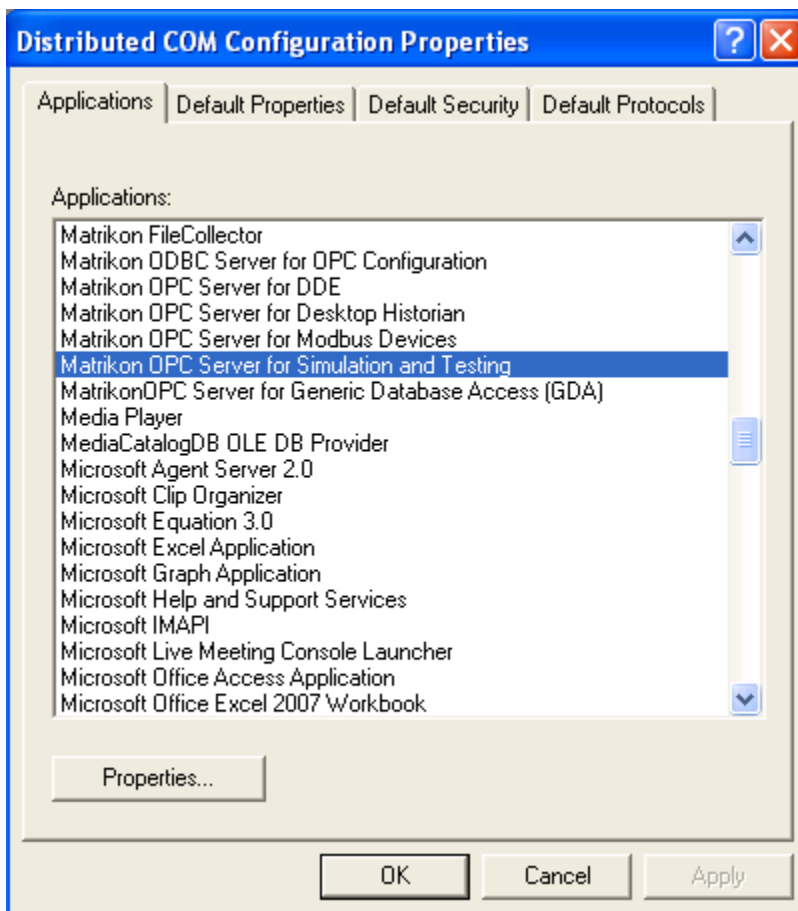


Figure 39 - Distributed COM Configuration Properties Window

4. Click on the **Security** tab to set the security for the server.
5. The **Distributed COM Configuration Security** tab (Figure 40) appears.

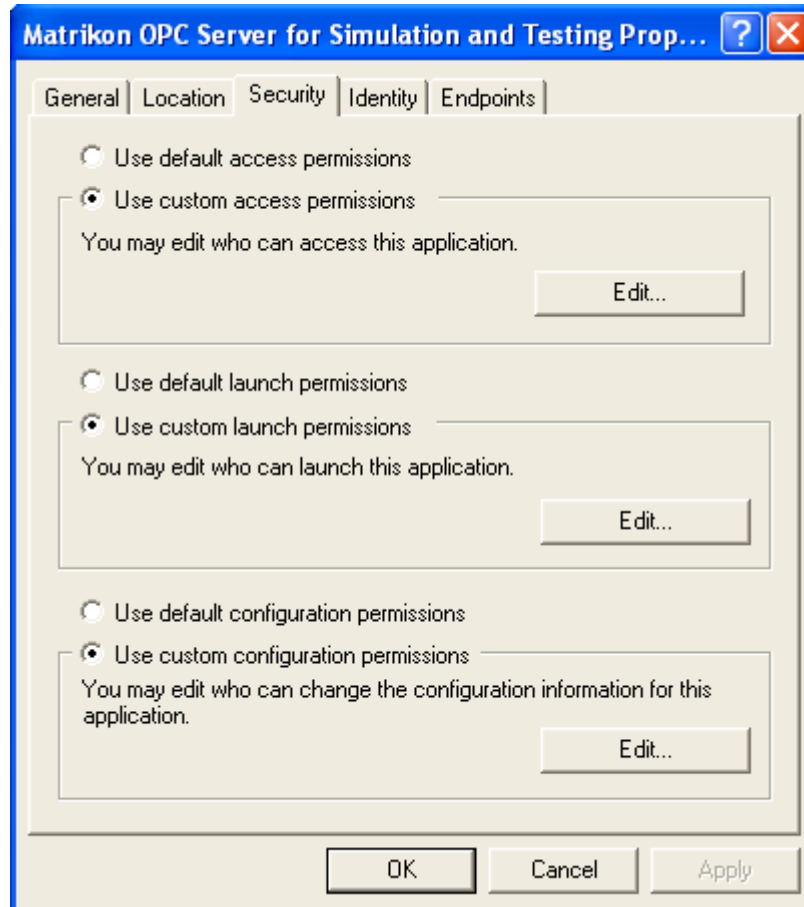


Figure 40 - Distributed COM Configuration Security Tab

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 41) appears.

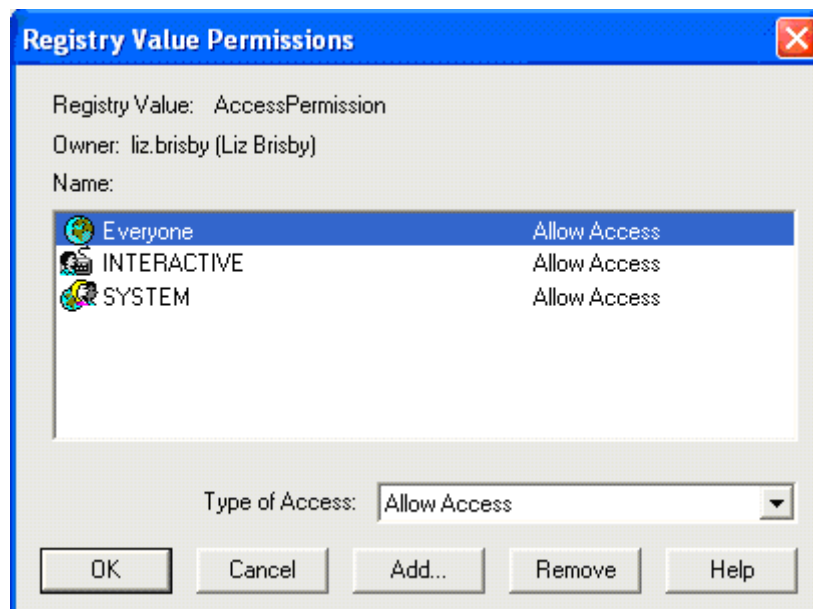


Figure 41 - Registry Value Permissions Window

9. To add users to the list click, **Add**.
10. The **Add Users and Groups** window (Figure 42) appears.

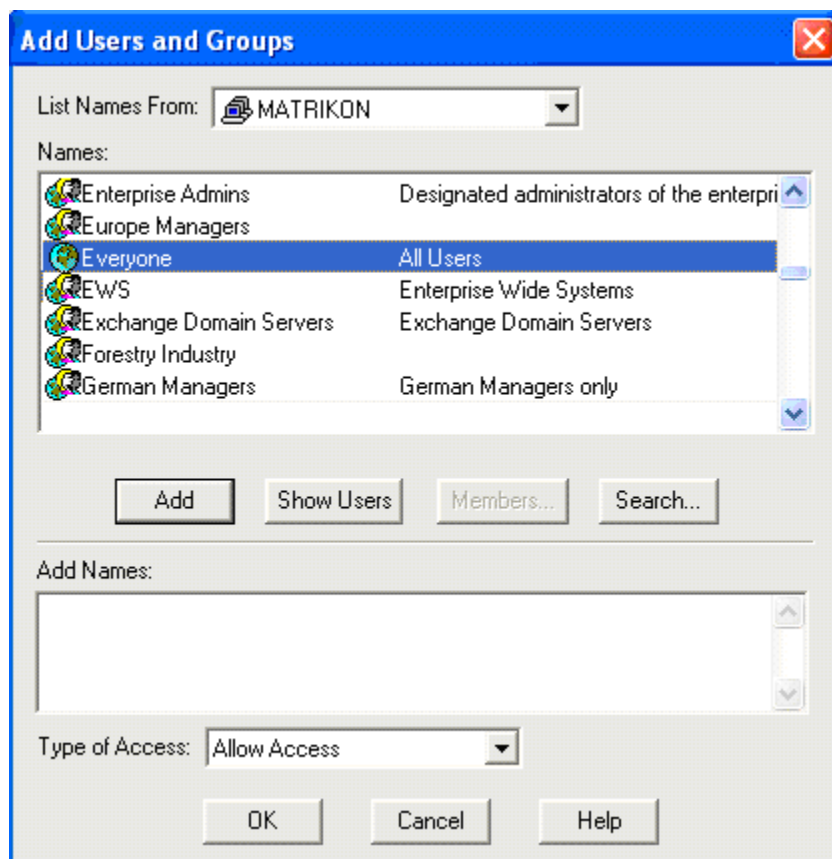


Figure 42 - Add Users and Groups Window

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

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

Notes:

- The procedure to set the launch permissions is similar to the above, but instead of choosing **Allow Access** for a user you would choose **Allow Launch**.
 - The Configuration Permissions contain an *Access Control List* of principals that are allowed to modify the configuration information for a server. In other words, it indicates who is allowed to alter the registry entries for installed servers as well as who is able to access the registry for the purposes of installing new servers. It is usually simpler to install and configure servers as a user with local administrative rights.
13. To connect to an OPC server from outside of the domain, create a local user account on both the server and the client machine with identical *username* and *password*. Then, add the local user on the OPC server to the DCOM permissions. Use the local account on the client machine to connect to the OPC server.

Server Identity

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



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

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

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

Default Protocols

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

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

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



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

Remote Program ID

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

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

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



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

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

Note: In the case of MatrikonOPC servers, the ID has the form *Matrikon.OPC.Device*. If you quickly type the first few letters, then **REGEDIT** should jump to the location of that key. Some servers may have both a version-specific as well as a version-independent program ID. In this case both IDs should be copied to the client machine.

5. For each program ID, select the key and choose **Export Registry File** from the **Registry** menu. Enter a file name, and then click **Save**. Be careful not to overwrite other export files that you are creating.
6. Copy the exported **REG** files to the client machine.
7. Merge the **REG** files into the registry of the client machine.

Note: This should simply be a matter of double clicking on the file from the desktop of the client machine. Alternatively, run **REGEDIT** on the client machine and choose **Import Registry File** from the **Registry** menu, selecting each file in turn. This must be done as a user who has write access to the local registry.

8. Use **REGEDIT** to check that the program IDs have in fact, been copied.
9. Delete the **REG** files since they are no longer needed.

Appendix B Aliases

Scaling Expressions

Alias scaling expressions may use any of the expression constructs listed in Table 42.

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 42 - Expressions Constructs for Alias Scaling

Advanced Calculations

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

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

If the OPC item being referenced in a calculation is not found within the servers address space, the server attempts to add it. If successful, the OPC server uses the **Alias Subscription Rate** to update the OPC item. The **Alias Subscription Rate** is configured in the **Advanced Options** panel.

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

Advanced alias calculations may use any of the operators listed in Table 43.

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

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

Table 43 - Calculation Operators for Alias Scaling

Alias scaling calculations may use any of the functions listed in Table 44.

Construct	Description	Examples
abs	Absolute value.	<code>abs(x)</code>
acos	Arccosine	<code>acos(x)</code>
asin	Arcsine	<code>asin(x)</code>
atan	Arctangent	<code>atan(x)</code>
avg	Returns the average of a set of values.	<code>avg(v1,v2,v3,...)</code>
bin	Converts a binary number to a decimal number.	<code>bin(binNumber)</code>
ceil	Ceiling.	<code>ceil(x)</code>
cos	Cosine.	<code>cos(x)</code>
cosh	Hyperbolic cosine.	<code>cosh(x)</code>
fact	Returns the factorial of x: $x*(x-1)*(x-2)*...(x-x+1)$.	<code>fact(x)</code>
floor	Floor.	<code>floor(x)</code>
hex	Converts a hexadecimal number to a decimal number.	<code>hex(hexNumber)</code>
if	If the condition is true, returns val1 else returns val2.	<code>if(condition, val1, val2)</code>
isNaN	Returns 1 if the number is a NaN value.	<code>isNaN(value)</code>
log	Natural logarithm.	<code>log(x)</code>
log10	Base-10 logarithm	<code>log10(x)</code>
max	Returns larger of a set of values.	<code>max(v1,v2,v3,...)</code>
max	Returns larger of two values.	<code>max(x,y)</code>
max	Returns larger of three values.	<code>max(x,y,z)</code>
min	Returns smaller of a set of values.	<code>min(v1,v2,v3,...)</code>

Construct	Description	Examples
min	Returns smaller of two values.	min(x,y)
min	Returns smaller of three values.	min(x,y,z)
rand	Random value between 0 and 1.	rand()
rand	Random value between min and max.	rand(min, max)
round	Round the fractional part of a number.	round(x)
sin	Sine.	sin(x)
sinh	Hyperbolic sine.	sinh(x)
sqrt	Square root.	sqrt(x)
sum	Returns the sum of a set of values.	sum(v1,v2,v3,...)
tan	Tangent.	tan(x)
tanh	Hyperbolic tangent.	tanh(x)

Table 44 - Calculation Functions for Alias Scaling

CSV File Format

Note: The CSV file format does not support Alias Event custom category configuration settings. If aliases referencing custom categories are exported to CSV, all custom categories must be created before import.

The alias import/export file contains lines of comma-separated values. Each line contains the fields listed in Table 45.

- 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).

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)

Field	Description
	1 = poll continuously at the specified update rate
Update Rate	Update rate (milliseconds) to use with the Poll Always option.
Scaling	Scaling type for the alias. 0 = none 1 = linear 2 = square root 3 = gain/offset 4 = expression 5 = calculation

Table 45 - 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 46.

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

Table 46 - 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 47.

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

Table 47 - 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 48.

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

When the scaling field specifies calculation (5) scaling, the line contains the additional fields listed in Table 49.

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

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

Scaling Algorithms

For each type of scaling, a different algorithm (Table 50) 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 50 - Scaling Algorithms

Appendix C Standard Data Types

The Standard data types and their descriptions are listed in Table 51.

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 51 - Standard Data Types

Appendix D Microsoft Excel as a DDE Client

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

DDE Read

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

=SERVICE|TOPIC! NAME

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

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

Special Characters in Excel

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

=SERVICE|TOPIC!'NAME'

=SERVICE|'TOPIC'!'NAME'

=SERVICE|'TOPIC'!NAME

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

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

DDE Write

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

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

Net DDE

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

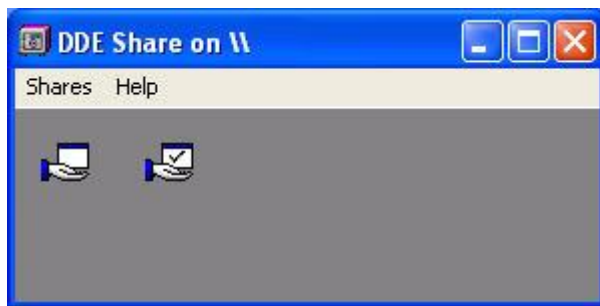


Figure 43 - DDE Share

NetDDE must first be configured using the DDEShare application (*DDEShare.exe*) as shown in Figure 43. Each SERVICE and TOPIC pair, or "NetDDE Share", that is to be available through NetDDE must be assigned a unique name.

Appendix E Configuring Dynamic Data Exchange (DDE)

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

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

DDE service can be enabled or disabled using a checkbox (refer to **Advanced Options** for more information, including the location of, this checkbox). Note that these options will not be available if the server does not support DDE.

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

SERVICE_NAME |ITEM! SCANDETAILS

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

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

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

Changes to the DDE options do 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.

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**.

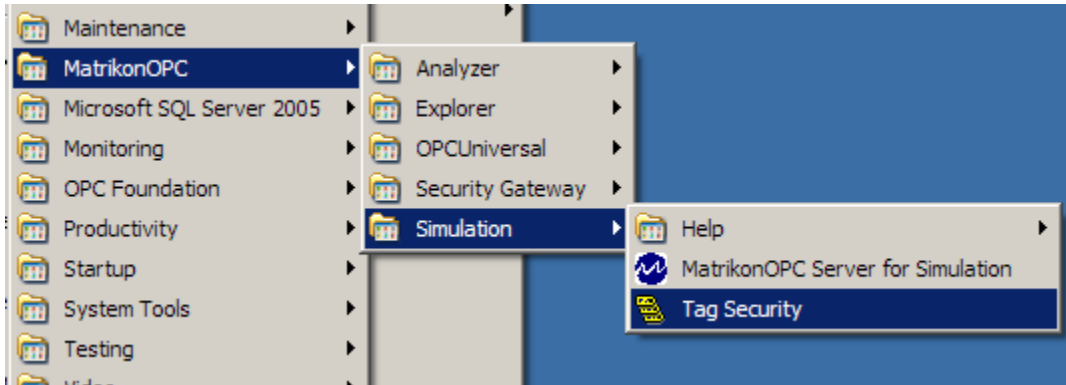


Figure 44 - Start Menu Navigation

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 45) appears.



Figure 45 - Enter Server Password Window

2. Enter the password created during the installation of the OPC server.
Note: The default password provided for you during installation (if you chose to use the default) is **MatrikonOPC**.
3. Click on the **OK** button.
4. The **MatrikonOPC Tag Security Configuration Utility** screen (Figure 46) appears.

Layout

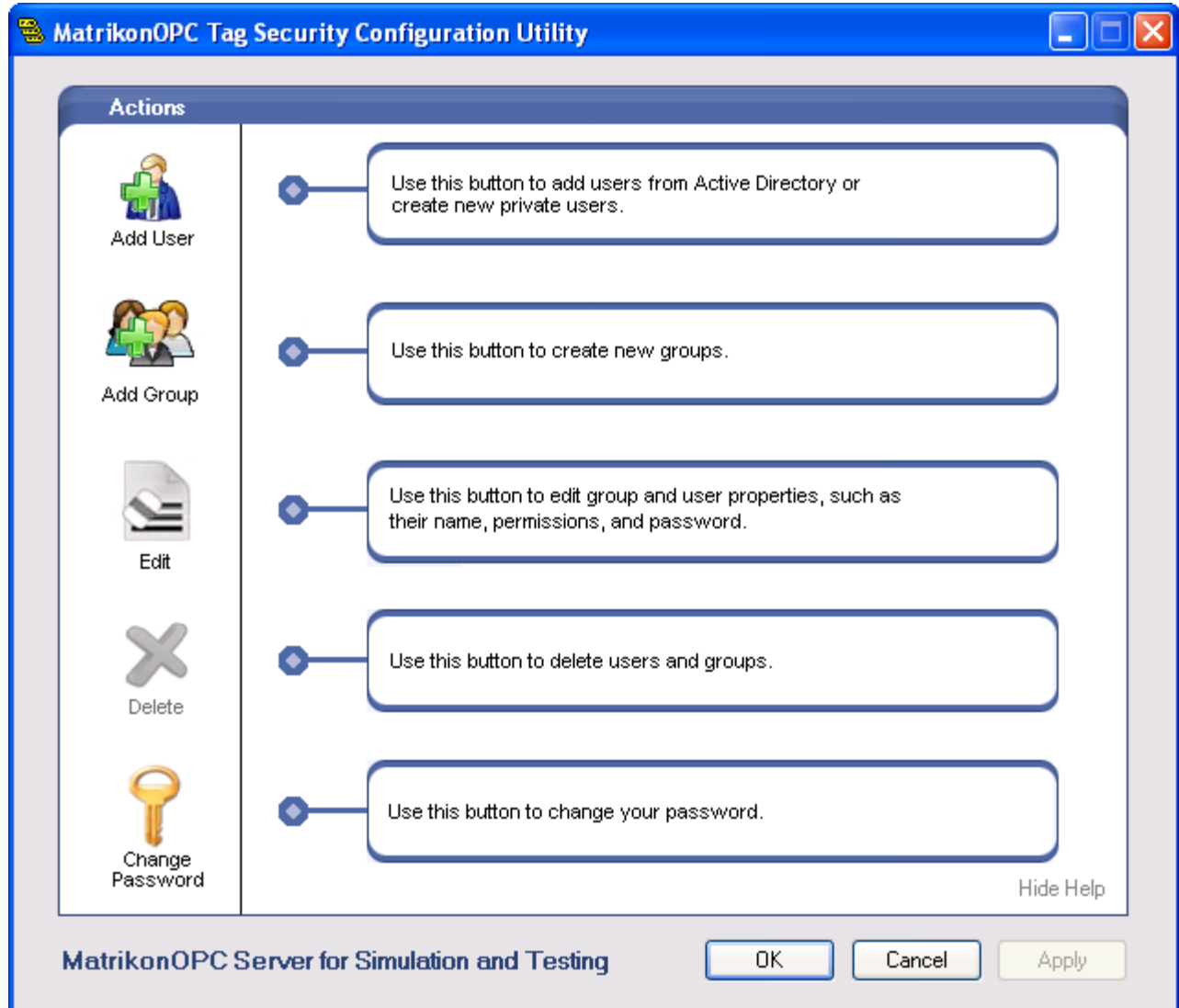


Figure 46 - MatrikonOPC Tag Security Configuration Utility Main Screen

The **MatrikonOPC Tag Security Configuration Utility** screen displays the name of the OPC server that is being configured for tag security. In Figure 46 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 47). 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.

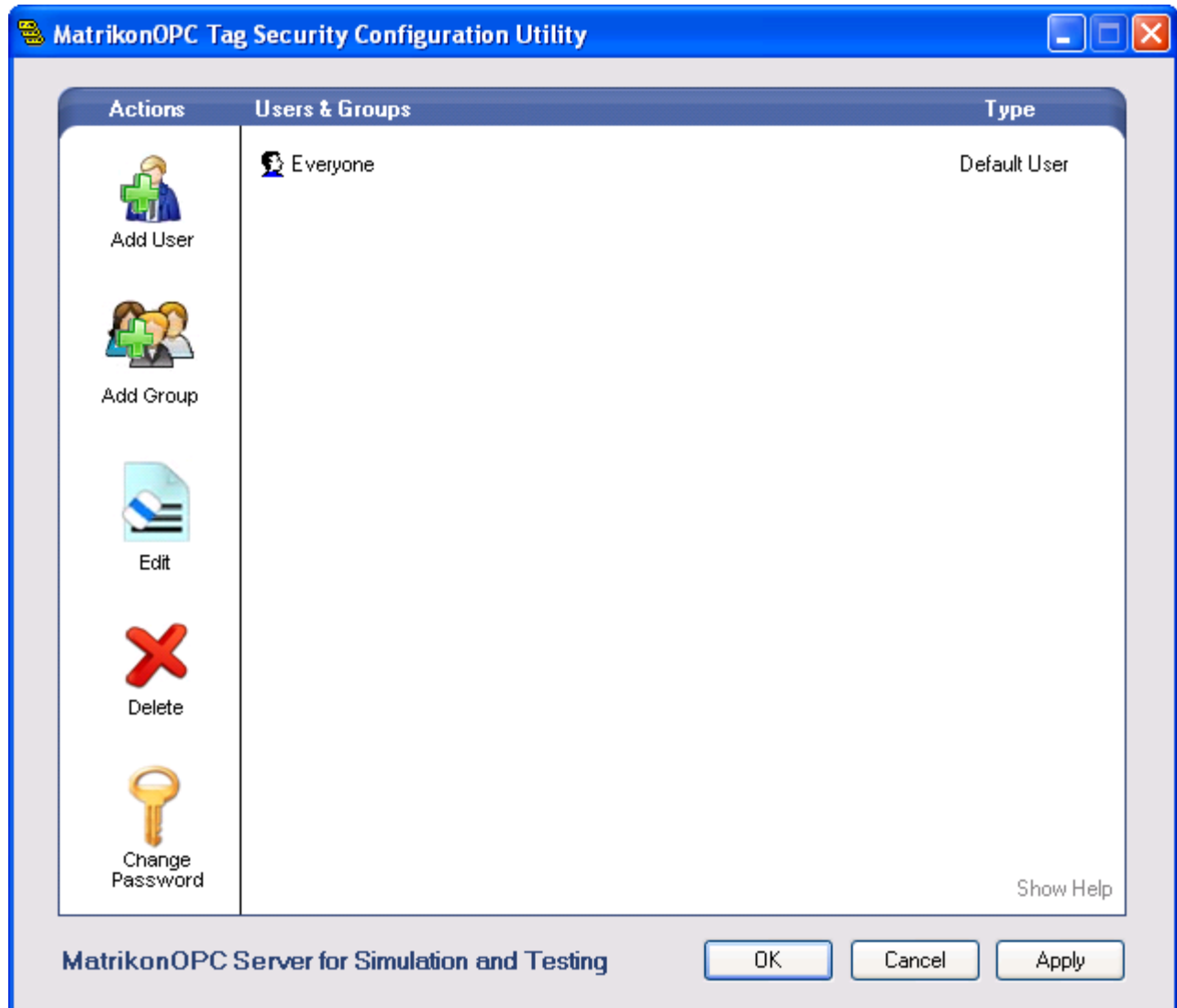


Figure 47 - MatrikonOPC Tag Security Configuration Utility Main Screen: Users & Groups

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

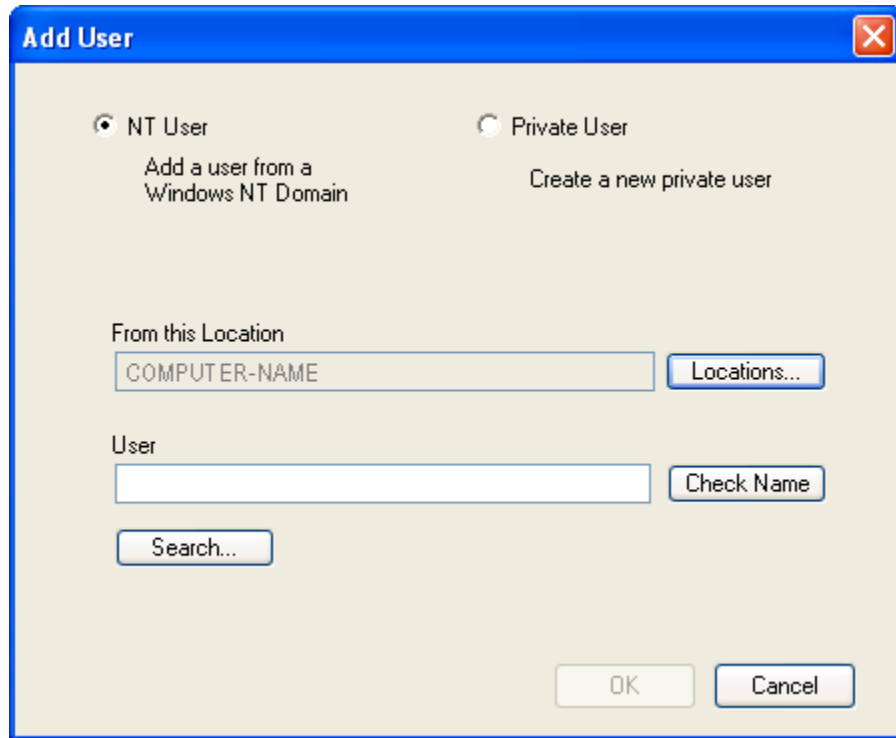


Figure 48 - Add User Window (NT)

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 49 for a sample list of defined users and groups).
6. The **Edit <Username>** window (Figure 54) appears. Follow the instructions in the **Edit User** section for adding permissions.

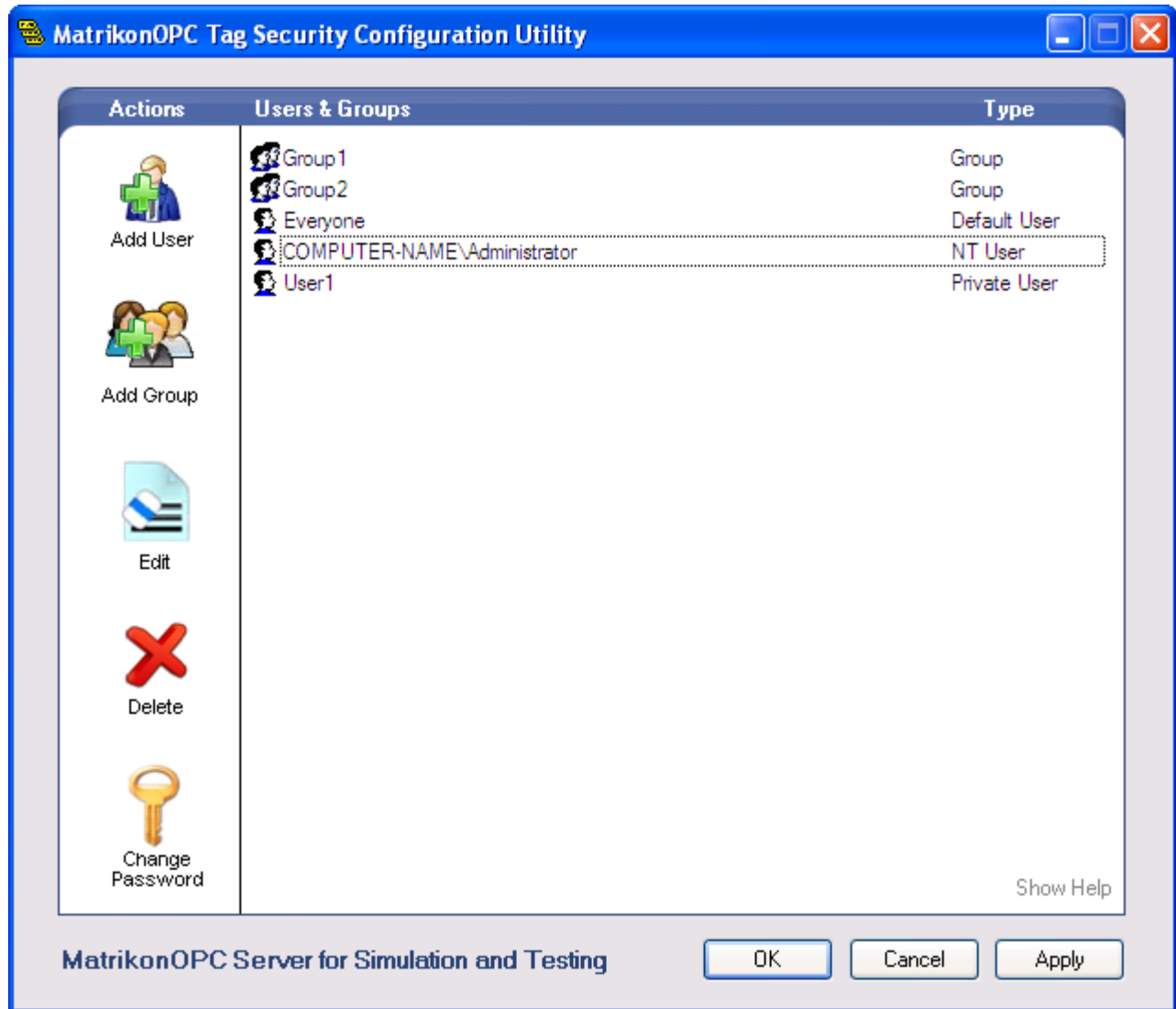


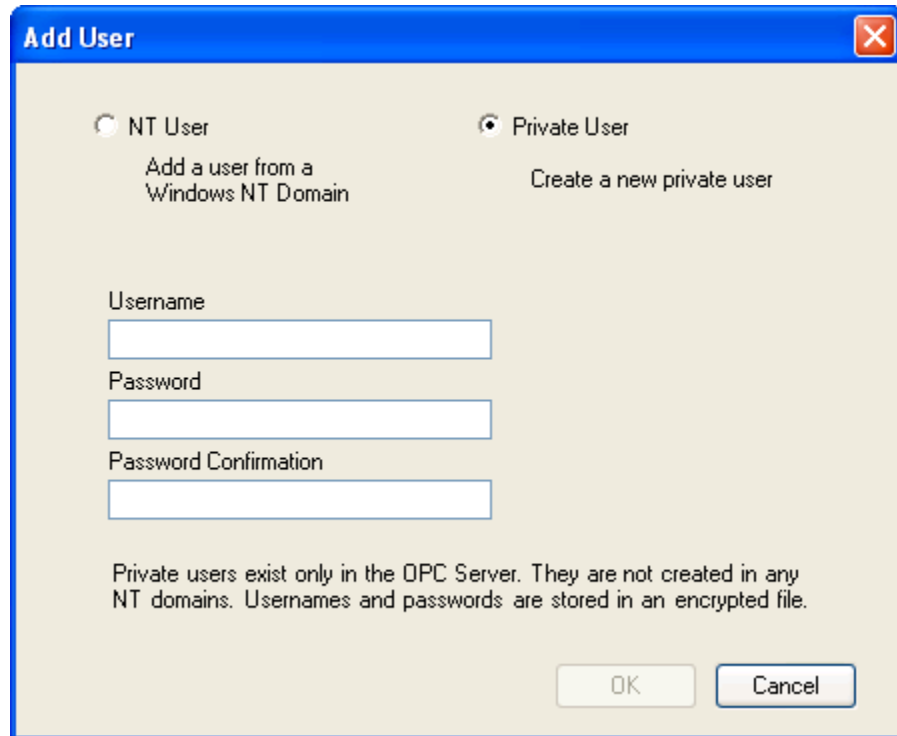
Figure 49 - Defined Users and Groups

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 48) appears.
3. Select the **Private User** option button (Figure 50).



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

Figure 50 - 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 49 for a sample list of defined users and groups).

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

Add Group

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

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

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

NT Group

To add an NT group:

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

- The **Add Group** window (Figure 51) appears. The **NT Group** option button is selected by default. This will allow the addition of an NT group from a Windows NT Domain.

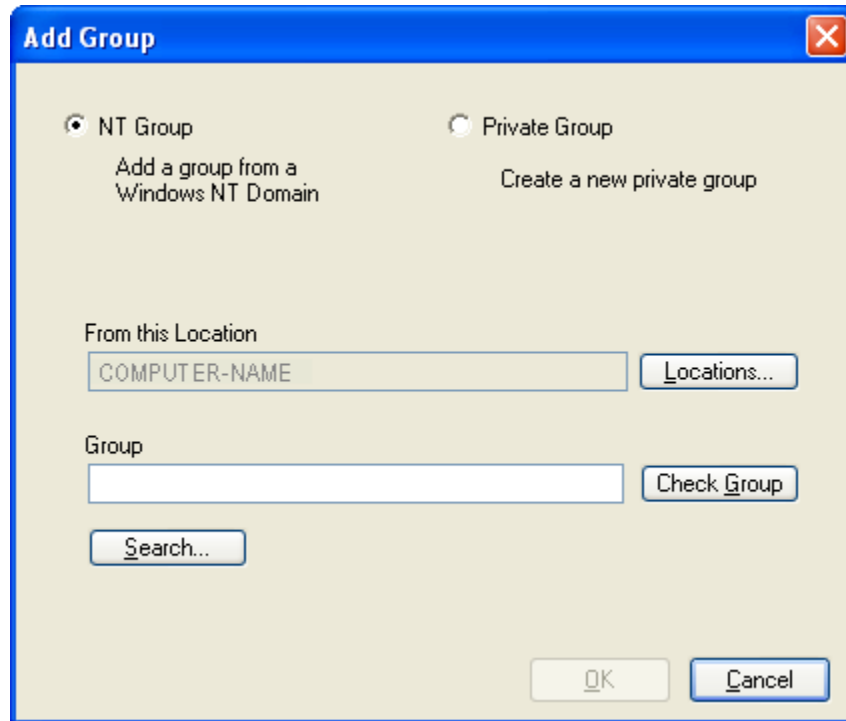


Figure 51 - Add Group Window (NT)

- By default, the local machine name appears in the **From this Location** field. To browse to a different location, click the **Locations** button.
- The **Group** field can be entered manually. Clicking on the **Check Group** button performs validation on the entered group. The group names are the same as the Windows NT domain group names used on the network. To avoid manually entering a group, click on the **Search** button, and select a group from the displayed list of groups.
- To add the selected group, click on the **OK** button. The group is then added to the list of users and/or groups currently defined (refer to Figure 49 for a sample list of defined users and groups).
- The **Edit <Groupname>** window (Figure 61) appears (for NT Groups, there is only the **Permissions** tab). Follow the instructions in the **Edit Group** section for adding permissions.

Private Group

To add a Private Group:

- From the **MatrikonOPC Tag Security Configuration Utility** main screen, click on the **Add Group** button.
- The **Add Group** window (Figure 51) appears.
- Select the **Private Group** option button (Figure 52).

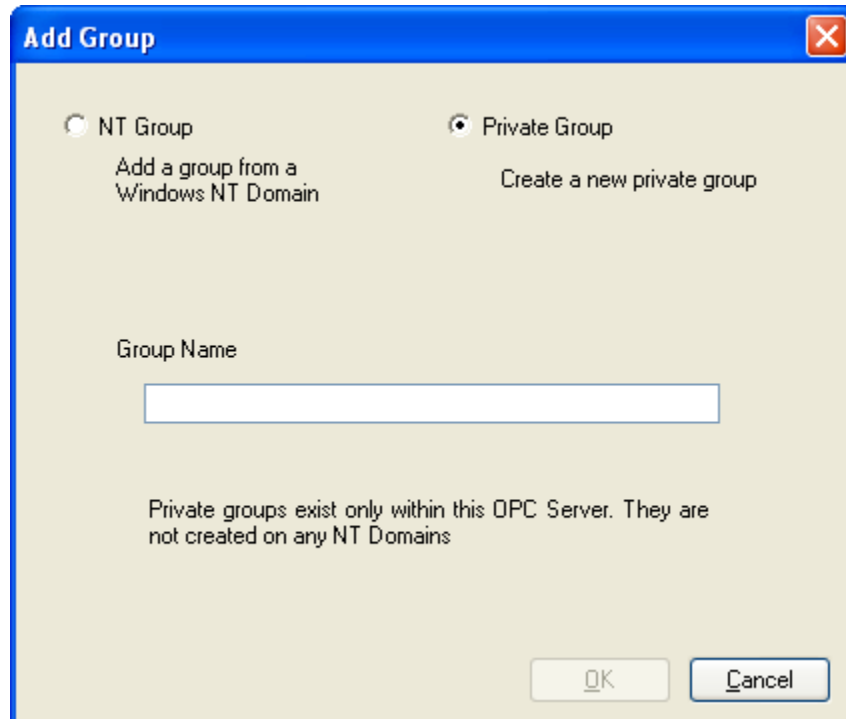


Figure 52 - Add Group Window (Private)

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 49 for a sample list of defined users and groups).
6. The **Edit <Groupname>** window (Figure 61) 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 53) appears.

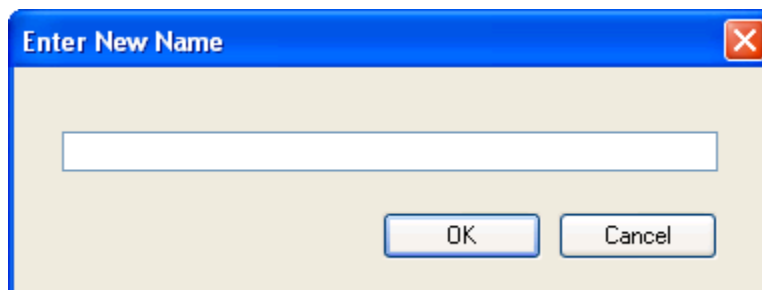


Figure 53 - Enter New Name Window

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 54) 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.

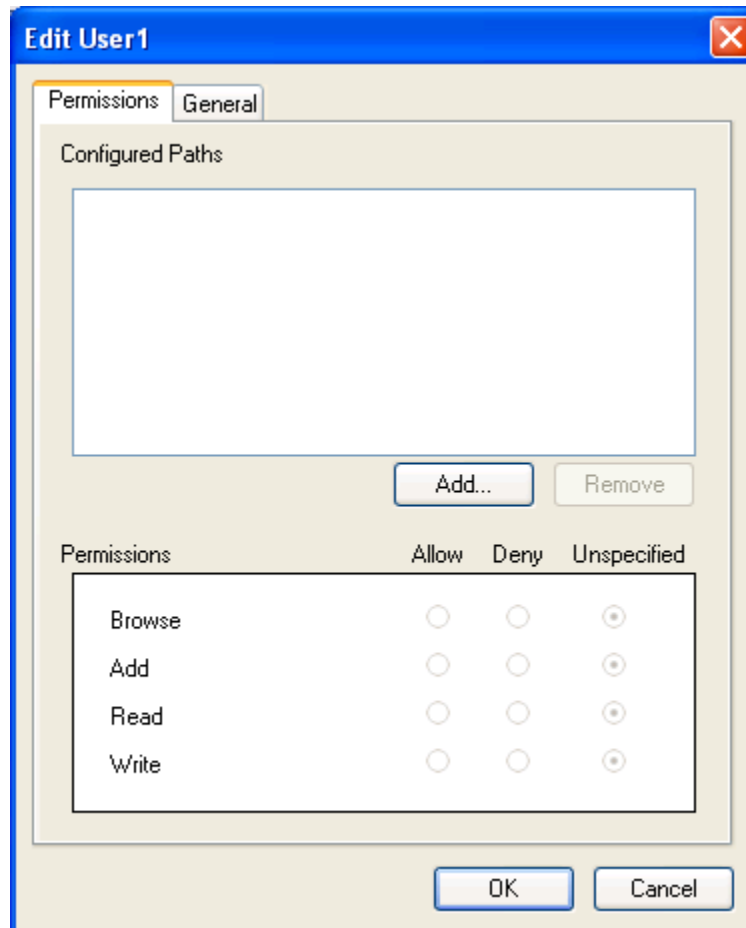


Figure 54 - Edit <Username> Window (Permissions Tab)

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

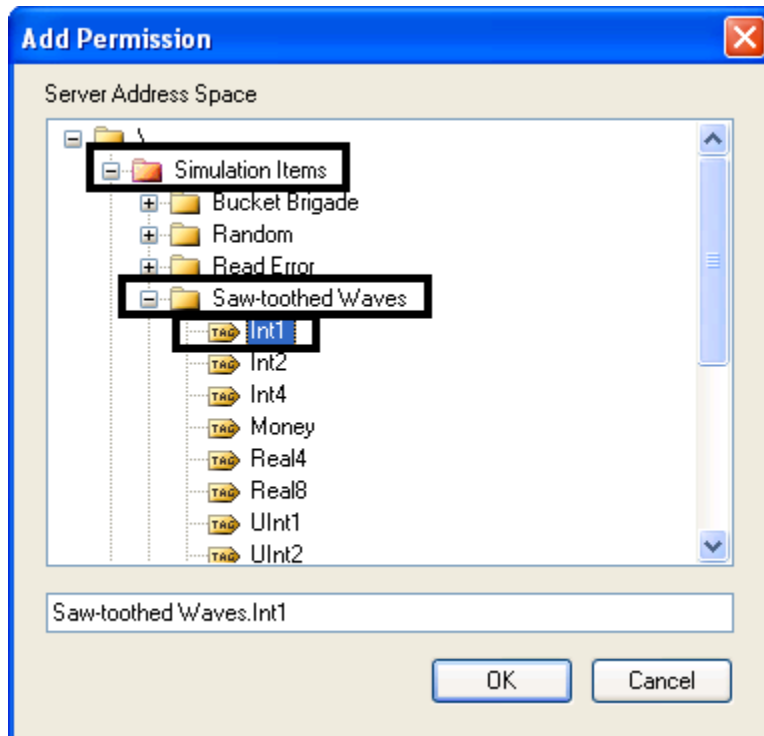


Figure 55 - Add Permission Screen (Server Address Space)

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

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

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

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

To edit a user's permissions:

1. Click on the **Add** button to begin configuring permissions for the current user.
2. The **Add User Permission** window (Figure 56) 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.

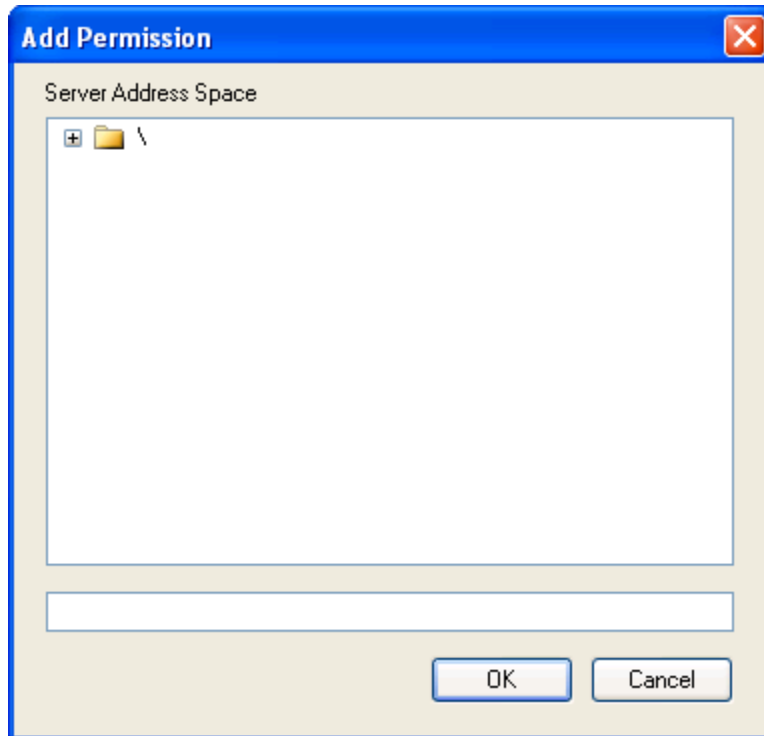


Figure 56 - Add User Permission Window

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 color (see Figure 57) 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**.

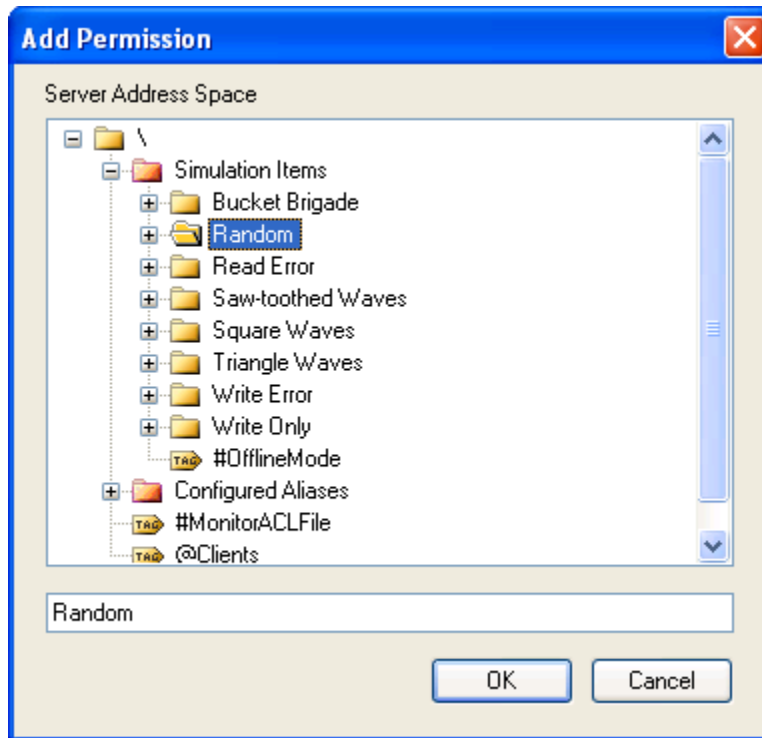


Figure 57 - Add Permission Window: Browsing Server Address Space

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 58.

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.

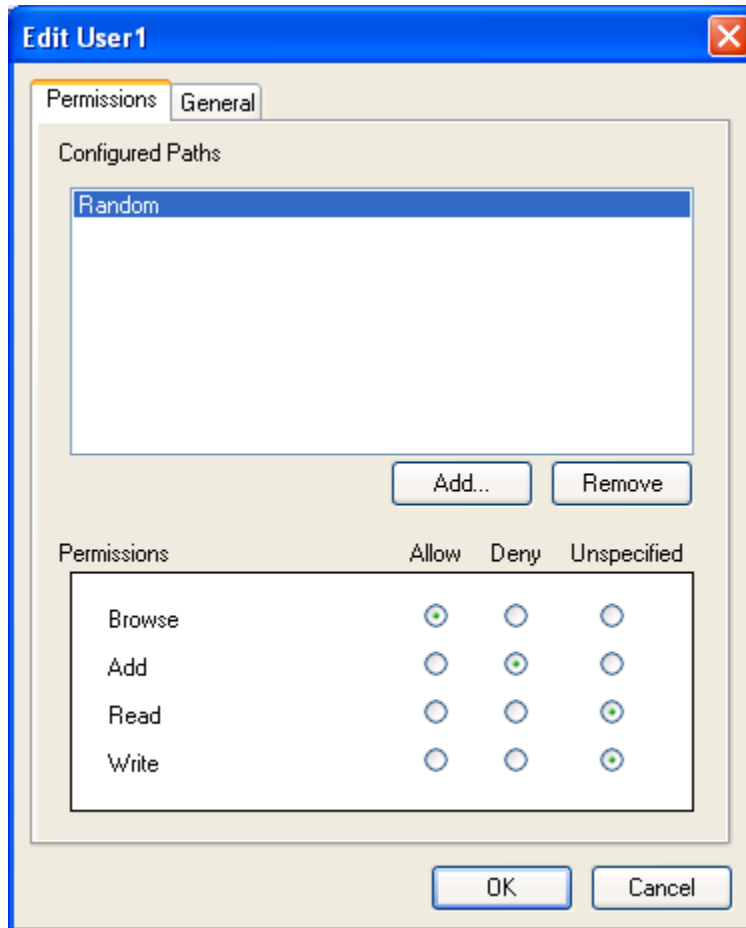


Figure 58 - Edit <Username>: Example

On the **General** tab (Figure 59) 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 59 - Edit <Username> Window (General Tab)

To change the user's password:

1. Click on the **Reset Password** button. The **Reset Password** window (Figure 60) appears.

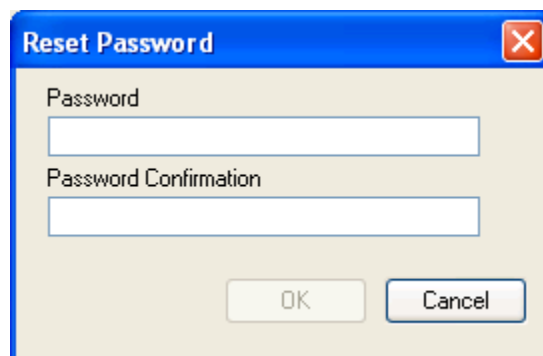


Figure 60 - Reset Password Window

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 61) 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.

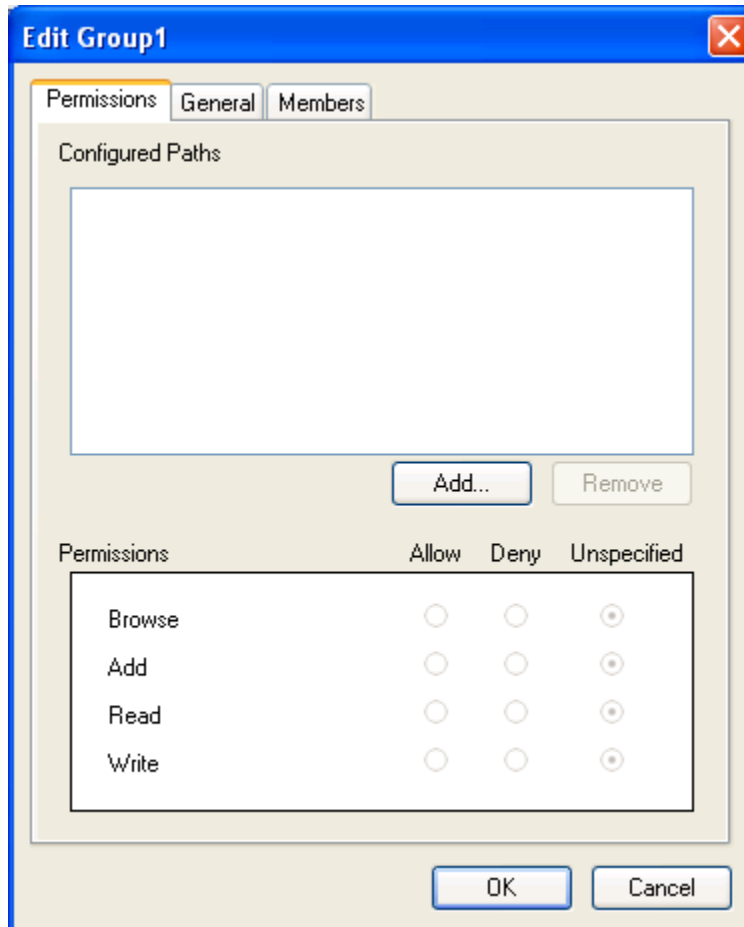


Figure 61 - Edit <Groupname> Window (Permissions Tab)

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 62) 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 62 - Edit <Groupname> Window (General Tab)

On the **Members** tab (Figure 63), the users that are part of the current group are defined. By default, the **Group Members** screen section is empty. In Figure 63, **User1** has been added to **Group1**.

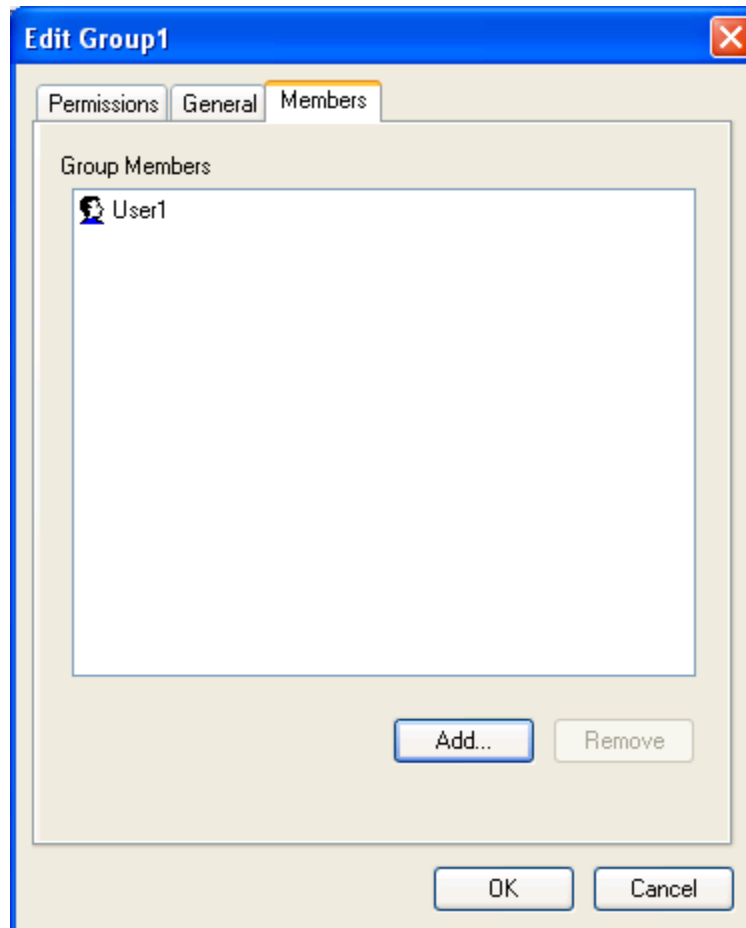


Figure 63 - Edit <Groupname> Window (Members Tab)

To add one or more members to the group:

1. Click on the **Add** button. The **Add Existing User** window (Figure 64) appears.

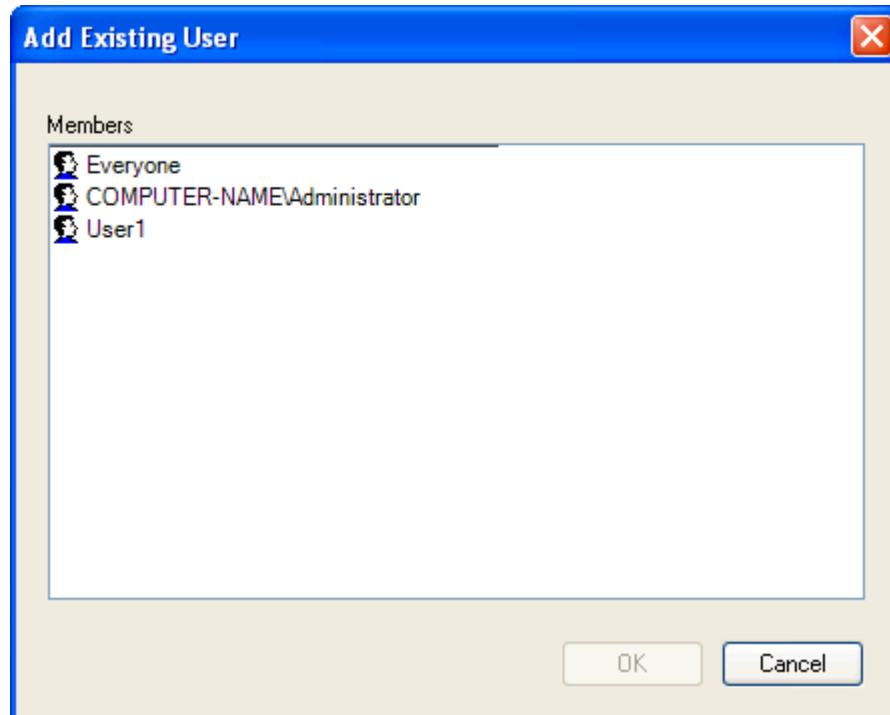


Figure 64 - Add Existing User Window

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 63).

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 49), 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 46).
2. The **Change Password** window (Figure 65) appears.



The dialog box titled "Change Password" contains three text input fields and two buttons. The first field is labeled "Please enter the old password for this OPC Server". The second field is labeled "Please enter the new password for this OPC Server". The third field is labeled "Please confirm the new password". The buttons are labeled "OK" and "Cancel".

Figure 65 - 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 52:

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

Table 52 - 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 53 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 53 - 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 54 lists all defined users and groups and their associated permissions. Table 55 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 54 - Example 2: Permissions

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

Table 55 - 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).

While the server is running, if the **ACL.sec** file is moved or deleted from its location above, security functions as it did before the file was moved. If the server is re-started with the **ACL.sec** file missing, no users will have permissions to do anything (i.e., browsing, adding, reading, writing) and must re-configure their security settings.

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 49), 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 49). If the user is found and the password provided is correct, the *Logon()* result is successful and the user name provided replaces the NT user that was obtained through impersonation. If not found, the *Logon()* result is failure and the NT user remains as the name used for security permissions. When the OPC client calls *Logoff()*, the NT user becomes the name used for security permissions.

Determining Permission

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

1. Identity
2. Location
3. Type

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

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

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

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

1. Check whether the exact location is found in the **Configured Paths** list for the **identity**. If found:
 - a. Check whether the permission type (**browse**, **add**, **read**, or **write**) is specified (Figure 58). 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 56 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 56 - 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 57 shows the value behavior for each data type:

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

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

Table 57 - 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 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 61850/61400-25 CD into the CD drive.
2. If the MatrikonOPC InstallAware screen does not automatically appear, double-click the installation .exe file. The **MatrikonOPC Server – InstallAware Wizard** verifies its contents (Figure 66).

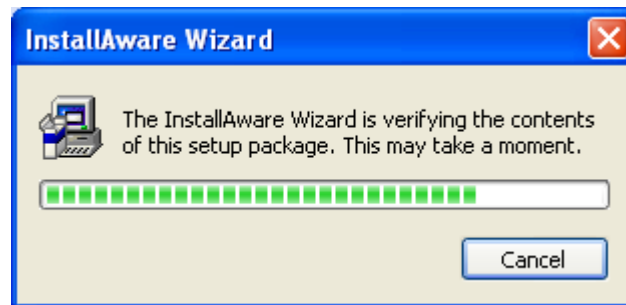


Figure 66 - InstallAware Wizard Verification Window

3. Either a **Pre-Requisites** screen (Figure 67) appears, or you are taken directly to the **Licensing Agreement** (Figure 68) screen. If the **Licensing Agreement** screen is the displayed screen, go to step 5.
4. If the **Pre-Requisites** screen appears, then click on the **Next** button to install the listed pre-requisites.

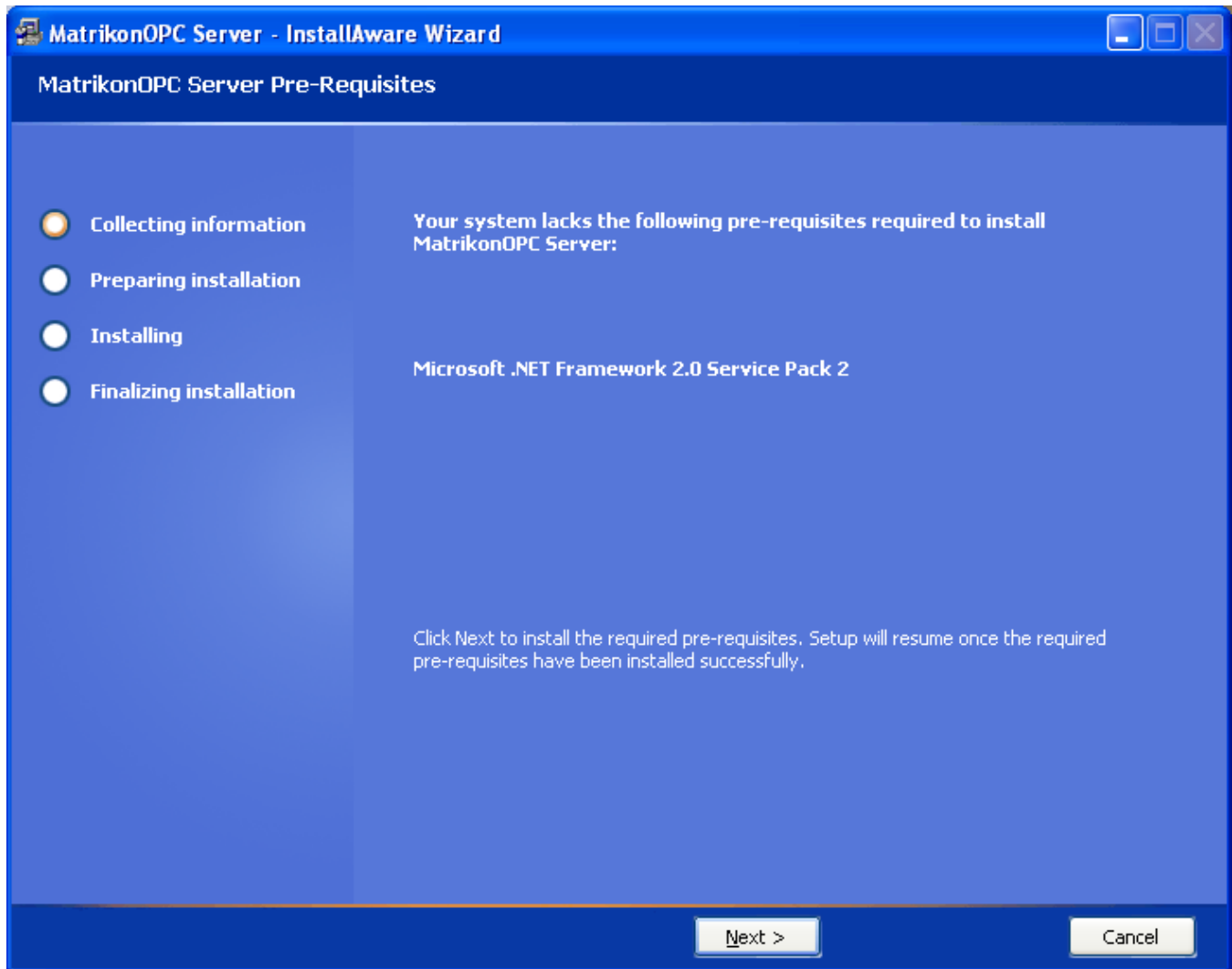


Figure 67 - Pre-Requisites Screen

5. After all pre-requisites have been installed, the **License Agreement** screen (Figure 68) appears.

Note: 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 return to the previous screen, 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.

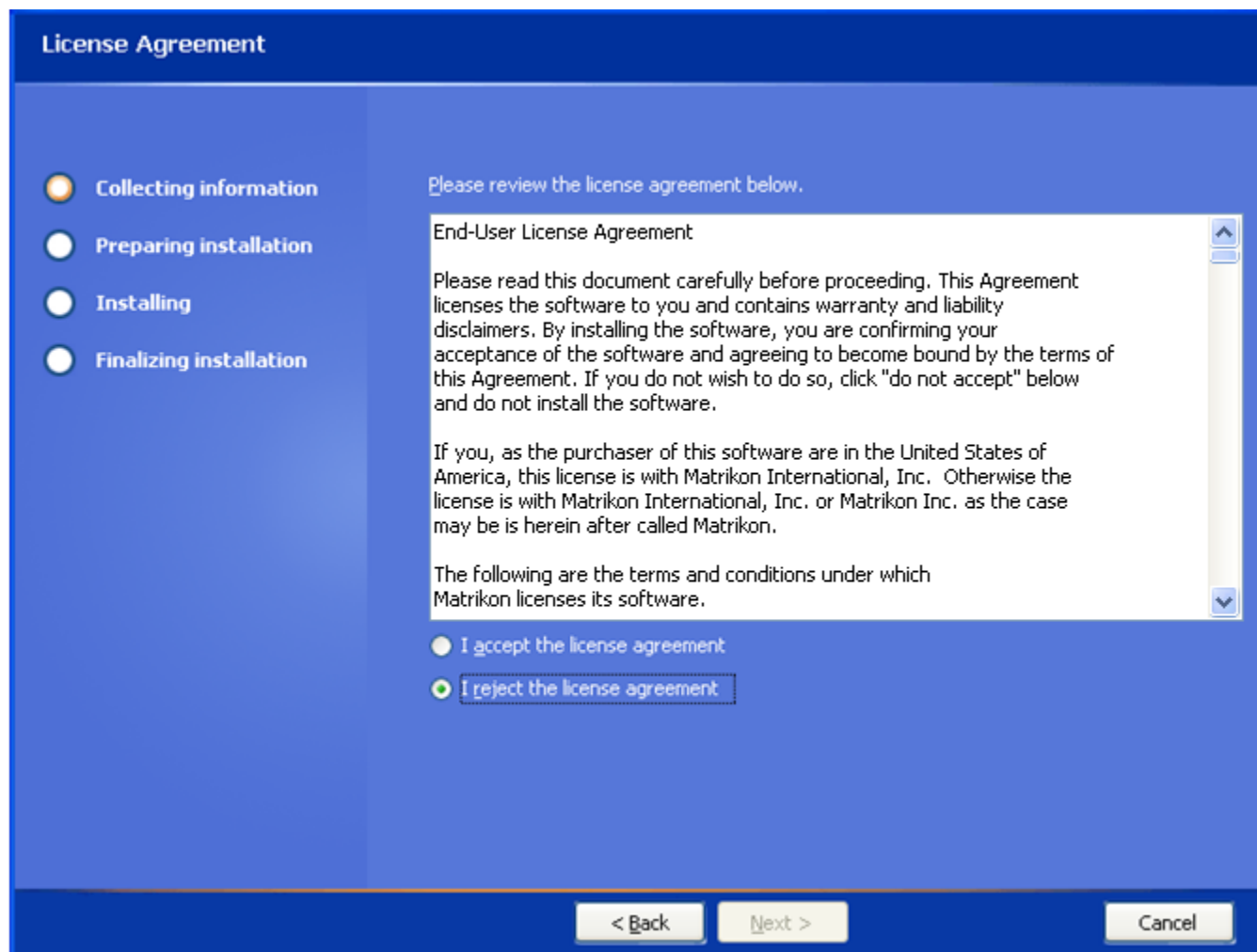


Figure 68 - License Agreement Screen

6. Read the **Software License Agreement**, using the scroll bar to view the entire message.
7. Select the **I accept the license agreement** option button.
8. Click on the **Next** button. The **Setup Type** screen (Figure 69) appears.

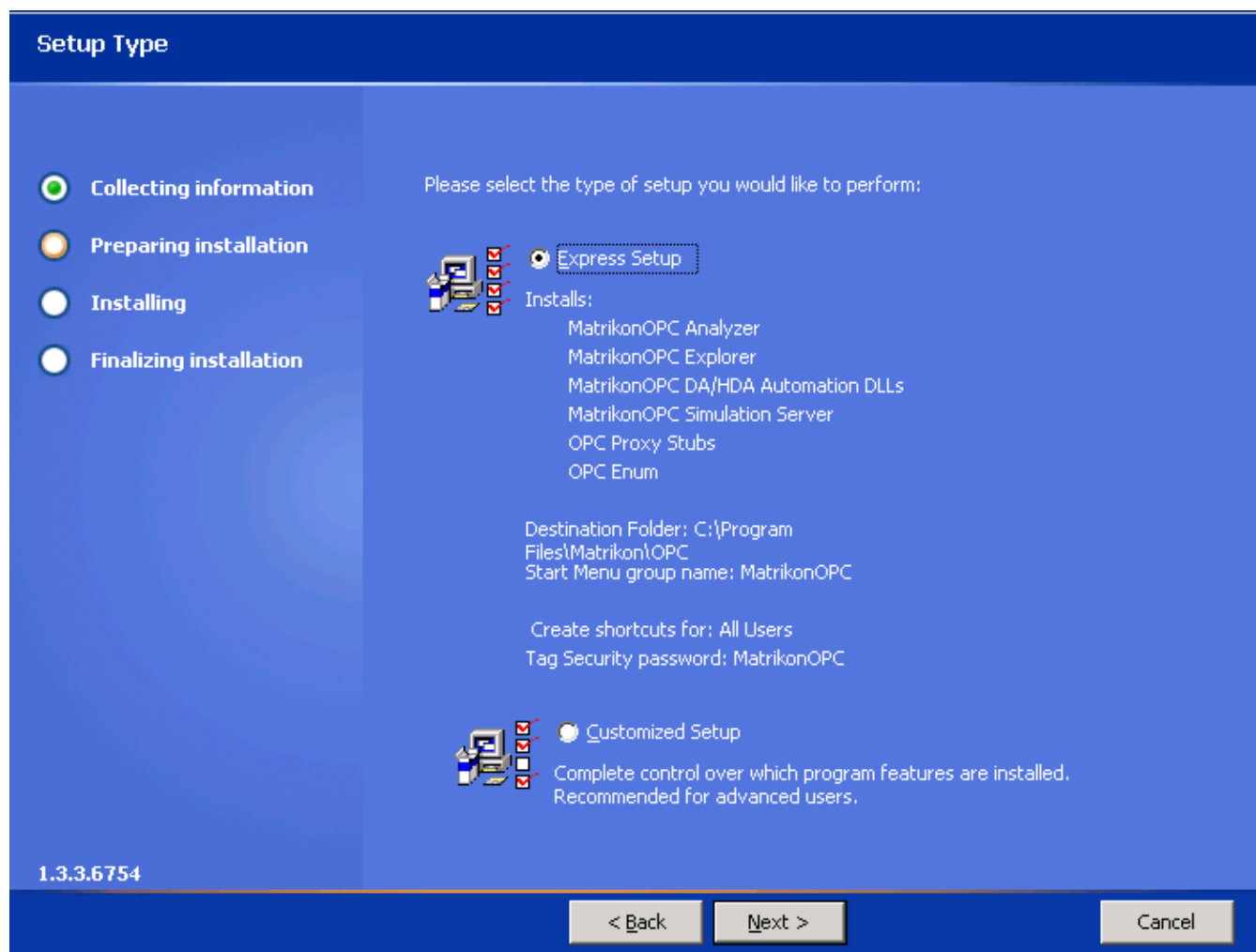


Figure 69 - Setup Type Screen

9. Select the type of setup to be performed.

Note: MatrikonOPC recommends that you select the **Express Setup** option.

10. Click on the **Next** button. The **Destination Folder** screen (Figure 70) appears.

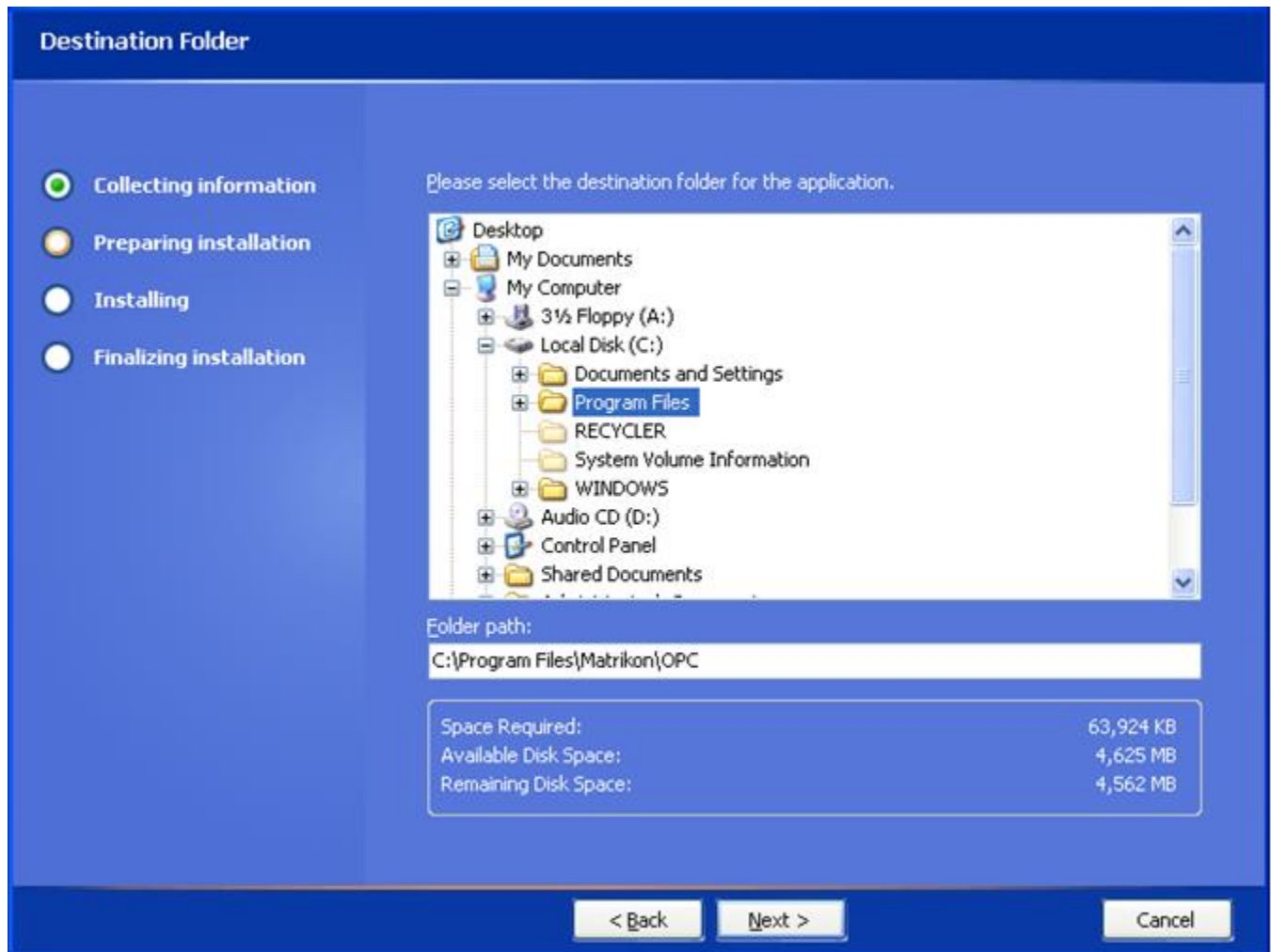


Figure 70 - Destination Folder Screen

11. Select the folder in which to install the MatrikonOPC server, or accept the default location displayed in the **Folder path** field.
12. Click on the **Next** button. The **Start Menu** screen (Figure 71) appears.

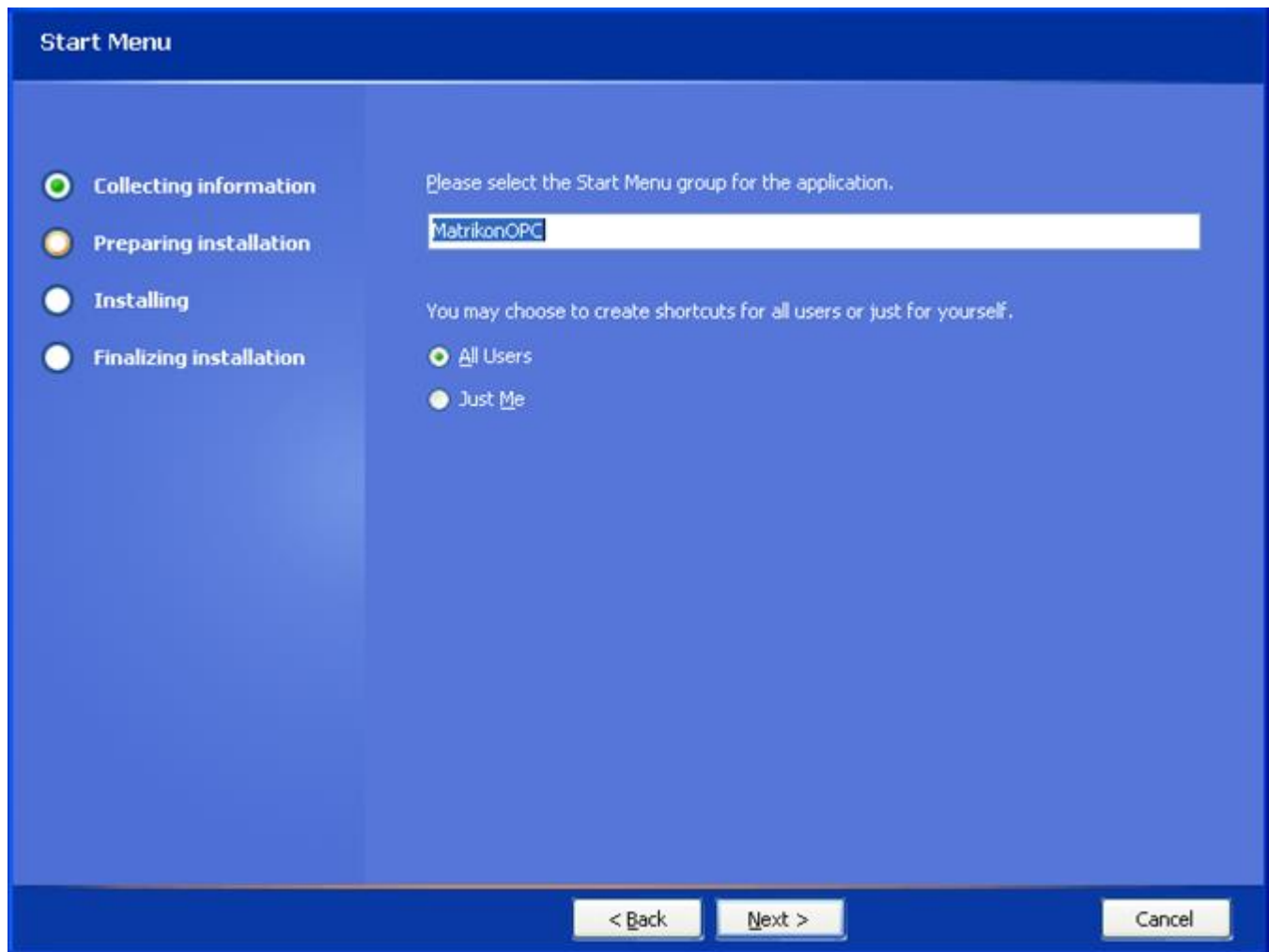
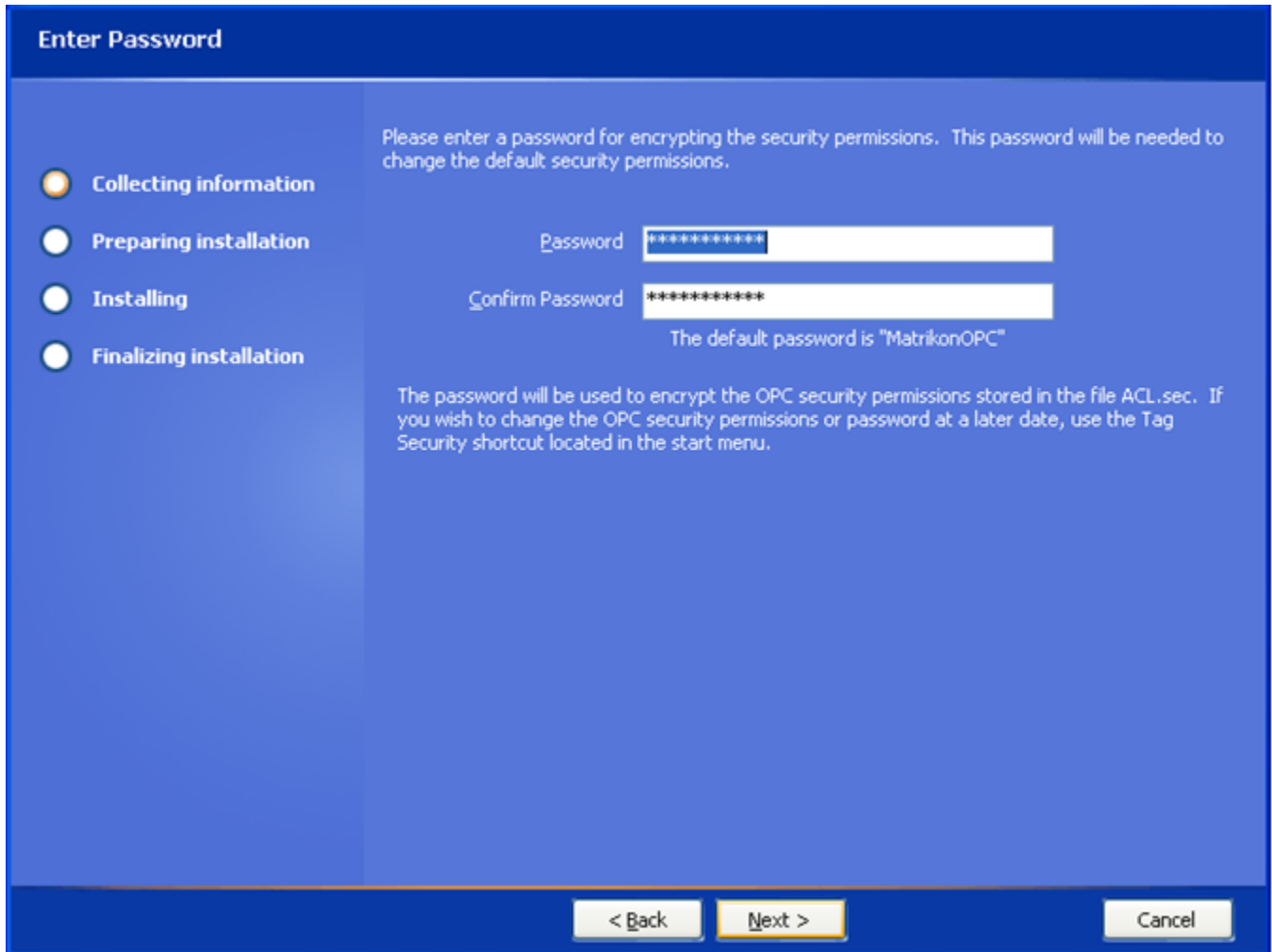


Figure 71 - Start Menu Screen

13. 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.
14. Click on the **Next** button. The **Enter Password** screen (Figure 72) 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.

Figure 72 - Enter Password Screen

15. 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**.

16. Click on the **Next** button to accept the default password. The **Licensing** screen (Figure 73) appears.

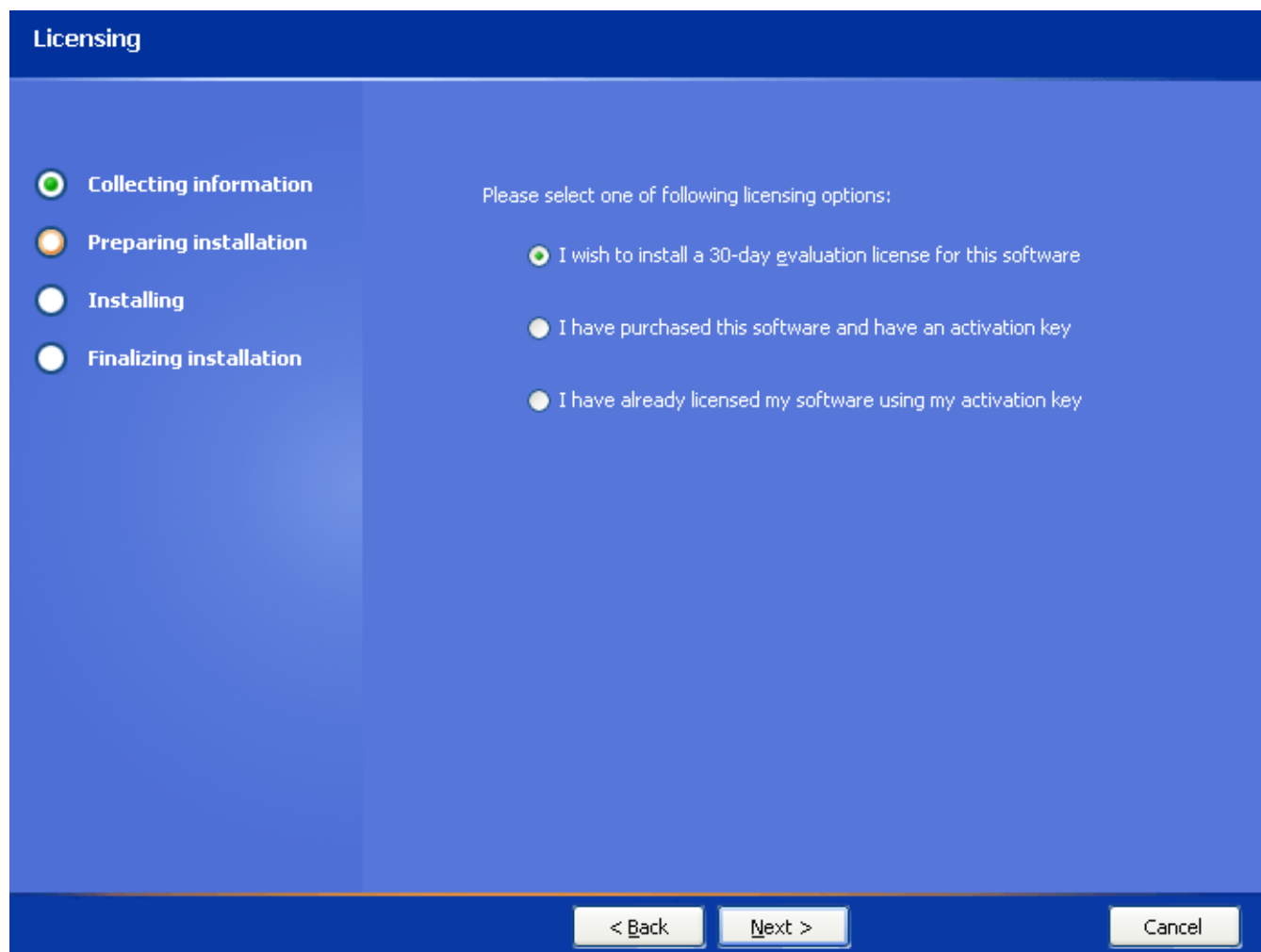


Figure 73 - Licensing Screen

17. Select the applicable licensing option.
18. Click on the **Next** button. The **Ready to Install** screen (Figure 74) appears.

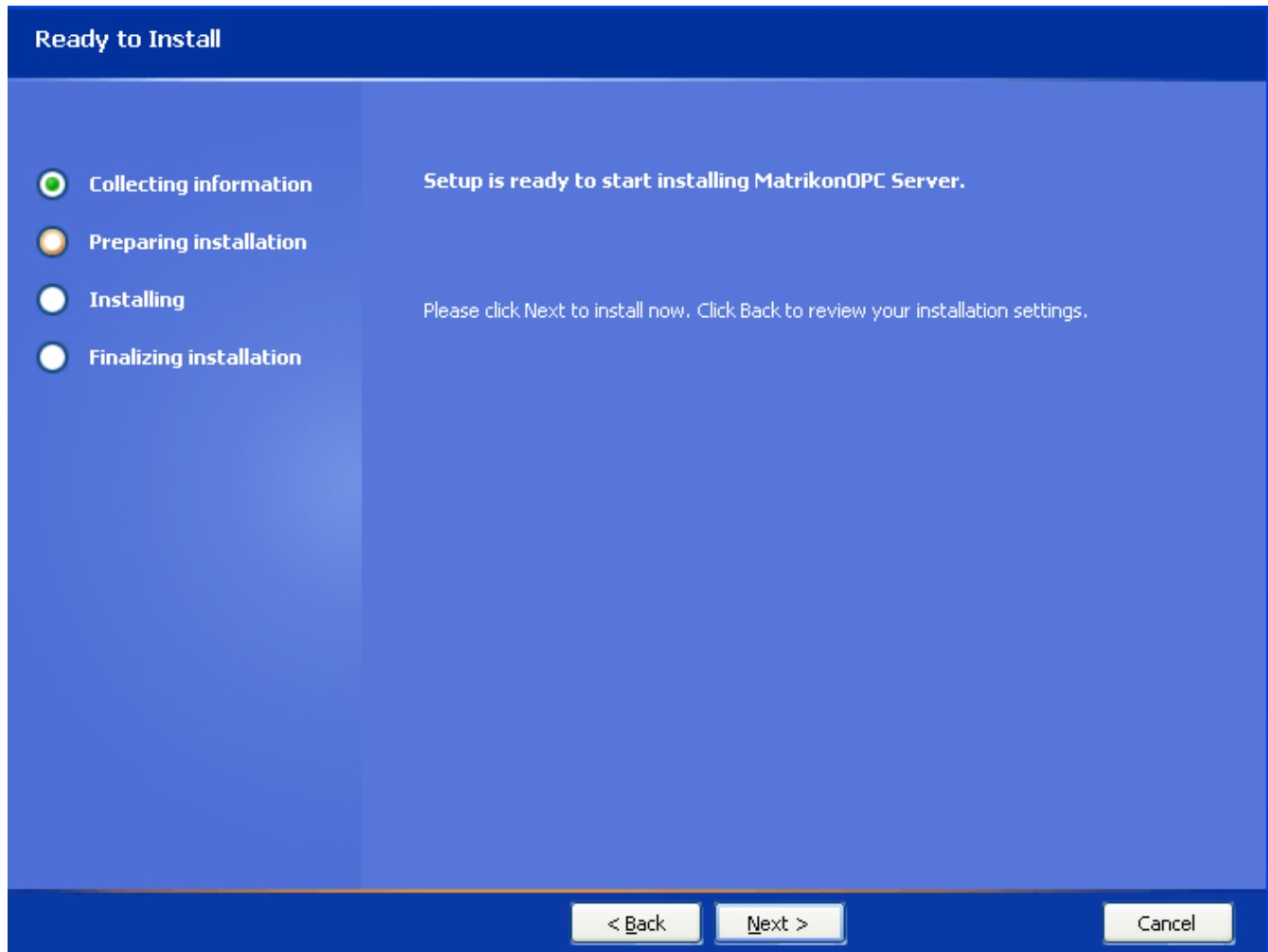


Figure 74 - Ready to Install Screen

19. Click on the **Next** button. The **Installing MatrikonOPC Server for IEC 61850/61400-25** screen (Figure 75) 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.

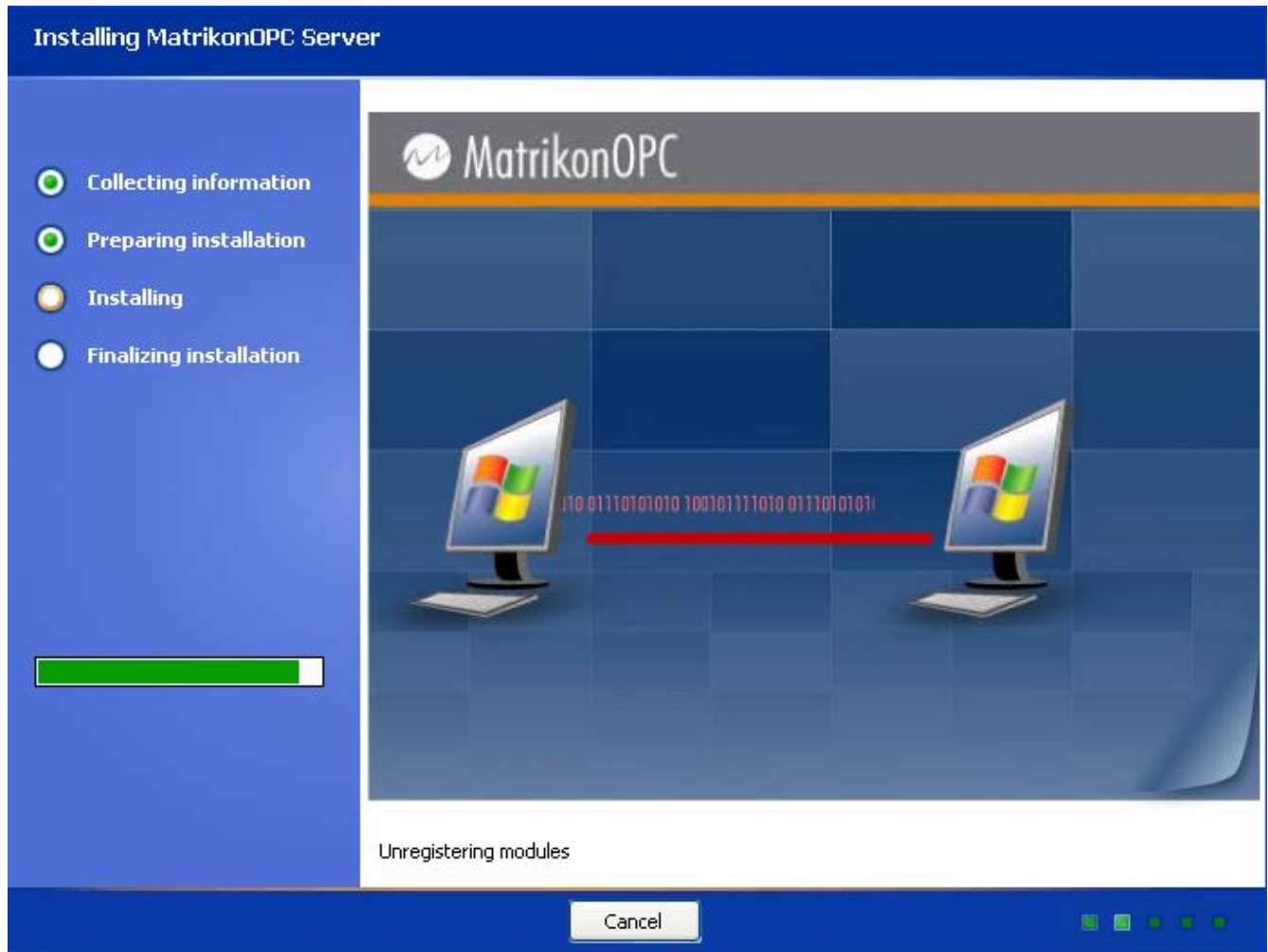


Figure 75 - Installing MatrikonOPC Server Screen

20. When the installation has finished, the **MatrikonOPC Server for IEC 61850/61400-25 Setup Complete** screen (Figure 76) appears stating that the MatrikonOPC server has been successfully installed.

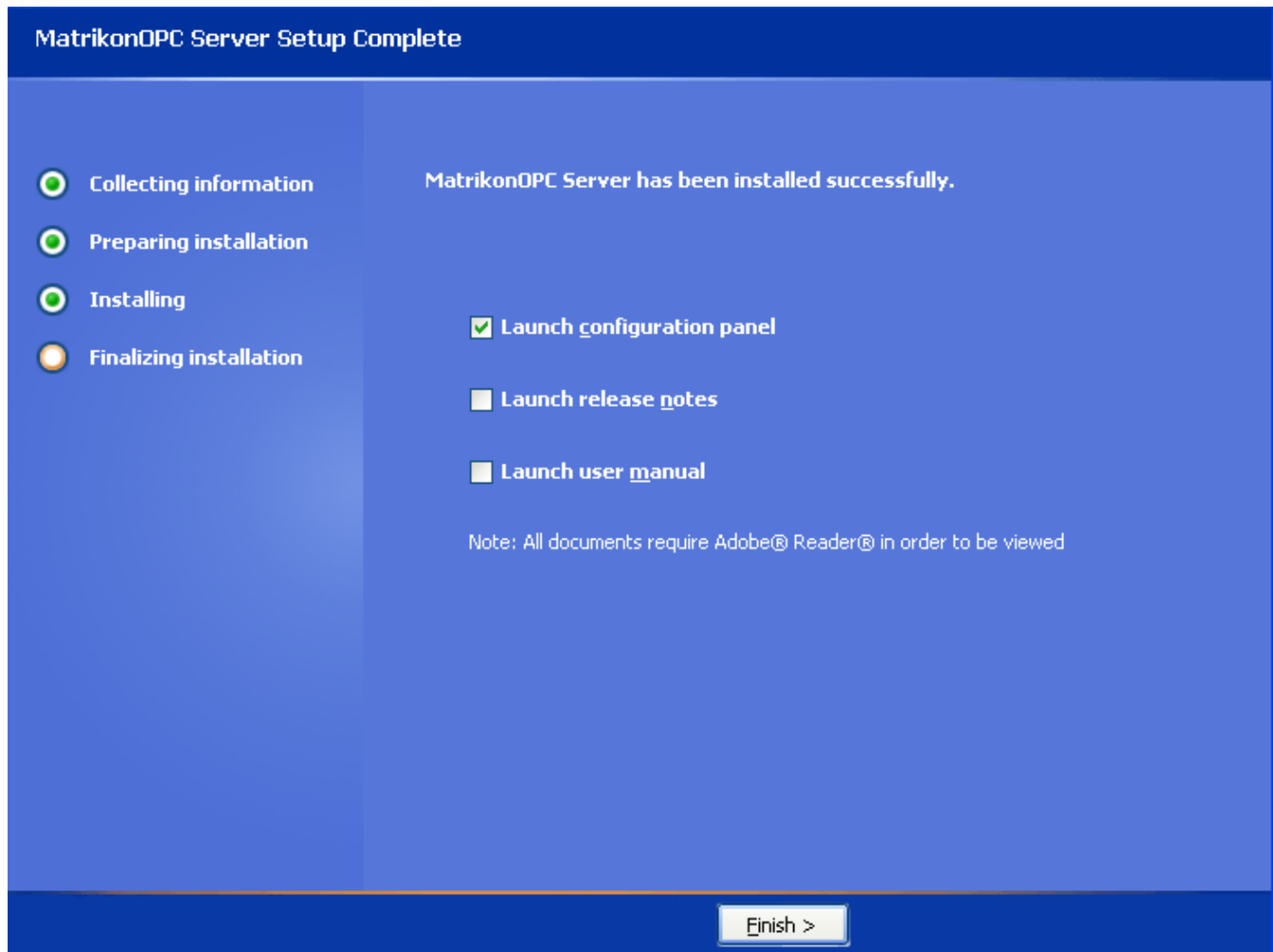


Figure 76 - MatrikonOPC Server Setup Complete Screen

21. 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

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

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



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

Appendix I 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 58 are installed by default, in the following location:

C:\Program Files\Matrikon\OPC\IEC61850

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.
Altova.dll AltovaXML.dll CalcEngine.dll CalcEngineResource.dll CalcEngineServerPS.dll CalcEngineWrapper.dll CalculationGraph.dll clipsdll.dll dbghelp.dll icudt40.dll icuin40.dll icuuc40.dll log4cxx.dll NetPortalQueryServerPS.dll OpcDataDelivery_u.dll ProcessNetDataDelivery.dll Scheduler.dll ScriptLibrary.dll xerces-c_2_8.dll	Calculation Engine binary files.
lsapiw32.dll RmsApiProxy.dll	Licensing engine files.
Licensing Procedures.pdf	<i>Licensing Procedures</i> document.
MatrikonOPC Server for IEC 61850_61400-25 Release Notes.pdf	<i>Release Notes</i> for this product.
MatrikonOPC Server for IEC 61850_61400-25 Quick Start Guide.pdf	<i>Quick Start Guide</i> for this product.
MatrikonOPC Server for IEC 61850_61400-25 User Manual.pdf	This <i>User's Manual</i> .
OPCIEC61850.exe	MatrikonOPC Server for IEC 61850/61400-25 executable.
ProgID.txt	Security information file used by the encryption utility.
PSTCFGIEC61850Lib.ocx	ActiveX configuration panels.

Table 58 - Files Installed in "IEC61850" Folder

The files listed in Table 59 are installed by default, in the following location:

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

File Name	Description
OPCAalyzer Logs\	Logs generated by MatrikonOPC Analyzer.
ACLConfig.exe	MatrikonOPC Tag Security Configuration Utility that configures tag-level security in MatrikonOPC servers.
EULA.pdf	License document.
OEM_Matrikon_OPC.dll	MatrikonOPC OEM Badge Library.
OPCAuto.dll	MatrikonOPC Automation Component – enables developers to access OPC data from client applications developed using Automation tools such as <i>Visual Basic</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 such as <i>Visual Basic</i> , <i>VBA</i> , and <i>VB Script</i> .
opchda10_auto.doc	Developer documentation for the HDA Automation Component.
opchda_ps.dll	The proxy-stub file to allow OPC Clients to make remote connections to an OPC HDA server.
OPCHDAAuto.dll	MatrikonOPC HDA Automation Component – enables developers to access OPC HDA data from client applications developed using Automation tools.
PSTCFG.exe	Matrikon Product Configuration Utility.
PSTCFGBasicInnerLayerLib.ocx	Server ActiveX configuration panel.
PSTCFGInterface.dll	Matrikon Product Configuration Library.
PSTcfgps.dll	Matrikon Product Configuration Marshalling Library.
PXPComfigps.dll	Matrikon Product Configuration Library.

Table 59 - Files Installed in "Common" Folder

The files listed in Table 60 are installed in the **WINDOWS\system32** folder:

File Name	Description
EXPREVAL.DLL	Expression Evaluation Library for Alias Equations.
OPC_AEPS.DLL	OPC Alarms and Events 1.0 Interfaces Marshalling Library.
OPCBC_PS.DLL	OPC Batch Custom 2.00 Proxy/Stub Library.
OPCCOMN_PS.DLL	OPC Common Interfaces and Marshalling Library.
OPCDXPS.DLL	OPC Data eXchange 1.00 Proxy/Stub Library.
OPCENUM.EXE	OPC Server List Component.
OPCHDA_PS.dll	OPC Historical Data Access 1.20 Proxy/Stub Library.
OPCPROXY.DLL	OPC Data Access 2.0 and 1.0a Interfaces and Marshalling Library.

File Name	Description
OPCSEC_PS.DLL	OPC Security 1.00 Proxy/Stub Library.
ACTXPRXY.DLL	ActiveX Interface Marshalling Library.

Table 60 - Files Installed in "system32" Folder

Appendix J Un-Installation

To successfully un-install MatrikonOPC Server for IEC 61850/61400-25, using the **Add or Remove Programs** from the Microsoft Windows **Control Panel** is recommended.

To un-install MatrikonOPC Server for IEC 61850/61400-25:

1. Click on the **Start** button and highlight the **Control Panel** item.
2. From the displayed menu, select **Add or Remove Programs**.
3. The **Add or Remove Programs** window (Figure 77) is displayed.
4. Scroll through the list of currently installed programs and updates to find and select **MatrikonOPC Server for IEC 61850/61400-25**.

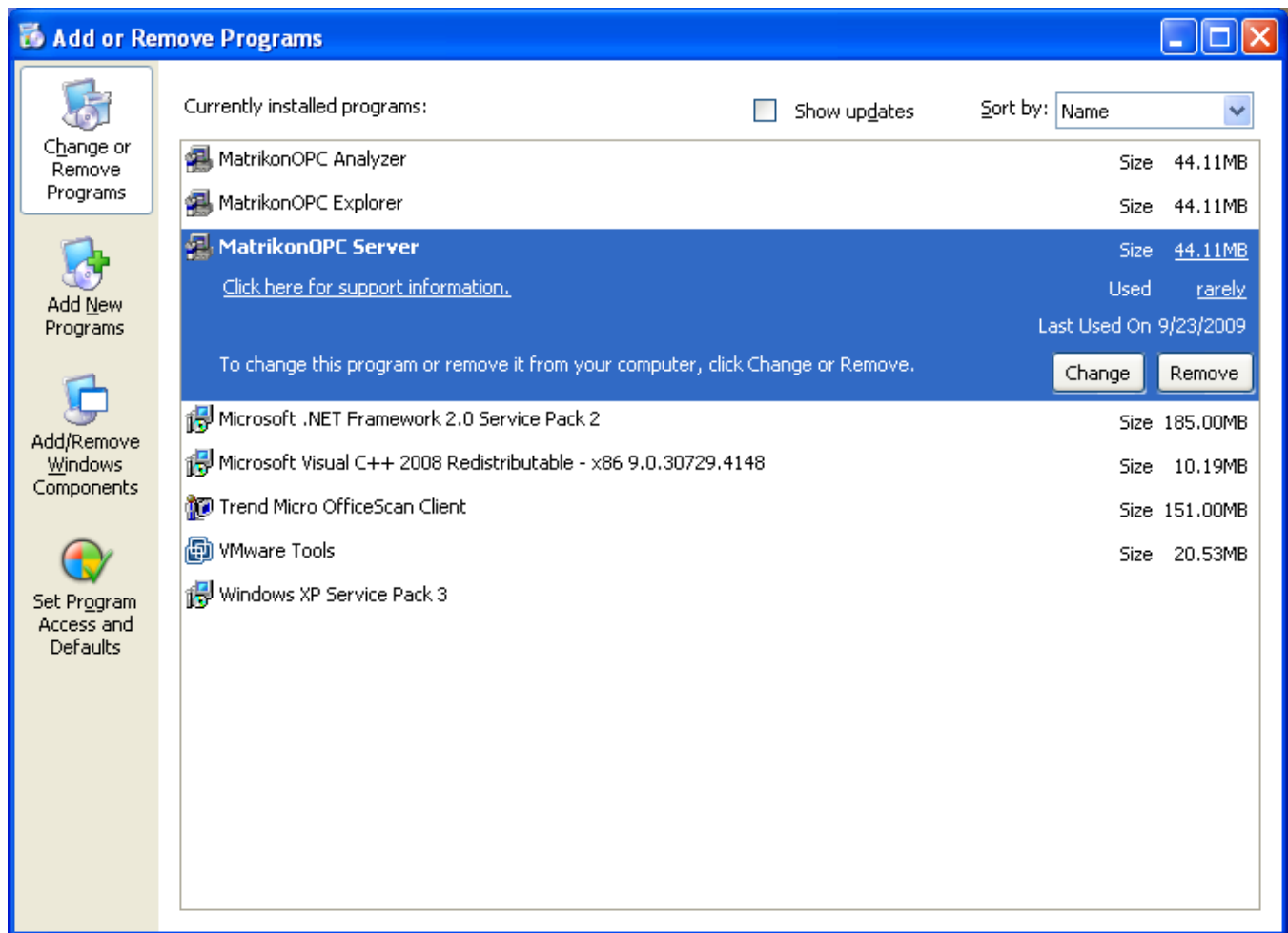


Figure 77 – Add or Remove Programs

5. Click on the **Remove** button associated with the MatrikonOPC Server for IEC 61850/61400-25 program to initiate the un-install process.
6. The **MatrikonOPC Server for IEC 61850/61400-25 – InstallAware Wizard** appears, and the **Welcome to MatrikonOPC Server for IEC 61850/61400-25 Maintenance** screen (Figure 78) is displayed.

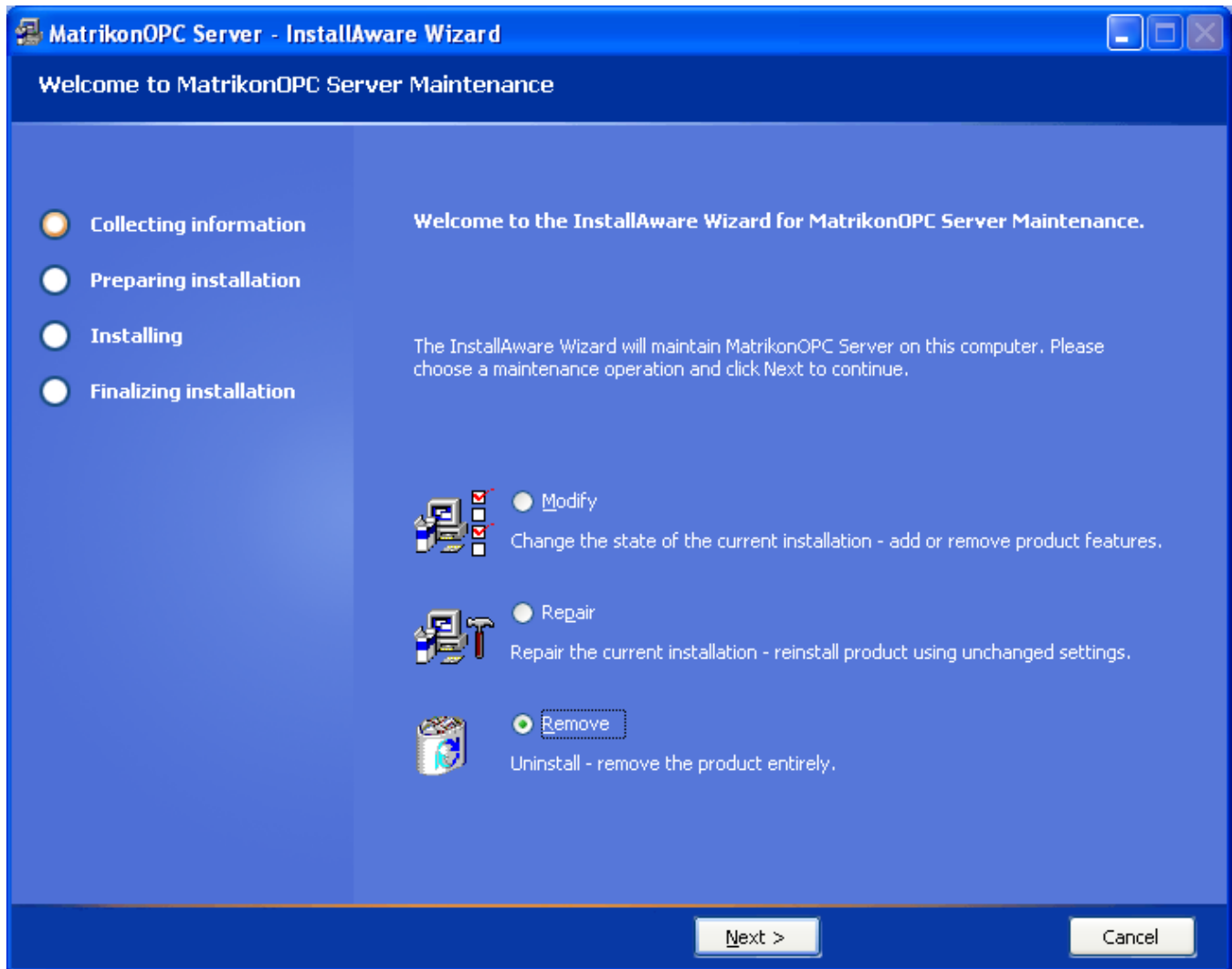


Figure 78 - Welcome to MatrikonOPC Server for IEC 61850/61400-25 Maintenance Screen

7. Select the **Remove** option button to un-install MatrikonOPC Server for IEC 61850/61400-25 entirely.
8. Click on the **Next** button. The **Ready to Uninstall** screen (Figure 79) is displayed.

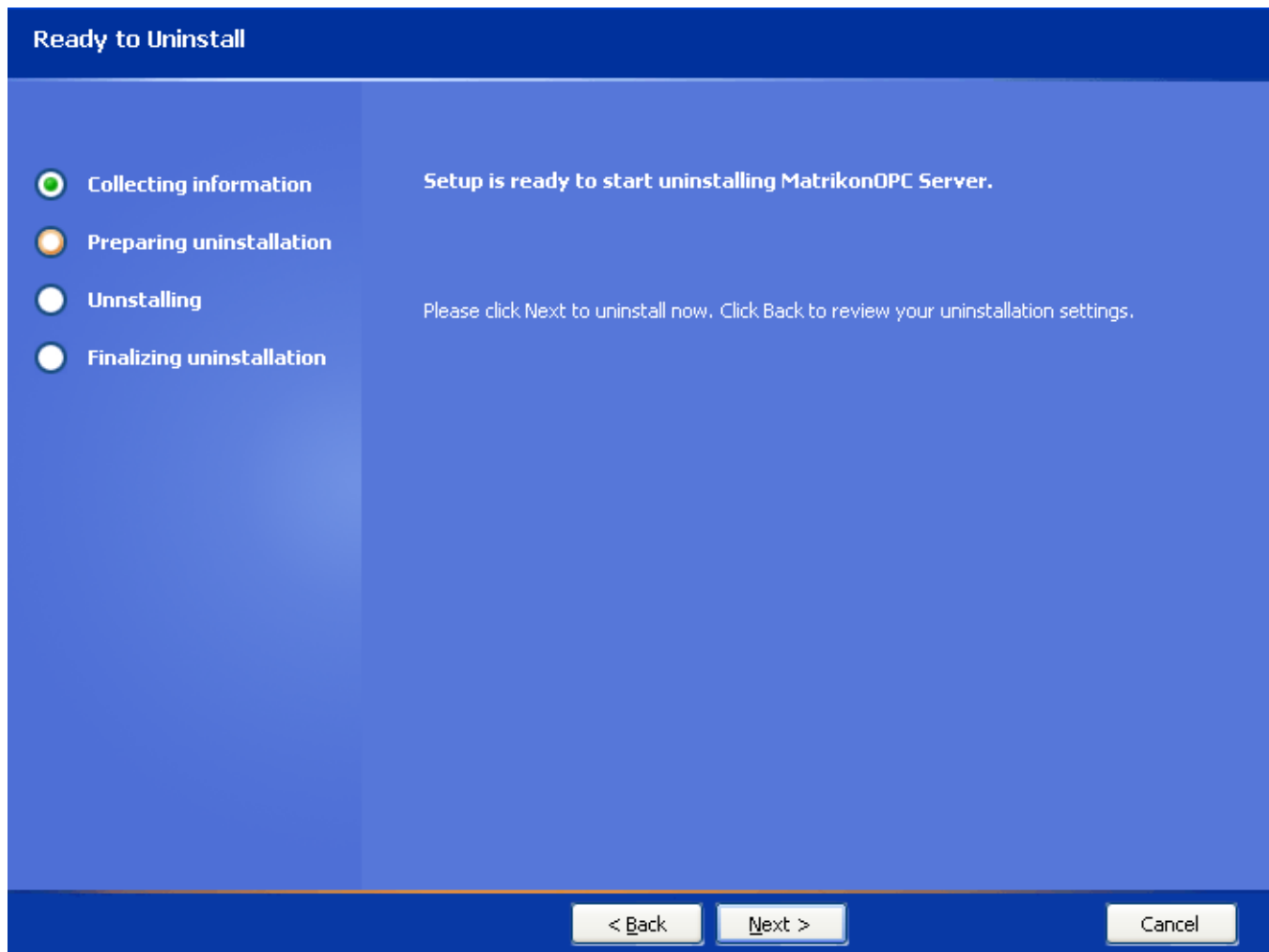


Figure 79 - Ready to Uninstall Screen

9. Click on the **Next** button.
10. The **Uninstalling MatrikonOPC Server for IEC 61850/61400-25** screen (Figure 80) appears and the un-install takes place.

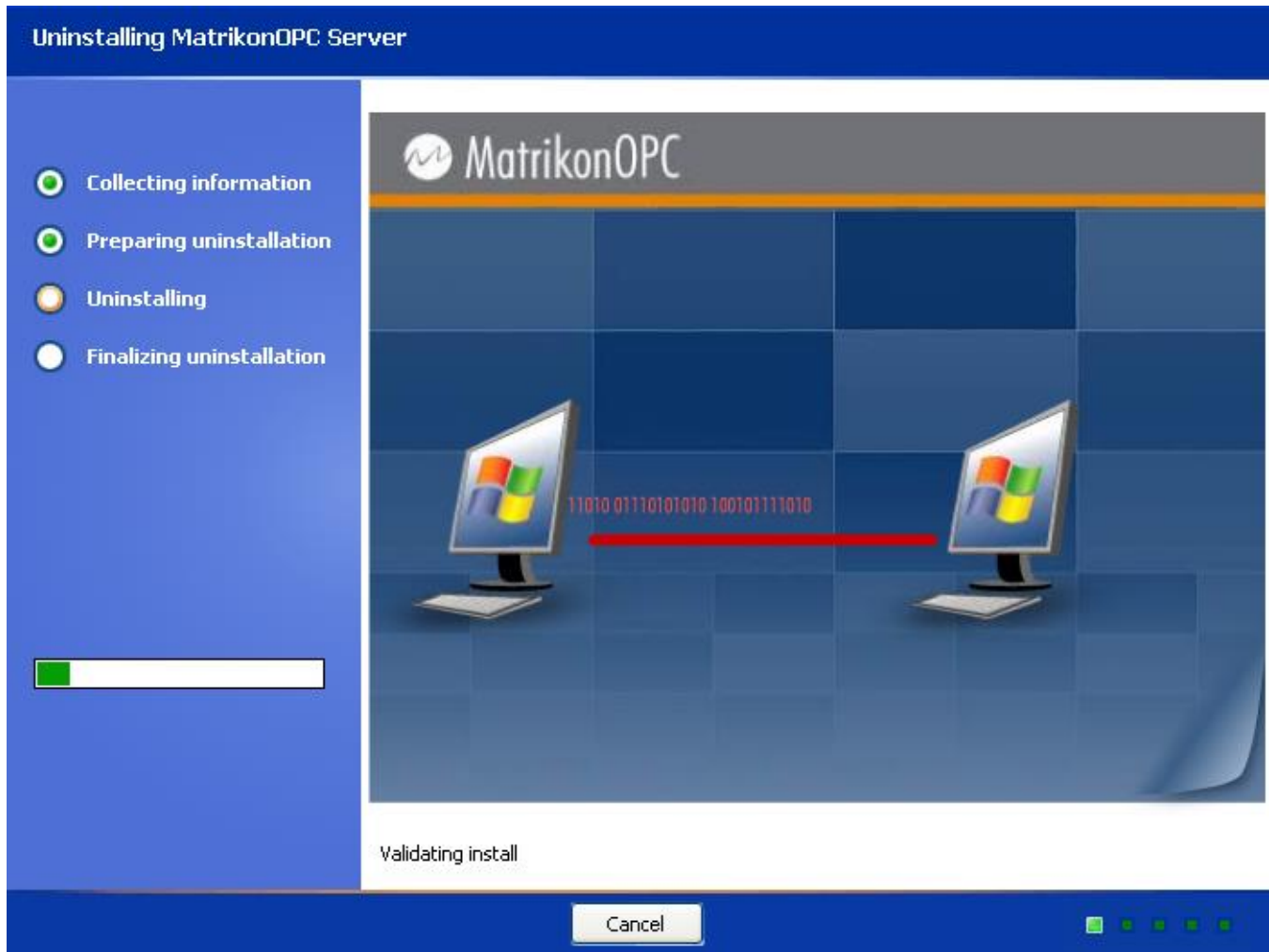


Figure 80 - Uninstalling MatrikonOPC Server for IEC 61850/61400-25 Screen

11. When the un-install has finished, the **MatrikonOPC Server for IEC 61850/61400-25 Setup Complete** screen (Figure 81) appears stating that MatrikonOPC Server for IEC 61850/61400-25 was successfully un-installed.

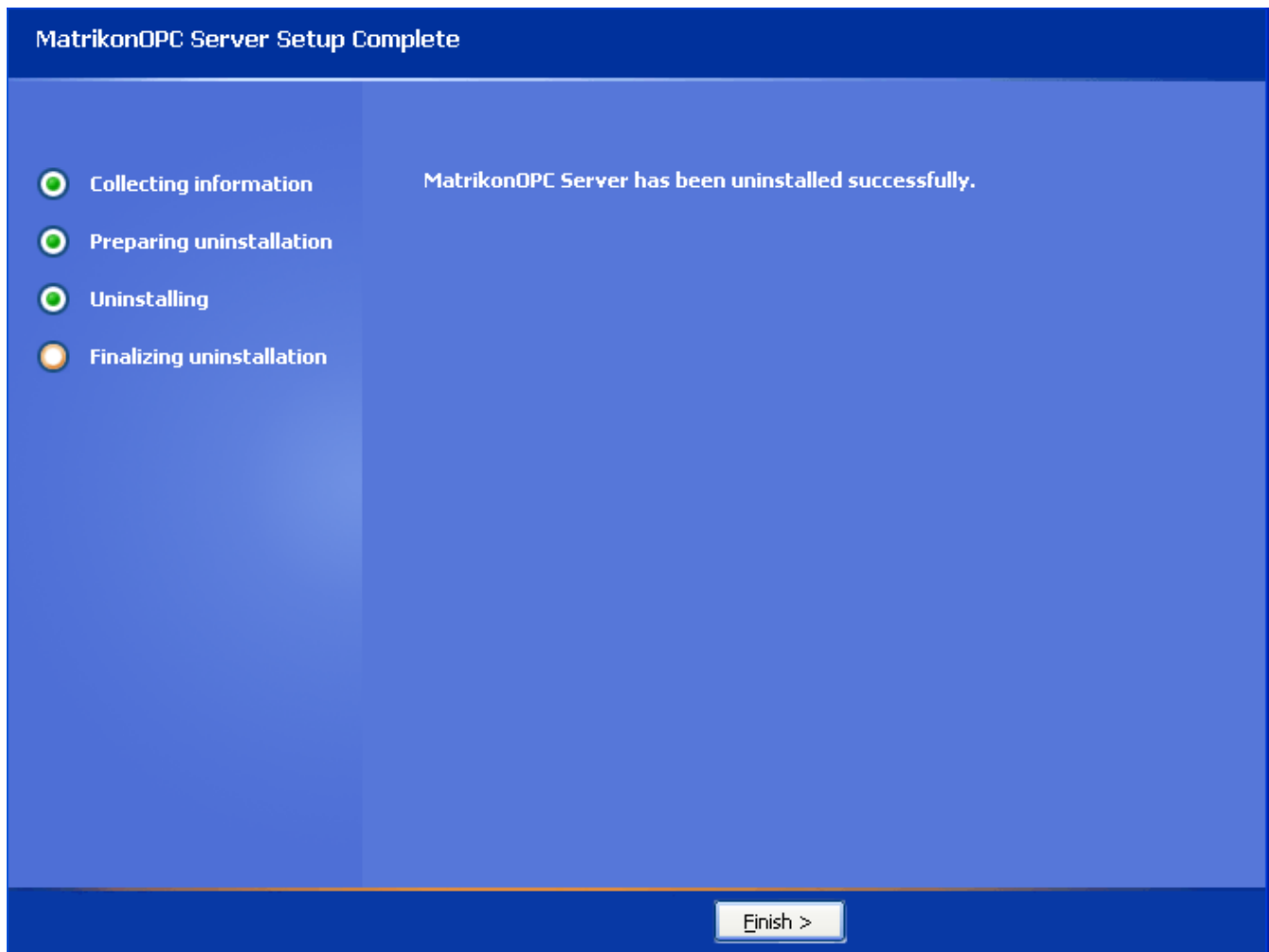


Figure 81 - MatrikonOPC Server for IEC 61850/61400-25 Setup Complete Screen

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.