Integration Objects'

Solution for Industrial Network Security and Connectivity

OPCNet Broker® DA HDA AE

Version 4.2 Rev.2



USER GUIDE

OPCNet Broker® User Guide Version 4.2 Rev 2
Published April 2026

Copyright © 2003-2026 Integration Objects. 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 the prior written permission of Integration Objects.

Windows®, Windows NT® and .NET are registered trademarks of Microsoft Corporation.

OPCNet Broker is a registered trademark of Integration Objects.

OPC Foundation Self-Tested for Compliance logo is a trademark of the OPC Foundation and may be used only by written permission of the OPC Foundation. Any unauthorized use of the Self-Tested for Compliance logo is prohibited.

OPC Foundation Self-Tested for Compliance logo indicates that this product has been tested by the manufacturer to be compliant with the following OPC Specification(s):
Data Access 2.05a/3.0
Historical Data Access 1.2
Alarms and Events 1.1

Additional information about compliance testing, logo program and a summary of test results are available at www.opcfoundation.org for the following Self-Tested Product(s):

OPCNet Broker DA v4.2.2
OPCNet Broker HDA v4.2.2
OPCNet Broker AE v4.2.2

TABLE OF CONTENTS

PREFACE **9**
INTRODUCTION **11**
1. OVERVIEW **11**
2. ARCHITECTURE **12**
3. ONB FEATURES **13**
4. OPC COMPATIBILITY **13**
5. SYSTEM REQUIREMENTS **13**
GETTING STARTED **15**
1. PRE-INSTALLATION CONSIDERATIONS **15**
2. INSTALLING AND RUNNING **15**
2.1. ONB Server Side *16*
2.1.1. Installing *16*
2.1.2. Start-up *16*
2.1.3. Logging *19*
2.2. ONB Client Side *20*
2.2.1. Installing *20*
2.2.2. Start-Up *20*
2.2.2.1. In-Process Context *21*
2.2.2.2. Out-Process Context *22*
2.2.3. Logging *28*
3. REMOVING ONB **28**
3.1. ONB Server Side *28*
3.2. ONB Client Side *28*
4. UPDATE EXISTING INSTALLATION **29**
CONFIGURATION **31**
1. ONB SERVER SIDE **31**
1.1. Communication Parameters *32*
1.2. Data Recovery *33*
1.2.1. Overview *33*
1.2.2. In-memory Recovery Option *34*
1.2.3. SQL Historian Recovery Option *36*
1.3. Security *42*
1.3.1. Overview *42*
1.3.2. User's Management –Server Side Authentication *43*
1.3.2.1. Add a Server Side Account *44*
1.3.2.2. Refresh Users List *45*
1.3.2.3. Remove a Server Side Account *45*

1.3.2.4. Set Password 46
1.3.2.5. Save Server Side Authentication Configuration 46
1.3.2.6. Cancel Server Side Authentication Current Configuration 46
1.3.3. User's Management –Client Side Authentication 46
1.3.3.1. Add a User Mapping 47
1.3.3.2. Edit an Existing User Mapping 48
1.3.3.3. Remove a User Mapping 49
1.3.3.4. Remove All 49
1.3.3.5. Use Default Server account for Non-Configured Users 49
1.3.3.6. Save Client Side Authentication Configuration 50
1.3.3.7. Cancel Client Side Authentication Current Configuration 50
1.3.4. Encryption Providers 50
1.3.5. Admin Credential 52
1.4. Credentials for User Account 53
1.5. Logging Options 54

2. ONB CLIENT SIDE 57

2.1. Session Management 60
2.2. OPC Server List Management 60
2.2.1. Adding ONB Connection 60
2.2.2. Adding ONB Connection Manually 65
2.2.3. Displaying/Modifying OPC Server Configuration 66
2.2.4. Removing An OPC Server 70
2.2.5. Removing ONB Connection 70
2.2.6. Clean ONB Connections 71
2.2.7. Refresh ONB Connection 71
2.3. Communication Configuration 72
2.4. Security Configuration 74
2.5. Displaying/Updating ONB Connection 77
2.6. Redundancy 79
2.6.1. Overview 79
2.6.2. Configuration 79
2.7. Automatic OPC Reconnection 83
2.7.1. Overview 83
2.7.2. OPC Reconnection Scenario 83
2.7.3. Configuration 85
2.8. Configure Authorized OPC Clients 87
2.9. Log Settings 88
2.10. License Status 90

USING OPCNET BROKER 91

1. OVERVIEW 91

2. REQUIRED STEPS 91

2.1. ONB Configuration 91
2.1.1. Default Mode 91
2.1.1.1. OPCNet Broker Server Side Configuration 91
2.1.1.2. OPCNet Broker Client Side Configuration 92
2.1.2. Using User Authentication 93
2.1.2.1. OPCNet Broker Server Side Configuration 93
2.1.2.2. OPCNet Broker Client Side Configuration 94
2.1.3. Compression Configuration 96

2.1.3.1. OPCNet Broker Server Side Configuration 96
2.1.3.2. OPCNet Broker Client Side Configuration 96
2.2. OPC Communication Through ONB 97

TABLE OF FIGURES

Figure 1: ONB Architecture 11
Figure 2: ONB Layers 12
Figure 3: OPCNet Broker Server Start Menu 16
Figure 4: ONB Server Tray Icon Menu 17
Figure 5: ONB Server Configuration Interface 18
Figure 6: OPCNet Broker Client Start Menu 20
Figure 7: Communication Parameters 23
Figure 8: Security and Reconnection Parameters 24
Figure 9: Clean the Machine from the ONB Connections 29
Figure 10: ONBS Tray Icon 31
Figure 11: ONBS Settings 32
Figure 12: Data Recovery Settings 34
Figure 13: In-memory Data Recovery 35
Figure 14: In-memory Buffer Configuration 35
Figure 15: SQL Historian Data Recovery 36
Figure 16: OPC DA Data Recovery Configuration from SQL 37
Figure 17: OPC AE Data Recovery Configuration from SQL 38
Figure 18: Map OPC AE Database Fields 39
Figure 19: Map OPC DA Database Fields 40
Figure 20: Clear Mapping 40
Figure 21: Clear all Mapped Fields 41
Figure 22: Security Settings 42
Figure 23: Server Side Users Management Tool 43
Figure 24: Add Users 44
Figure 25: User Password 44
Figure 26: Add Domain Account 45
Figure 27: Delete User 45
Figure 28: Set Password 46
Figure 29: Client Side Users Management Tool 47
Figure 30: Add User Mapping– Step 1 47
Figure 31: Add User Mapping – Step 2 48
Figure 32: Edit User Mapping 49
Figure 33: Configure Default User Mapping 50
Figure 34: Encryption Provider Configuration 50
Figure 35: Configuration of Padding & Cipher Modes 51
Figure 36: Choosing the Cipher Mode 51
Figure 37: ONB Login Window 52
Figure 38: Change Admin Credential 53
Figure 39: User Account Settings 54
Figure 40: Logging Settings 55
Figure 41: Select Folder Dialog 56
Figure 42: Log Levels 56

Figure 43: ONB Client Configuration Tool Admin Login 58
Figure 44: Admin Credential 58
Figure 45: Edit Admin Credential 59
Figure 46: ONB Client Configuration Tool – Main Window 59
Figure 47: Toolbar 60
Figure 48: ONB Client License Status 60
Figure 49: Browse Network 61
Figure 50: Security Mode 62
Figure 51: Advanced Settings 63
Figure 52: Added ONB Connection (Tree View) 64
Figure 53: Add ONB OPC Server Manually 66
Figure 54: OPC Server Properties 67
Figure 55: Remove ONB connection 70
Figure 56: Clean ONB Connections 71
Figure 57: Default Configuration 74
Figure 58: Encryption, Server Side Authentication Mode 75
Figure 59: Encryption, Client Side Authentication Mode 76
Figure 60: ONB Connection Properties 78
Figure 61: Set Redundant OPC Server 80
Figure 62: OPC Server Redundancy Service 82
Figure 63: OPC Reconnection - Connection Is Up 83
Figure 64: OPC Reconnection - OPC Server Goes Down 84
Figure 65: OPC Reconnection - Start Reconnection 84
Figure 66: Automatic Reconnection Settings 86
Figure 67: Authorized OPC Clients 87
Figure 68: Adding Authorized OPC Clients 87
Figure 69: Logging Settings Dialog 88
Figure 70: Log Levels 89
Figure 71: ONB Client License Status 90
Figure 72: Add ONB Connection Dialog 92
Figure 73: Security Settings Dialog 93
Figure 74: Add ONB Connection Using Security 94
Figure 75: Security Settings 95
Figure 76: Enable Compression 96
Figure 77: Outprocess Context 97
Figure 78: Connect to Tunneled OPC Server 98
Figure 79: ONB Communication Example 98

LIST OF TABLES

Table 1: Out-Process Context Parameters 27
Table 2: Communication Parameters for ONB Server 33
Table 3: User Mapping Fields 48
Table 4: Logging Parameters 57
Table 5: Add ONB Connection Fields 62
Table 6: Communication Parameters for ONB Client 74
Table 7: Security Settings 77
Table 8: ONB Client Log Parameters 90

PREFACE

ABOUT THIS USER GUIDE

This guide contains the following chapters:

- **Introduction**: Discusses the need for Integration Objects' OPCNet Broker, describes its main features and lists the system requirements for installing and running it.
- **Getting Started**: Explains how to install and run ONB components following a typical configuration.
- **Configuration**: Describes how to configure ONB on both the client and server sides.
- **Using OPCNet Broker:** Explains how to use, configure and run ONB for different scenarios.

TARGET AUDIENCE

This document is intended for Integration Objects' OPCNet Broker users. Basic knowledge of OPC DA (Data Access), OPC HDA (Historical Data Access) and OPC AE (Alarms & Events) standards is assumed.

DOCUMENT CONVENTIONS

Convention	Description
`Monospaced type`	Indicates a file reference
Bold	Click/selection action required
	Information to be noted
Italics	Measurements and Units
Blue bold italics	Reference to other sections, or to other Integration Objects User Guides

CUSTOMER SUPPORT SERVICES

Phone	Email
Americas: +1 713 609 9208 **Europe-Africa-Middle East** +216 71 195 360	Support: customerservice@integrationobjects.com Sales: sales@integrationobjects.com Online: www.integrationobjects.com

INTRODUCTION

OPCNet Broker (ONB) ensures fast, reliable and secure OPC remote communication by overcoming DCOM bottlenecks. This manual describes DCOM's limitations and shows how OPCNet Broker can securely enable OPC communication in distributed networks, even through firewalls and multiple domains.

1. Overview

Microsoft DCOM represents a significant configuration challenge when the OPC Client and Server applications are installed on two separate machines. DCOM configuration becomes even more difficult when running through different WANs, domains and the Internet, as this technology is neither Internet-friendly nor firewall-friendly. How to overcome DCOM configuration complexity becomes a challenge for OPC developers.

OPCNet Broker is Integration Objects' solution to bypass these DCOM headaches and improve the existing distributed systems.

ONB is a software layer composed of two parts:

1. ONB Server side
2. ONB Client side

These components should be installed between existing OPC Server and OPC Client as shown in the following diagram:

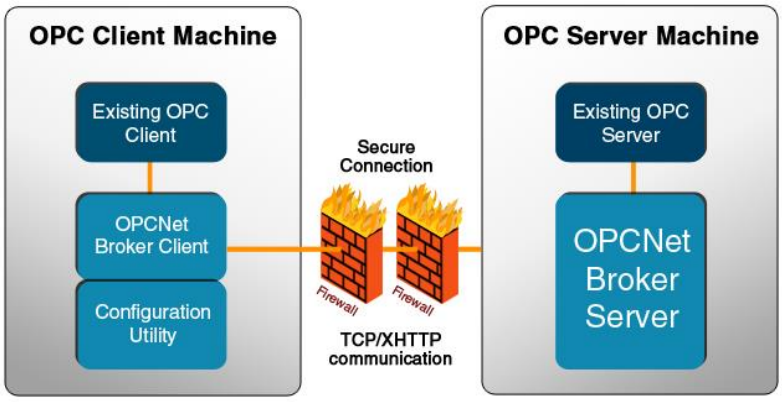


Figure 1: ONB Architecture

2. Architecture

The OPCNet Broker Client layer (ONB-C) should be installed on the same machine as the OPC client(s) (Node A) to enable local access to remote OPC DA/HDA/AE servers.

The OPCNet Broker Server layer (ONB-S) should be installed on the same machine as the OPC server(s) (Node B).

ONB-S manages communications with all OPC DA/HDA/AE servers registered on the same machine (Node B). ONB-C and ONB-S can communicate through **TCP** or **XHTTP** protocols. ONB communications can be performed in a **secured mode**.

The following is a global architecture of OPCNet Broker:

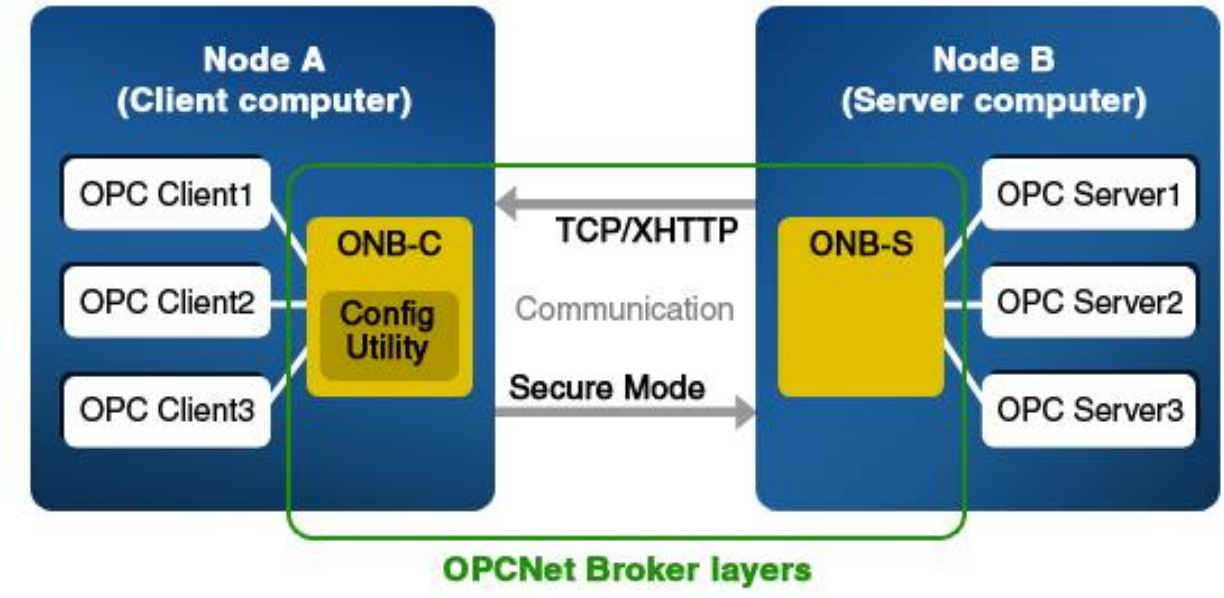


Figure 2: ONB Layers

OPCNet Broker can communicate with any OPC client supporting in-process or out-process servers. How to use ONB with in-process or out-process servers is described in the following sections. In fact, for in-process servers, the existing OPC Client will communicate with OPC servers that had been **locally registered** using the OPCNet Broker Configuration Utility.

- For out-process OPC DA servers, the existing OPC DA Client will communicate with the Integration Objects OPCNet Broker OPC DA Server "IntegrationObjects.OPCNetBroker.1".

- The existing OPC HDA Client will communicate with the OPC HDA Server "IntegrationObjects.OPCHDANetBroker.1".

- The OPC AE Client will communicate with the OPC AE server "IntegrationObjects.OPCAENetBroker.1".

The "IntegrationObjects.OPCNetBroker.1", "IntegrationObjects.OPCHDANetBroker.1" and "IntegrationObjects.OPCAENetBroker.1" Servers are **registered locally** in the OPC Client machine.

3. ONB Features

ONB ensures fast, reliable and secure OPC remote communication by overcoming DCOM complexity and limitations.

This easy-to-deploy and maintainable solution allows you to:

- Track client/server communications and limit the number of opened ports within your firewalls to minimize security holes.
- Configure your communication schema with less complexity.
- Connect OPC components from different domains.
- Define access privilege policies for OPC servers and OPC tags.
- Define secure OPC clients list.
- Secure the OPC communications using encryption & authorization modes.
- Enable accessibility for clients behind NAT, firewall and proxy.
- Benefit from guaranteed call timeout.
- Establish data transmission in a secure mode:
    - Data integrity by using encryption/decryption.
    - User authentication to avoid unauthorized access.
- Benefit from point and click graphical user interface (GUI) for configuring:
    - ONB connections.
    - OPC server and tags security.
- Ensure automatic ONB reconnection within a specified TimeSpan whenever the network link is broken.
- Ensure automatic OPC reconnection if the OPC connection is lost.
- Display event log messages for both Server and Client components.
- Support and manage remote connections in a transparent way.
- Manage redundant OPC servers.

4. OPC Compatibility

Currently, ONB supports OPC Data Access (DA) 2.05 and 3.0, OPC Historical Data Access (HDA) 1.1 and 1.2 and OPC Alarms and Events (AE) 1.10.

5. System Requirements

OPCNet Broker was successfully installed and executed under the following operating systems:

- Windows XP
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

For DA communication:

- The OPC client machine must have an OPC DA 2.05/3.0 client and the OPC server machine an OPC DA 2.05/3.0 server.

For HDA communication:

- The OPC client machine must have an OPC HDA 1.2 client and the OPC server machine an OPC HDA 1.2 server.

For AE communication:

- The OPC client machine must have an OPC AE 1.1 client and the OPC server machine an OPC AE 1.1 server.

Integration Objects' free OPC DA/A&E clients and HDA demo clients are available on our website: https://www.integrationobjects.com/.

GETTING STARTED

1. Pre-Installation Considerations

In order to properly run the ONB-S and ONB-C, install these software components on both OPC server and client computers:

- Microsoft .NET Framework version 4 or 2 depending on your Windows OS version

  o Deploy OPCNet Broker supporting .Net Framework version 4.0 for Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows 7, Windows 8, Windows 10 and Windows 11.

  o Deploy OPCNet Broker supporting .Net Framework version 2.0 for Windows Server 2003 and Windows XP.

- OPC Core Components, which consists of all shared OPC modules including the DCOM proxy/stub libraries, the OPC Server Enumerator, .NET wrappers, etc.

  You may install the OPC Core Components 2.00 Redistributable 1.06 delivered with the current package or download it from the OPC Foundation website.



- **In addition to the above components, MDAC (Microsoft Data Access Components) should be installed on the server side.**
- **The OPCNet Broker Server side should be installed on the same machine as the OPC server.**
- **The OPCNet Broker Client side should be installed on the same machine as the OPC client.**

2. Installing and Running

This section explains how to install and run the OPCNet Broker components on both the server and the client sides.



The ONB Server Side and ONB Client Side must use the same software version in order to establish communications.

2.1. ONB Server Side

2.1.1. Installing

To install the ONB Server Side:

1. Open the downloaded package, right click on the ONB-S Setup file and select “Run as administrator” from the displayed menu.
2. Follow the installation wizard as it guides you through the different setup steps.
3. If OPC Core Components are not installed on your machine, check the **Install OPC Core Components** option.
4. Click **Finish**.

The installation copies all necessary files to the target folder, creates a shortcut icon to launch the ONB Server from the start menu and makes an un-installation entry in the Add/Remove Programs Window in the Control Panel.

2.1.2. Start-up

The OPCNet Broker Server is started manually from the start menu.
To manually start the ONB Server, click on **Start ➔ Programs ➔ Integration Objects ➔ OPC Gateway ➔ OPCNet Broker ➔ Server ➔ OPCNet Broker Server Side**



Figure 3: OPCNet Broker Server Start Menu

When starting, a small icon appears in the tool tray at the right-hand side of the Task Bar. Right click on the icon to display the following menu.

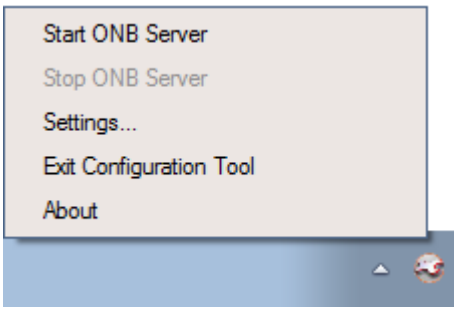


Figure 4: ONB Server Tray Icon Menu

Using this menu, you can manage the ONB Server (start, stop and configure all server parameters).

Click on **Start ONB Server** to launch the ONB Server service. Otherwise, invoke the Service Control Manager and start the ONB Server service “Integration Objects’ OPCNet Broker Server”.

Click on **Stop ONB Server** to stop the ONB Server service.

Note that the ONB Server tray icon menu is updated dynamically according to the ONB Server status (running, stopped, hidden or shown).

Click on **Settings** to configure the ONB Server. These settings include communication, security, user account and logging. You can refer to the ***Configuration*** chapter for details. The displayed configuration interface is shown below:

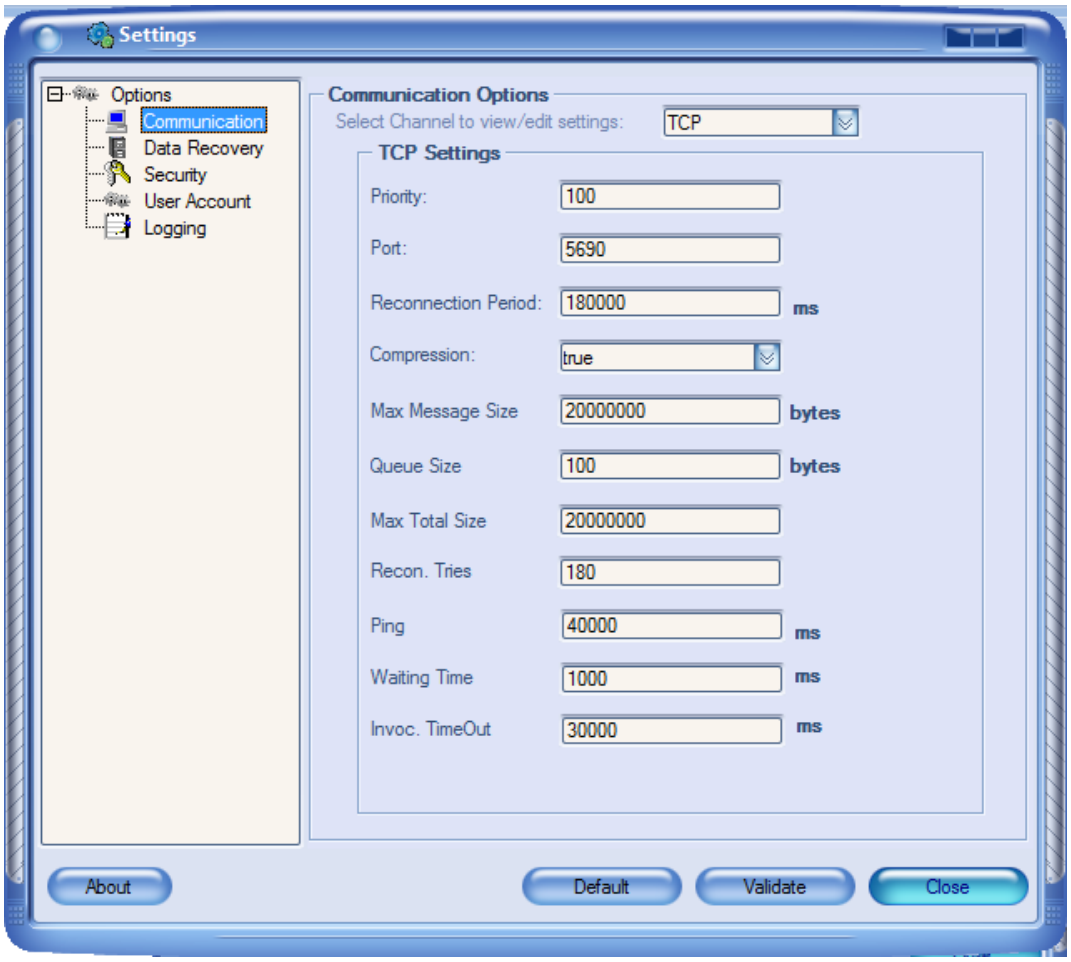


Figure 5: ONB Server Configuration Interface

Click **Exit Configuration Tool** to exit the ONB Server configuration tool without stopping the server.

Click **About** to show the ONB Server version.

Before starting the ONB Server, configure the following using the configuration interface:

- Communication parameters: Click on **Options➔ Communication** and set the ports numbers for both channels TCP and XHTTP. The XHTTP channel is disabled by default.

- Data Recovery parameters: Click on **Options➔ Data Recovery** and configure your data recovery option.

- Security parameters: Click on **Options ➔ Security** and check/uncheck the **Require ONB Client authentication** option to accept/reject unsecured communications.

- If you need to configure the ONB Server to use security policies, define user accounts using the users management tool found in **Options➔ Security**.

- You can configure the encryption provider by selecting **Zero Proof Authorization** or **Symmetric Algorithm**. This option can be found in **Options➔ Security**.

- In case you enabled the OPC Tag Security by checking the **Enable OPC Tag Security** option, configure access permissions to OPC servers and OPC tags using the OPC Tag Security tool.



OPC Tag Security is an add-on to ONB and is disabled by default. You can refer to the *OPC Tag Security User Manual* for more details.

ONB Server Configuration is described in more details in the ***Configuration*** chapter.



1. **The ONB Server should be started before any ONB client connection attempt.**
2. **If you make any change in your OPC Tag Security configuration, you should restart the ONB Server.**

2.1.3. LOGGING

The ONB Server produces the **ONBS_Log.log** default log file under the OPCNet Broker Server installation folder. This file records errors and debugging information for the server.

All service events are also recorded in the Application Event Viewer under the **ONB.Service** source.

If any difficulties occur with the ONB Server, these recorded messages can be extremely valuable for troubleshooting. Under normal operations, the server logs contain very little information.

Logging parameters can be changed at start-up by using the ONB Server configuration interface.

2.2. ONB CLIENT SIDE

2.2.1. INSTALLING

To install the ONB Client Side component:

1. Open the downloaded package, right click on the ONB-C Setup file and select “Run as administrator” from the displayed menu.
2. Follow the installation wizard as it guides you through the different setup steps.
3. If the OPC Core Components is not installed on your machine, check the **Install OPC Core Components** option.
4. Click **Finish**.



Make sure that .NET Framework is installed before proceeding to the ONB Client installation. Refer to the pre-installation considerations section for more details.

The installation copies all necessary files to the target folder, creates a shortcut icon to launch the OPCNet Broker Client Configuration Tool from the start menu and makes an uninstall entry in the Add/Remove Programs Window in the Control Panel to remove all ONB Client components.

Click on **Start ➔ Programs ➔ Integration Objects ➔ OPC Gateway ➔ OPCNet Broker ➔ Client ➔ ONB Client Configuration Tool.**

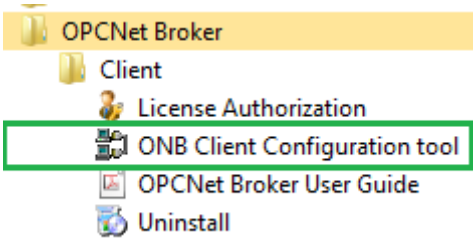


Figure 6: OPCNet Broker Client Start Menu

2.2.2. START-UP

We will assume that you have properly configured the ONB Server side as described in ***section 2.1***. Now, you need to connect to a remote OPC Server from your machine.

This section explains how to configure the ONB Client Side (ONB-C) and start communication through ONB by using your existing OPC client.

ONB Client Side (ONB-C) configuration depends on the manner your OPC client connects to OPC servers: in-process or out-process context.

2.2.2.1. IN-PROCESS CONTEXT

If your OPC client supports connection to in-process servers, follow these instructions:

1. Make sure that the target ONB Server is started properly.
2. Run the ONB Client Configuration Tool using an administrator account:
   a. Open a new session.
   b. Click on the **ONB Connections** root node and check if any previous ONB connection to the target machine that holds the ONB Server is already configured.
   c. If this is your first utilization of the OPCNet Broker Client or the ONB connection is not shown in the ONB Connections list, add a new ONB connection (see the ***Configuration*** chapter for more details).
   d. Configure the communication parameters. You may keep the default values.
   e. Configure the security parameters if you need secure ONB communication. In this case, carefully enter the user credentials: the Login and Password parameters. None of these parameters can be left empty. The transmitted data will be encrypted.
   f. Check that the target OPC server exists in the ONB connection servers list. If not, refresh the servers list (click on the **ONB Connection ➔ Refresh** menu or press the related button from the toolbar).
3. Close the Configuration Tool.



Only use the Configuration Tool to configure a new ONB Connection or to refresh an existing one.

4. Run your OPC DA/HDA/AE client and select the target OPC Server within the local OPC Servers list with a new assigned server name.

Refer to the ***Configuration*** chapter to successfully perform Step 2.
The steps above are described with more details in the ***Using OPCNet Broker*** chapter (OPC DA example).



Steps 2 and 3 can be skipped if the target ONB connection is already configured and contains the target OPC server.

2.2.2.2. OUT-PROCESS CONTEXT

If your OPC client does not support connections to in-process servers and only connects to out-process servers, follow these instructions:

1. Click on **ONB Connection,** then **Settings** and finally choose **Out-Process Context.** You will get a window that allows you to configure communication and security and reconnection parameters. The two figures below show a sample for client configuration:

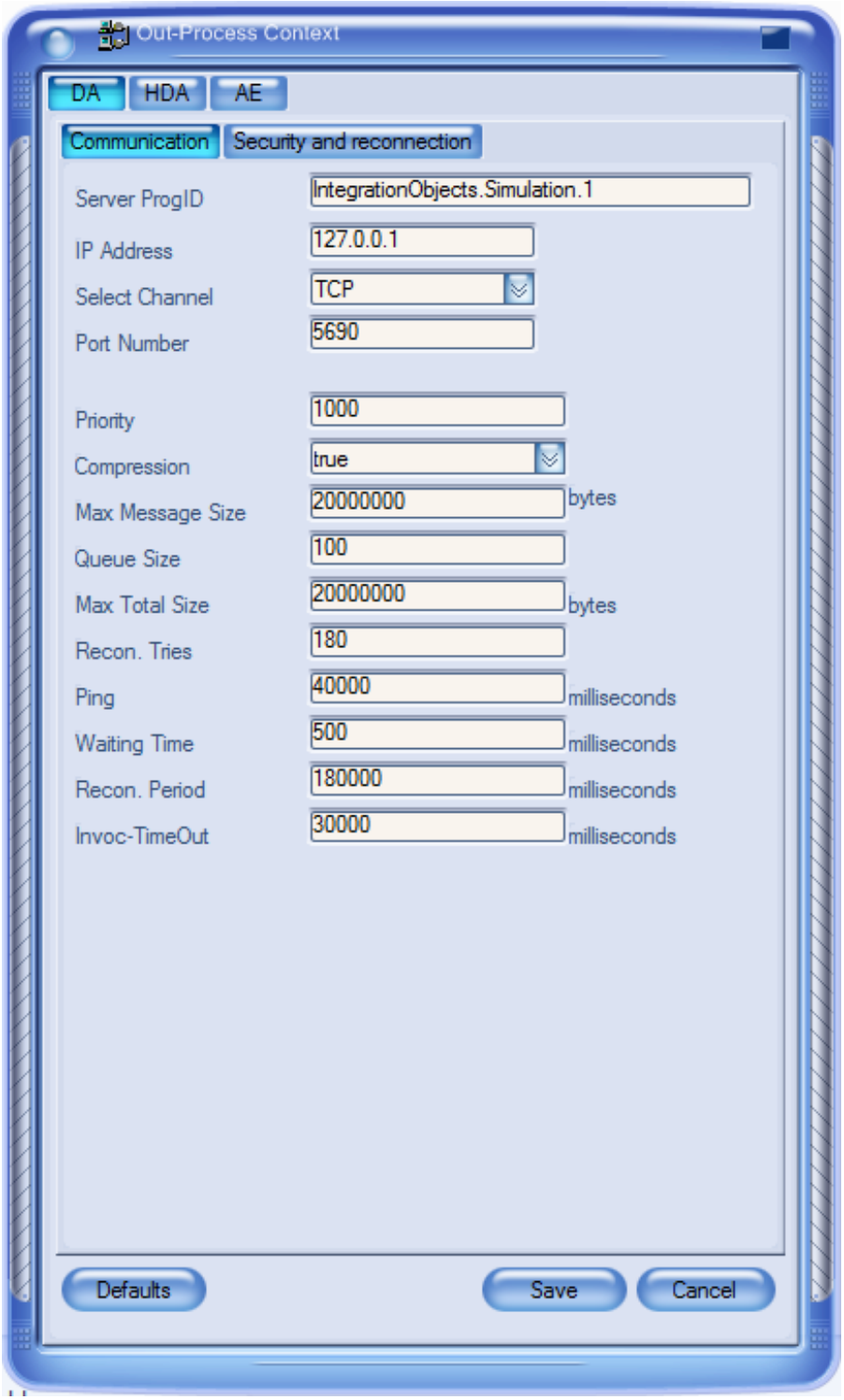


Figure 7: Communication Parameters

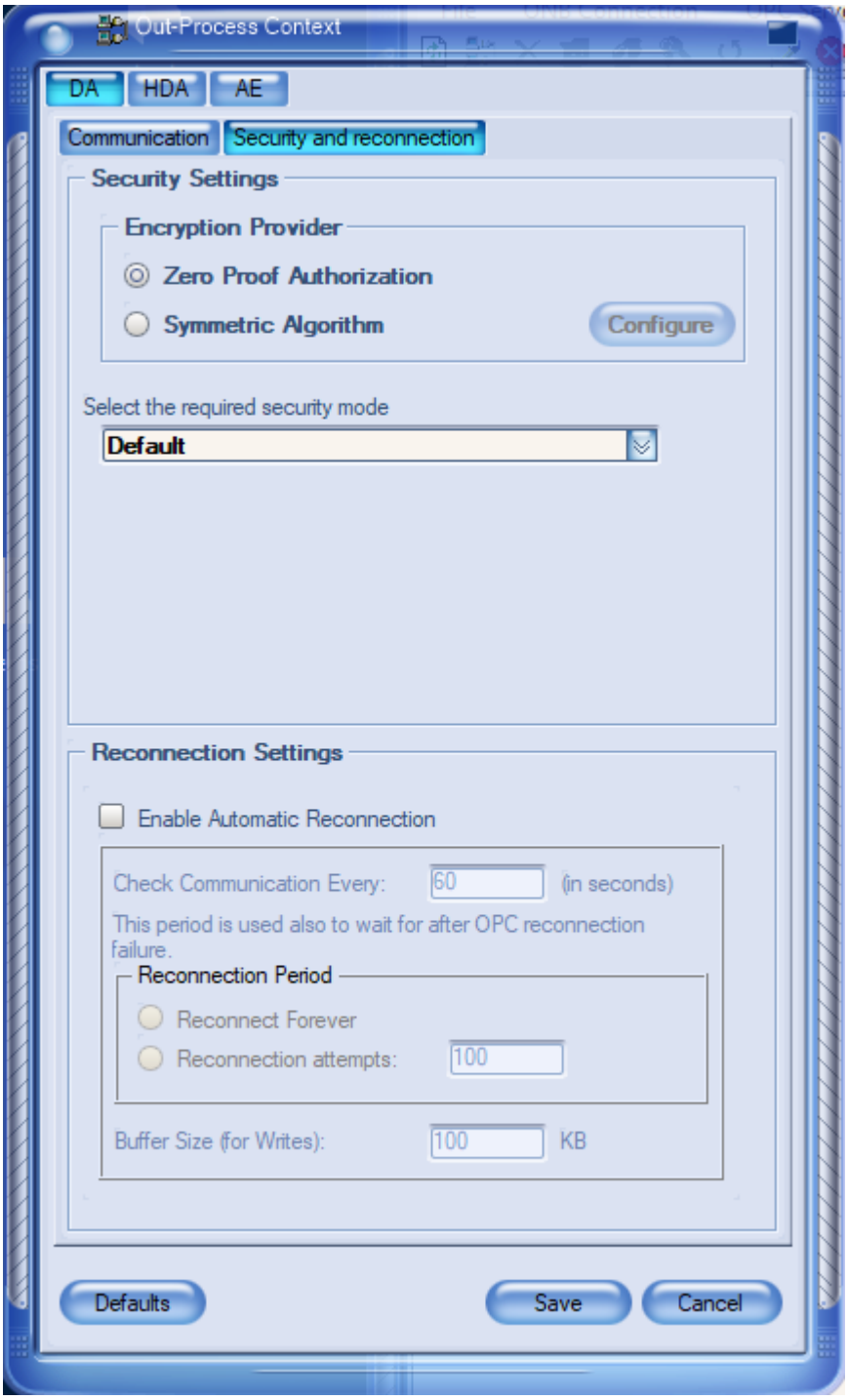


Figure 8: Security and Reconnection Parameters

The following table explains all the parameters shown in the previous figures.

Parameter	Description	Default Value
Server ProgID	The requested OPC server name.	
IP Address	The IP Address/Hostname of the remote host holding the OPC Server.	127.0.0.1
Channel	The channel to use for data transmission via ONB. Possible values: • TCP channel • XHTTP channel	TCP
Port	The port to use for data transmission.	5690 for TCP 5790 for XHTTP
Priority	An integer value representing the priority assigned to this connection. The higher the priority is, the higher is the chance for this connection to be established first.	1000
Compression	This parameter takes one of these values: • True: Data will be compressed. • False: No compression feature.	true
Max Message Size	The maximum size of a message transmitted in the communication. *Unit = bytes*	20000000
Queue Size	The total number of queued messages.	100
Max Total Size	The maximum total size of queued messages. *Unit = bytes*	20000000

Recon. Tries	The number of reconnection attempts before declaring that the ONB Server connection is lost.	180
Ping	ONB Client sends ping message to the ONB Server within this ping time. *Unit = milliseconds*	40000
Waiting Time	The time to wait after every reconnection failure. *Unit = milliseconds*	500
Recon. Period	When the ONB server connection is broken, it is expected to re-establish the connection within the specified time interval. Otherwise, the ONB client declares the ONB connection as closed. *Unit = milliseconds*	180000
Invoc-TimeOut	The ONB request is recognized as failed when the ONB Client does not receive a response from the ONB Server within this time period. *Unit = milliseconds*	30000
Security Mode	This parameter indicates whether the communication will be performed using one of the security mode. Possible values: • Default • Encryption, Server Side Authentication Mode • Encryption, Client Side Authentication Mode	Default
Credential	Specifies the network credentials. ONB takes this parameter into consideration when the security mode is set to “Encryption, Server Side Authentication” Mode. Communications will be performed using	

	credentials specified by the following: • Login • Password	
Login	The login. This should be an NT user account.	
Password	The password. This can be the NT password set by the Windows administrator or a custom password.	
Automatic reconnection	This parameter indicates whether the OPC reconnection is enabled or not. By default, OPC reconnection is disabled .	Disabled
OPC Reconnection Tries	The reconnection attempts' number.	100
OPC Reconnection Period	The period to wait for between OPC reconnection attempts. *Unit = seconds*	60
Buffer Size	The buffer size to use for stored writes during the period when the OPC Server is down. *Unit = kilobytes*	100

Table 1: Out-Process Context Parameters



At the very least, the underlined parameters, such as Server ProgId, should be set. In case you are using security:

a. **The password cannot be empty.**
b. **(Login, Password) pair should be valid. That means it is the same credentials configured at the ONB Server side.**

2. Click on the server name **IntegrationObjects.OPCNetBroker.1** existing in the local OPC Servers list after Out-Process configuration.
    - For DA communication:
        1. Run your OPC DA client.

2. Click on the server name **IntegrationObjects.OPCNetBroker.1** figuring in the local OPC Servers list.

- For HDA communication:
  1. Run your OPC HDA client.
  2. Click on the server name **IntegrationObjects.OPCHDANetBroker.1** from the local OPC Servers list.
- For AE communication:
  1. Run your OPC AE client.
  2. Click on the server name **IntegrationObjects.OPCAENetBroker.1** from the local OPC Servers list.

2.2.3. LOGGING

Like the server side, ONB-C generates a log events file under the ONB Client installation directory with a LOG file extension.

You can configure log parameters through the configuration tool (refer to the ***Configuration*** chapter).

3. Removing ONB

This section deals with OPCNet Broker un-installation.

3.1. ONB SERVER SIDE

To remove the ONB server from your machine, click on the **Uninstaller** shortcut icon from the start menu.

The ONB Server can also be removed manually as follows:

1. Click on **Start**.
2. Click on **Settings**.
3. Click on **Control Panel**.
4. Click on **Add/Remove Programs**.
5. In Add/Remove Programs dialog screen, select **Integration Objects OPCNet Broker Server Side**.
6. Click on **Change/Remove**, then **OK**.

3.2. ONB CLIENT SIDE

To remove the ONB client from your machine, click on the **Uninstaller** shortcut icon from the start menu.

The ONB Client can also be removed manually as follows:

1. Click **Start.**
2. Click **Settings**.
3. Click **Control Panel**.
4. Click **Add/Remove Programs.**
5. In Add/Remove Programs dialog screen, select **Integration Objects OPCNet Broker Client Side**.
6. Click **Change/Remove**, then **OK**.

When removing the ONB Client the Setup wizard will give you, as shown in the following figure, the option to remove the configured ONB Connections from the windows registry.

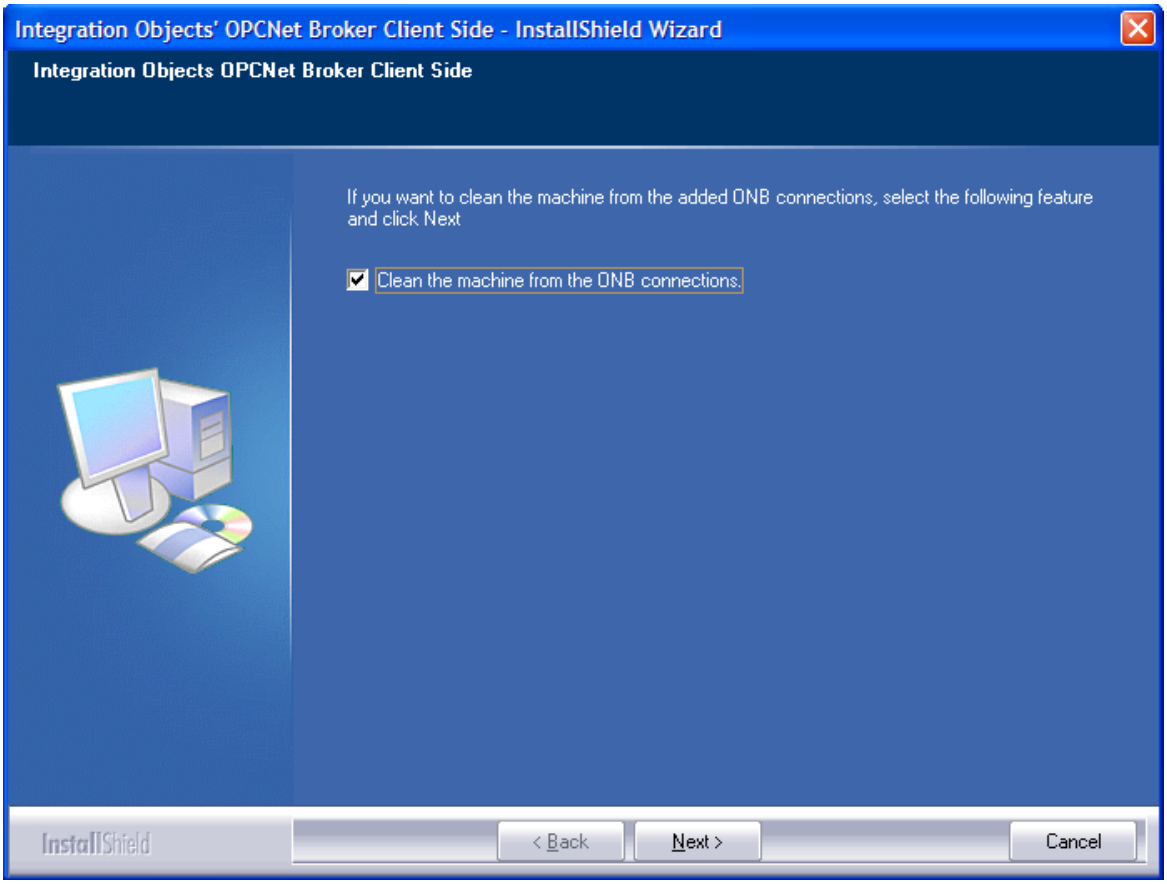


Figure 9: Clean the Machine from the ONB Connections

4. Update Existing Installation

In order to upgrade or downgrade an existing ONB Client/Server installation, follow the procedure below:

1. Uninstall the existing version using the uninstaller shortcut or the Add/Remove programs. In case of ONB Client installation, make sure to select the “Clean the Machine from the ONB Connections” option during the uninstallation.

2. Restart your machine.
3. Install the new ONB version using the corresponding setup and an administrator account.

CONFIGURATION

1. ONB Server Side

The ONB Server side should be configured before the ONB Client side. To configure the ONB Server, click on **Settings** from the server menu shown below:

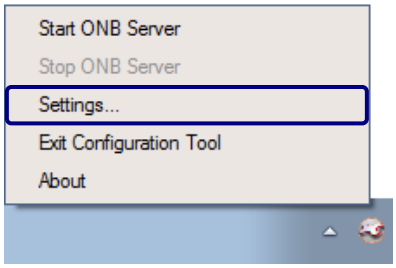


Figure 10: ONBS Tray Icon

You will get the following server configuration main window:

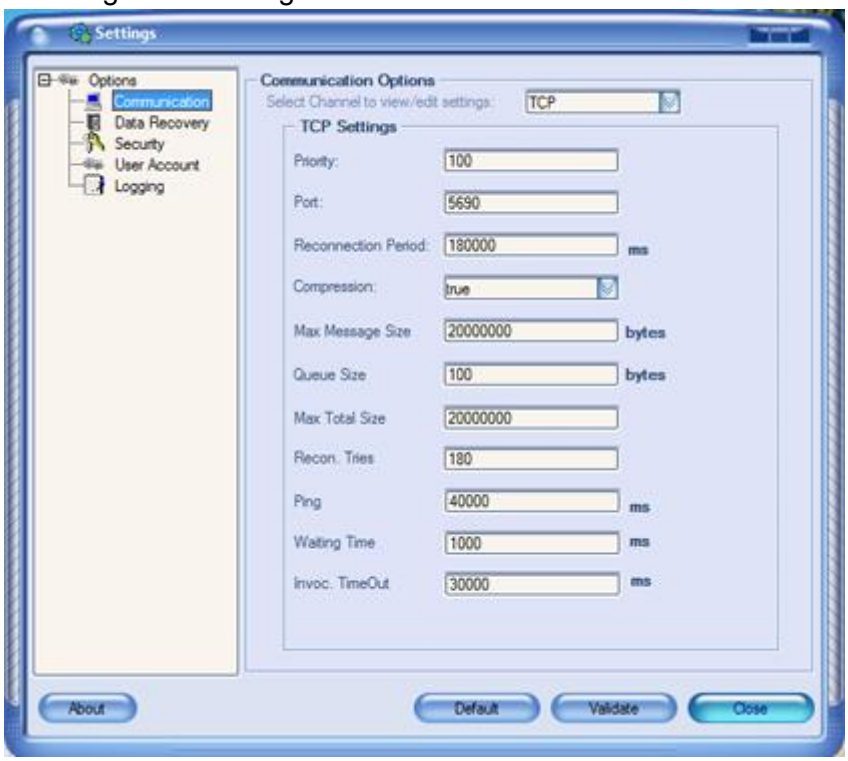


Figure 11: ONBS Settings

1.1. COMMUNICATION PARAMETERS

Select **Communication** to define the communication parameters for both TCP and XHTTP channels. They are listed in the following table:

Communication Options	Description	Default Value
Select Channel	This combo box contains two options: • TCP: TCP channel • XHTTP: XHTTP channel	TCP
The following parameters are configured per channel:		
Port	This is the port on which the server will listen to connected ONB clients through the selected channel. **It is recommended to modify the default port number.**	5690 for TCP and 5790 for XHTTP
Priority	An integer value representing the priority assigned to this connection. The higher the priority is, the higher is the chance for this connection to be established first.	100
Reconnection Period	When the ONB Client connection through the TCP channel is broken, it is expected to re-establish the connection within the specified time interval. Otherwise, the ONB Server declares the ONB connection as closed. *Unit = milliseconds*	180000
Compression	To enable compression on the server side, you should set this flag to true. Possible options: • True: Enable compression. • False: Disable compression	true
Max Message Size	The maximum size of a transmitted message. *Unit = bytes*	20000000
Queue Size	The total number of queued messages.	100

Max Total Size	The maximum total size of queued messages. *Unit = bytes*	20000000
Recon. Tries	The number of reconnection attempts before declaring that the ONB Server connection is lost.	180
Ping	ONB Client sends ping messages to the ONB Server within this ping time. *Unit = milliseconds*	40000
Waiting Time	The time to wait for after every reconnection failure. Unit = milliseconds	1000
Invoc. TimeOut	The ONB request is recognized as failed when the ONB Client does not receive a response from the ONB Server within this time period. *Unit = milliseconds*	30000

Table 2: Communication Parameters for ONB Server

As shown in the above screen dialog, currently OPCNet Broker supports both TCP and XHTTP channels.

Click **Apply** to save your changes.

1.2. Data Recovery

1.2.1. Overview

In case the ONB communication link experiences network or machine availability issues, the user can use the data recovery option in the ONB server side to re-send the events that were not received by the OPC AE Client or data by the OPC DA Client.

The lost events and/or data will be retrieved either from in-memory buffers or from a SQL Server historian if available.
By default, this option is **Disabled**.

Select **Data Recovery** from the options dropdown list to configure the data recovery option, as shown in the screenshot below:

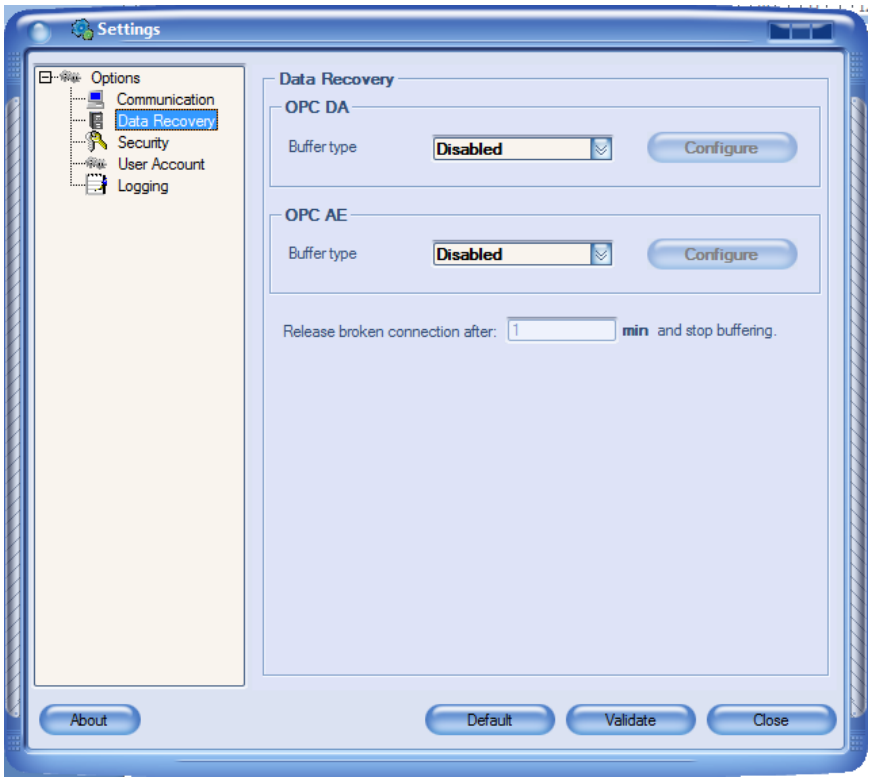


Figure 12: Data Recovery Settings

1.2.2. In-memory Recovery Option

To retrieve the data from the ONB Server in-memory buffer, select the option **In-memory** in the buffer type as shown in the figure below:

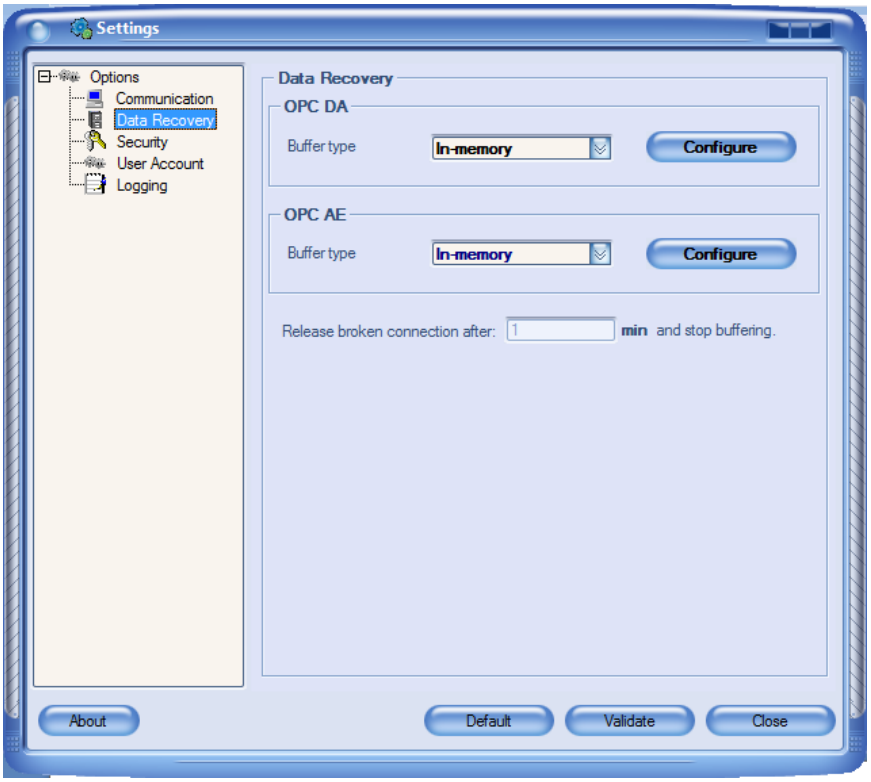


Figure 13: In-memory Data Recovery

When choosing the in-memory option, the respective configure button will be enabled. Click the configure button and the following window will be prompted:

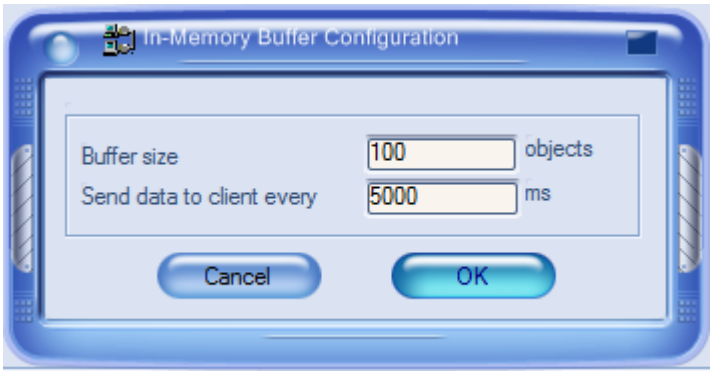


Figure 14: In-memory Buffer Configuration

Same window and parameters apply to DA and AE.
Set your parameters and click OK to save them:

- Buffer size: The number of failed operations stored in the buffer.

- Send data to client every: The ONB Server will periodically try to send failed operations each time the specified period expires, until these operations are successfully received by the ONB Client.

This option should be enabled in the initial configuration so the ONB Server can fill out its buffer when the communication link between the client and server side is down.

1.2.3. SQL HISTORIAN RECOVERY OPTION

Select **SQL Historian** from buffer type to retrieve data and/or events from the configured SQL database:

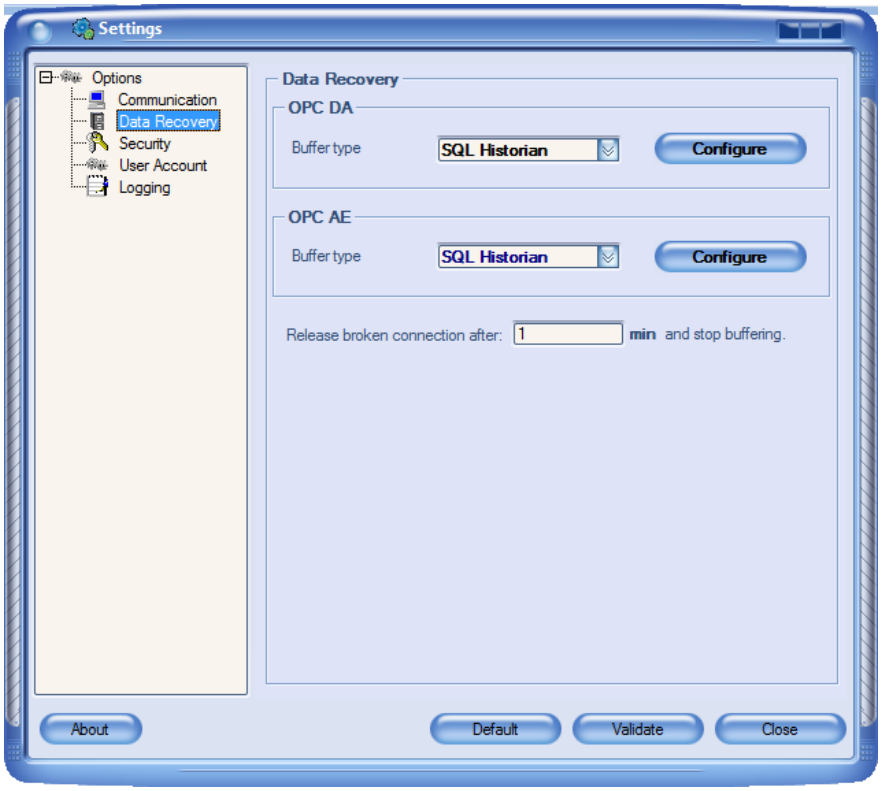


Figure 15: SQL Historian Data Recovery

The SQL Historian option is licensed separately.
To enable the ONB Server to detect the communication breaks and send the lost data automatically, this option should be enabled in the initial configuration. Otherwise, retrieving the missing data will require a restart of the ONB Server.

If you are retrieving OPC DA data, the configuration window will be as illustrated below:

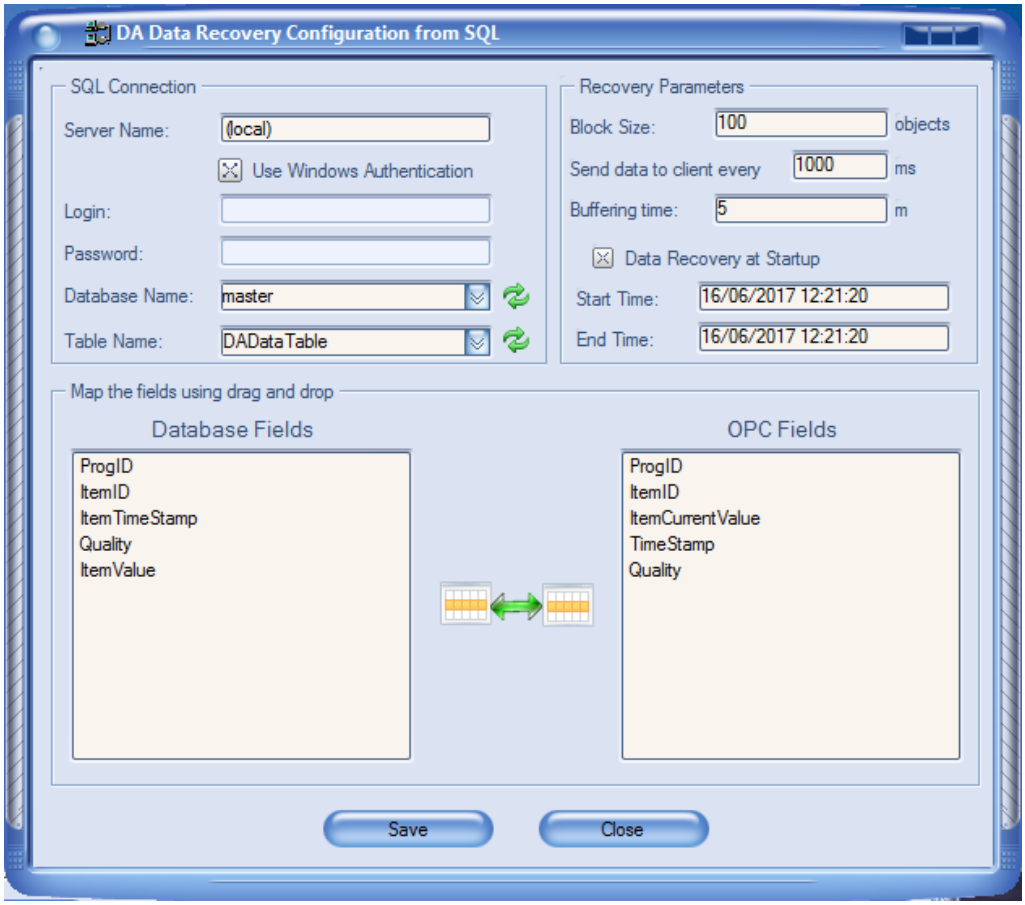


Figure 16: OPC DA Data Recovery Configuration from SQL

To configure the connection to the SQL Server, you need to specify:

- The IP of the SQL Server
- The login and password of the SQL account
- The database name
- The table name

If you are retrieving OPC AE events, the configuration window will be as shown below:

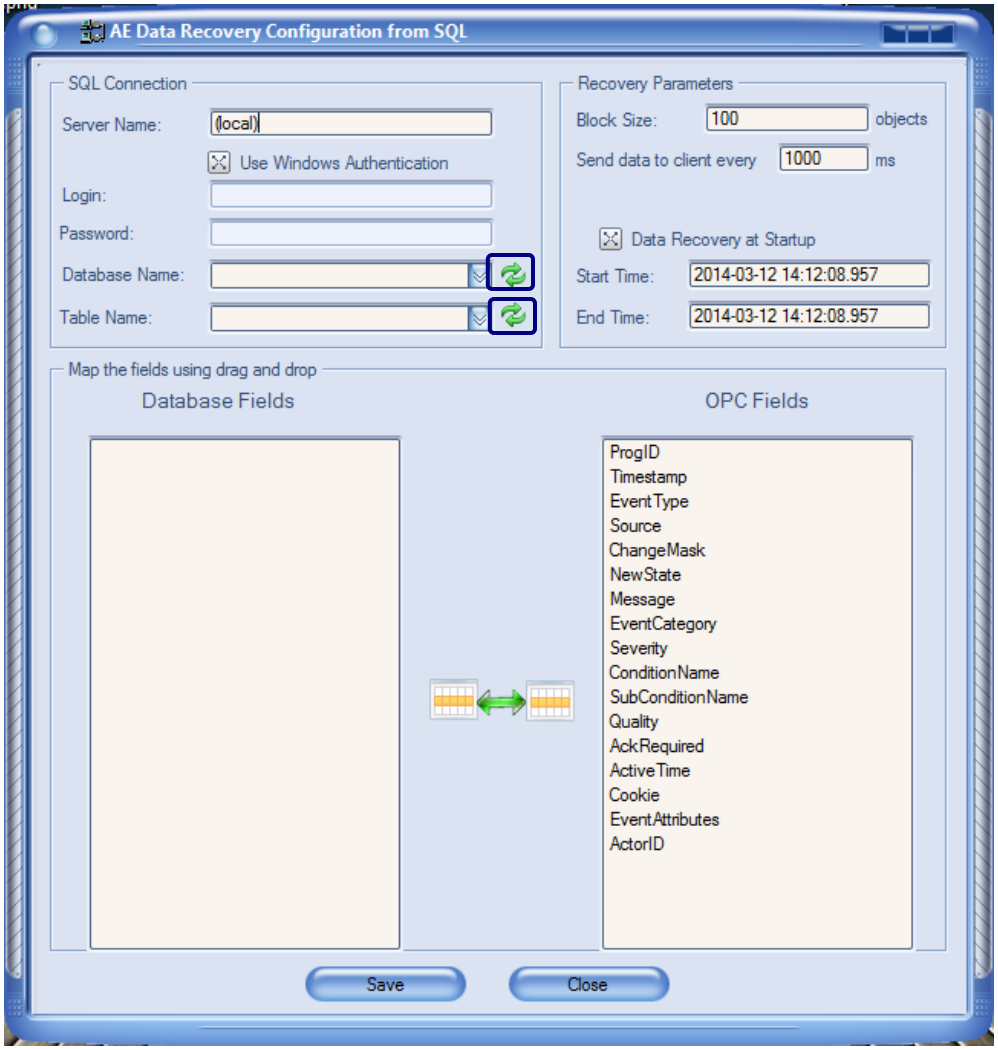


Figure 17: OPC AE Data Recovery Configuration from SQL

Click the refresh icon, to refresh the tables and databases available under the selected server.

For the first configuration, if you already have data in your SQL table that you want to send to the client side, check the **Data Recovery at Startup** and configure the Start and End time.

You need to map all OPC Fields in order to save the configuration.
To do so, proceed by a simple drag and drop between the two fields. The mapped fields will be shown as follows:

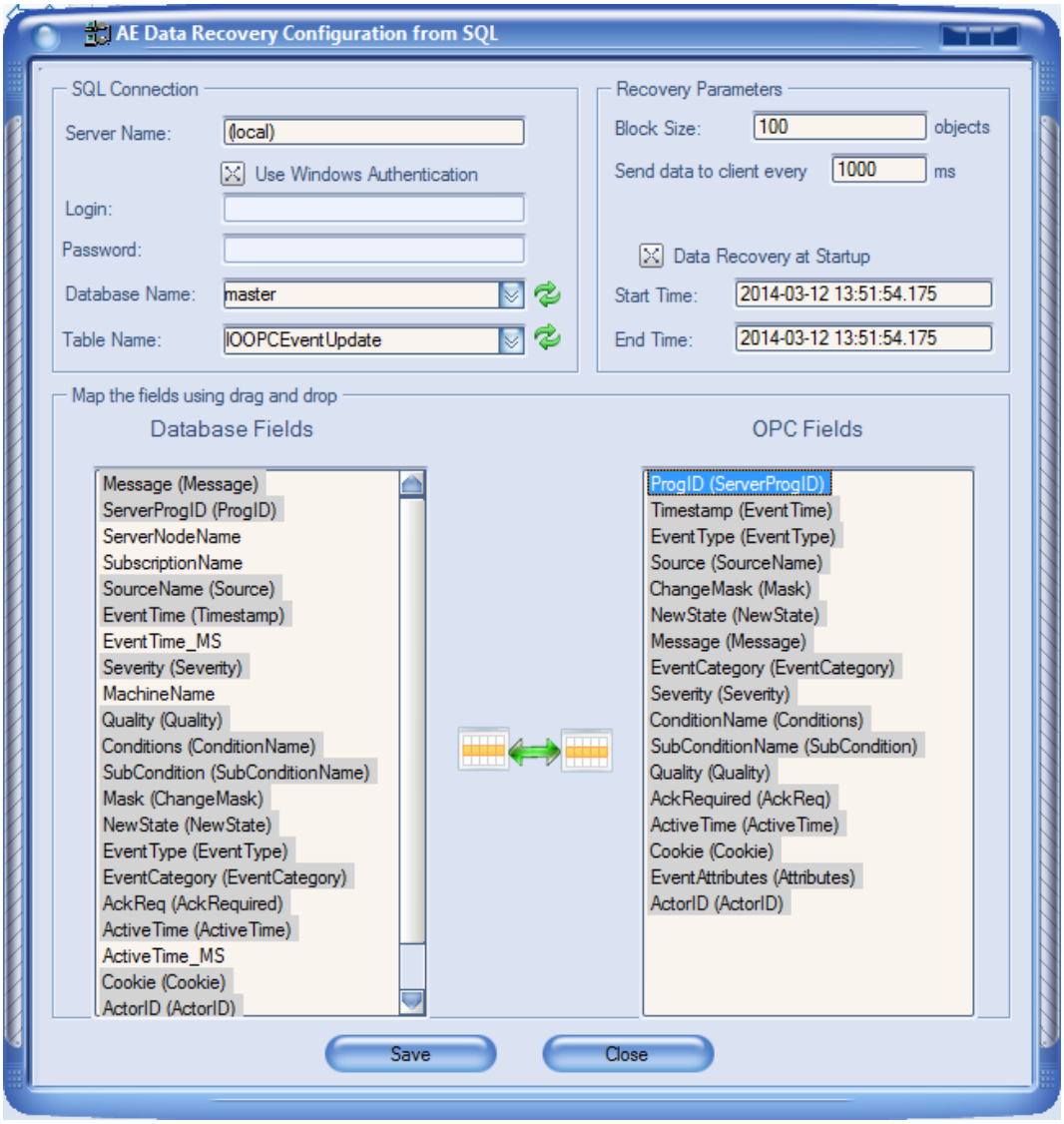


Figure 18: Map OPC AE Database Fields

The same applies for the OPC DA fields:

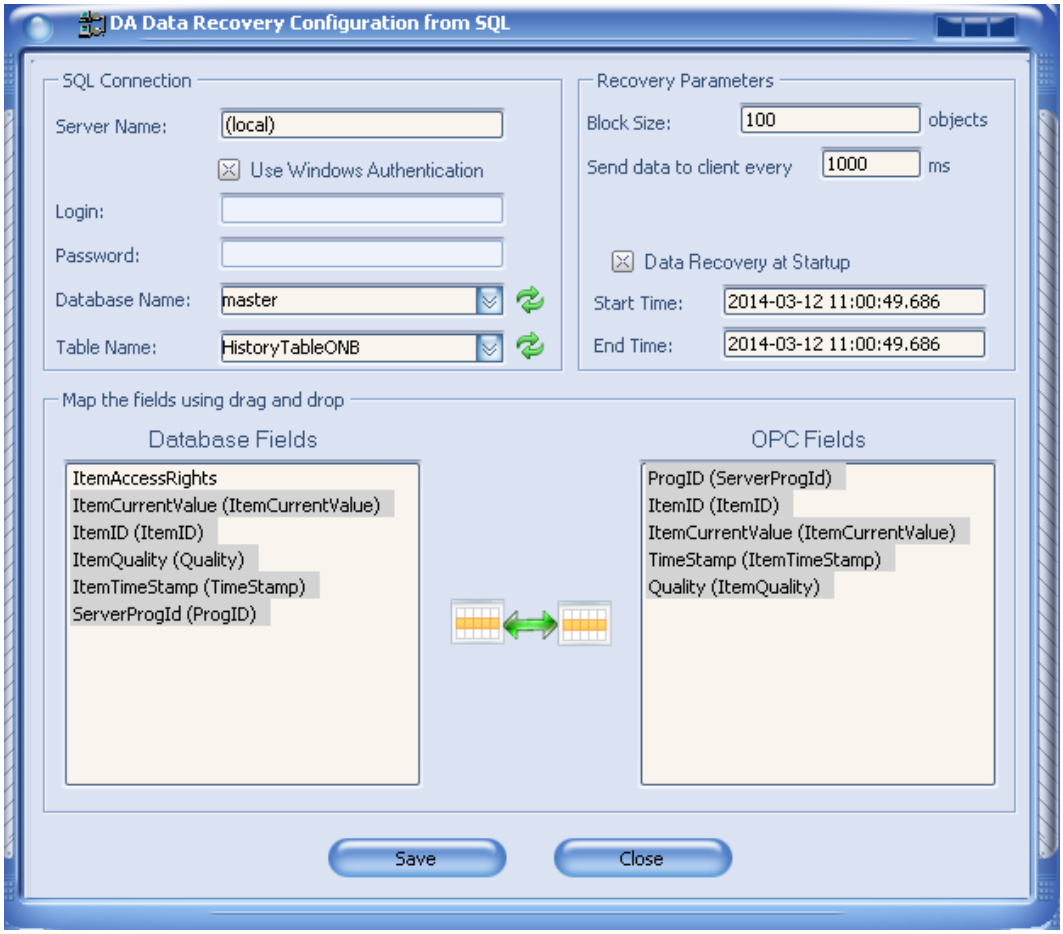


Figure 19: Map OPC DA Database Fields

To remove a mapped field, right click on it and select "Clear mapping".

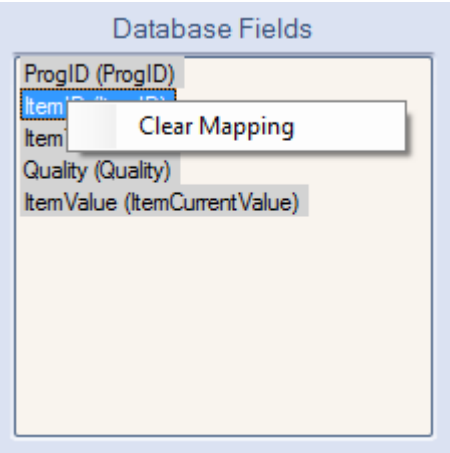


Figure 20: Clear Mapping

To remove all the mapped fields, right click on a blank area either in the database fields table or OPC fields and then click on "Clear All Mapping".

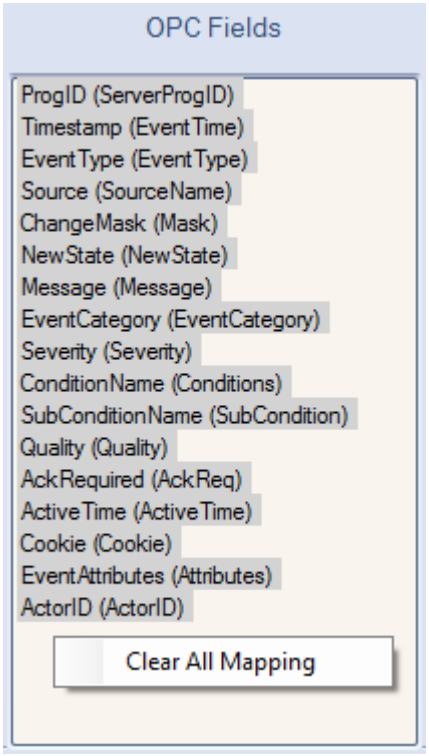


Figure 21: Clear all Mapped Fields

1.3. SECURITY

1.3.1. OVERVIEW

Select **Security** to define security options. You will get the following screen:

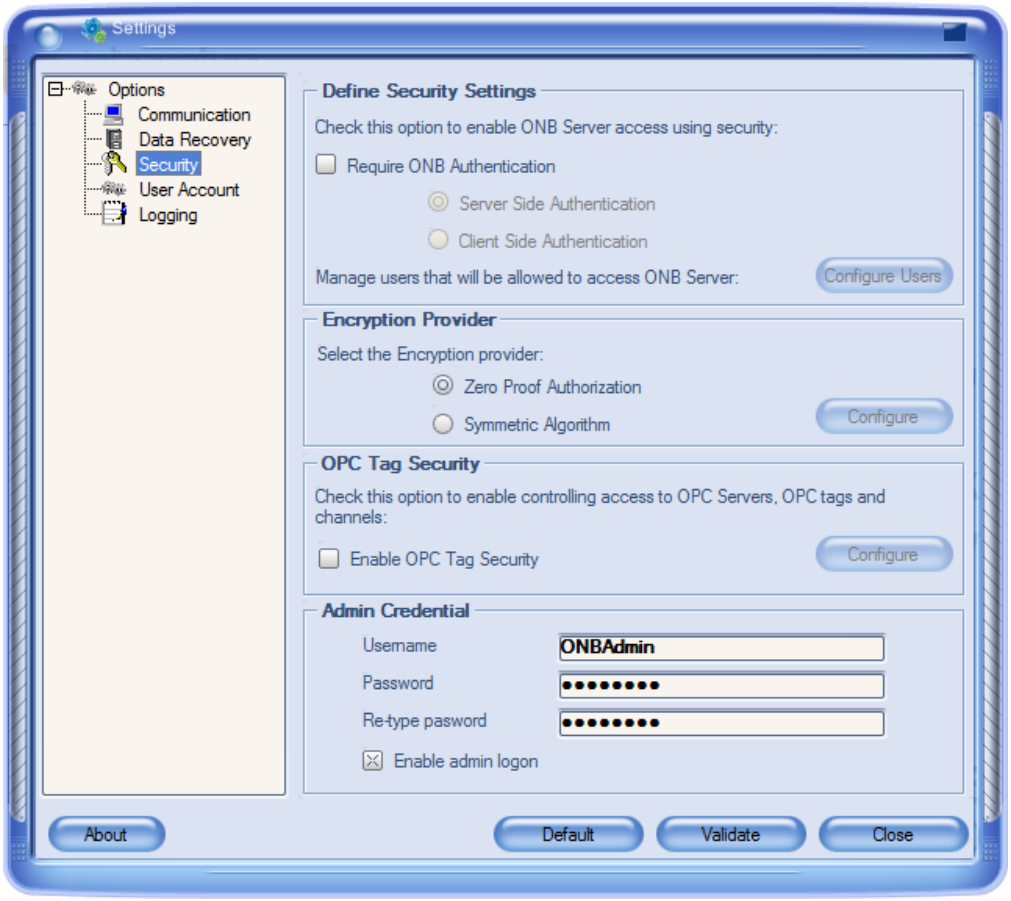


Figure 22: Security Settings

You should:

- Check the **Require ONB authentication** option to request ONB client authentication via login and password. In this case, if the provided information is not valid, the client connection will be rejected.

  There are two secure authentication modes:
  - Server Side Authentication
  - Client Side Authentication

- Uncheck this option to allow access to any client trying to connect to the ONB Server either using security or not.

To configure the users' accounts who are allowed to access the ONB Server from remote hosts, click **Configure Users**. The Integration Objects Users Management Tool will then be displayed. This configuration utility allows you to:

- Add/Remove NT Windows/Domain user accounts
- Set user passwords

The encryption provider section allows to configure the encryption provided to be used for the communications between the ONB Server and Client.

The admin credential section allows to edit the username and password of the ONB admin account.

The OPC Tag Security section is installed by default with the OPC Data Access feature. The OPC Tag security feature is not enabled by default. How to enable and use this software is explained in the ***Integration Objects OPC Tag Security User Manual***.

1.3.2. USER'S MANAGEMENT –SERVER SIDE AUTHENTICATION

User configuration is required to secure ONB communications. This tool manages NT user accounts configured on the ONB server machine.

If you have checked the **Server Side Authentication** option in the ONB Sever Security Settings, the Users Management main window will be shown as below when clicking the **Configure Users** button:

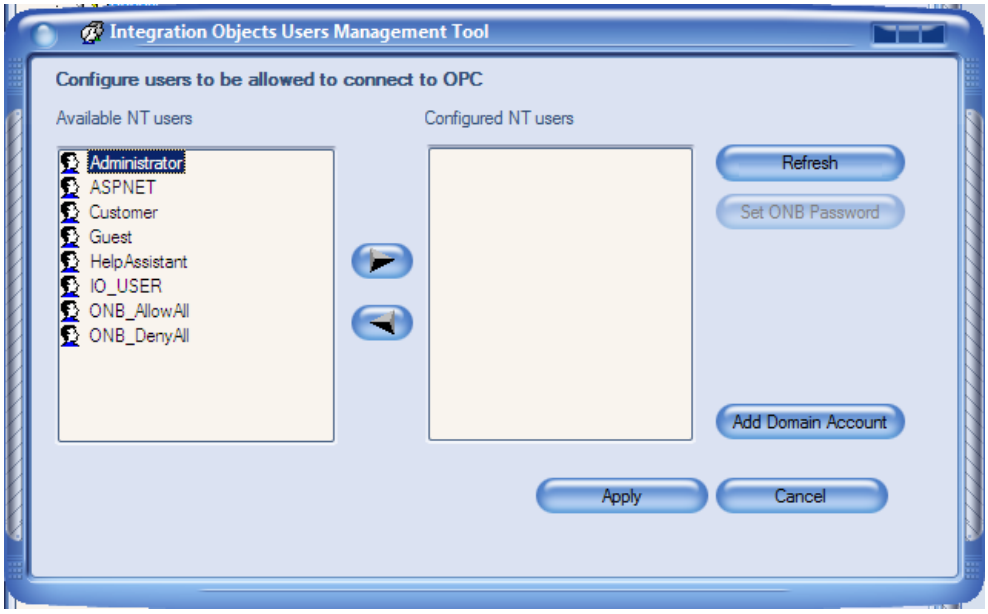


Figure 23: Server Side Users Management Tool

1.3.2.1. ADD A SERVER SIDE ACCOUNT

Select the Server Side account from the available NT users list and then click  to add it to the list of configured users.

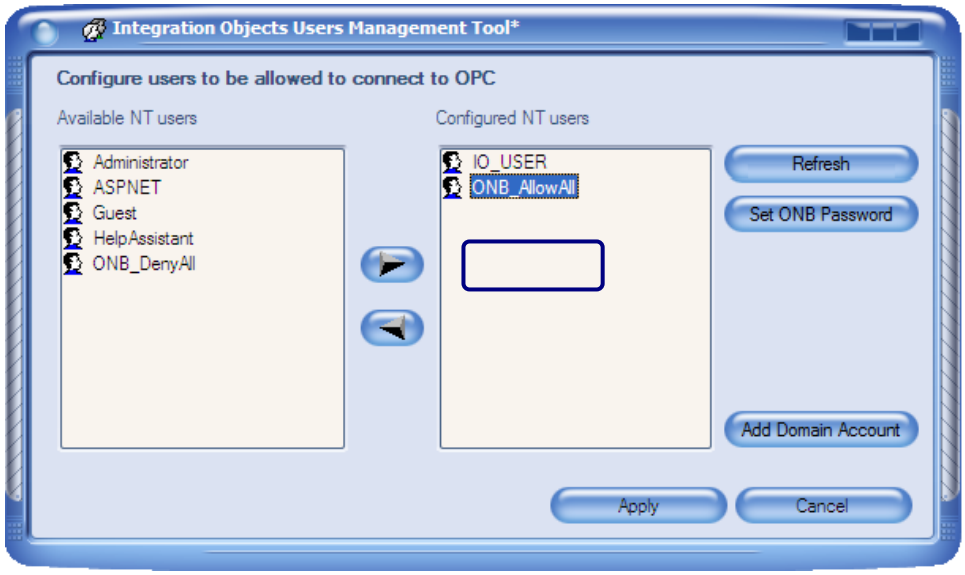


Figure 24: Add Users

You will be asked to set the password as illustrated in the figure below.



Figure 25: User Password

Enter the NT user account password or a custom password. An empty value is not permitted. Then, click **OK**.

You can also add domain accounts by clicking the "**Add Domain Account**" button the following screen will appear:



Figure 26: Add Domain Account

Enter the Domain name, the Domain account and the password. An empty value is not permitted. Then, click **OK**.

1.3.2.2. Refresh Users List

Click **Refresh** to refresh the list of NT users.

1.3.2.3. Remove a Server Side Account

To remove one user from the list of configured users, select the requested user then click  as shown below:

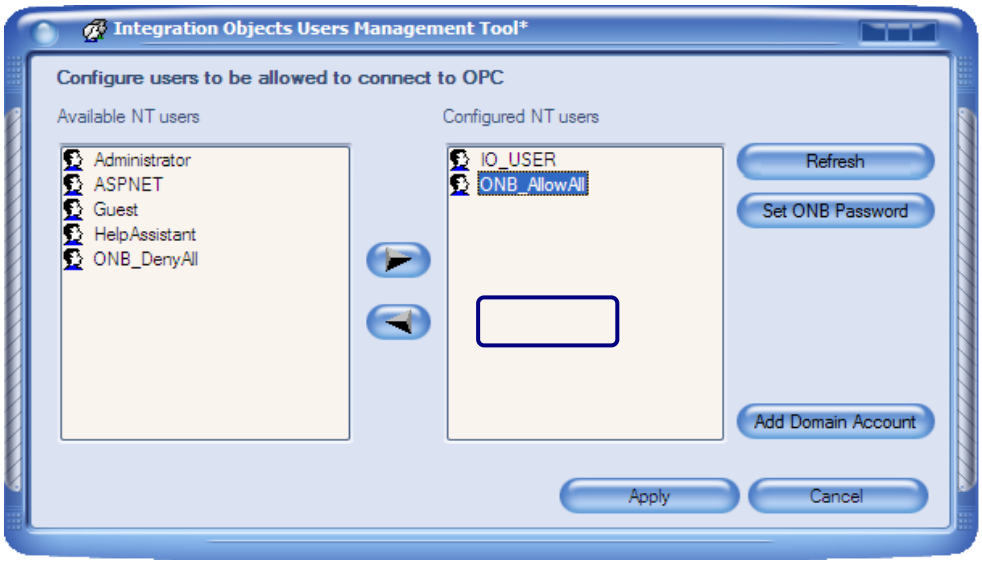


Figure 27: Delete User

1.3.2.4. SET PASSWORD

To set a user password, select the requested user and click **Set Password**.

You will get a similar dialog screen:



Figure 28: Set Password

Set the password and confirm it: you can enter the NT user account password or a custom password. An empty value is not permitted.

1.3.2.5. SAVE SERVER SIDE AUTHENTICATION CONFIGURATION

To save the current configuration, click the **Apply** button in the Users Management Tool window.
Saved changes will take effect after restarting the ONB Server.

1.3.2.6. CANCEL SERVER SIDE AUTHENTICATION CURRENT CONFIGURATION

To exit the Users Management Tool and to cancel the current configuration, click **Cancel**.

1.3.3. USER'S MANAGEMENT –CLIENT SIDE AUTHENTICATION

The user management tool can also be used to manage the ONB Client Accounts when using the “Client Side Authentication” mode.
If you have checked **Client Side Authentication** option in the ONB Sever Security Settings, the Users Management main window will be shown as below when clicking the **Configure Users** button:

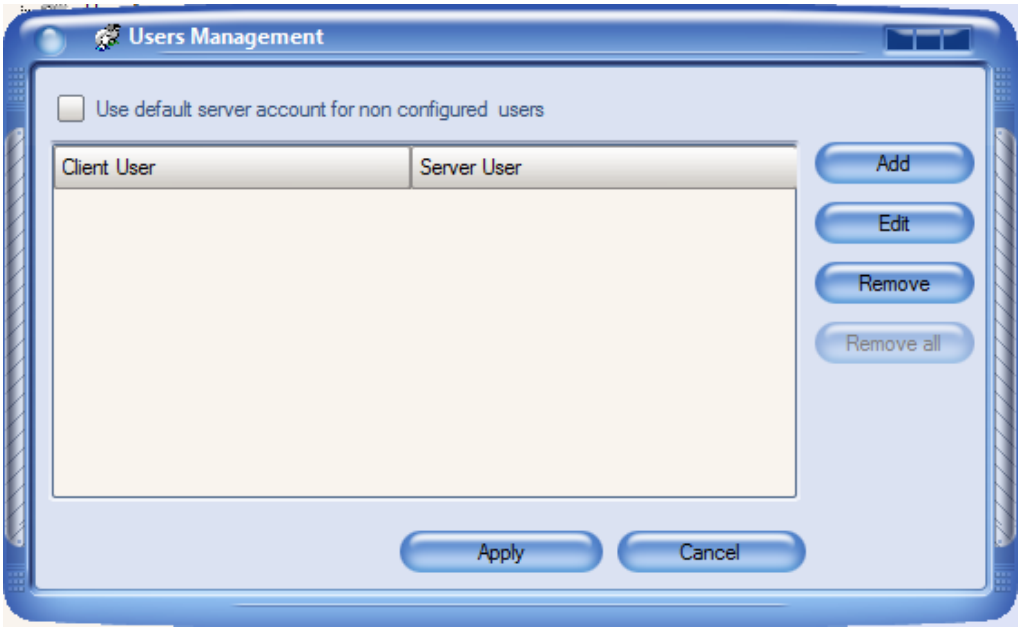


Figure 29: Client Side Users Management Tool

1.3.3.1. ADD A USER MAPPING

To add a new user mapping, click **Add**. The following screen will appear:



Figure 30: Add User Mapping– Step 1

The following screen shows the “Add User Mapping” dialog filled out.

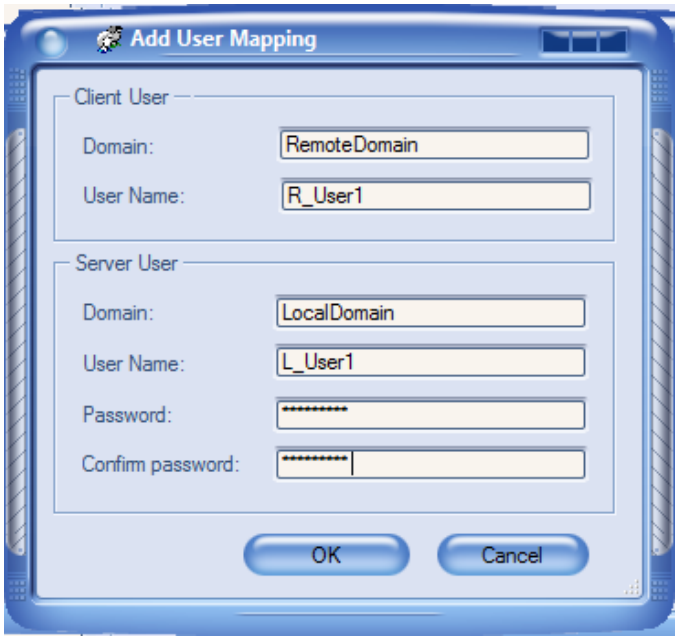


Figure 31: Add User Mapping – Step 2

Fill in all the fields as described in the table below.

Parameter		Description
Client User	Domain	Domain name of the client user
	Login	Login of the client user
Server User	Domain	Domain name or machine name of the server user or machine name where the ONB server was installed.
	User Name	User name of the server user
	Password	Password of the server user
	Confirm password	Password of the server user

Table 3: User Mapping Fields

1.3.3.2. Edit an Existing User Mapping

To update a configured user mapping, select the mapping click **Edit**. The following dialog will be prompted:



Figure 32: Edit User Mapping

1.3.3.3. Remove a User Mapping

To remove an existing user mapping, you just need to select the mapping and then click **Remove**.

1.3.3.4. Remove All

Click **Remove All** to remove all user mappings.

1.3.3.5. Use Default Server account for Non-Configured Users

If the "**Use default server account for non-configured users**" option is checked, all non-mapped users will be allowed to connect using a default user mapping.

When you select this option, the following screen will appear to configure the default user mapping:



Figure 33: Configure Default User Mapping

1.3.3.6. Save Client Side Authentication Configuration

To save the current Client Side users configuration, click **Apply** button in the Users Management Tool window.
Saved changes will take effect after restarting the ONB Server.

1.3.3.7. Cancel Client Side Authentication Current Configuration

To exit the Users Management Tool and to cancel the current configuration, click **Cancel**.

1.3.4. Encryption Providers

Using the ONB Server security settings window, you can configure the encryption provider.
You can select the required encryption provider as illustrated in the following figure:

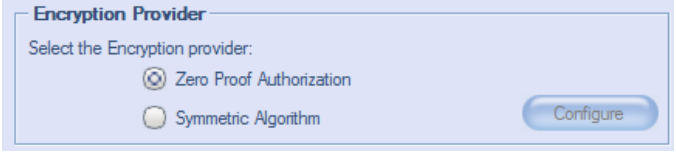


Figure 34: Encryption Provider Configuration

Below you can find the available providers:

- Zero Proof Authorization: This security provider provides authentication, encryption and content integrity checking services.
- Symmetric Algorithm: This security provider allows you to secure the ONB communication by providing the possibility to configure the padding and cipher modes.
  When selecting this provider, you will be able to configure the Padding and Cipher modes by clicking the **Configure** button.
  If you click on the **Configure** button, you will get the following screen:

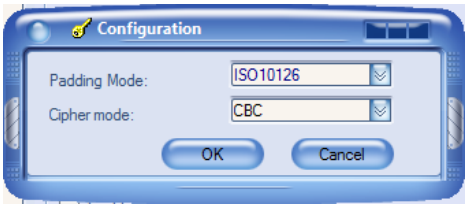


Figure 35: Configuration of Padding & Cipher Modes

Below you can find the padding modes list:

- **ANSIX923**: The ANSIX923 padding string consists of a sequence of bytes filled with zeros before the length.
- **ISO10126**: The ISO10126 padding string consists of random data before the length.
- **PKCS7**: The PKCS #7 padding string consists of a sequence of bytes, each of which is equal to the total number of padding bytes added.

After selecting the padding mode, you can select the Cipher mode as illustrated on the following figure:

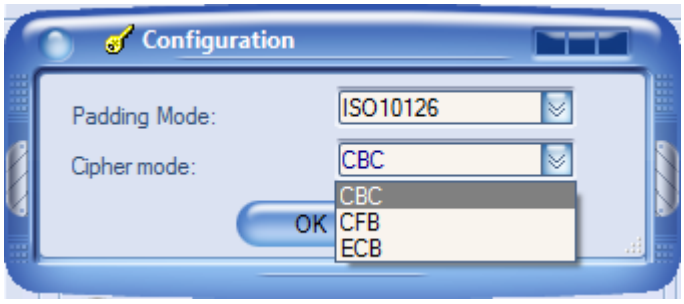


Figure 36: Choosing the Cipher Mode

Below you can find Cipher modes list:

- **Cipher Block Chaining (CBC):** In CBC mode, each block of plaintext is XORed with the previous ciphertext block before

being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

- **Cipher Feedback (CFB):** The Cipher Feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC encryption performed in reverse.
- **Electronic Codebook (ECB):** The message is divided into blocks, and each block is encrypted separately.

1.3.5. Admin Credential

In order to secure the ONB server settings, the ONB Server settings configuration window is protected by login and password.
When you right click on the ONB server tray icon and then click on Settings, you will get the following authentication screen:

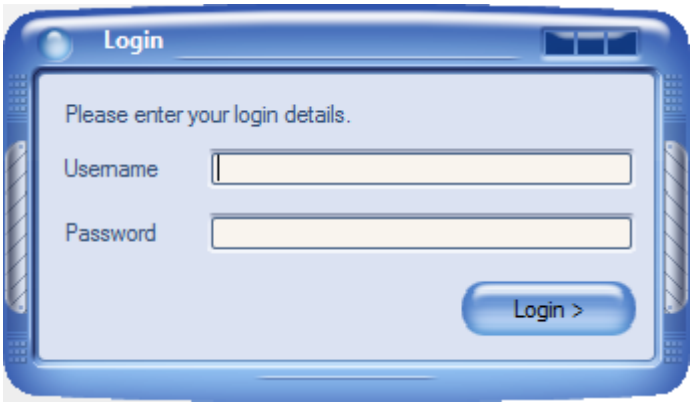


Figure 37: ONB Login Window

The default credential is the following:
Login: ONBAdmin
Password: ON8@dmin

You can change the default admin credential in the ONB server settings window and under the security option. Refer to "**Admin Credential**" section to change the credential as follows:

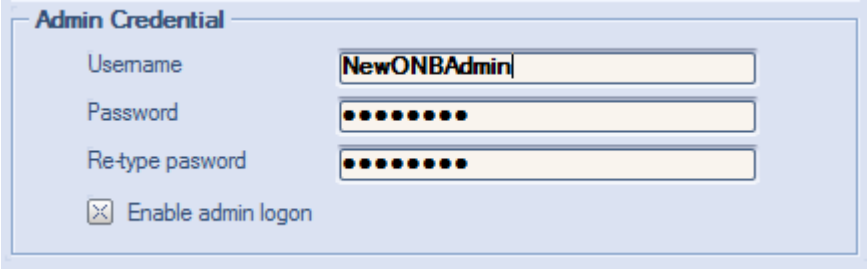


Figure 38: Change Admin Credential

Click on **Validate** to save the new configuration.

It is recommended that users change the default password once they complete the installation.

1.4. CREDENTIALS FOR USER ACCOUNT

To ensure the principle of least privilege, the administrator can configure as illustrated below the user account to have the minimum right privileges to run the ONB Server. To do so, he has to grant the user account these permissions by entering the user ID, the domain and clicking the Grant permission button. If the entered information is correct, the user account will be configured automatically.
This will allow you to start the ONB Service using a non-administrator user account.

Click on **Validate** to save your changes.

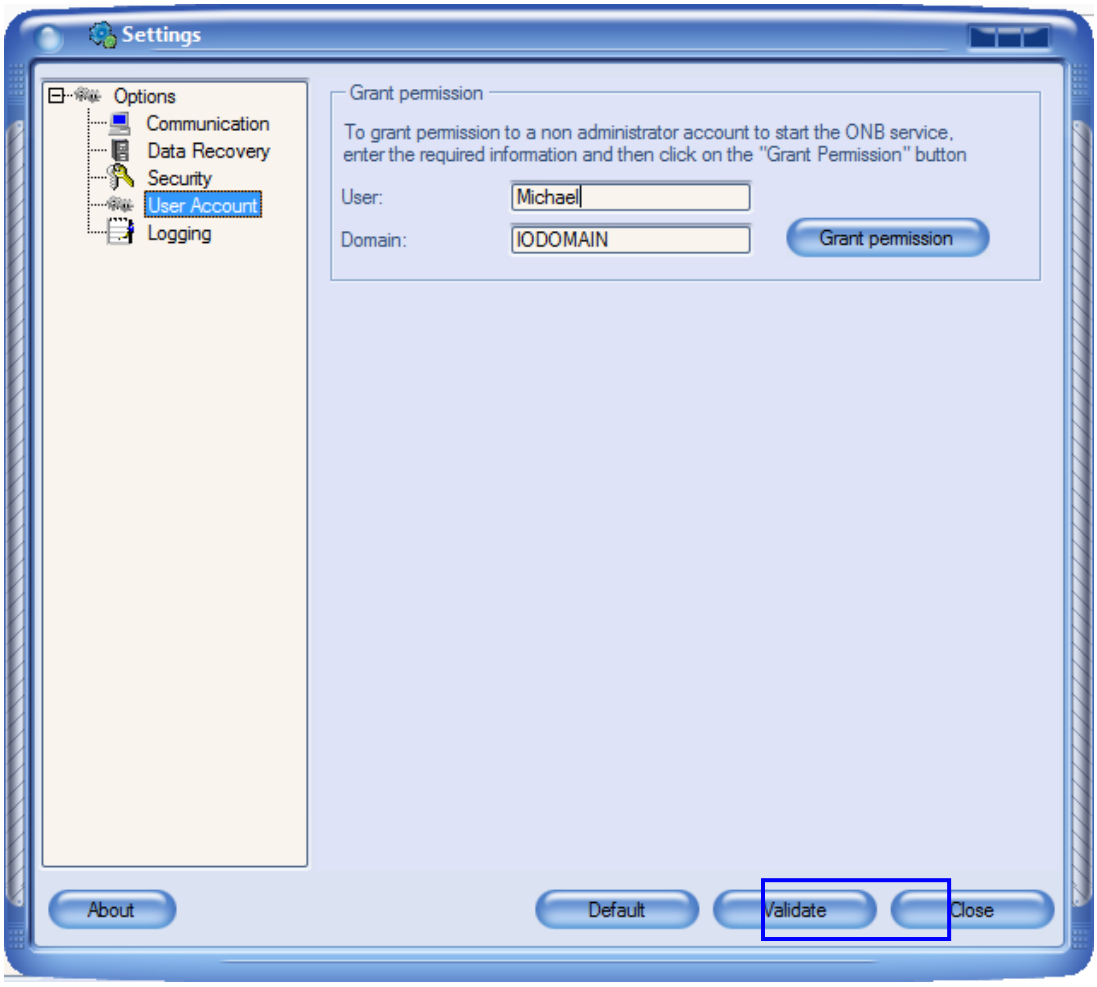


Figure 39: User Account Settings

1.5. Logging Options

Select **Logging** to define logging options. The displayed window is shown below:

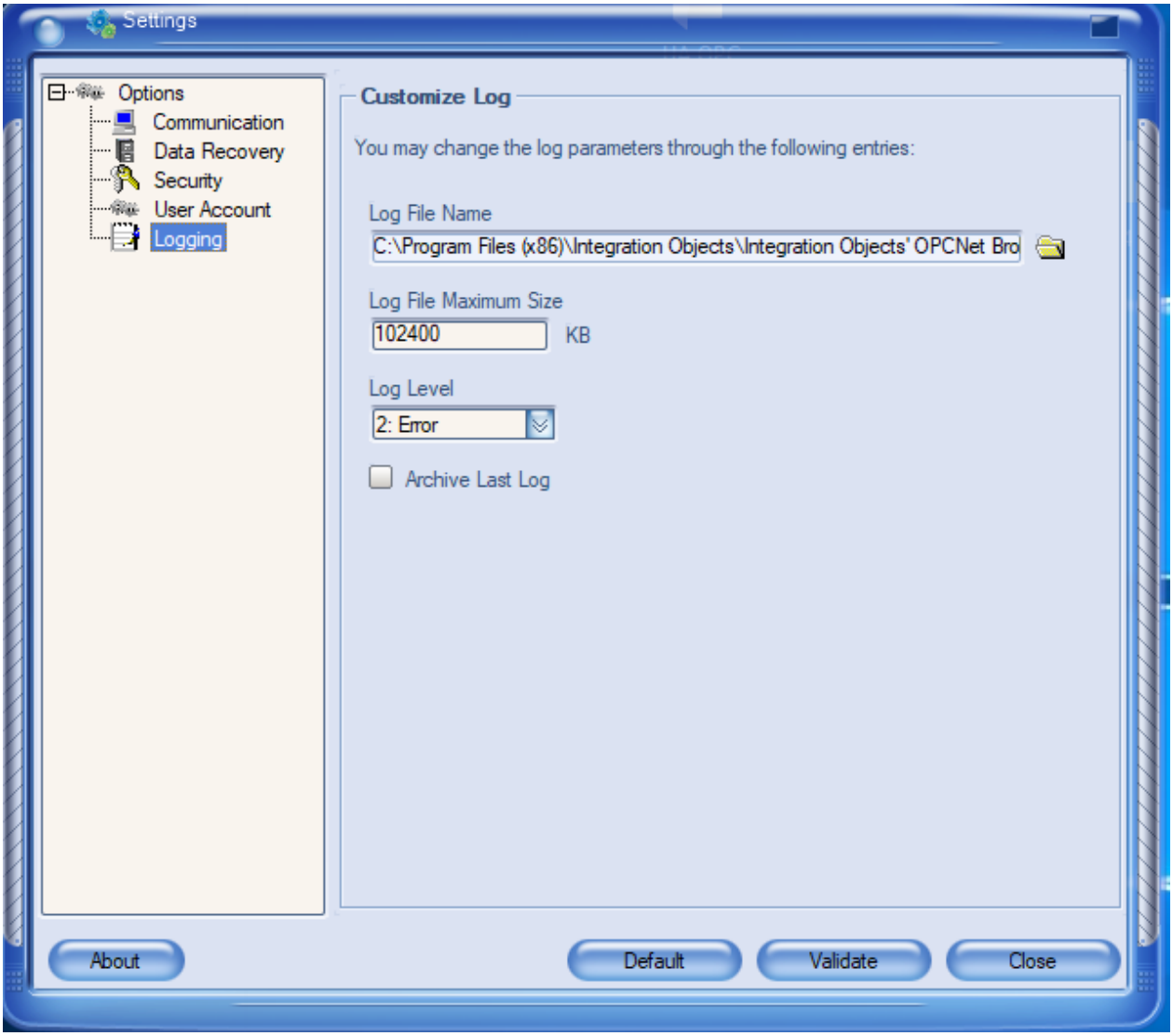
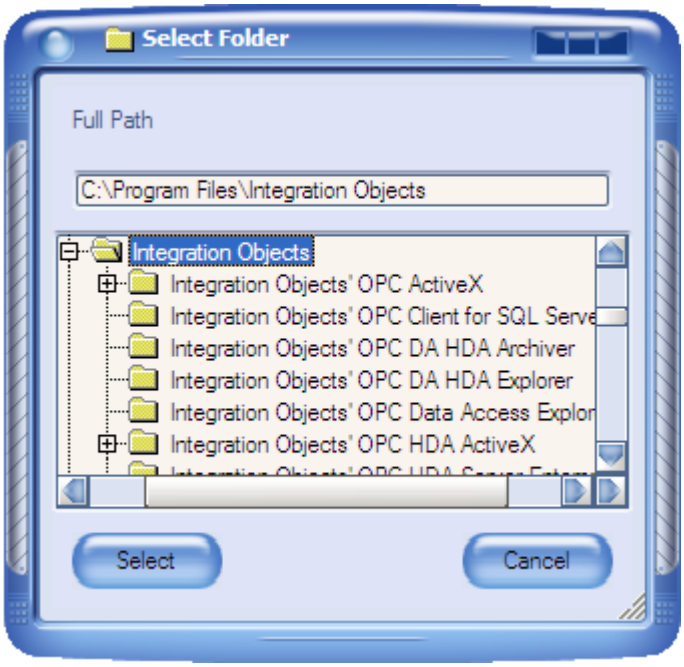
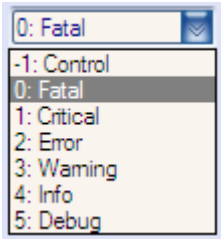


Figure 40: Logging Settings

The following table describes all logging parameters:

Parameter	Description
Log File Name	You can rename the log event file generated by the ONB Server program. Click on the folder icon to choose a different folder to place the generated ONB Server log event file. You will get the following

	dialog screen:  **Figure 41: Select Folder Dialog**
Log Level	Depending on your needs, you may use a high log level to display full information describing program execution step by step or use a low level under normal behavior. Select a value from this combo box:  **Figure 42: Log Levels** Available options: • **Debug**: Debug messages. This is the highest level. • **Info**: Information messages. • **Warning**: Warnings. • **Error**: Errors. This is the default log level. • **Critical**: For critical errors. • **Fatal**: Fatal errors. Critical and fatal errors could stop ONB execution. • **Control**: This is the lowest log level. We recommend using

	this level for better performance. The log levels are ordered so that each log level includes all log messages of all lower log levels.
Log File Maximum Size	The maximum log file size, in kilobytes
ArchiveLastLog	Check the **ArchiveLastLog** option if you want to copy old logs to an intermediate file with incremental extension before being overwritten whenever the maximum file size is reached. Otherwise, any pre-existing log file is overwritten at start-up.

Table 4: Logging Parameters

Click on **Validate** to save your changes.

2. ONB Client Side

For out-process context, the ONB Client is configured by editing the configuration file ONBSettings.ini.

For in-process context, the ONB Client is configured through the Client Configuration Tool.

In this section, we will focus on the Client Configuration Tool. Using this utility, you can:

- Manage the OPC DA/HDA/AE Servers list on a given remote host by adding, removing and editing ONB connections.
- Configure all communication parameters for a given ONB connection such as the remote host name or IP Address, the port number at which all Server/Client communications will be transmitted, the maximum size of transmitted messages, etc.
- Configure all security parameters for a given ONB connection such as the network credentials in case of using security.
- Configure authorized OPC Clients
- Set the logging flags and parameters for the Client Side for both in-process and out-process contexts.

All these features are described in details in the following sections.
Once the "**Admin Credential**" option is enabled, you will be asked to enter the login and password when opening the ONB Client configuration tool as follows:



Figure 43: ONB Client Configuration Tool Admin Login

The default credential for the ONB Client configuration tool is the following:
Login: ONBAdmin
Password: ON8@dmin

It is recommended that users change the default password once they complete the installation.

In order to change this default credential, you just need to click on **Settings** then click on **Admin credential** as following:

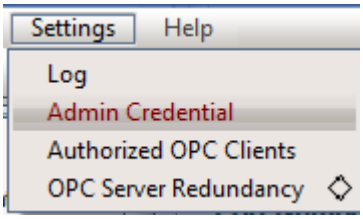


Figure 44: Admin Credential

When you click on Admin credential, you have to fill the new credential as following:

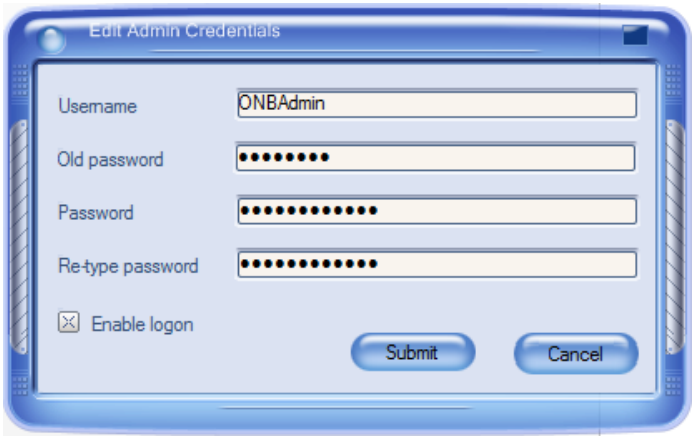


Figure 45: Edit Admin Credential

The main window of this configuration tool is illustrated below:

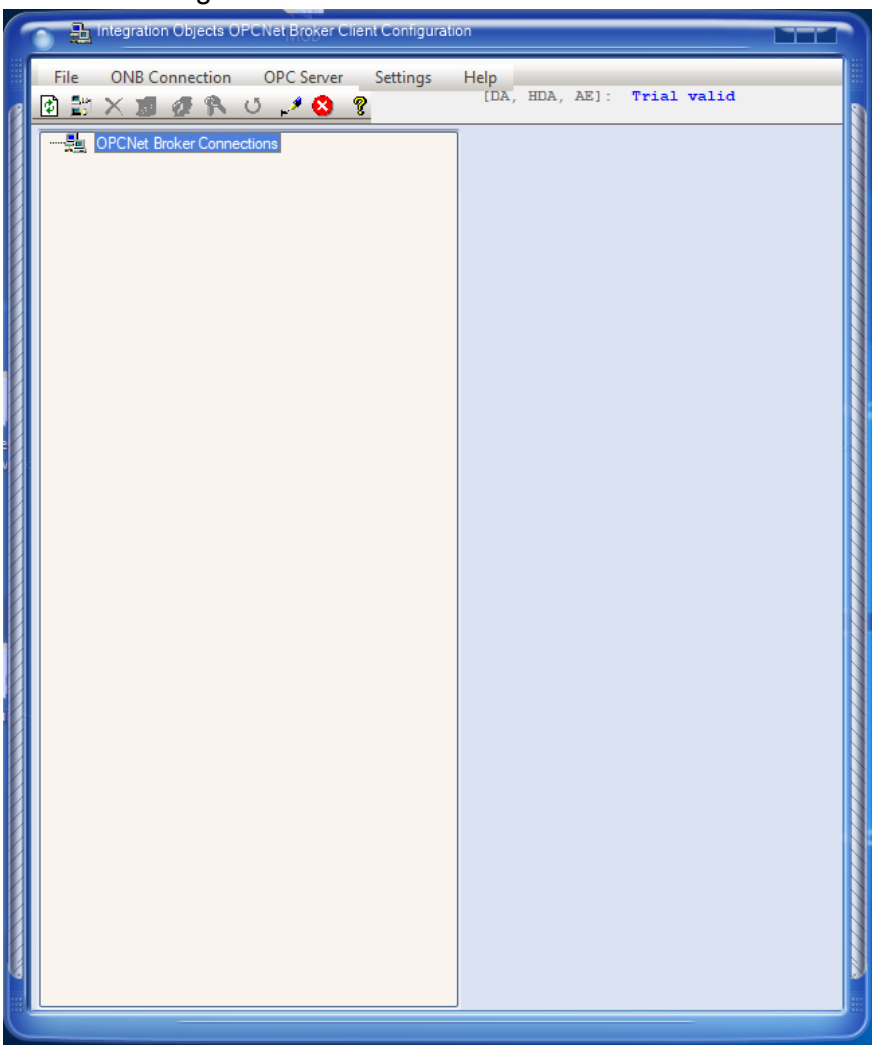


Figure 46: ONB Client Configuration Tool – Main Window

And it contains the following toolbar and a text indicators for the license status:



Figure 47: Toolbar

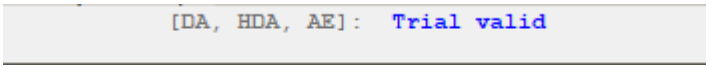


Figure 48: ONB Client License Status

Menus and toolbar buttons will be described in detail in the next sections.

2.1. Session Management

This section details the session menu entries under the File menu.

- **Close Application**
  To exit the configuration tool, click on the **File ➔ Exit** menu, use this button  from the toolbar or press **Alt+F4** on the keyboard as a shortcut.

2.2. OPC Server List Management

2.2.1. Adding ONB Connection

If the OPC Client resides in your local machine and you want to communicate with a remote OPC DA/HDA server located in a remote host (for example, having the host name: **io**), select the **OPCNet Broker Connections** node from the tree view and follow these steps:

- Click on **ONB Connection ➔ Add**.
- Or use the button  from the toolbar.
- Or click on the **Add** contextual menu.
- Or press **Ins** on the keyboard.

The following screen dialog will appear:



Figure 53: Add ONB Connection

The default IP Address is the IP address of the localhost.

You can click on the network icon to browse the available machines. You will get a similar dialog screen:

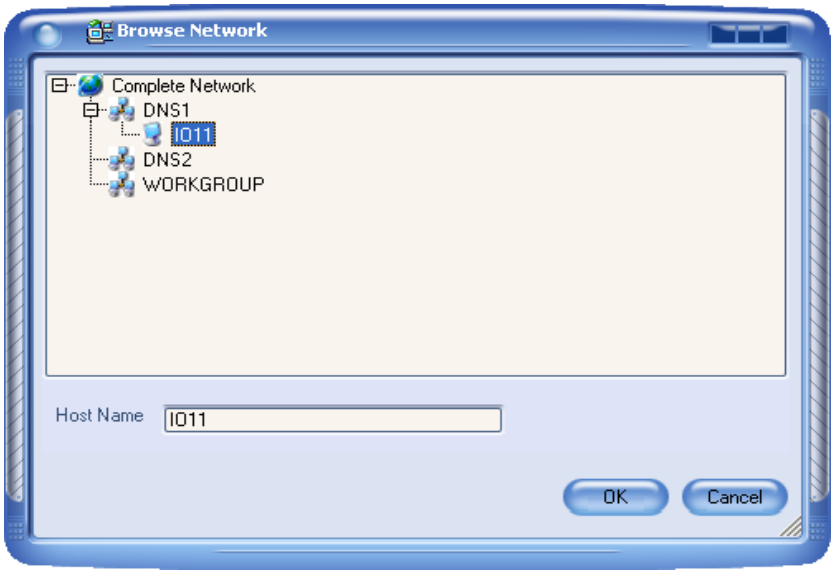


Figure 49: Browse Network

Double click the requested host and click **OK** to obtain the host name of the required machine.

Enter the following:

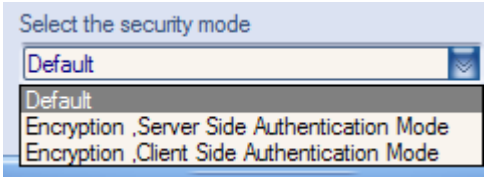
Parameter	Description
Channel name	The channel type (TCP or XHTTP).
IP Address/Host name	The remote host (where resides the remote OPC Server) name or IP Address.
Port	The port number on which all OPC communications will be transmitted (by default 5690 for the TCP Channel and 5790 for the XHTTP Channel).
Using security for Client Configuration Tool	Check this option if you want to use security. This section deals with setting security for the Client Configuration Tool. Later, you may update your security settings for OPC communication.  **Figure 50: Security Mode** If you select “Encryption, Server Side Authentication Mode”, the Login and Password text boxes will be enabled. Enter valid credentials to successfully connect to the ONB Server and retrieve the remote OPC servers. Empty values are not allowed. If you select “Encryption, Client Side Authentication Mode”, ONB will authorize the OPC connection based on the account used to run the OPC client application. Note that the security feature includes encryption.

Table 5: Add ONB Connection Fields

You can configure more parameters when adding the ONB Connection by clicking on **Advanced** button. You will get the following screen:

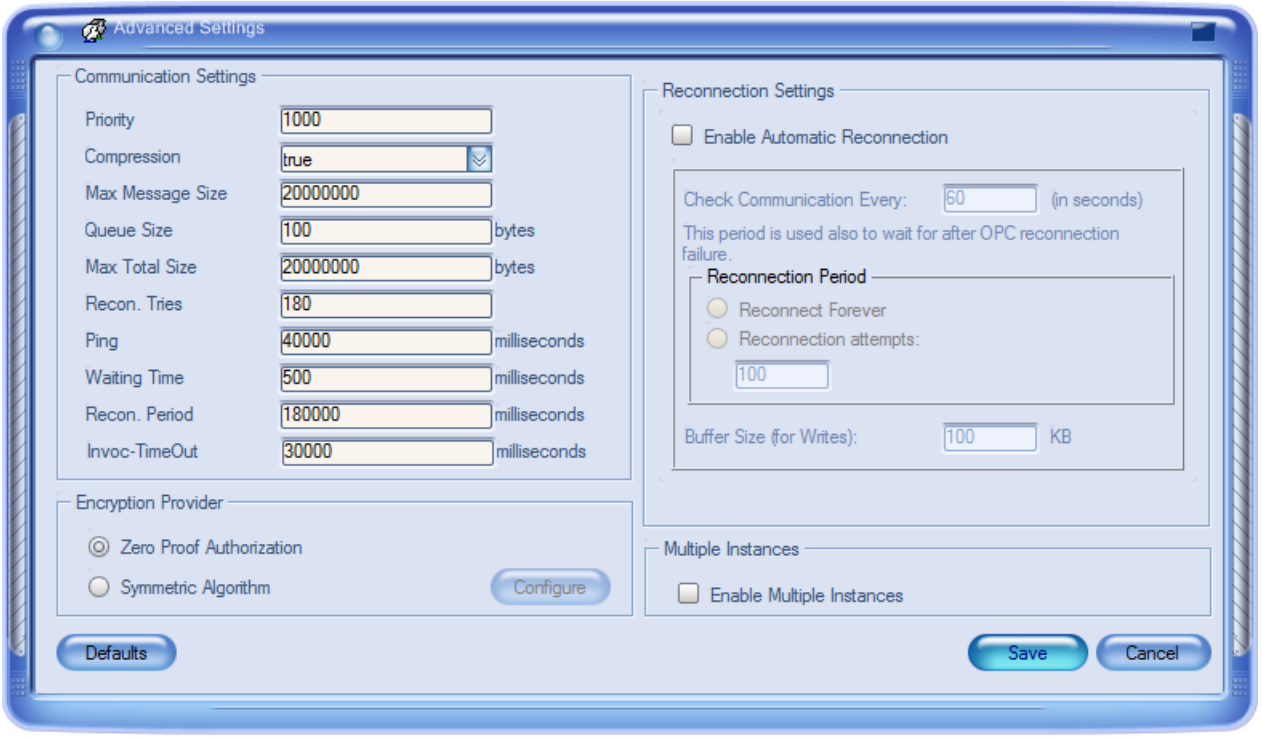


Figure 51: Advanced Settings

You should choose the same encryption provider as configured in the ONB server side.
If you select “Symmetric Algorithm”, you should select the same padding Cipher and padding modes.

If you select the **Enable Multiple Instances** option, you will be able to run each OPC connection separately.

Once the IP Address, Port, Channel and Security Mode are configured, click **OK** or press **Enter**. All retrieved OPC Servers from the specified remote host will be then displayed on the tree view as shown in this screen:

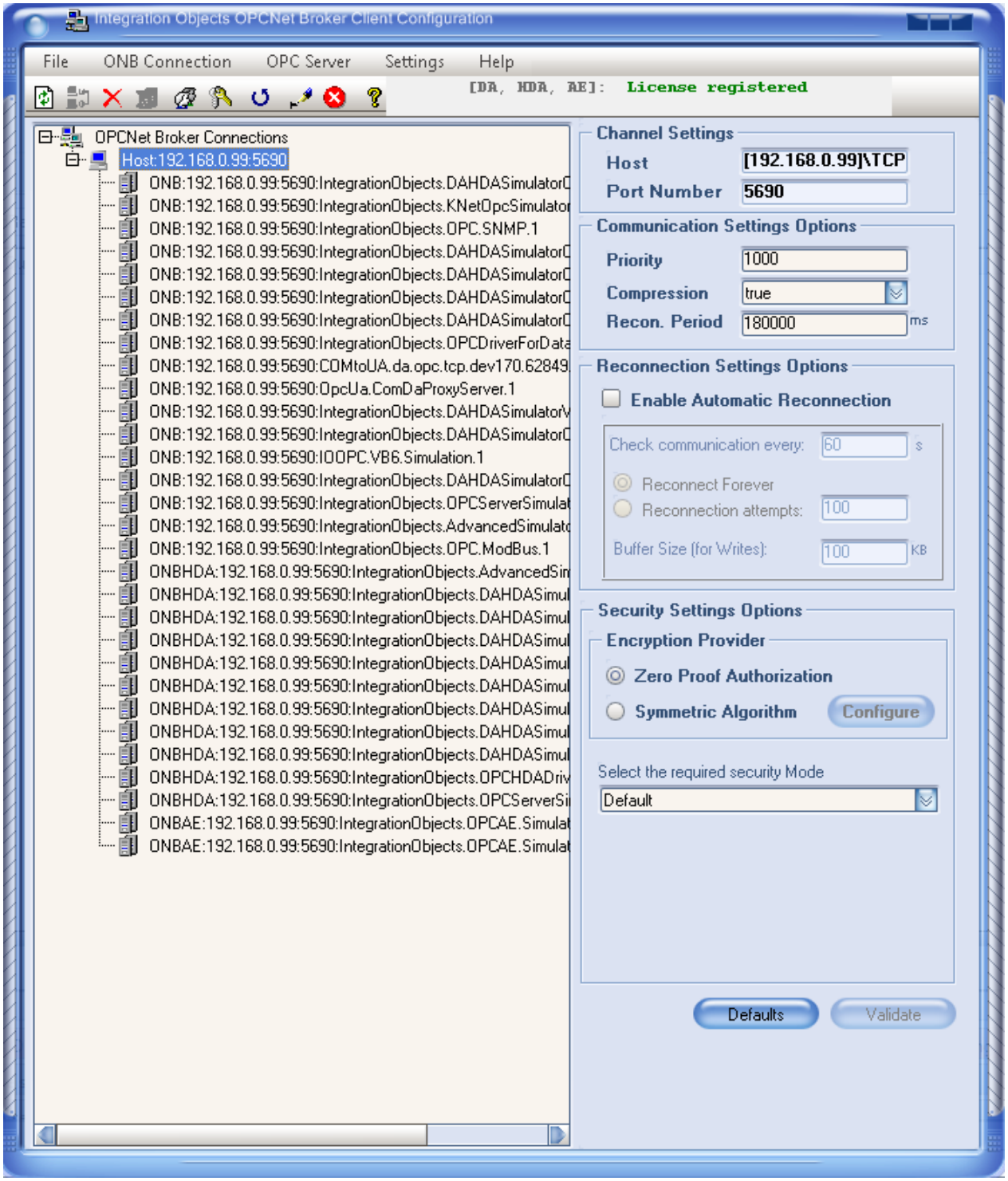


Figure 52: Added ONB Connection (Tree View)

These OPC Servers are assigned with default names.

Default assigned server names have the following syntax:

- DA

```
ONB:<remote hostname>:<Port>:<original OPC Server program ID>
```

Example: ONB:io:5690:IntegrationObjects.OPC.PI

- HDA

```
ONBHDA:<remote hostname>:<Port>:<original OPC Server program ID>
```

Example: ONBHDA:io:5690:IntegrationObjects.OPC.PI

- AE

```
ONBAE:<remote hostname>:<Port>:<original OPC Server program ID>
```

Example: ONBAE:io:5690:IntegrationObjects.OPCAE.Simulation



If you are using a firewall, make sure that the configured TCP port is open between the ONB client and server side. It is recommended to modify the default TCP port.



Make sure that your antivirus does not interfere with the ONB communication.

2.2.2. Adding ONB Connection Manually

If the OPC Client resides in your local machine and you want to communicate with a remote OPC DA/HDA server located in a remote host and only with this server, you can add the wanted server manually.
You can select:

- On **ONB Connection ➔ Add server manually**.
- Or on **Add server manually** contextual menu.

The following screen dialog will appear:

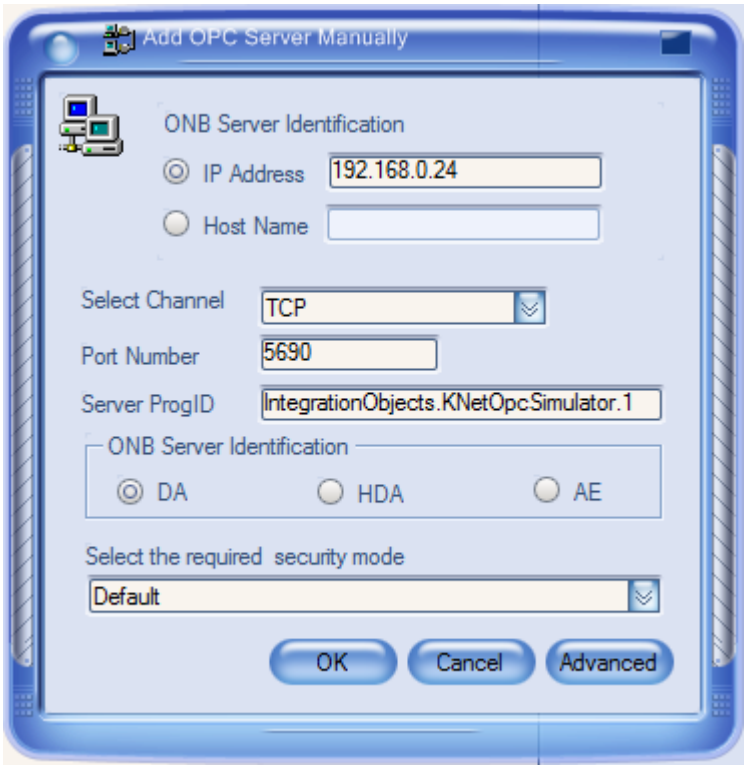


Figure 53: Add ONB OPC Server Manually

This option is similar to the add ONB Connection. The only difference is that in here you can manually add a specific OPC Server.
You just have to enter your server ProgID and select its OPC specification.
This option does not require a connection to the ONB Server side.

2.2.3. Displaying/Modifying OPC Server Configuration

The ONB Client Configuration Tool gives you the possibility to customize some OPC server characteristics like the server name and vendor information. This will allow you mask the original OPC server information for information protection purposes.
You can also configure the “Use Impersonation” option allowing you to pass the user credentials when connecting the OPC server.
For this purpose, select the OPC server that you are interested in, as shown in this screen:

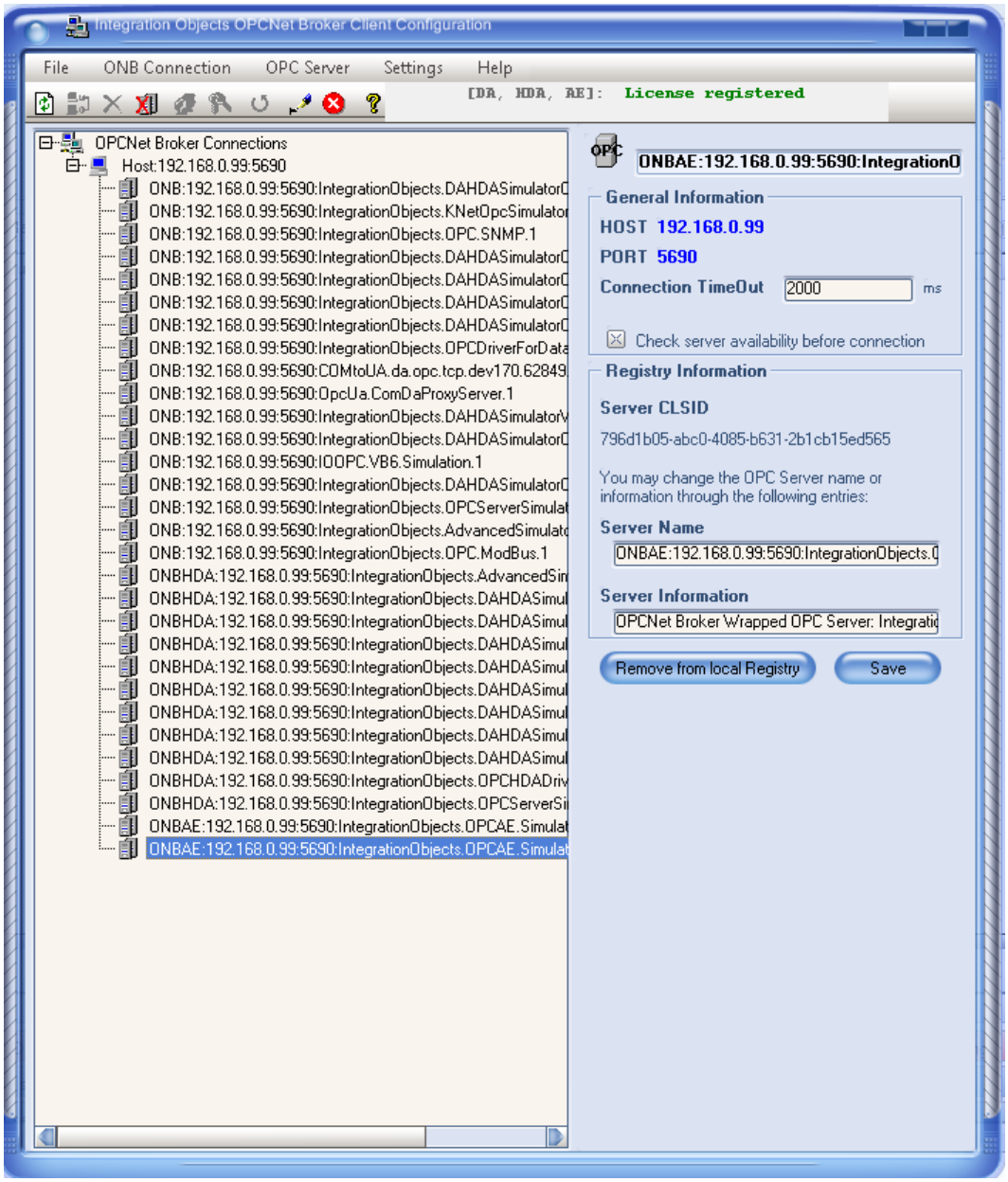


Figure 54: OPC Server Properties

General Information

This displays the selected OPC Server general properties: the host IP Address/Name, the configured port number and the connection timeout.

Registry Information

This displays the selected OPC Server registration information. You have the possibility to modify the server name and information and thus protecting the original OPC server information.

To keep your changes, click **Save**.

Unregister OPC Server

To remove the OPC Server from the registry, click **Remove from local Registry**. You will be asked to confirm this action, as shown below:

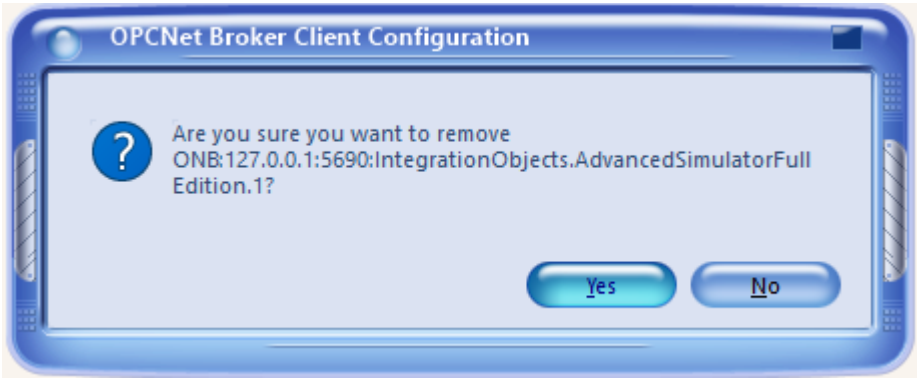


Figure 60: Removing OPC servers

Client Side Impersonation: Use Impersonation

When using the “Encryption, Client Side Authentication” mode, you will be able to turn ON or OFF the “Use Impersonation” option.

If “Use Impersonation” is enabled, All OPC clients running with a mapped account can establish OPC connection through the ONB tunnel. The ONB Server will look up the Windows/Domain accounts mapping in the server side and impersonate the appropriate user when connecting to the OPC servers. This means that the ONB Server will pass the user credential to the OPC servers. The OPC servers may then behave differently based on what user is connected, for example restrict access.

The following figure illustrates the impersonation mechanism:

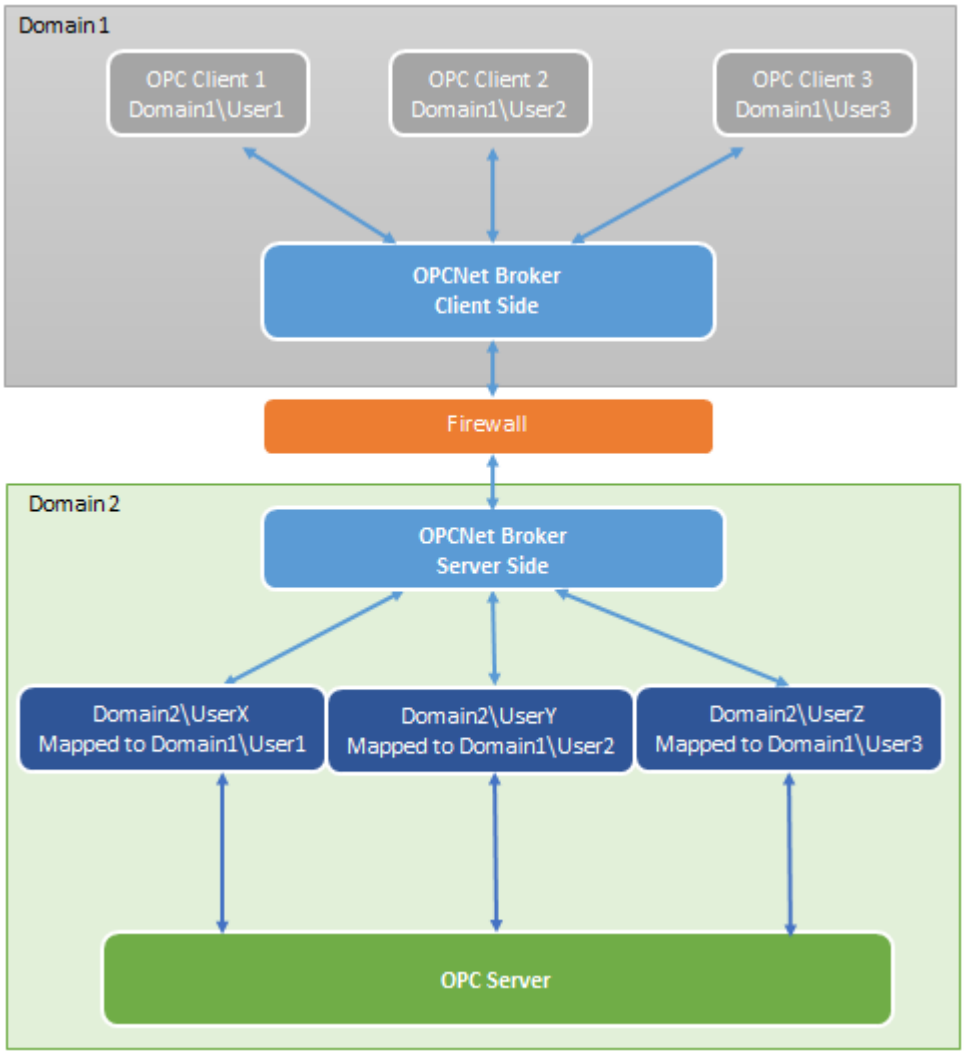


Figure 61: ONB Client Side Authentication - Using Impersonation

Only OPC client running with Domain1\User1, Domain1\User2 or Domain1\User3 can connect to the OPC Server.

When enabling the "Use Impersonation" option and running the OPC Client using Domain1\User1, Domain1\User2 or Domain1\User3, the ONB Server will pass respectively the credential of UserX, UserY, UserZ to the OPC server.

- If "Use Impersonation" is disabled, the ONB server will not pass the credential to the OPC server. The control of the user account will stop at the ONB server level.

2.2.4. Removing An OPC Server

An ONB connection node contains a list of registered OPC servers. You may need to remove a specified OPC server from this list. To do so:

- Select the OPC Server from the list.
- Click on the button  from the toolbar. Before proceeding with server deletion, the application shows a message box asking for confirmation.
- Click **Yes** (if you click **No**, your request will be rejected).



If the removed OPC server is the last entry in the ONB connection node, then the corresponding ONB connection will be removed automatically.



You can also remove an OPC server by selecting it from the tree view and clicking on the Remove from local registry **button.**

2.2.5. Removing ONB Connection

To remove the whole list of retrieved OPC servers from a remote host:

- Select the ONB connection that you want to delete.
- Click on **ONB Connection ➔ Delete** menu, click the button  from the toolbar or click **Delete** in the contextual menu. Before proceeding with ONB connection deletion, the application shows a message box asking your confirmation as following:

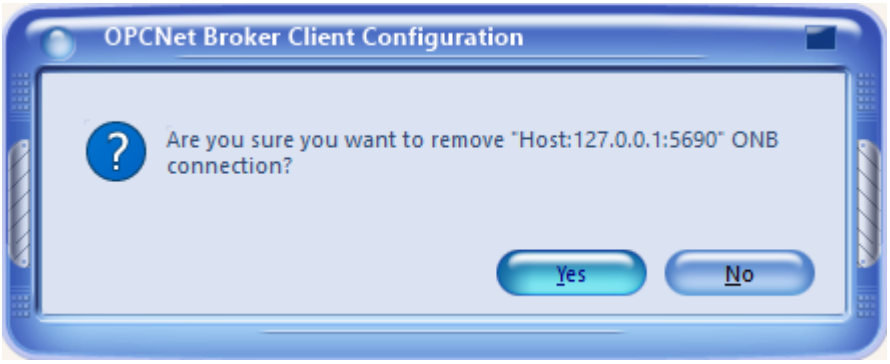


Figure 55: Remove ONB connection

- Click **Yes** (if you click **No**, your request will be rejected). Afterwards, all OPC servers belonging to the selected ONB connection are unregistered: this node and its leaves are removed from the tree view.



You can clean the ONB Client machine from all the added ONB connections by executing the program "ONBCleanUpRegistry.exe" found under the ONB Client installation folder or from the clean up registry context menu.

2.2.6. Clean ONB Connections

You can clean the ONB Client machine from all the added ONB connections by:

- Executing the "ONBCleanUpRegistry.exe" tool located in the ONB Client installation folder,
- Or, clicking on File -> "CleanUp Registry" in the ONB Client configuration tool.

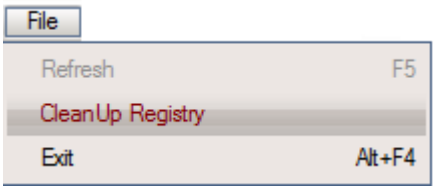


Figure 56: Clean ONB Connections

2.2.7. Refresh ONB Connection

You can refresh a specific ONB connection or all ONB connections at the same time.

Refreshing a specific ONB Connection

For an existing ONB connection, the configuration tool provides a way to retrieve new registered OPC servers from the remote machine.

To refresh an existing ONB connection:

- Select an ONB connection.
- Click on **ONB Connection ➔ Refresh** menu, click on the button  from the toolbar, click on the **Refresh** contextual menu or press **F5** on the keyboard. The Client Configuration tool will then load new registered OPC servers from the connected machine.



If you would like to refresh removed OPC servers, you will be prompted to restore them.

Refreshing all ONB Connections

To refresh all ONB Connections, select the Root node **"OPCNet Broker Connections"** and click **Refresh**, click on the **Refresh** contextual menu or press **F5** on the keyboard.

2.3. COMMUNICATION CONFIGURATION

When an ONB connection is created, the communication parameters are set to default values. To customize these settings:

- Select the **ONB Connection** node that you are interested in,
- Click on **ONB Connection ➔ Settings ➔ Communication** menu, use this button  from the toolbar or click on the **Communication Properties** contextual menu.

You will get the following screen dialog:

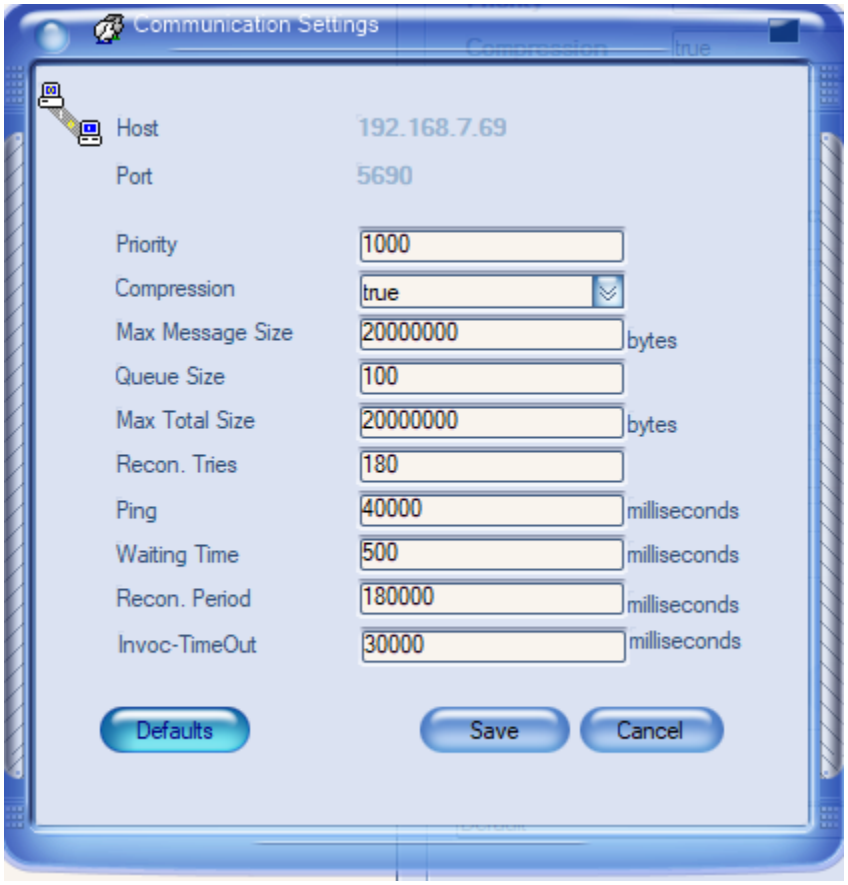


Figure 64 Communication Settings Dialog

- Then, you are invited to enter a set of communication parameters described in the table below.

Parameter	Description	Default Value
Priority	An integer value representing the priority assigned to this connection. The higher the priority is, the higher is the chance for this connection to be established first.	1000
Compression	This field takes one of these values: • True: Data will be then compressed • False: No compression feature	true
Max Message Size	The maximum size of a transmitted message. *Unit = bytes*	20000000
Queue Size	The total number of queued messages.	100
Max Total Size	The maximum total size of queued messages. *Unit = bytes*	20000000
Recon. Tries	The number of reconnection attempts before declaring that the ONB Server connection is lost.	180
Ping	ONB Client sends ping message to the ONB Server within this ping time. *Unit = milliseconds*	40000
Waiting time	The time to wait for after every reconnection failure. *Unit = milliseconds*	500
Recon. Period	When the ONB Server connection is broken, it is expected to re-establish the connection within the specified time interval. Otherwise, the ONB Client declares the ONB connection as closed. *Unit = milliseconds*	180000
Invoc-TimeOut	The ONB request is recognized as failed when the ONB Client does not receive a response from the ONB Server within this time period.	30000

	Unit = milliseconds	

Table 6: Communication Parameters for ONB Client

- Click on **Save** or press **Enter** to save your changes.



You can contact Integration Objects' customer service team to discuss the recommended configuration for your architecture and setup.

2.4. SECURITY CONFIGURATION

When an ONB connection is created, the security parameters are set to default values. To customize these settings:

- Select the **ONB connection** node that you are interested in,
- Click on **ONB Connection ➔ Settings ➔ Security** menu, use this button  from the toolbar or click on the **Security Properties** contextual menu.

You will get the following screen dialog:



Figure 57: Default Configuration

- By default, the **Default** option is selected. You can keep this option or select one of the two other options: **Encryption, Server Side Authentication Mode** and **Encryption, Client Side Authentication Mode**.

If you select **Encryption, Server Side Authentication Mode**, you will get the following dialog:

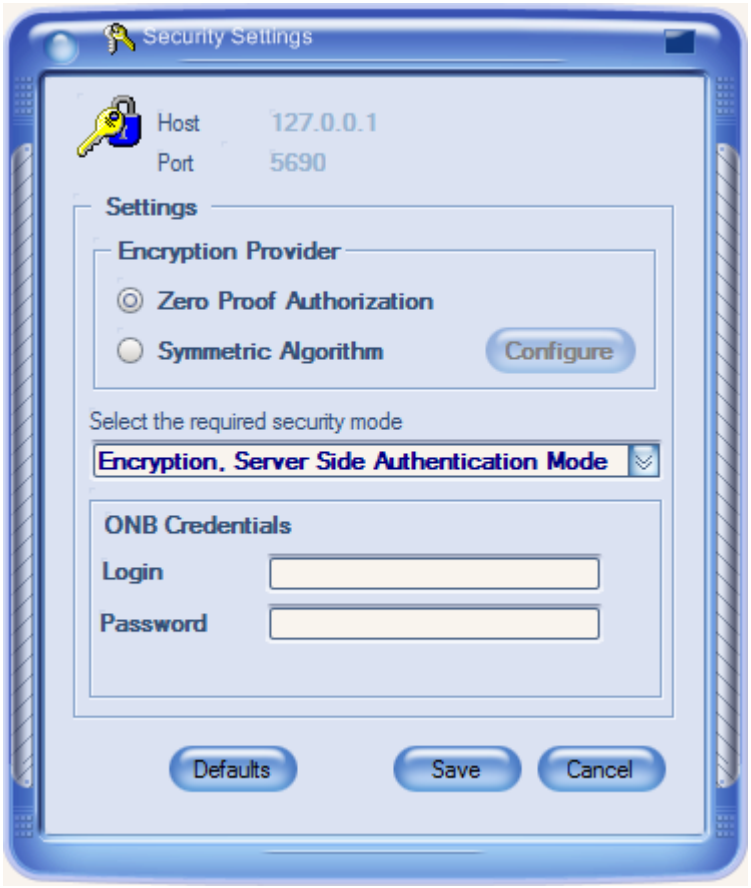


Figure 58: Encryption, Server Side Authentication Mode

Enter valid values for Login and Password. Empty values are not allowed.

If you select **Encryption, Client Side Authentication Mode**, you will get the following dialog:

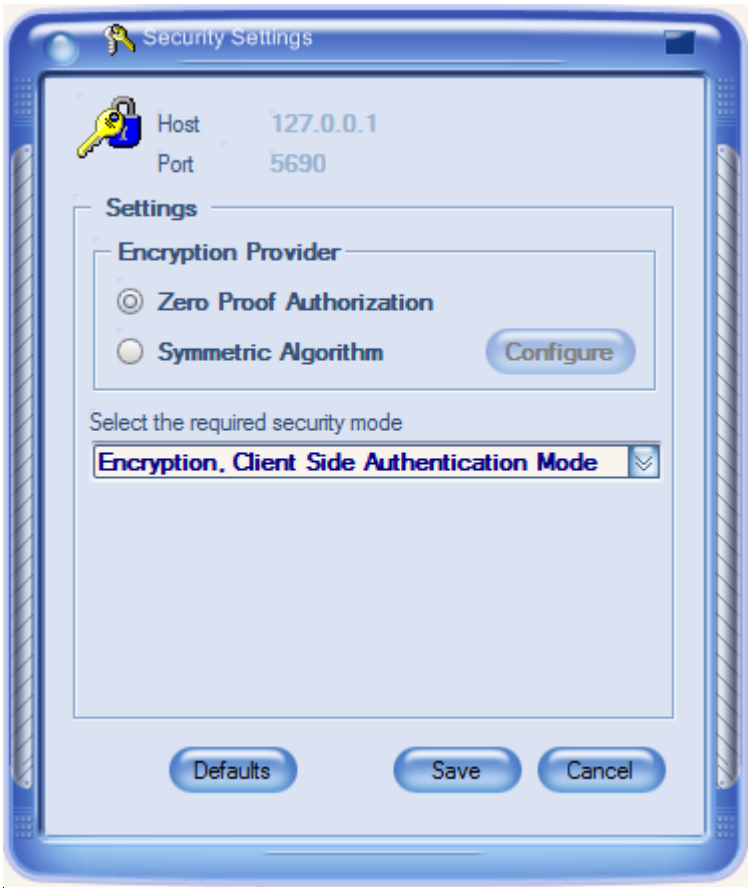


Figure 59: Encryption, Client Side Authentication Mode

Enter valid values for Login, Password and Domain. Empty values are not allowed.

Click **Save** or press **Enter** to save your changes.

The following table describes security parameters:

Parameter	Description
Default	Check this option if you want to disable the user authentication features for ONB data transmission.
Encryption, Server Side authentication	Check this option if you want to enable the Encryption, Server Side Authentication feature for ONB data transmission. The login/password text boxes will then be enabled. Enter valid values (the same values configured on the ONB

	Server side). Besides authentication, security includes data encryption.
Encryption, Client side authentication	Check this option if you want to enable the Encryption, Client Side Authentication feature for ONB data transmission.

Table 7: Security Settings

2.5. DISPLAYING/UPDATING ONB CONNECTION

To display both communication and security parameters for a given ONB connection, click on the ONB connection that you are interested in.

The settings relative to the selected ONB connection are shown in the following screen:

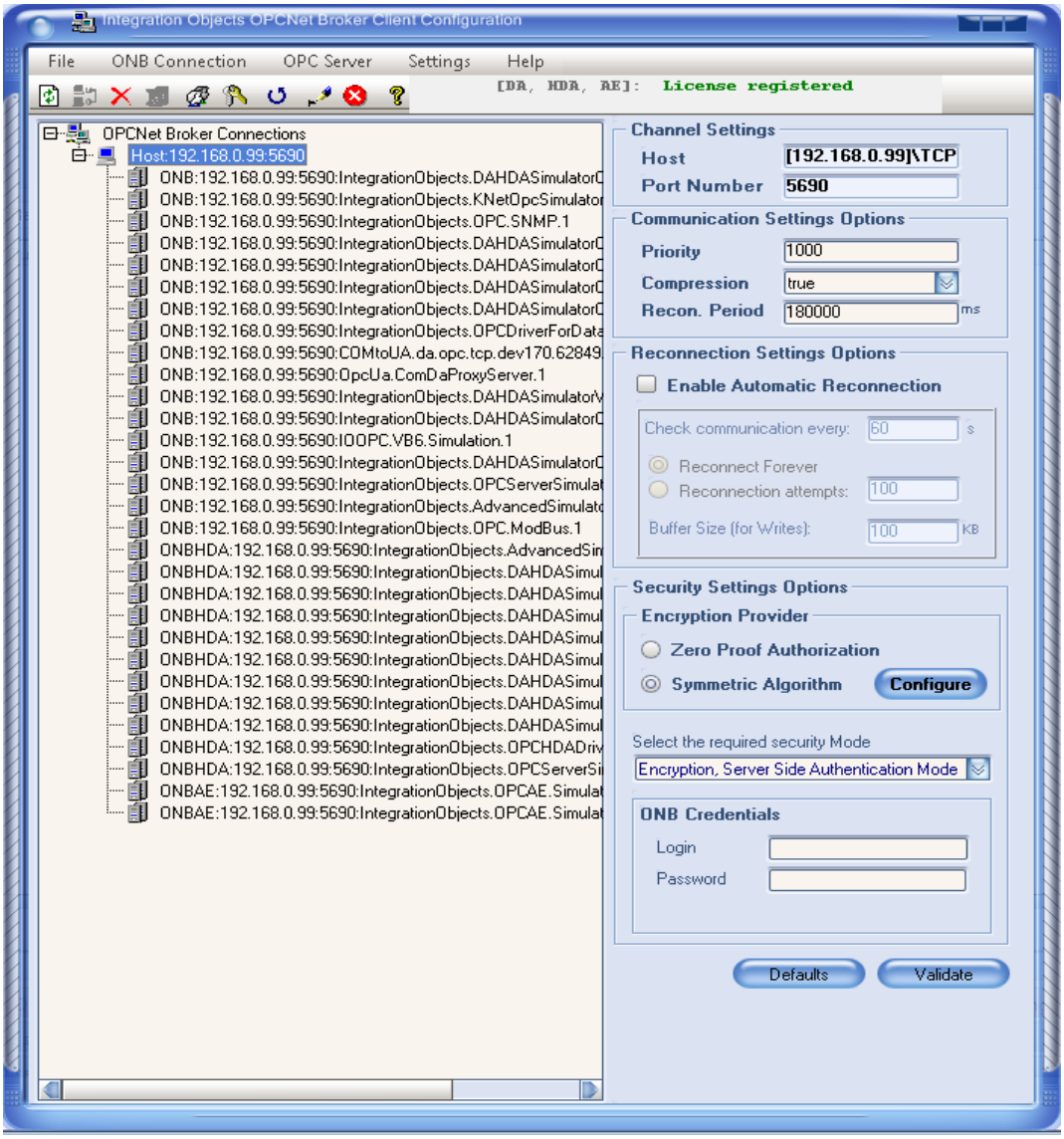


Figure 60: ONB Connection Properties

Communication Settings

This section displays the selected ONB connection's current communication properties.

Reconnection Settings Options:

This section displays the selected ONB connection's current reconnection status.

Security Settings

This section displays the selected ONB connection's current user authentication properties.

You may change communication, reconnection or security settings. To save changes, click **Save Changes**. Otherwise, click **Leave without changing**.

2.6. REDUNDANCY

2.6.1. OVERVIEW

The OPCNet Broker increases the availability of your OPC data by an easy implementation of redundancy for your OPC servers.
You can configure multiple redundant pairs. The OPCNet Broker will be responsible for switching to the secondary OPC server when any problem arises with the data coming from the primary OPC server.

2.6.2. CONFIGURATION

In order to configure the redundancy for you OPC Server settings:

- Add at least two ONB connections: one containing your primary OPC server and the other containing the backup OPC server.
- Right click on the OPC Server from the available OPC Servers list
- Click on **Set redundant OPC Server**

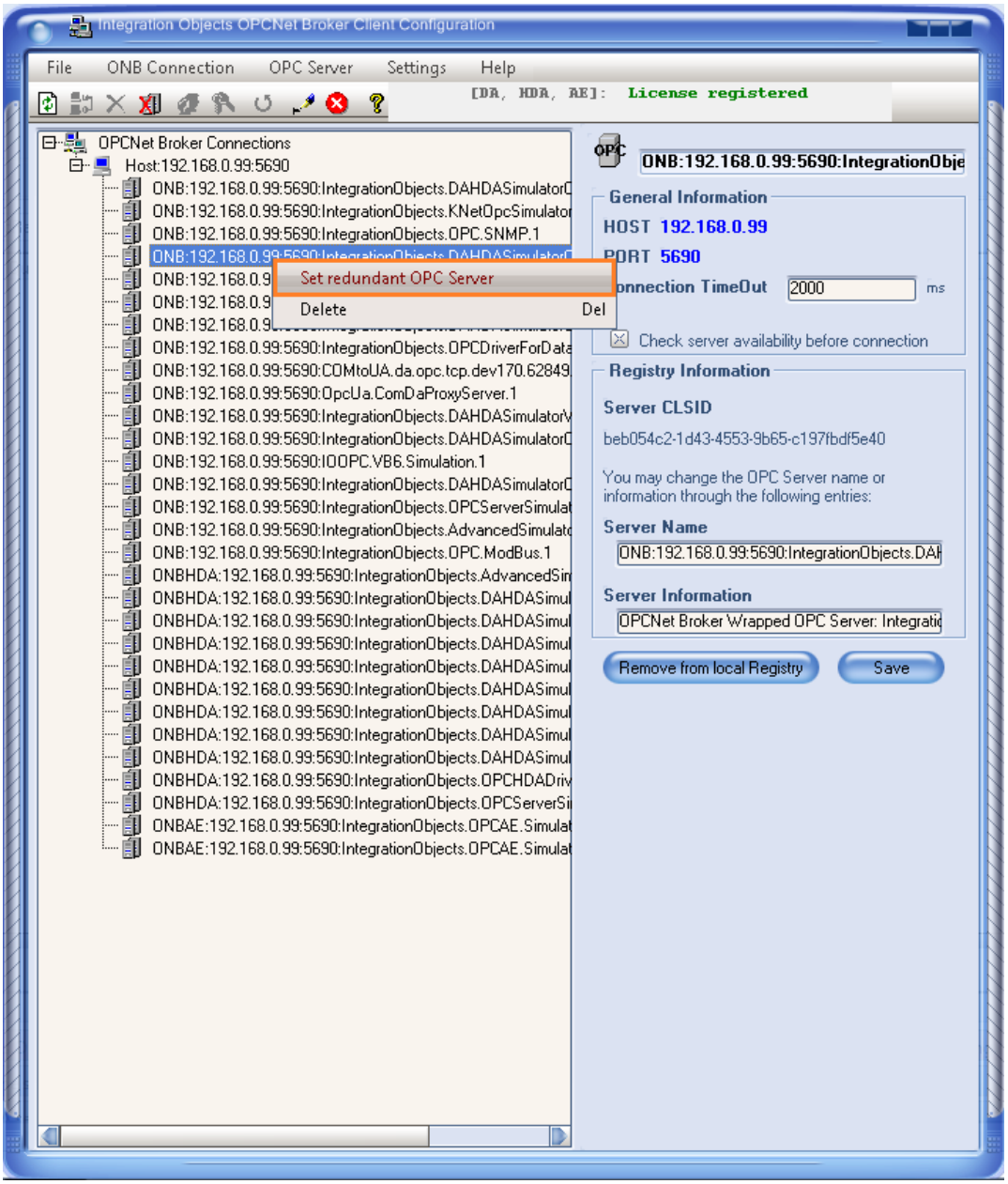


Figure 61: Set Redundant OPC Server

- Enter the redundant OPC Server progID and select the detection parameters:
  - **Check TCP communication availability:** The OPCNet broker Client side will switch to the redundant OPC Server in case the communication with the OPCNet broker Server of the Primary OPC Server machine is not healthy.

- **Get OPC Server Status**: The OPCNet Borker Client will switch to the redundant server if the primary OPC server in the distant machine is down.
- **Configure a watchdog tag**: This setting will enable watchdog functionality. Once enabled, The OPCNet Borker Client will switch to the redundant OPC Server if the configured watchdog tag stops changing its value during a specific timeout.
- **Watchdog timeout:** It defines the maximum time allowed for the watchdog tag to remain unchanged. If no changes in values occur within this specified timeout, the OPCNet Borker Client will switch to the redundant OPC Server.

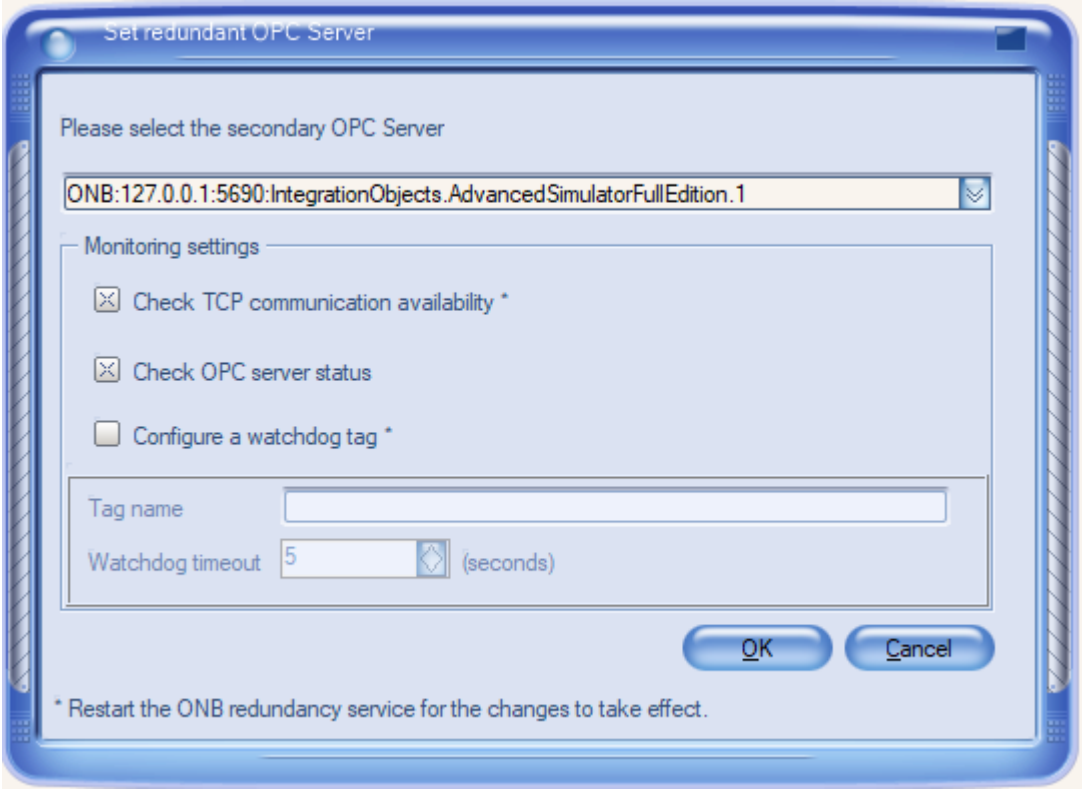


Figure 70: Configure Redundant OPC Server

The OPCNet broker redundancy service will monitor the availability of the distant machine or OPCNet broker server and switch to the redundant OPC Server accordingly.

The configuration of the redundant OPC Server must be before the connection to the primary OPC Server from an OPC Client. Otherwise, you need to redo the connection.

In order to install and run this monitoring service:

- Go to **Settings ➔ OPC Server Redundancy**
- Click on **Install Service** to install and start the redundancy service

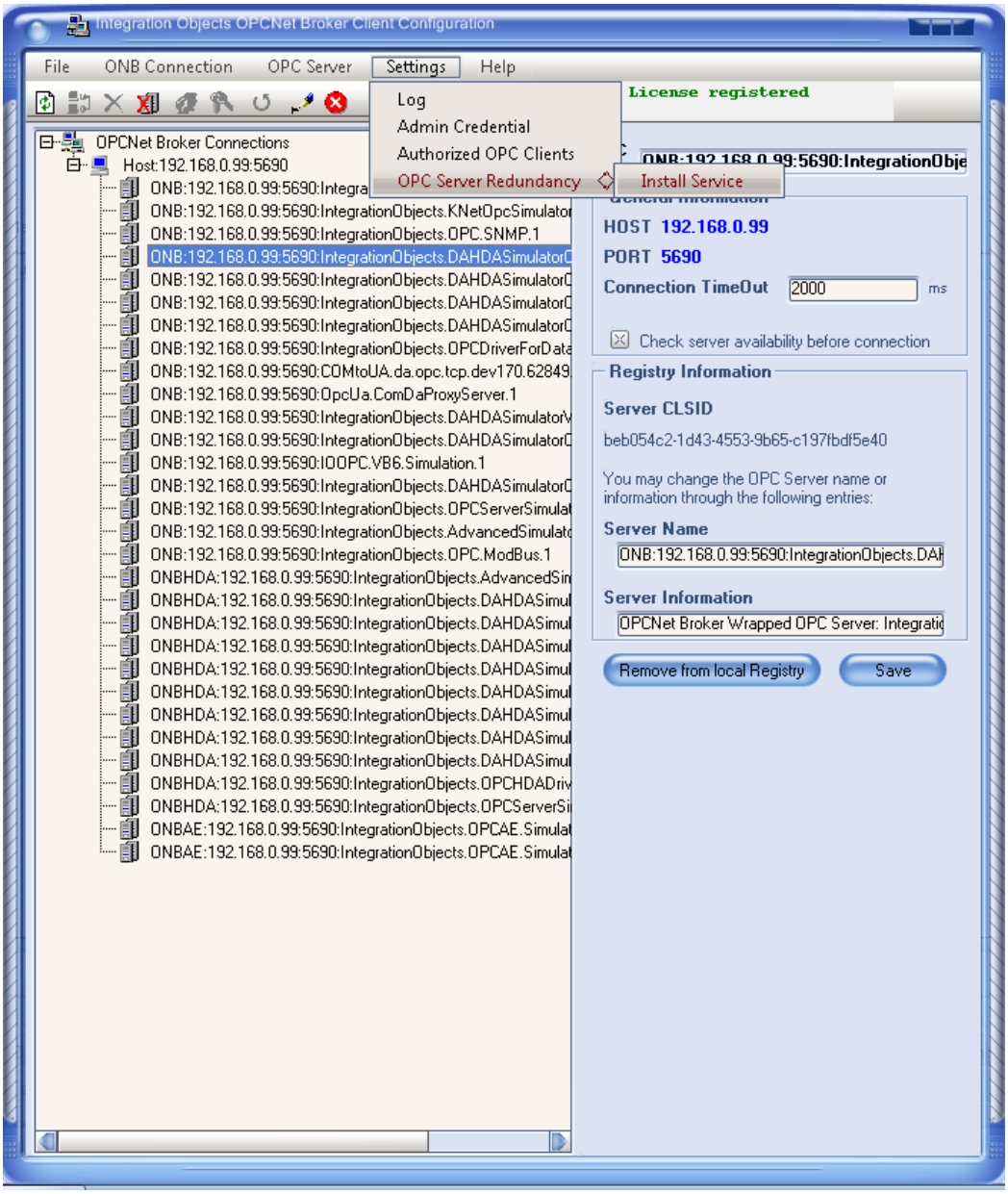


Figure 62: OPC Server Redundancy Service

2.7. Automatic OPC Reconnection

2.7.1. Overview

Since its first release, ONB has supported the functionality of ONB Reconnection. Whenever the network link is broken, ONB tries to re-establish the connection over the given reconnection period. If it succeeds, all reads and writes during the network problem period are processed and there is no loss of data.

But what happens when the OPC Server crashes?

First implemented in the release of ONB 1.4.0, the product launches an automatic OPC reconnection whenever the communication is stopped due to an OPC Server problem. ONB starts the OPC reconnection procedure according to the configured parameters (reconnection tries, reconnection period, etc.). When the OPC connection is re-established, ONB restores itself to the same state as when the OPC connection was broken.

2.7.2. OPC Reconnection Scenario

In this section, a typical OPC Reconnection scenario is presented.

1. The following figure illustrates the initial state: the OPC connection is up.

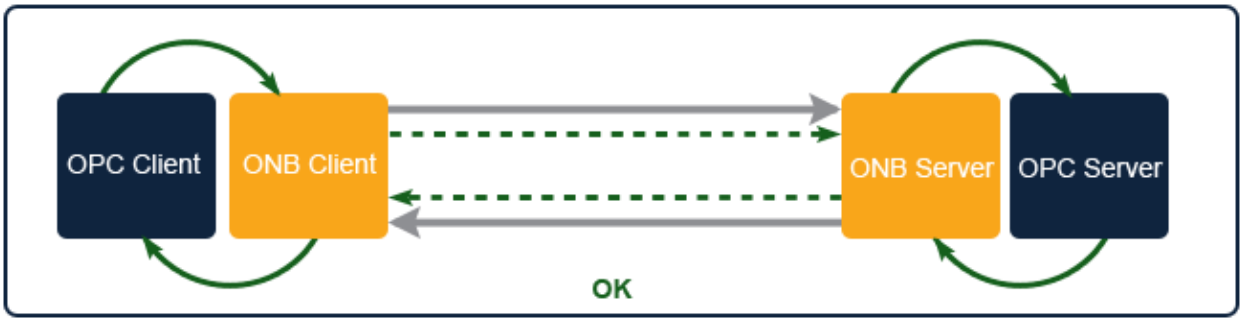


Figure 63: OPC Reconnection - Connection Is Up

2. The OPC Server goes down, knowing that the OPC Client is in state A.

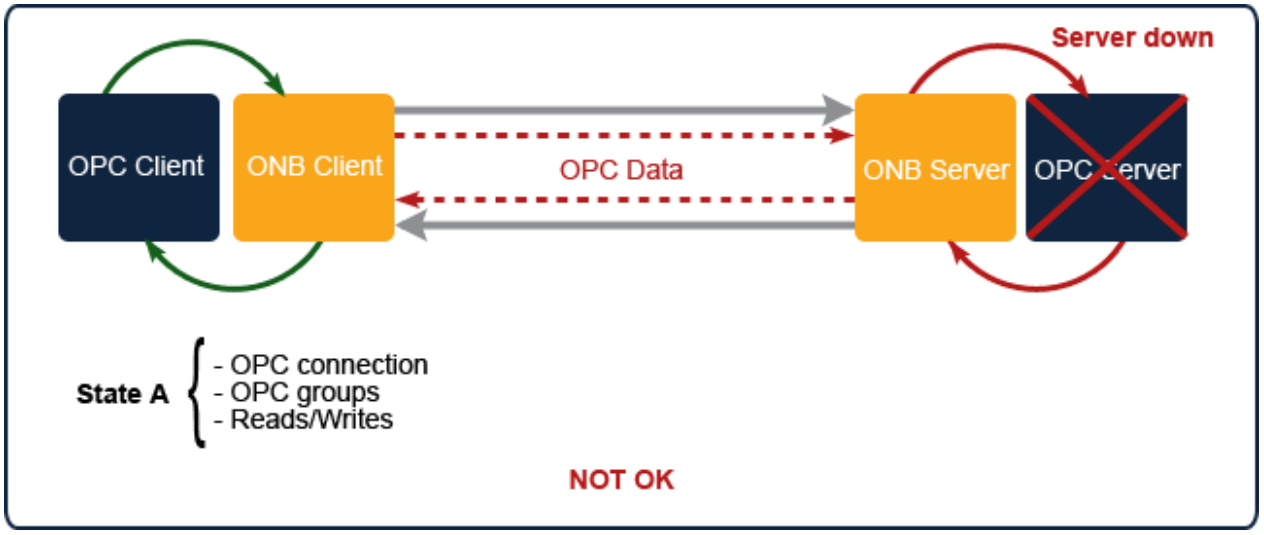


Figure 64: OPC Reconnection - OPC Server Goes Down

The ONB Client is no longer receiving data from the ONB Server. Consequently, it starts the OPC reconnection procedure.

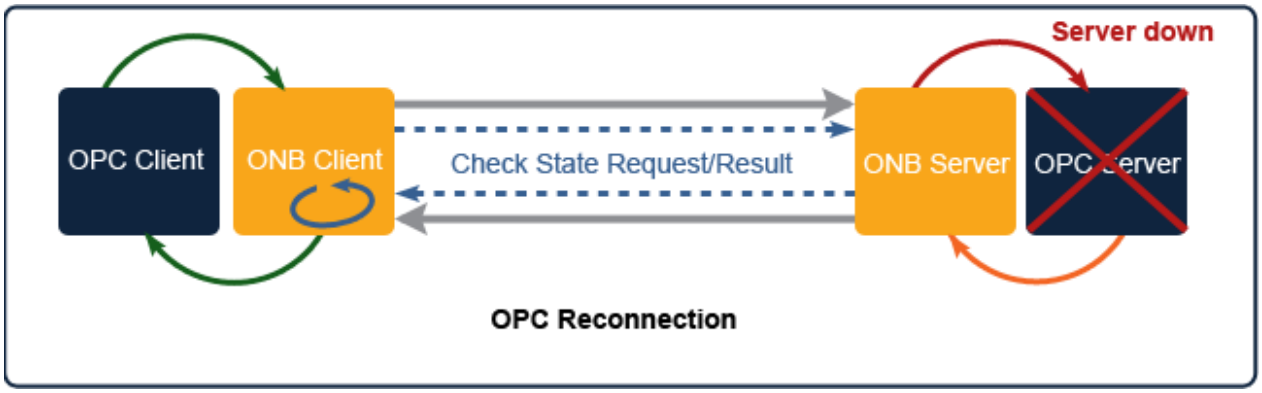


Figure 65: OPC Reconnection - Start Reconnection

3. The OPC reconnection procedure has succeeded. The OPC sever is up and the OPC connection is re-established.

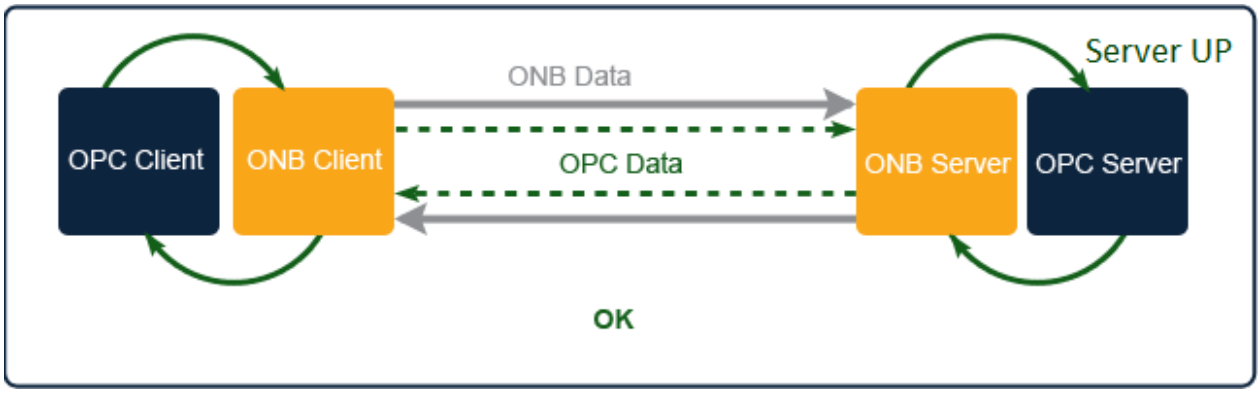


Figure 75: OPC Reconnection - OPC Server Is Up

2.7.3. CONFIGURATION

To configure the OPC reconnection settings:

- Select the ONB connection that you are interested in,
- Click on **ONB Connection ➔ Settings ➔ Automatic Reconnection** menu, click on this button  from the toolbar or click on the **Settings ➔ Automatic Reconnection** contextual menu.

You will get the following dialog screen:

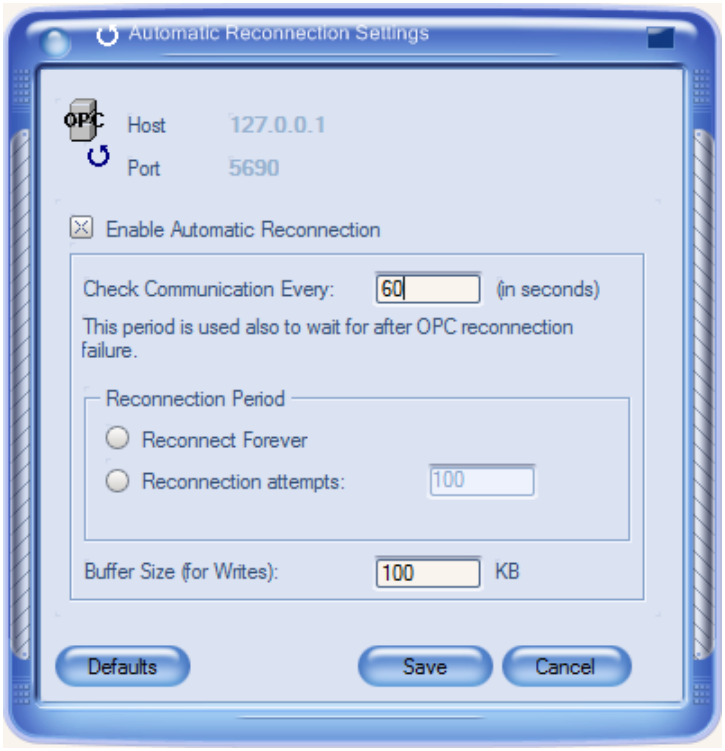


Figure 66: Automatic Reconnection Settings

- Set the reconnection parameters:
  - Check the **Enable Automatic Reconnection** box to configure its settings.

Once the automatic reconnection is enabled:

- Set the period (in seconds) of reconnection checking. This will also be the period separating two OPC reconnection attempts.
- If you want to specify the reconnection period, set the **Reconnection Attempt.** Otherwise, select the **Reconnect Forever** option where ONB will try to reconnect to the OPC Server indefinitely until the reconnection is re-established.
- Define the buffer size. This buffer will be used in case an OPC connection failure happens while the OPC client is sending write operations. If the size of the write operations exceeds the buffer size, the ONB client will delete the least recent operations.



- **The Automatic Reconnection is available for the OPC DA, HDA and A&E specification.**
- **If the OPC Client supports the Automatic Reconnection, it is recommended to disable the automatic reconnection feature in ONB.**

2.8. CONFIGURE AUTHORIZED OPC CLIENTS

The OPCNet broker give you the possibility to configure authorized OPC clients. This feature will secure the use of the OPC link from unauthorized applications.
In order to configure the authorized OPC clients list, you just need to open the ONB Client Configuration Tool and click on **Settings** then **Authorized OPC Clients** as illustrated below:

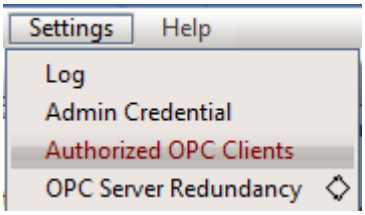


Figure 67: Authorized OPC Clients

When you click on the **Authorized OPC Clients**, you will get the following screen:

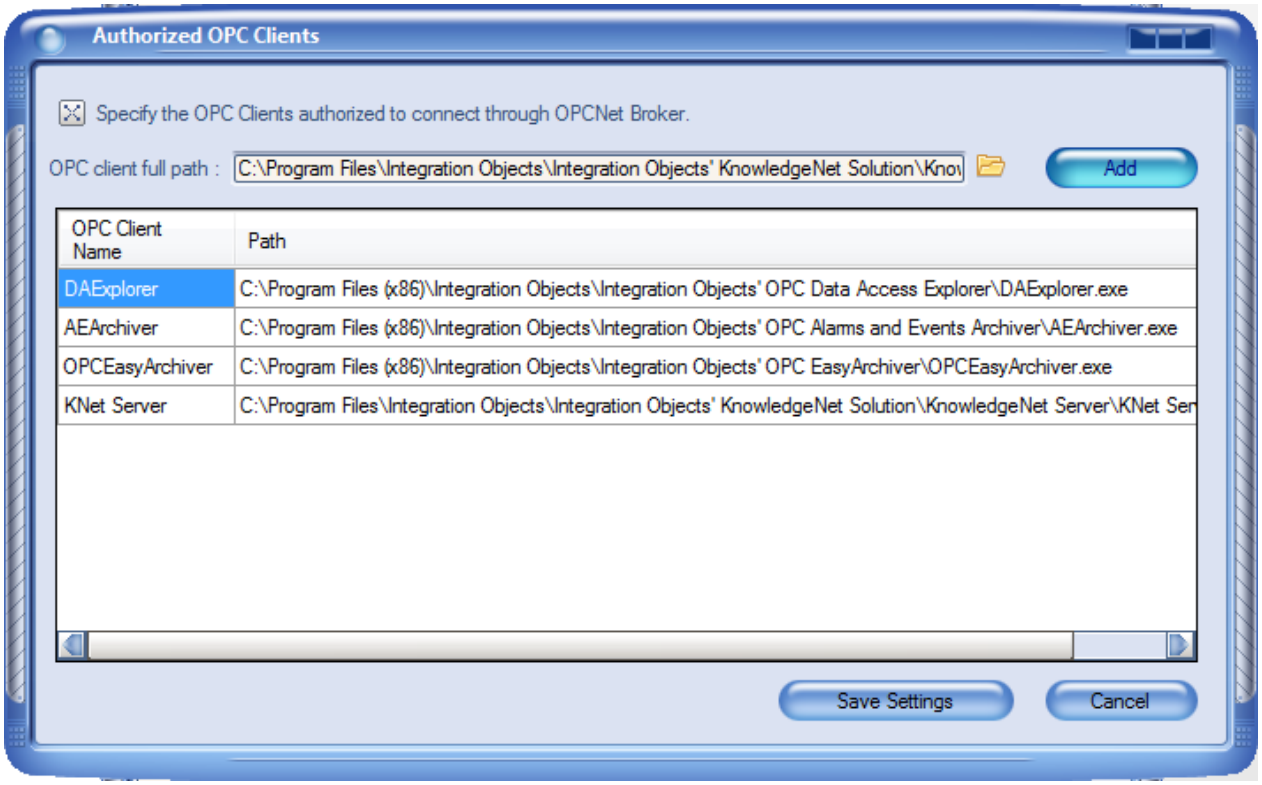


Figure 68: Adding Authorized OPC Clients

In order to add Authorized OPC Client you just need to browse for the OPC Client component and then click on **Add**.

After adding configuring the authorized OPC Clients list, you must click on **Save Settings**.
In order to activate this feature, you need to enable the option "**Specify the OPC Clients authorized to connect through OPCNet Broker**"

2.9. LOG SETTINGS

The ONB Client Configuration Tool gives you the possibility to display/edit log settings for the ONB Client Side.

In order to view these settings, you should:

- Click on the **Logging ➔ Configure** menu or this button from the toolbar.

You will get the following dialog box that shows the current logging parameters:

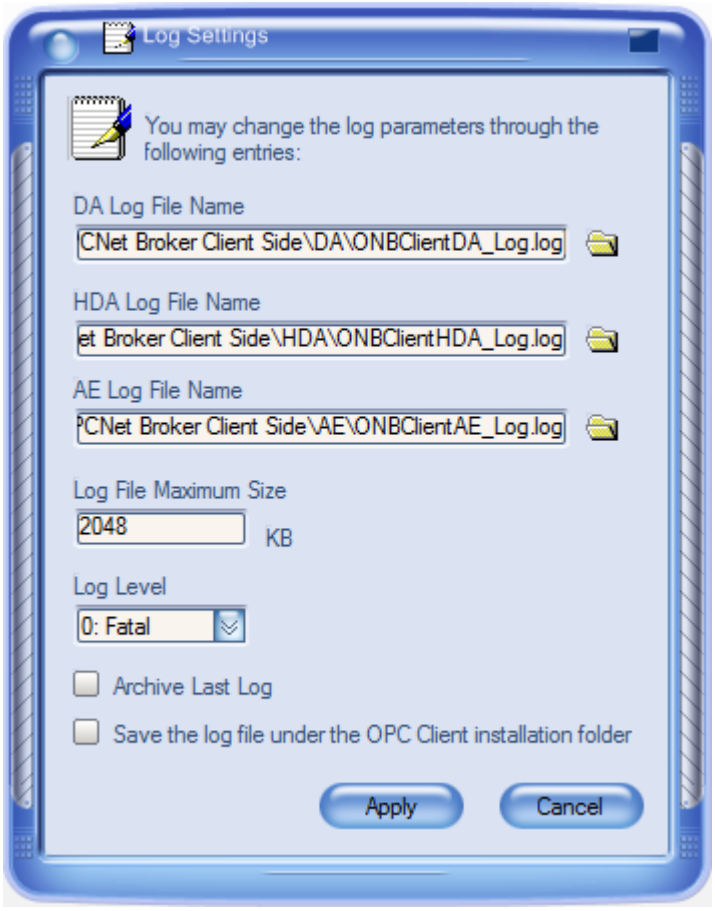
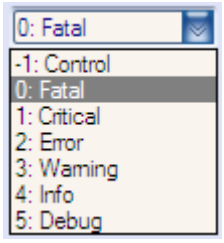


Figure 69: Logging Settings Dialog

Log parameters are described in the following table:

Parameter	Description
Log File Name	You can rename the log events file generated by the ONB-C program. There are three log files, one log file for each specification.
Log Level	Depending on your needs, you may use a high log level to display full information describing program execution step by step or use a low level under normal behavior. Select a value from this combo box:  **Figure 70: Log Levels** Possible options: • **Debug**: Debug messages. This is the highest level. • **Info**: Information messages. • **Warning**: Warnings. • **Error**: Errors. • **Critical**: For critical errors. • **Fatal**: Fatal errors. Critical and fatal errors could stop ONB execution. • **Control**: This is the lowest log level. We recommend using this level for better performance. The log levels are ordered so that each log level includes all log messages of all lower log levels.
Log File Maximum Size	The maximum log file size, in kilobytes
ArchiveLastLog	You can check the **ArchiveLastLog** option if you want to copy old logs to an intermediate file with incremental extension, before being overwritten whenever the maximum file size is reached. Otherwise, any pre-existing log file is overwritten at start-up.

Save the log file under the OPC Client installation folder	You can have a separate log file for each connected OPC client. This is a very important option.

Table 8: ONB Client Log Parameters

Enter your parameters and click **Apply** or press **Enter** to save your changes.

2.10. LICENSE STATUS

Text indicators at the top right side of the ONB Client Configuration Tool are used to display the license status of the ONB Client features, as follows:

- License registered: if the ONB Client license is activated
- Trial valid: if the ONB Client trial license is used and the demo period still valid
- Trial expired: if the ONB Client trial license expired
- Backdating: this status occurs if the ONB Client trial license is used and the system date was changed.

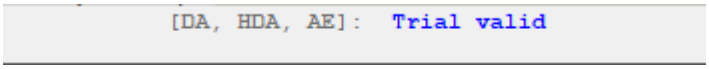


Figure 71: ONB Client License Status

USING OPCNET BROKER

1. Overview

Once the OPCNet Broker is installed and properly configured on your C/S machines, you can connect your OPC DA/HDA/AE Clients to any OPC DA/HDA/AE Server in the network without any DCOM configuration and system rebooting.

In this chapter, we will use OPC DA as our example. Assume that your OPC Client is installed on machine "IO_CLIENT" and tries to connect to an OPC Server (ex. progID = *IntegrationObjects.Simulation.1*) installed on remote machine "io".

Without ONB, you would have to run the DCOMCNFG utility and go through all the DCOM configuration difficulties.

With ONB, simply install and configure ONB-S on "io", ONB-C in "IO_CLIENT" and click on the **ONB:io:5690:IntegrationObjects.Simulation.1** (OPC DA server) shown in the list of local OPC Servers for machine "IO_CLIENT" (for in-process context).

2. Required Steps

If the OPC Server and the OPC Client communicate through a firewall, it must be properly configured. The following are the required steps to successfully run OPCNet Broker.

2.1. ONB Configuration

This section describes how to configure ONB (the server and client sides) for a TCP communication:

- Default mode
- Using Security: Includes authentication and encryption

2.1.1. Default Mode

2.1.1.1. OPCNet Broker Server Side Configuration

1. For its first use, configure the ONB Server with the server configuration utility.

2. Next, start the ONB Server to make it available for listening to clients' connection attempts.

2.1.1.2. OPCNET BROKER CLIENT SIDE CONFIGURATION

This configuration sample is given using in-process context.

1. For the first utilization, configure the ONB Connection by using the ONB Configuration Tool (see the ***Configuration*** chapter). To do so, open a new session. Then, click **Add ONB Connection** and enter the requested parameters:



Figure 72: Add ONB Connection Dialog

Click **OK**, then a new node **Host:IO:5690** will be added to the tree view. All retrieved OPC servers from the remote machine "io" are registered in the local machine with default assigned server names **ONB:io:5690:ServerName**.

2. Check if **ONB:io:5690:IntegrationObjects.Simulation.1** figures in the tree view under the **Host:io:5690** node. If not, select the **Host:io:5690** node and click **Refresh**.

3. Select the **Host:io:5690** node and click on the **ONB Connection ➔ Settings ➔ Communication** menu to set communication parameters such as **Recon. Period**.

4. Click on the **ONB Connection ➔ Settings ➔ Security** menu and select the **Default** option as shown in this dialog screen:

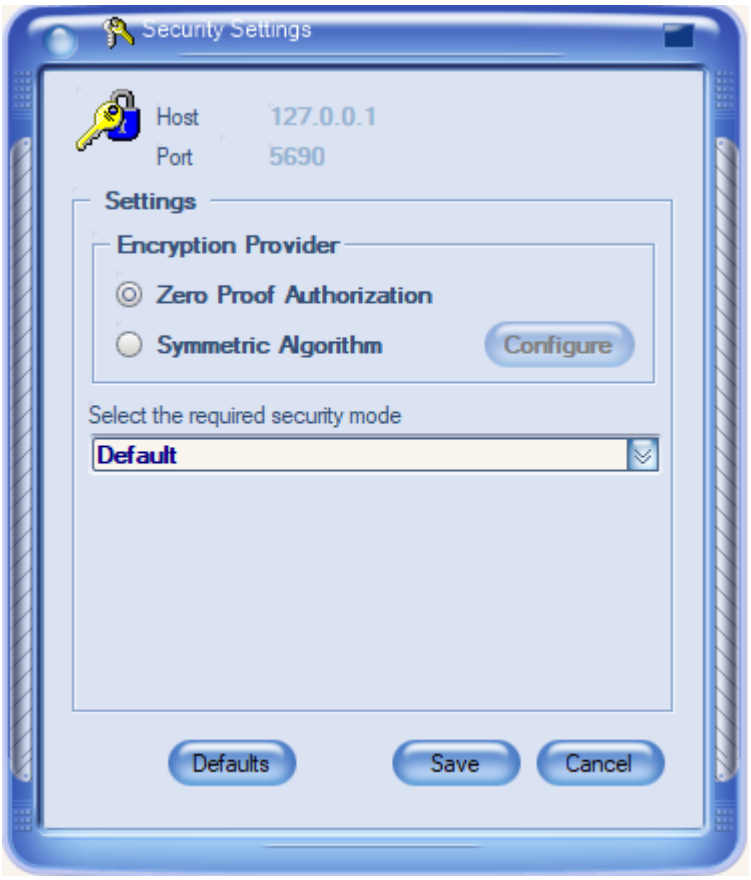


Figure 73: Security Settings Dialog

5. Click the **Save** button.

6. Close the Client Configuration Tool.

2.1.2. Using User Authentication

2.1.2.1. OPCNet Broker Server Side Configuration

For the first utilization, besides communication settings, you should configure security for the server through the server configuration utility.

Start the ONB Server configuration from **ONB Server Menu ➔ Settings** and proceed as follows:

1. Select **Security** and click **Configure Users** to configure user accounts, for example (Login: test, Password: test).
2. If you want to use OPC Tag Security, enable the OPC Tag security module. To do so, check the **Enable OPC Tag Security** option and click **Configure** to start OPC Tag Security tool to configure OPC servers and OPC tags permissions as described in the OPC Tag Security user's manual.
3. Start the ONB Server.

2.1.2.2. OPCNet Broker Client Side Configuration

1. For the first use, configure the ONB connection by using the ONB Client Configuration Tool (refer to the ***Configuration*** chapter). To do so, open a new session. Then, click **Add ONB Connection** and enter the requested parameters:

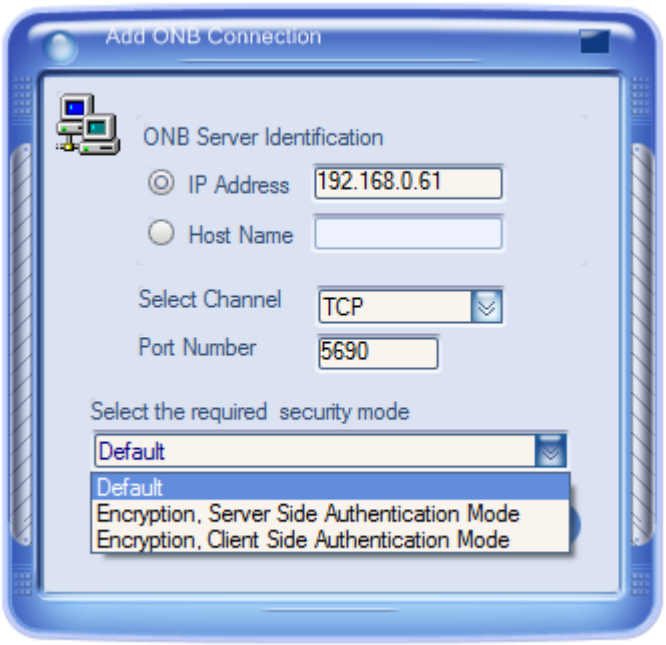


Figure 74: Add ONB Connection Using Security

Enter valid values for Login and Password. (Login, Password) pair should be the same as the configured credentials list at the ONB Server side.

Both login and password fields are both case sensitive.

Click **OK**. A new node **Host:io:5690** will be added to the tree view. All retrieved OPC servers from the remote machine "io" are registered in the local machine with default assigned server names **ONB:io:5690:ServerName**.

2. Check if **ONB:io:5690: IntegrationObjects.Simulation.1** figures in the tree view under the **Host:io:5690** node. If not, select the **Host:io:5690** node and click **Refresh**

3. Select the **Host:io:5690** node and click on **ONB Connection ➔ Settings ➔ Communication** menu to set communication parameters such as **Recon. Period**.

4. Click on the **ONB Connection ➔ Settings ➔ Security** menu and check the Supporting Security option as shown in this dialog screen:



Figure 75: Security Settings

5. Close the Client Configuration Tool.

2.1.3. Compression Configuration

You should enable compression in both the ONB Client and ONB Server sides in order to enable data compression regardless of the security settings. Otherwise, compression is disabled by default.

2.1.3.1. OPCNet Broker Server Side Configuration

Set the Compression server parameter to **true** through the configuration menu as shown below:

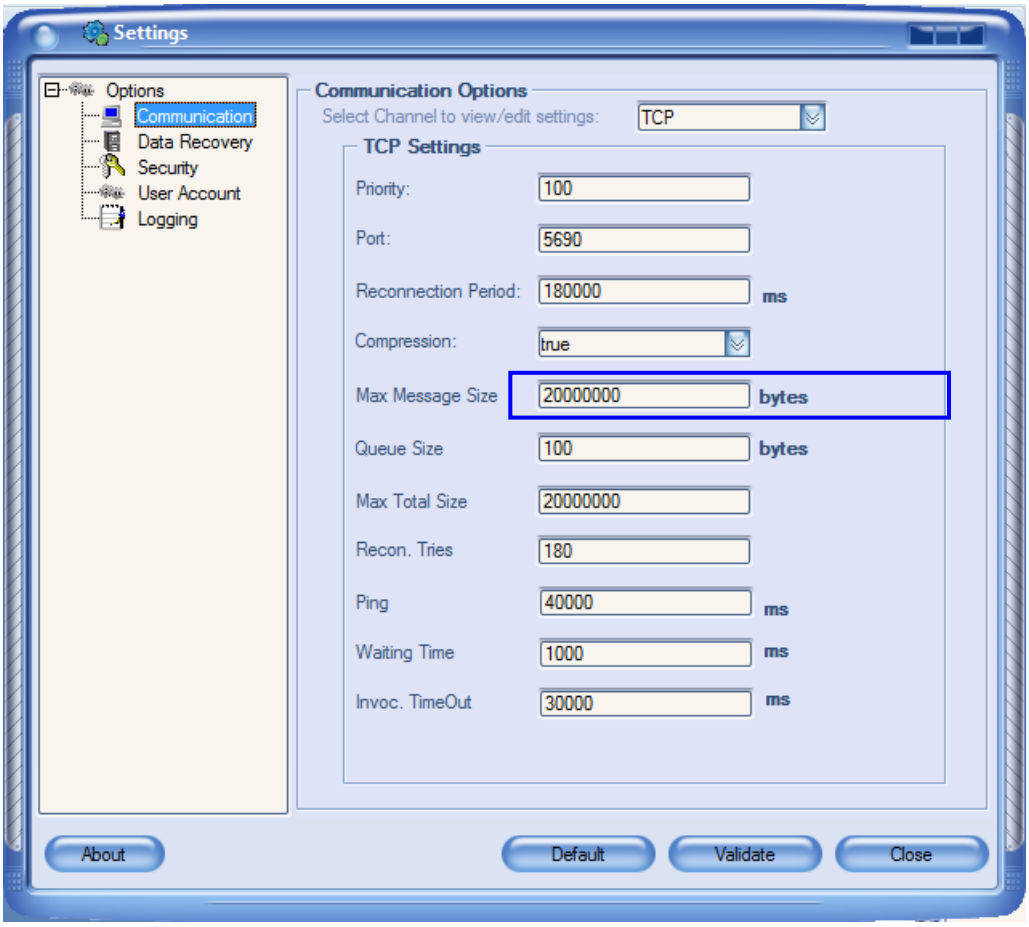


Figure 76: Enable Compression

Then click **Apply**.

2.1.3.2. OPCNet Broker Client Side Configuration

To enable compression for in-process context using the Client Configuration Tool, select the ONB connection **Host:io:5690** and select the **true** value from the Compression combo box at the right side.

To enable compression for out-process context, open the ONB Client configuration tool. Click on **Out-process Context** and then set the compression flag to **true**.

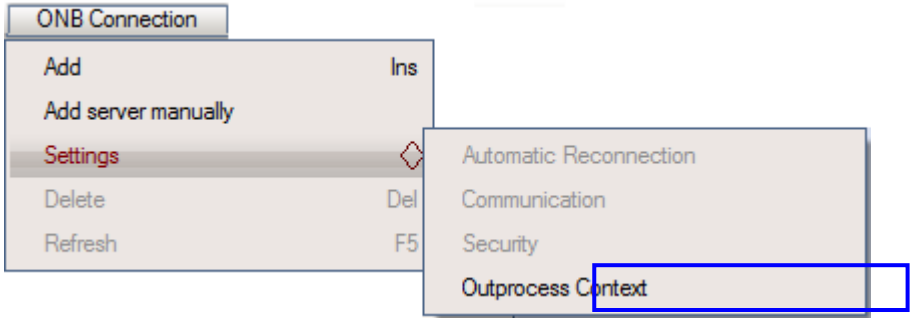


Figure 77: Out-process Context

2.2. OPC COMMUNICATION THROUGH ONB

This section describes how to connect the existing OPC Client (Integration Objects' OPC EasyArchiver) to the existing OPC Server (Integration Objects OPC Server for Simulation) using ONB.

To do so, start your OPC Client and then double-click on **ONB:127.0.0.1:5690:IntegrationObjects.AdvancedSimulator.1** from the local list as shown here:

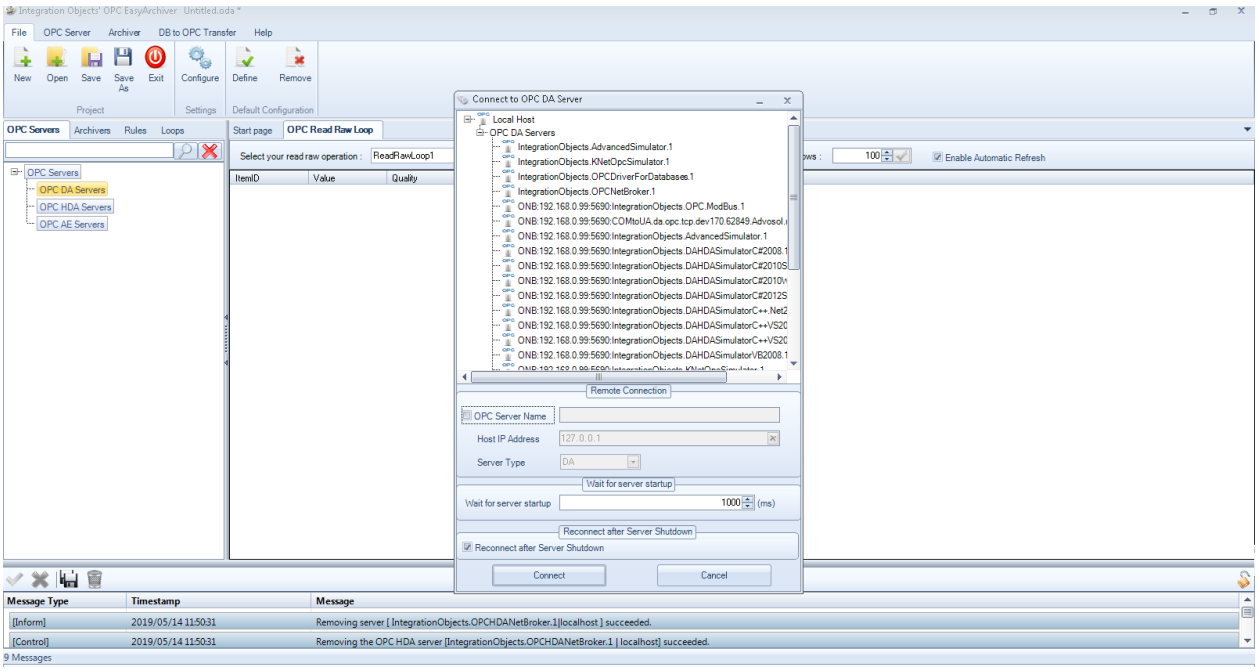


Figure 78: Connect to Tunneled OPC Server

If your OPC client does not support in-process servers, double-click on **IntegrationObjects.OpcNetBroker.1** from the local OPC servers list. After adding a group and items, you will receive data changes as shown in the following screenshot:

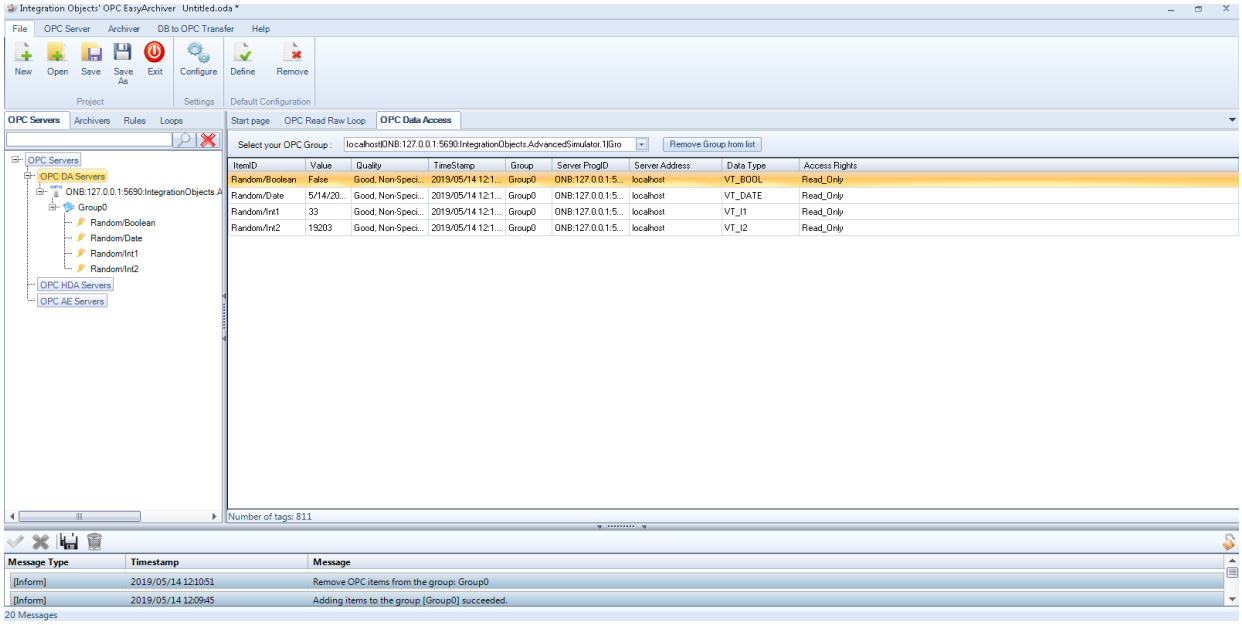


Figure 79: ONB Communication Example

For additional information on this guide, questions or problems to report, please contact:

Offices
- Americas: +1 713 609 9208
- Europe-Africa-Middle East: +216 71 195 360

Email
- Support Services: customerservice@integrationobjects.com
- Sales: sales@integrationobjects.com

To find out how you can benefit from other Integration Objects products and custom-designed solutions, please visit us on the Internet:

Online
- https://www.integrationobjects.com/