

Integration Objects'

Solution for OPC/OPC UA tunneling

OPC UA Wrapper
Version 3.2 Rev.0

USER GUIDE

OPC Compatibility
OPC Data Access 2.00
OPC Data Access 2.05
OPC Data Access 3.00
OPC Historical Data Access 1.20
OPC Alarms and Events 1.10
OPC Unified Architecture 1.02

OPC UA Wrapper User Guide Version 3.2 Rev.0
Published September 2019

Copyright © 2016-2019 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, or mechanical, by photocopying, recording, or otherwise, without the prior written permission of Integration Objects.

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

TABLE OF CONTENTS

PREFACE	8
INTRODUCTION	9
1. Overview	9
2. Architecture	9
3. Features	10
4. Operating Systems Compatibility	11
5. OPC Compatibility	11
GETTING STARTED	12
1. Pre-Installation Considerations	12
2. Installing and Running	12
3. Files Included in the Distribution	19
4. Starting-up	22
5. Removing the OPC UA Wrapper	22
Using OPC UA Wrapper	24
1. Main Interface Overview	24
2. OPC COM to OPC UA Wrapper	25
2.1. Wrappers Management	25
2.1.1. Add a Wrapper	25
2.1.2. Start a Wrapper	26
2.1.3. Stop a Wrapper	26
2.1.4. Remove a Wrapper	27
2.1.5. Edit Wrapper Settings.....	27
2.1.6. Add Servers to a Wrapper	30
2.1.7. Remove a Wrapped Server	32
2.2. View Wrapper Configuration Details	32
2.2.1. Wrapper Information.....	33
2.2.2. Security Policies.....	34
2.2.3. Certificates Management.....	35
3. OPC UA to OPC COM Proxy	36
3.1. Proxies Management	36
3.1.1. Add a Proxy	36
3.1.2. Remove a Proxy.....	39

3.1.3. Edit Proxy Settings.....	39
3.2. View Proxy Configuration Details.....	40
3.2.1. COM Configuration.....	40
3.2.2. UA Configuration.....	41
3.2.3. Alias Configuration	41
3.2.4. Certificates Management.....	44
3.3. Automatic Reconnection.....	44
OPC UA WRAPPER TRACING CAPABILITIES.....	46
Frequently Asked Questions.....	49

TABLE OF FIGURES

Figure 1: OPC UA Wrapper Architecture	10
Figure 2: Installation Welcome Dialog Box	12
Figure 3: License Agreement Dialog Box.....	13
Figure 4: Customer Information Dialog Box	14
Figure 5: Setup Type Dialog Box.....	14
Figure 6: Features Dialog Box	15
Figure 7: Choose Deployment Version Dialog Box.....	16
Figure 8: Choose Destination Folder Dialog Box	16
Figure 9: Installation Dialog Box	17
Figure 10: Install OPC Core Components Dialog Box.....	18
Figure 11: Install OPC UA Local Discovery Server Dialog Box	18
Figure 12: Installation Completed Dialog Box	19
Figure 13: Starting the OPC UA Wrapper Configuration tool	22
Figure 14: Uninstaller Icon in the Start Menu	22
Figure 15: OPC UA Wrapper Uninstall Confirmation.....	22
Figure 16: Windows 10 Startup Menu Uninstall Shortcut	23
Figure 17: Configuration Tool Main View	24
Figure 18: Add Wrapper	25
Figure 19: Add New Wrapper Dialog	25
Figure 20: The Wrapper Context Menu	26
Figure 21: Task Manager View – Service Started.....	26
Figure 22: Task Manager View – Service Stopped	27
Figure 23: Uninstall Wrapper	27
Figure 24: Wrapper Settings Dialog.....	28
Figure 25: Add OPC Servers Dialog	30
Figure 26: Add Local OPC Servers.....	31
Figure 27: Wrapped OPC Servers	32
Figure 28: Remove Wrapped Server	32
Figure 29: Wrapper Configuration Details View	33
Figure 30: Wrapper Information.....	33
Figure 31: Security Policies	34
Figure 32: Remove Users.....	35
Figure 33: Wrapper Certificates Management	36
Figure 34: Add Proxy.....	36
Figure 35: UA Endpoint Configuration Dialog	37
Figure 36: COM Server Configuration Dialog	38
Figure 37: UA to COM Proxies List.....	39
Figure 38: Remove Proxy	39
Figure 39: Proxy Settings Dialog	39
Figure 40: Proxy Configuration Details View.....	40
Figure 41: COM Configuration	41
Figure 42: UA Configuration	41
Figure 43: Proxy Certificates Management.....	44
Figure 44: Proxy Reconnection Configuration.....	45
Figure 45: Log Settings Dialog	47

Figure 46: License Authorization	49
Figure 47: License Authorization (Demo Expired Case)	50
Figure 48: Register OPC Core Components on Windows 7 64 bit	51
Figure 49: Register OPC Core Components on Windows 7 32 bit	52

LIST OF TABLES

Table 1: OPC UA Wrapper Main Files	21
Table 2: Wrapper Parameters	29
Table 3: Proxy Parameters	39
Table 4: Log Settings.....	48

PREFACE

ABOUT THIS USER GUIDE


This user guide:

- Describes the main features of the OPC UA Wrapper.
- Lists the system requirements for installing and running the OPC UA Wrapper.
- Explains how to run, configure, and use the OPC UA Wrapper application.

TARGET AUDIENCE

This document is intended for any potential users of Integration Objects' OPC UA Wrapper. Basic knowledge of OPC specifications is assumed.

DOCUMENT CONVENTIONS

Convention	Description
Monospaced type	Indicates a file reference
Bold	Click/selection action required
	Information to be noted

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

1. Overview

Integration Objects' OPC UA Wrapper is a powerful solution that enables any OPC UA client to communicate with COM based OPC DA2/DA3, HDA and A&E servers as if they were OPC UA servers and enables any OPC DA/HDA/AE client to communicate with UA servers as if they were OPC DA/HDA/AE servers.

This OPC UA Wrapper has the capability to:

- Discover local and remote classic OPC servers,
- Discover local and remote OPC UA servers,
- Manage security settings and authentication settings,
- Manage certificates,
- Map the address space of classic OPC servers to the address space of an OPC UA server,
- Map the address space of OPC UA servers to the address space of an OPC COM server,
- Read and write OPC item values,
- Read historical data,
- Read and acknowledge alarms and events,
- Read the vendor specific attributes of an OPC AE server.

2. Architecture

The following diagram illustrates the solution's typical system architecture. Integration Objects' OPC UA Wrapper acts as a bridge between classic OPC servers connected to the network and any OPC UA client and between UA servers connected to the network and any OPC COM client.

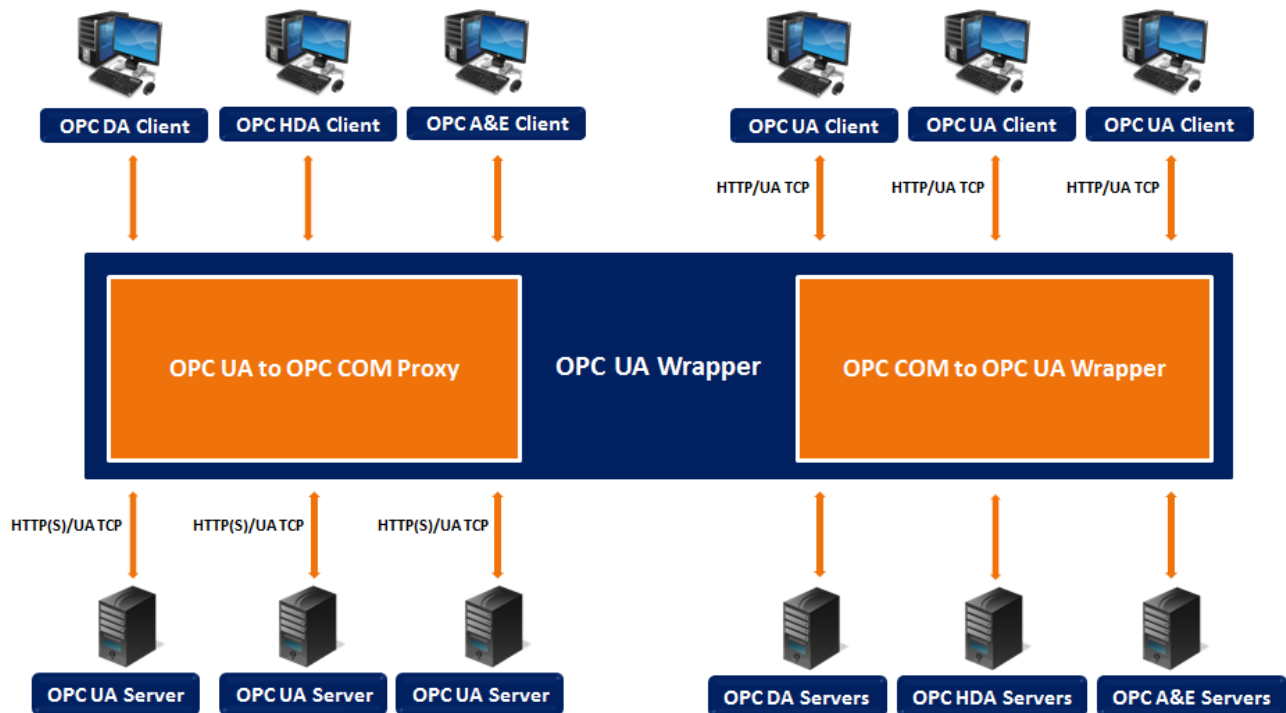


Figure 1: OPC UA Wrapper Architecture

3. Features

The Integration Objects' OPC UA Wrapper includes many features such as:

- **COM Server to UA Server:**
Integration Objects' OPC UA Wrapper provides access to your classic OPC servers from Unified Architecture clients as if they were UA servers.
- **UA Server to COM Server:**
Integration Objects' OPC UA Wrapper provides access to your Unified Architecture servers from classic OPC clients as if they were OPC COM servers.
- **Intuitive User Interface**
The configuration tool allows an intuitive manipulation of services and reduces configuration effort. With its graphical user interface, users can create, edit, start and stop COM to UA wrapper services as well as create, edit and remove COM to UA proxies.
- **Run as Windows Service**
Created wrappers are running as Windows services in the background.

- **OPC UA Security**

Integration objects' OPC UA Wrapper provides security features introduced in the OPC UA specification such as establishing secure communication channels, keeping track of sessions, using encryption and signing messages. The security modes to be used along with user identity tokens can be chosen, managed and changed by the user from the configuration tool.

- **Log Capabilities**

The application records messages in log files using different logging levels. This enables end-users to track the execution and diagnose any encountered problems. The log file gives information about successful actions and errors. This can facilitate the troubleshooting task.

4. Operating Systems Compatibility

Integration Objects' OPC UA Wrapper supports the following operating systems:

- Windows 10
- Windows 8
- Windows 7
- Windows Server 2016
- Windows Server 2012
- Windows Server 2008

5. OPC Compatibility

Integration Objects' OPC UA Wrapper supports the following OPC standard versions:

- OPC Data Access 2.00
- OPC Data Access 2.05
- OPC Data Access 3.00
- OPC Alarms & Events 1.10
- OPC Historical Data Access 1.20
- OPC Unified Architecture 1.02

GETTING STARTED

1. Pre-Installation Considerations

In order to properly run the OPC UA Wrapper, the following software components need to be installed on the target system:

- The OPC core components 3.00, which consist of all shared OPC modules including the DCOM proxy/stub libraries, the OPC Server Enumerator, .NET wrappers, etc.
- .NET Framework version 4.0 or higher.
- The OPC UA Discovery Server, which lists the OPC UA endpoints available on a given computer.



Also, make sure there is no firewall or antivirus blocking the application.

2. Installing and Running

To install the OPC UA Wrapper application:

- a. Double-click on the **Integration Objects' OPC UA Wrapper installation package**. The installation welcome dialog box will appear.

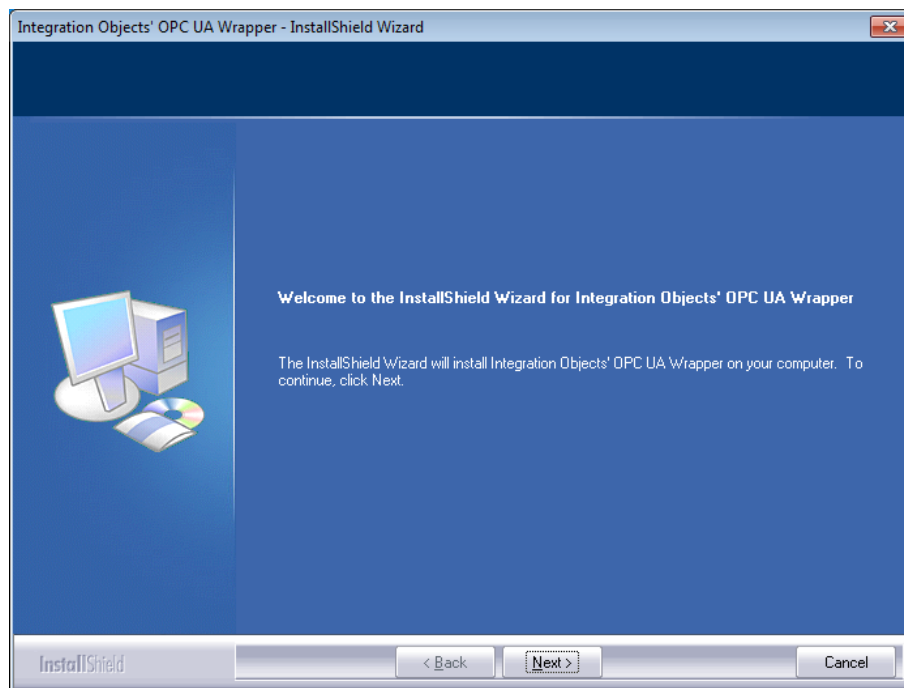


Figure 2: Installation Welcome Dialog Box

- b. Click the **Next** button. The license agreement will be displayed.

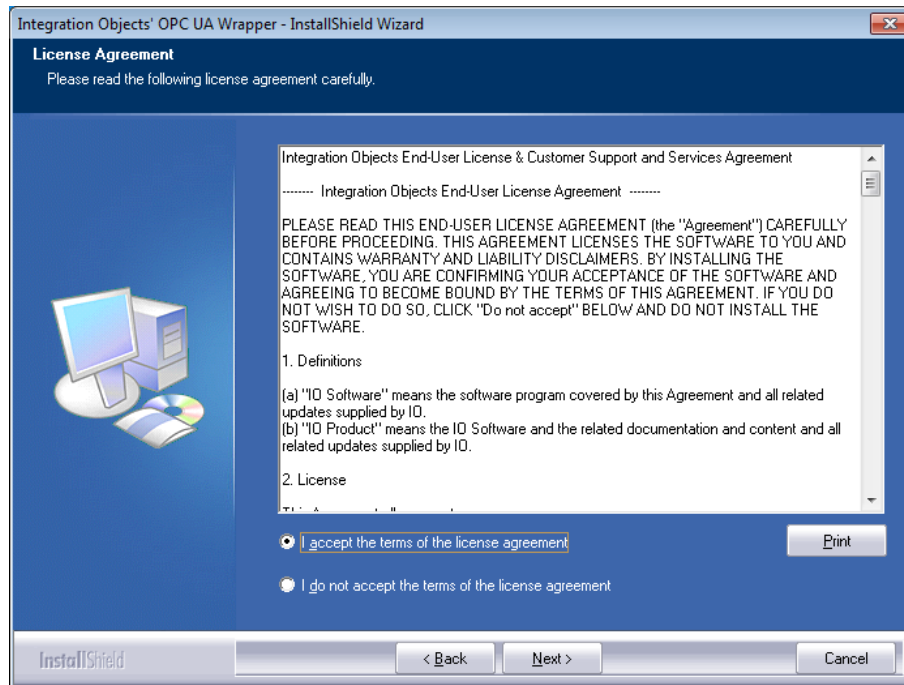


Figure 3: License Agreement Dialog Box

- c. After reading the license agreement and accepting all its terms, click the **Next** button. The customer information dialog box will appear.

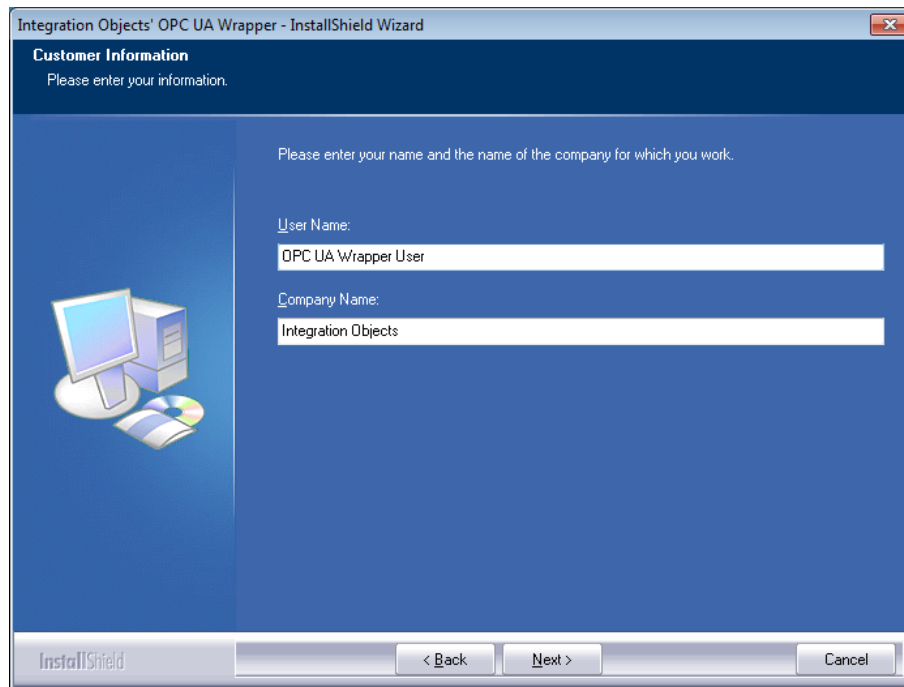


Figure 4: Customer Information Dialog Box

- d. Add the user and the company names and then click the **Next** button. The dialog box for choosing the setup type will be displayed.

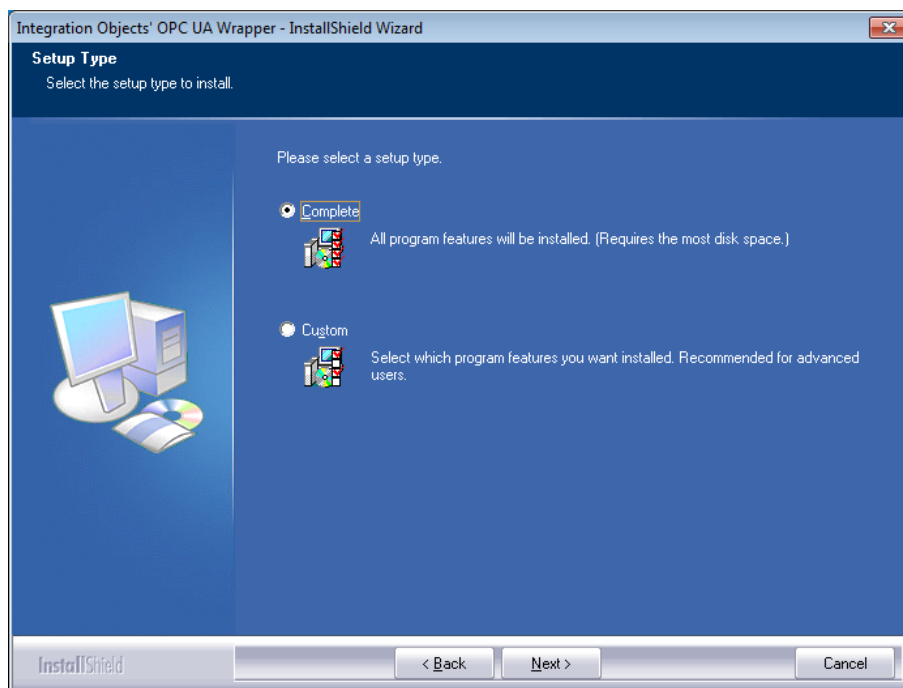


Figure 5: Setup Type Dialog Box

- e. If you choose the “**Complete**” setup type, all features will be installed. If you choose “**Custom**” setup type, the following dialog will be displayed and you will need to check the features that you want to install:

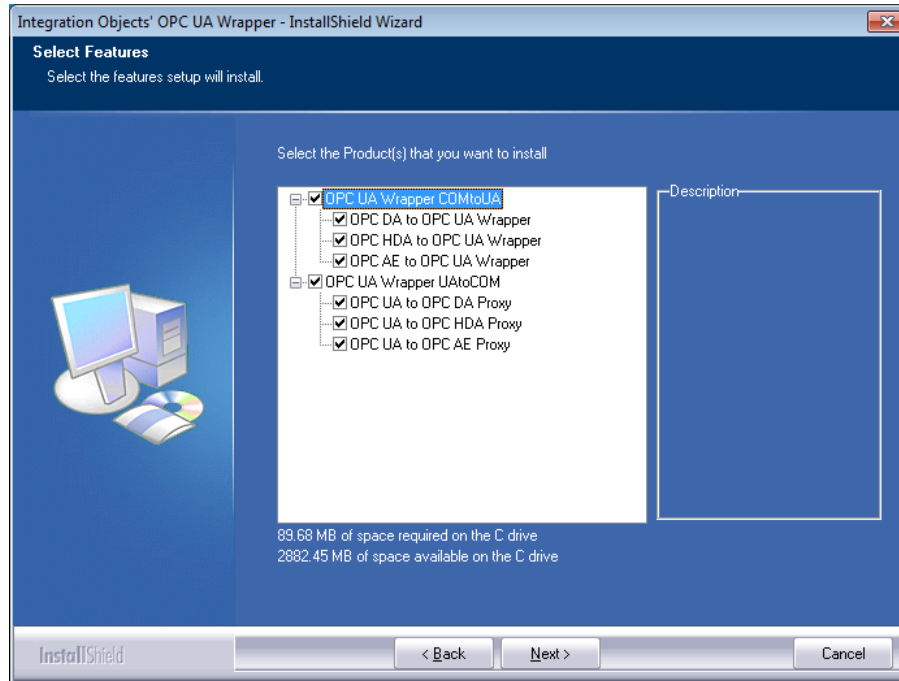


Figure 6: Features Dialog Box

The features can be installed separately and are also licensed separately.

- f. After selecting the features you want to install, click the **Next** button. The dialog box of choosing the UA Wrapper deployment version will be displayed.



The deployment version dialog box will be displayed only when your operating system is 64-bit version.

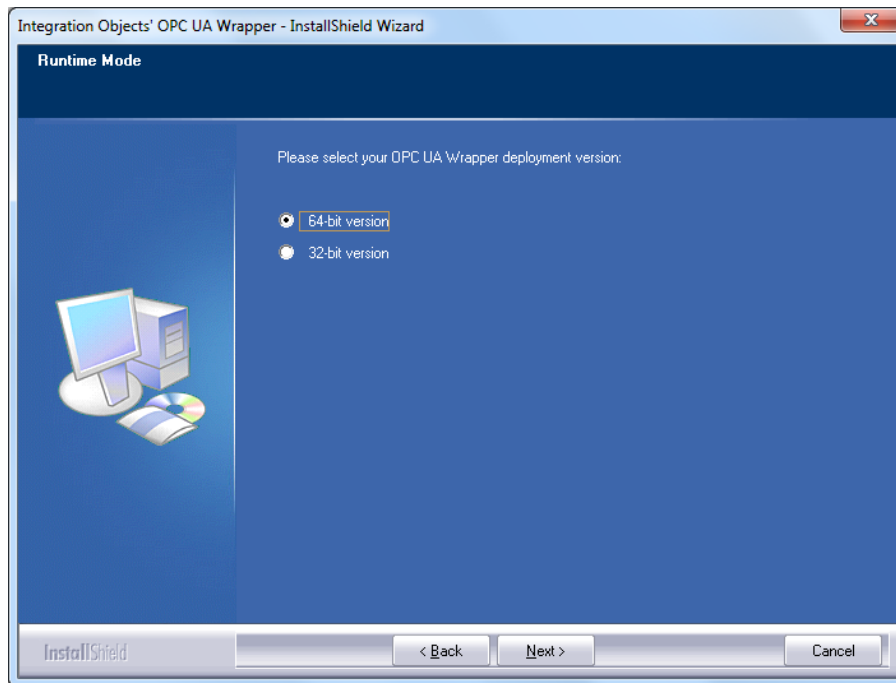


Figure 7: Choose Deployment Version Dialog Box

- g. Select your UA Wrapper deployment version then click the **Next** button. The dialog box of choosing the destination folder will be displayed.

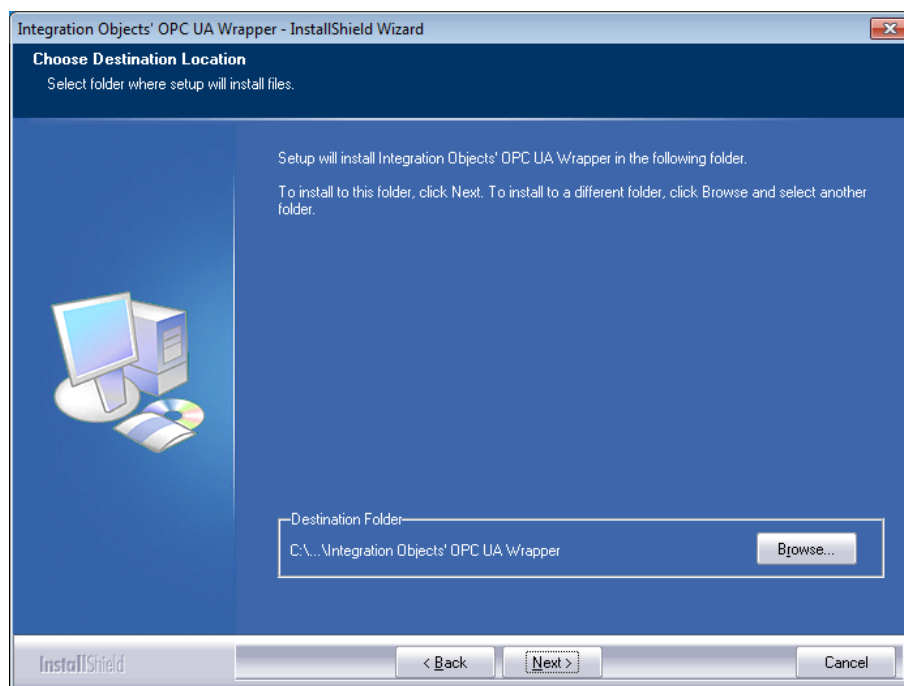


Figure 8: Choose Destination Folder Dialog Box

- h. Click the **Next** button to continue with the chosen installation path, or the **Browse** button to select a different destination folder. The installation dialog box will then appear.

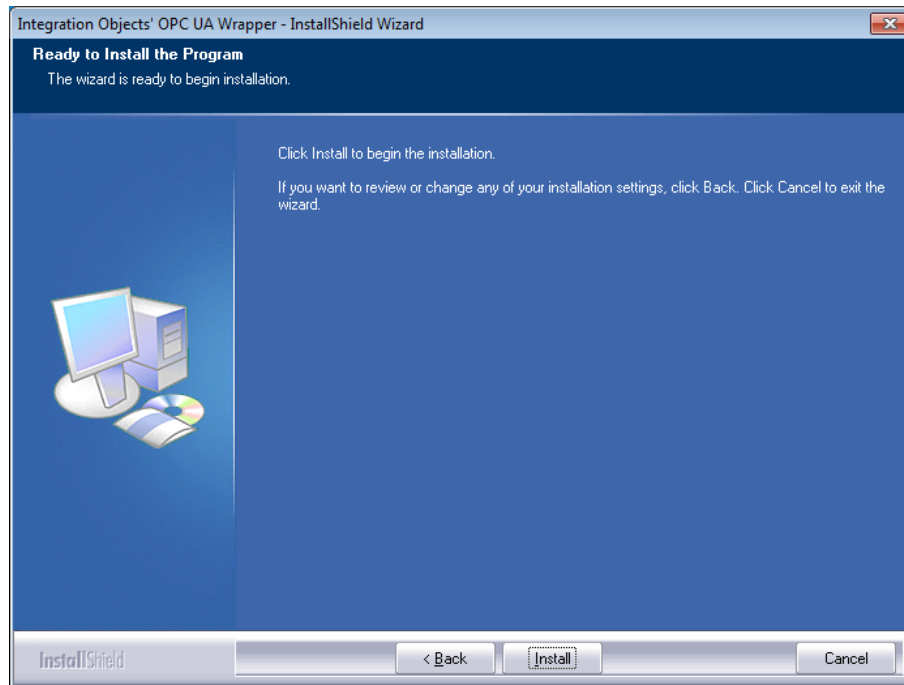


Figure 9: Installation Dialog Box

- i. Click the **Install** button to start installation.

The setup will, then, copy the necessary files to the chosen target folder, create shortcut icon to launch the OPC UA Wrapper configuration tool from the start menu and the desktop and make an uninstallation entry in Programs and Features in the Control Panel.

- j. If the OPC Core Components are not installed in your machine, you can select **Install OPC Core Components** option as shown in the figure below.

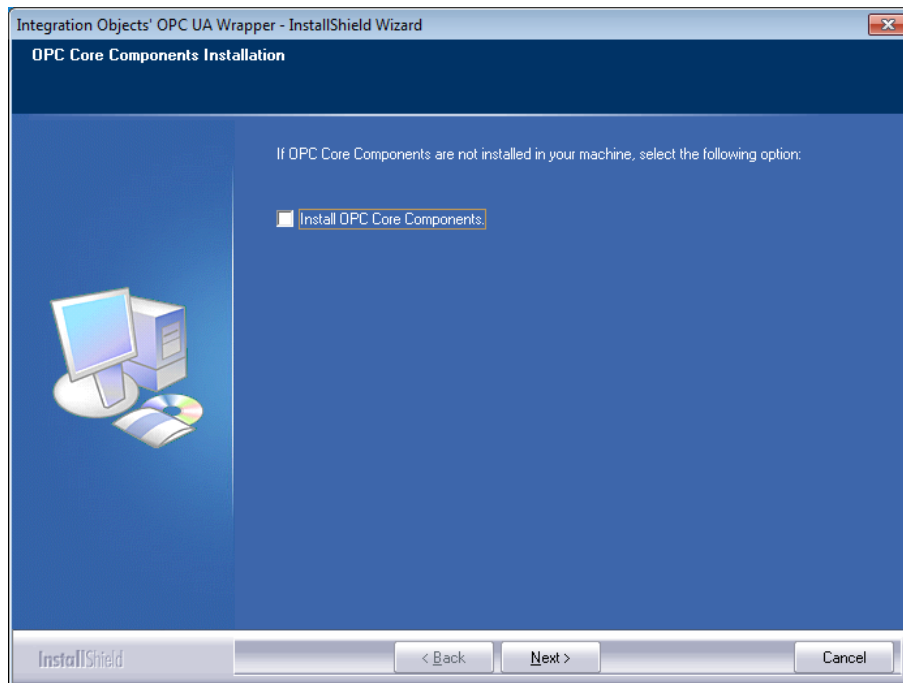


Figure 10: Install OPC Core Components Dialog Box

- k. Click the **Next** button to continue with the installation of the OPC UA Local Discovery Sever if it is not already installed. The dialog box for choosing to install the UA Local Discovery Server will be displayed as illustrated below.

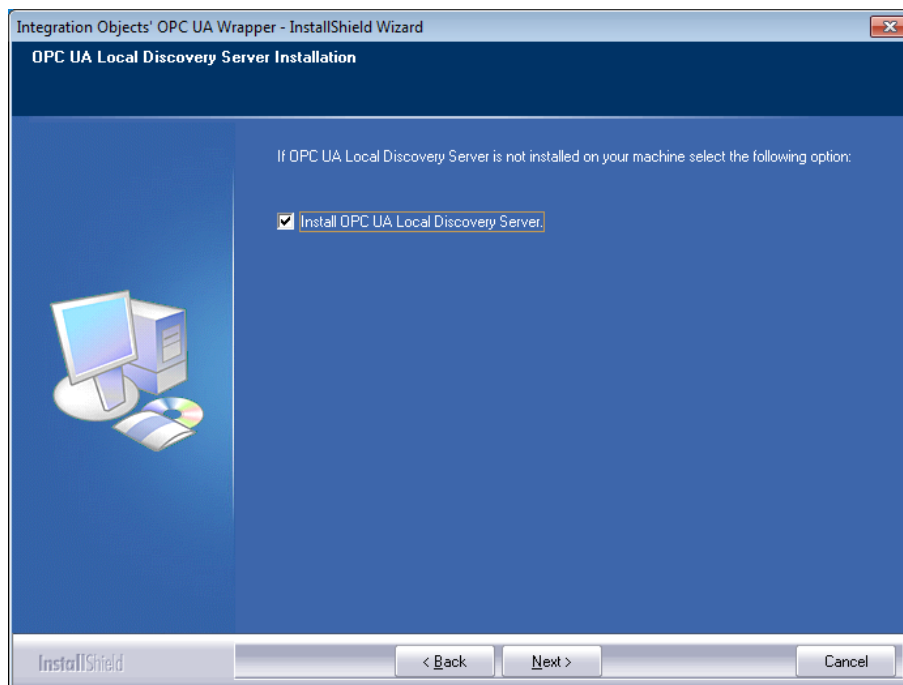


Figure 11: Install OPC UA Local Discovery Server Dialog Box

The Installation Complete dialog box will then be displayed, as illustrated in the figure below.

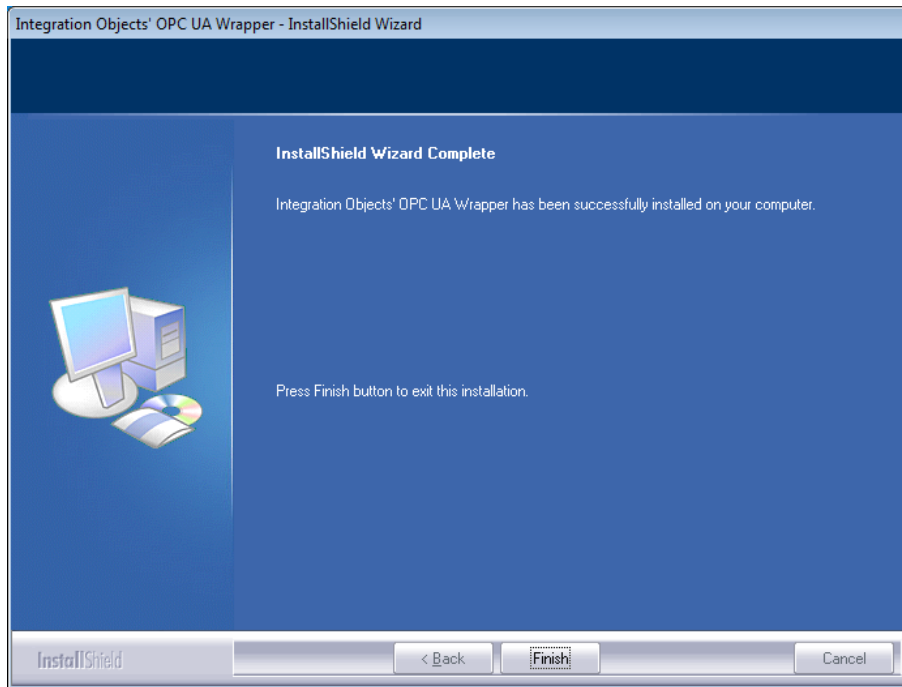


Figure 12: Installation Completed Dialog Box

3. Files Included in the Distribution

Once the installation is complete, you will get the following main files deployed under the target installation folder:

File Names	Description
OPCUAConfigurationTool.exe	OPC UA Wrapper configuration tool
Wrappers\Opc.Ua.CertificateGenerator.exe	OPC Foundation certificate generator
Wrappers\wrapper.exe	OPC UA Wrapper basic service
Proxy\I00PCUaToDAProxy.exe	OPC UA to DA Proxy server
Proxy\I00PCUaToAEProxy.exe	OPC UA to AE Proxy server

Proxy\IOOPCUAtoHDAProxy.exe	OPC UA to HDA Proxy server
License Authorization\LicenseAuthorization.exe	The license authorization tool allowing you to activate your licenses
WrapperLicenseService.exe	Service for managing OPC UA Wrapper license validation
IntegrationObjects.Opc.Ua.Client.dll IntegrationObjects.Opc.Ua.ClientControls.dll IntegrationObjects.Opc.Ua.ComInterop.dll IntegrationObjects.Opc.Ua.Configuration.dll IntegrationObjects.Opc.Ua.Core.dll IntegrationObjects.Opc.Ua.Server.dll IntegrationObjects.Utilities.dll IntegrationObjects.OPCNetClientSDK.dll IntegrationObjects.KNet.Forms.dll IntegrationObjects.KNet.Common.dll IntegrationObjects.KNet.Browser.dll IntegrationObjects.Logger.SDK.dll DevComponents.DotNetBar2.dll IntegrationObjects.Logger.SDK.UserControl.dll License.dll Interop.NetFwTypeLib.dll WrapperLicenseServiceSDK.dll	Core assembly files
Config.ini Wrappers\Config.ini Proxy\Config.ini	Configuration files
Documents\IO_DCOM_DA_HDA_Config_Guideline_WinSeven_Workgroup.pdf	The DCOM configuration for DA and HDA

Documents\ IO_DCOM_AE_Config_Guideline_WinSeven_Workgroup .pdf	The DCOM configuration for AE
Documents\OPC UA Wrapper Quick User Guide.pdf	The quick user guide
Documents\User Guide.pdf	The user guide

Table 1: OPC UA Wrapper Main Files

4. Starting-up

Integration Objects' OPC UA Wrapper configuration tool can be started manually from the shortcut in the start menu.

To do so, click on Start → Programs → Integration Objects → OPC UA Wrapper → OPC UA Wrapper

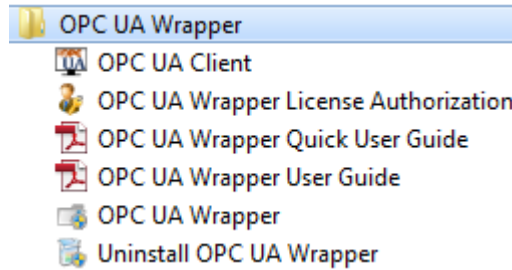


Figure 13: Starting the OPC UA Wrapper Configuration tool

5. Removing the OPC UA Wrapper

To uninstall the OPC UA Wrapper, follow the steps below:

1. Click the **Uninstall** shortcut icon available in the start menu, as illustrated below.

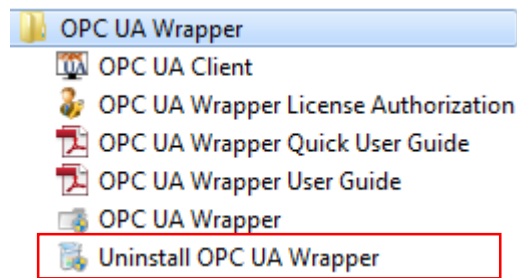


Figure 14: Uninstaller Icon in the Start Menu

The following dialog box will appear:

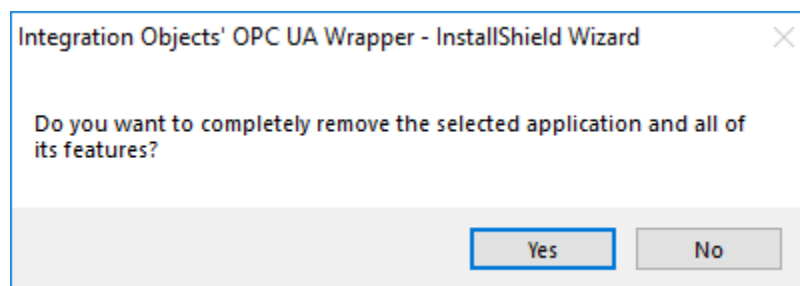


Figure 15: OPC UA Wrapper Uninstall Confirmation

2. Click the **Yes** button to start the uninstallation.
3. The wizard will then take you through the removal steps. At the end, click **Finish** when the un-installation is complete.



If you are using the windows 10, windows server 2012 or windows server 2016 operating system, the uninstaller needs to be run from the start menu as shown below.

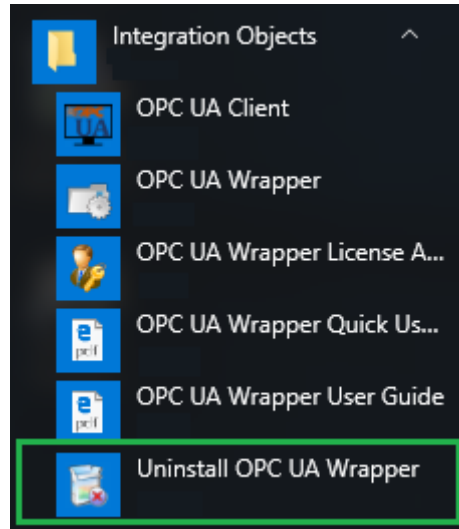


Figure 16: Windows 10 Startup Menu Uninstall Shortcut

The OPC UA Wrapper can also be manually removed as follows:

1. Go to the **Control Panel**.
2. Click **Programs and Features**.
3. In the Programs and Features dialog screen, select **Integration Objects' OPC UA Wrapper**.
4. Click **Change/Remove** then **OK**.

USING OPC UA WRAPPER

In this section, you will find an overview of the OPC UA Wrapper configuration tool as well as the configuration steps required to use the application.

1. Main Interface Overview

The OPC UA Wrapper configuration tool is a user-friendly graphical interface designed to visualize and customize the COM to UA wrapper services and the UA to COM proxies. The configuration tool will provide you with an easy and clear way for managing wrappers, wrapped servers, proxies, certificates, security settings and log settings.

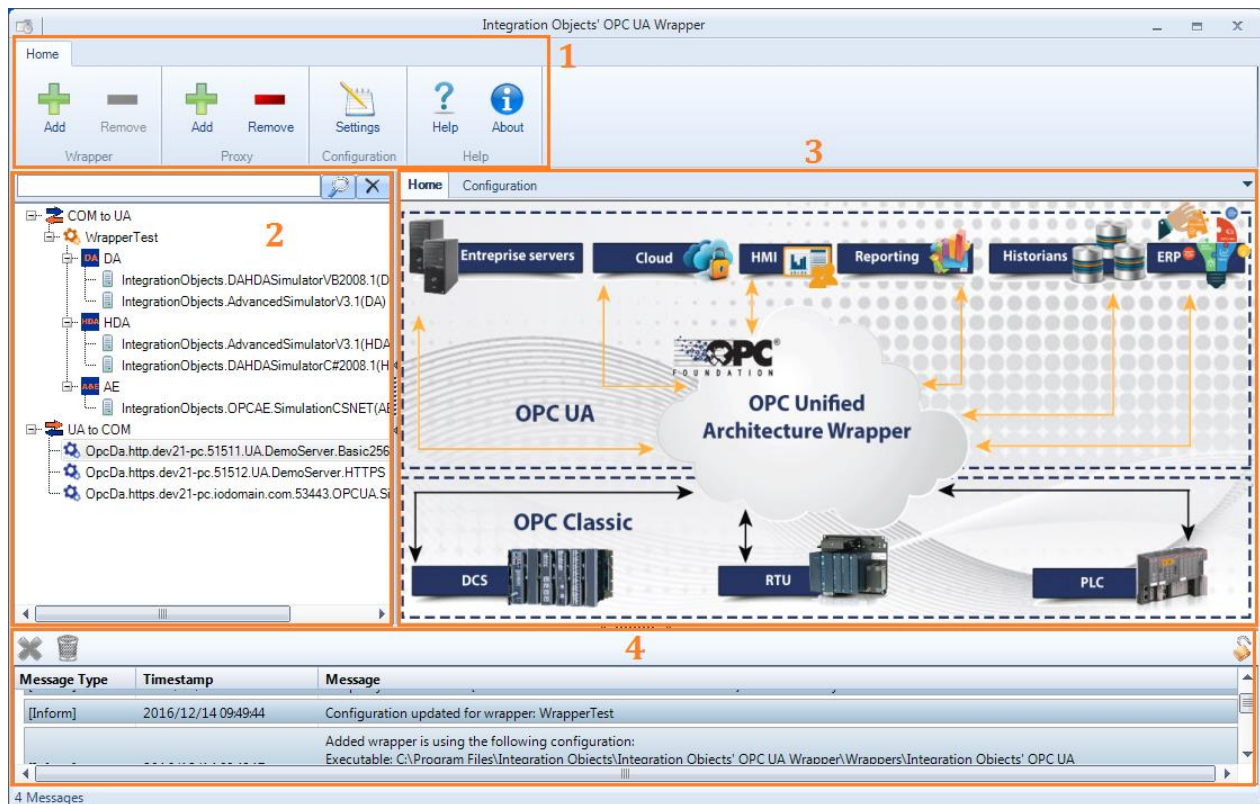


Figure 17: Configuration Tool Main View

There are four parts in the configuration tool user interface, as highlighted above:

- **Home menu bar (1):** contains the wrapper item bar, the configuration item bar, and the help item bar.

- **Wrappers & proxies list (2):** Tree browser displaying:
 - the created wrappers and their related wrapped OPC servers
 - The created proxies
- **Home page (3):** This is the home view of the application. You can switch to the configuration tab to configure the added wrapper.
- **Log view (4):** This part displays log messages. The most recent messages are displayed at the top of the messages list.

2. OPC COM to OPC UA Wrapper

2.1. Wrappers Management

2.1.1. Add a Wrapper

You can add a wrapper by clicking the **Add** button available in the Home menu or by right clicking the COM to UA root node and selecting **Add Wrapper** as shown below.



Figure 18: Add Wrapper

The Add Wrapper dialog box is shown in the figure below:

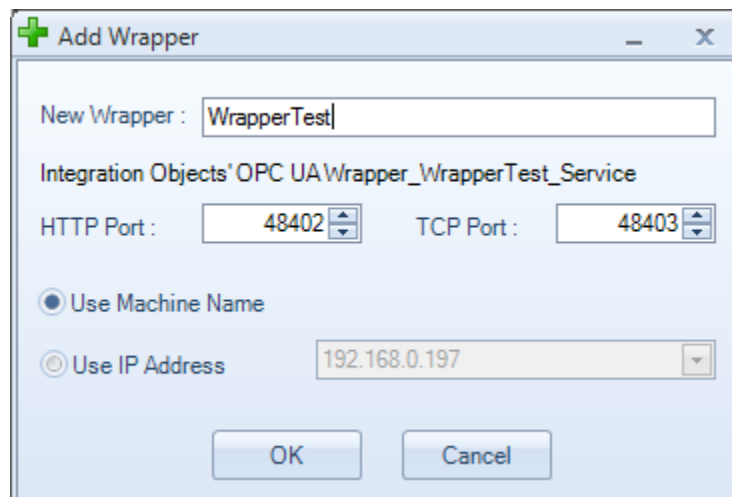


Figure 19: Add New Wrapper Dialog

Enter:

- The name for the wrapper you want to add. The name is a friendly one that will serve to identify your OPC UA server and must not contain any spaces or special characters.
- HTTP and the TCP ports numbers used for the Wrapper/Client communications.

To create the wrapper service URL, you can choose between:

- Using the machine name
- Using the IP address of the machine

After creating the wrapper, a new node will be added to the COM to UA root node. Right click on the wrapper node and the following menu will be displayed:

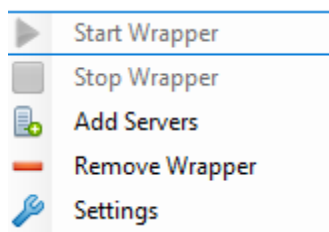


Figure 20: The Wrapper Context Menu

Using the wrapper context menu, you can:

1. Start the wrapper.
2. Stop the wrapper.
3. Add servers to the wrapper.
4. Remove the wrapper permanently from your machine.

Note that in the figure, Start and Stop wrapper are both inactive. This is because the wrapper does not have wrapped OPC servers yet.

2.1.2. Start a Wrapper

Once your wrapper is loaded into the configuration tool, it will be added to the tree under COM to UA root node. To start it, right click the wrapper and choose **Start Wrapper** from the wrapper context menu. A message in the log view will inform you about the progress.

Furthermore, you can open Windows task manager, navigate to Services tab and look for the service you started.

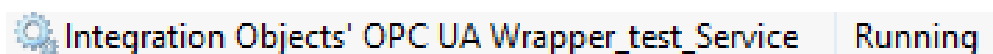


Figure 21: Task Manager View – Service Started

2.1.3. Stop a Wrapper

To stop the wrapper, click the **Stop Wrapper** button in the wrapper context menu and a message in the log view will inform you about the progress.

You can open Windows task manager, navigate to Services tab and look for the service you stopped. You should be able to see the following.

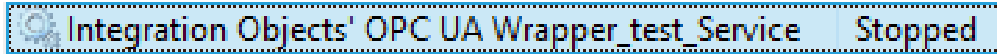


Figure 22: Task Manager View – Service Stopped

2.1.4. Remove a Wrapper

In order to uninstall the wrapper and remove its files from the machine, click the **Remove** button available in the Home menu or select **Remove Wrapper** from the wrapper context menu as illustrated in the figure below.

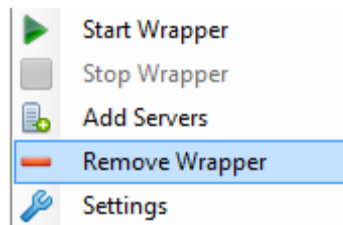


Figure 23: Uninstall Wrapper

You can check that the service was entirely removed from the Windows services list.

2.1.5. Edit Wrapper Settings

The OPC UA Wrapper comes with default settings for the wrapper services. These settings can be easily edited using the **Wrapper Settings** dialog presented below.

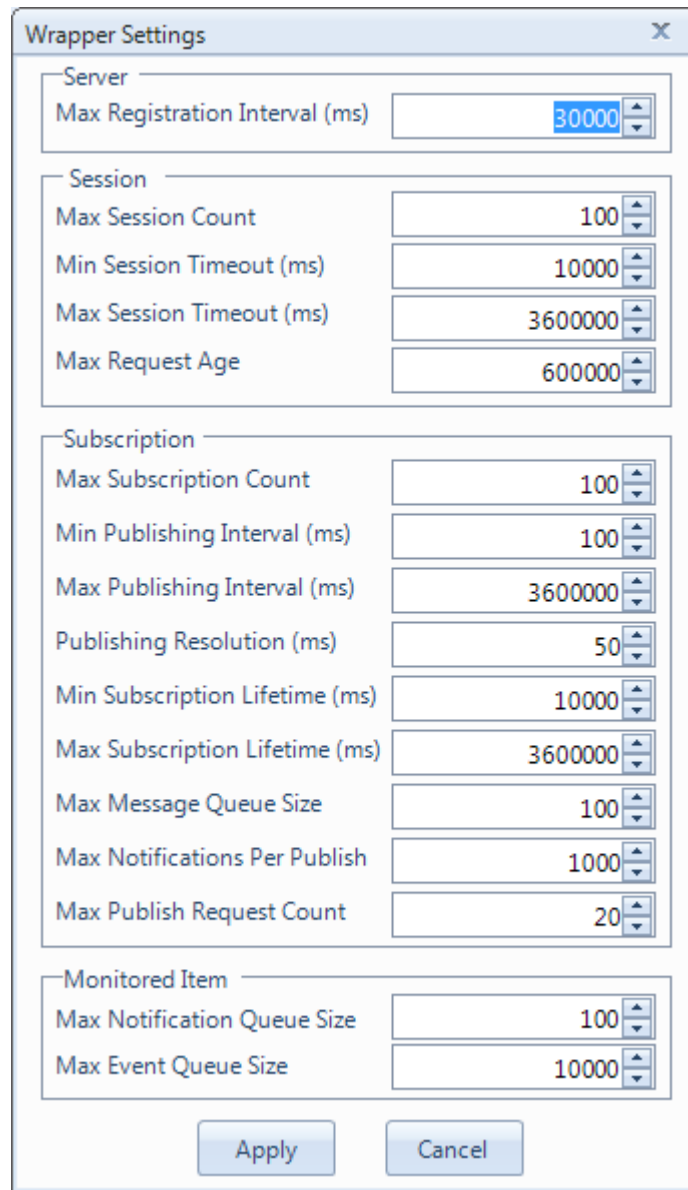


Figure 24: Wrapper Settings Dialog

The following table describes the wrapper settings:

Setting	Description	Default Value
Max Registration Interval	The maximum time between registration attempts with the local discovery server (in milliseconds).	30000
Max Session Count	The maximum session count.	100

Min Session Timeout	That minimum period of that a session is allowed to remain open without communication from the client (in milliseconds).	10000
Max Session Timeout	That maximum period of that a session is allowed to remain open without communication from the client (in milliseconds).	3600000
Max Request Age	The maximum age of an incoming request (old requests are rejected).	600000
Max Subscription Count	The max subscription count.	100
Min Publishing Interval	The minimum publishing interval supported by the server (in milliseconds).	100
Max Publishing Interval	The maximum publishing interval supported by the server (in milliseconds).	3600000
Publishing Resolution	The minimum difference between supported publishing interval (in milliseconds).	50
Min Subscription Lifetime	The minimum lifetime for a subscription (in milliseconds).	10000
Max Subscription Lifetime	How long the subscriptions will remain open without a publish from the client (in milliseconds).	3600000
Max Message Queue Size	The maximum number of messages saved in the queue for each subscription.	100
Max Notifications Per Publish	The maximum number of notifications per publish.	1000
Max Publish Request Count	The max publish request count.	20
Max Notification Queue Size	The maximum number of notifications saved in the queue for each monitored item.	100
Max Event Queue Size	The maximum size of event monitored item queues.	10000

Table 2: Wrapper Parameters

2.1.6. Add Servers to a Wrapper

You can add different local and remote OPC servers to a wrapper by right clicking the wrapper node and selecting **Add Servers**. The following dialog screen will appear:

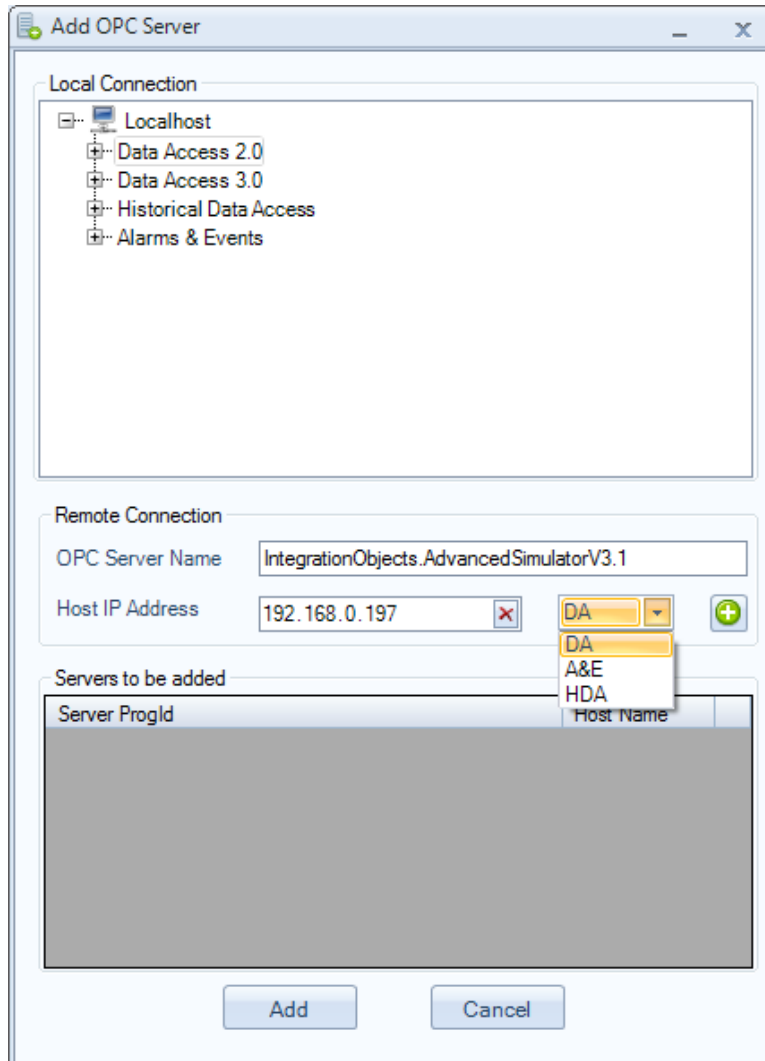


Figure 25: Add OPC Servers Dialog

You can either browse the list of the OPC servers available in your local machine, or manually configure a remote OPC server by entering:

- The OPC server name (Progid),
- The IP Address of the machine that hosts this OPC Server,
- The OPC server type (DA, HDA or A&E server) as shown in the figure above.

To add multiple OPC local Servers, you need to select the server name from the servers tree view and the selected servers will be added to the grid view to facilitate the visualization of the servers to be added. Use the **X** button to delete servers from this list.

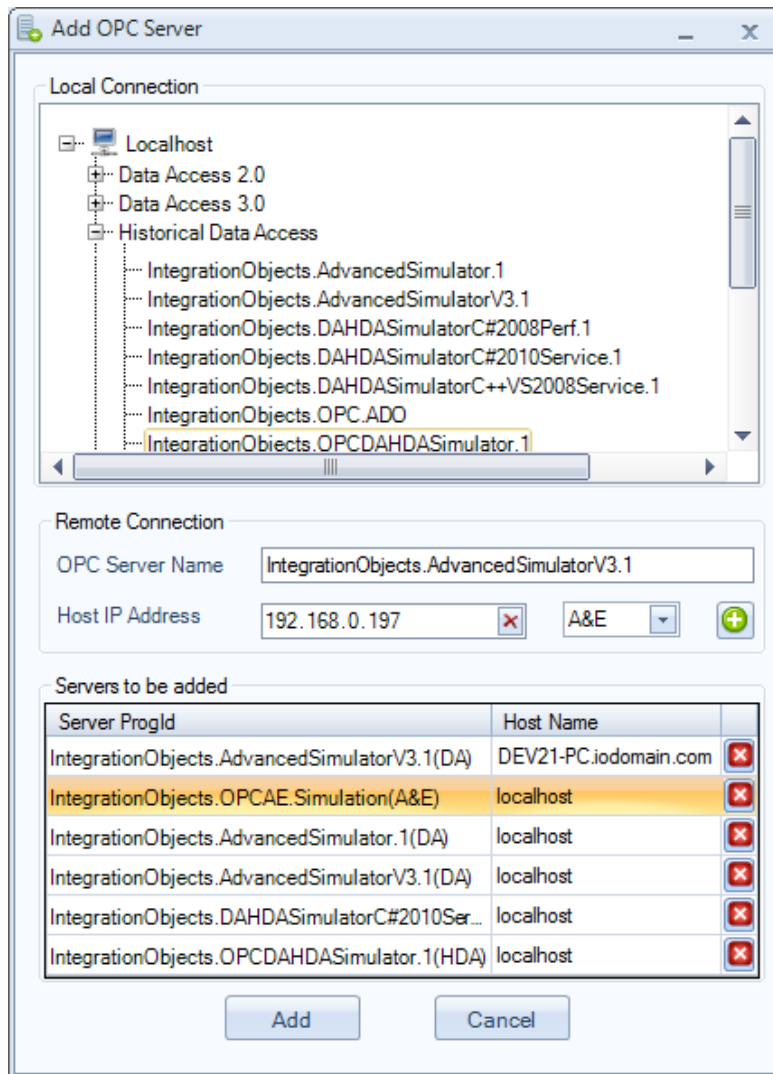


Figure 26: Add Local OPC Servers

Click the **Add** button to confirm your configuration. When you go back to the main window, you will be able to see that the servers have been successfully added under the desired wrapper as shown below.

You can also cancel the addition of the server by using the **Cancel** button as shown in the figure below.

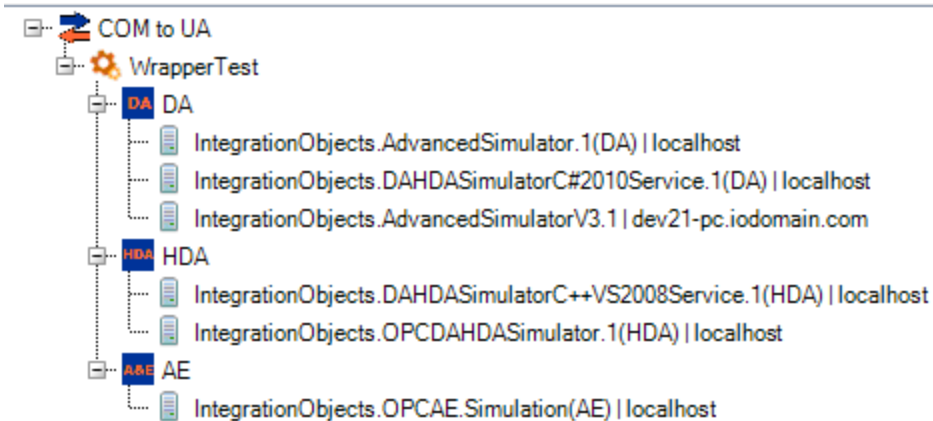


Figure 27: Wrapped OPC Servers

2.1.7. Remove a Wrapped Server

You can remove a wrapped OPC server by right clicking on the server node and selecting the **Remove Server** action from the displayed menu.

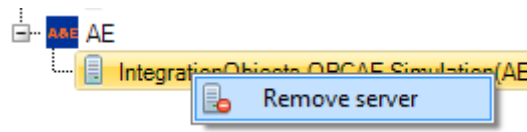


Figure 28: Remove Wrapped Server

2.2. View Wrapper Configuration Details

Once you are done with adding the wrapper, you can configure its security policy and certificates. Clicking on the wrapper node will display the configuration tab as illustrated in the figure below:

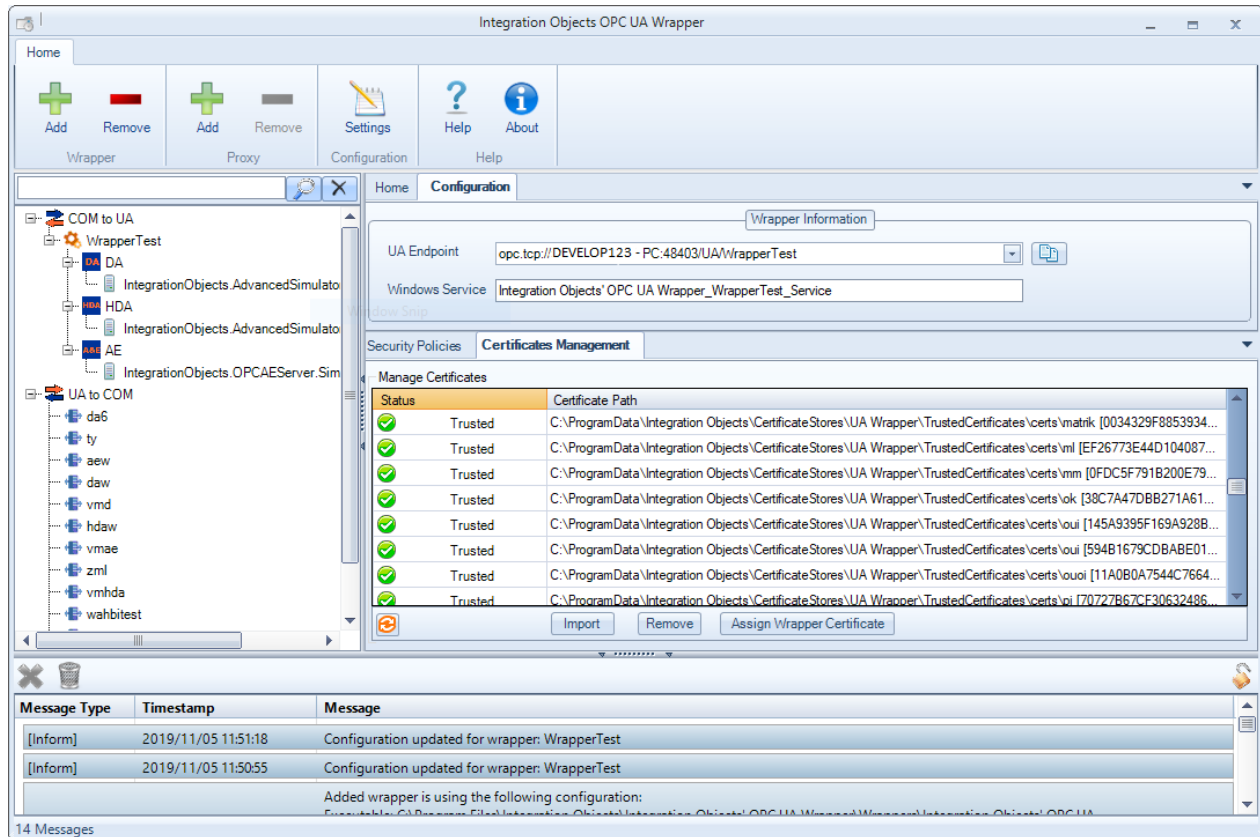


Figure 29: Wrapper Configuration Details View

2.2.1. Wrapper Information

The Wrapper Information section displays the following general information:

- UA Endpoint: the URL to be used in the UA client in order to connect to the wrapped servers.
- Protocol choice: You can choose from TCP and HTTP. The URL will be updated according to the selected protocol.
- Windows Service: the full name of the windows service associated to the wrapper.

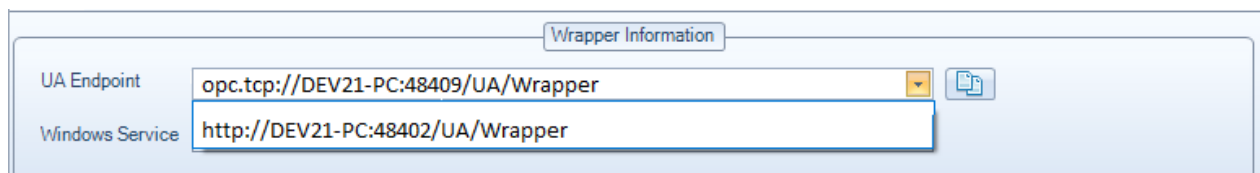


Figure 30: Wrapper Information

2.2.2. Security Policies

The user can select a security mode to be associated with the wrapped servers to instruct the OPC UA client to open a secure channel with them. Only the checked security modes will be enabled by the client.

i. Security Modes

Security modes are used to announce which security mechanisms wrapped servers support during communications. There are three different security modes available:

- None: This mode does not provide encryption or signing.
- Sign: This mode provides signing but not encryption. Available encryptions are Basic256 and Basic128Rsa15. The sign mode will be disabled unless you select at least one encryption type.
- Sign & Encrypt: This mode provides both signing & encryption. Available encryptions are Basic256 and Basic128Rsa15. The sign & encrypt mode will be disabled unless you select at least one encryption type.

ii. User Identity Tokens

User identity token represents the user's credentials that proves the identity of an entity. Descriptions of the user identity tokens are as follows:

- Anonymous: This type of connection allows users to connect to the server with no user authentication.
- Username: This type of connection prompts users for a username and password combination and grants access only to allowed users. If you wish to grant access for a new user, enter a username, a password and confirm it and then click **Add** as shown below.



The password must be at least 5 characters long.



The screenshot shows a dialog box titled "Security Policies" with a "Certificates Management" tab. It is divided into two main sections: "Security Modes" and "User Identity Tokens".

Security Modes:

- None
- Sign
 - Basic256
 - Basic128Rsa15
- Sign & Encrypt
 - Basic256
 - Basic128Rsa15

User Identity Tokens:

- Anonymous
- Username
 - Username:
 - Password:
 - Confirm Password:
 -

At the top right of the "User Identity Tokens" section, there is a red "Remove Users" button. At the bottom of the dialog, there are "Save" and "Cancel" buttons.

Figure 31: Security Policies

All the configured users information will be stored in separate xml files under the following path: "C:\ProgramData\Integration Objects\Accounts\ServiceName". To remove a user, click the **Remove Users** button and the following screen will be displayed.

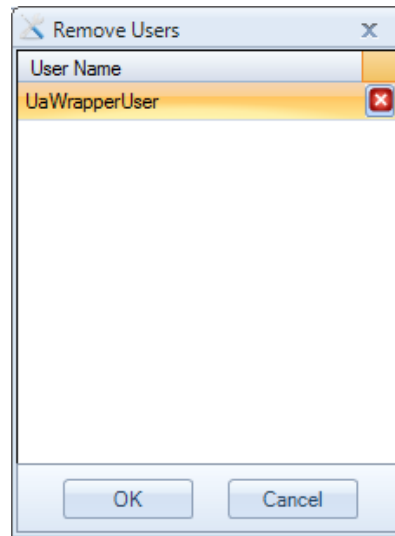


Figure 32: Remove Users

Once you are done with setting security policies and user identity tokens, click the **Save** button to apply your changes. If your wrapper is running, you will be prompted to restart it for the modifications to take effect.

2.2.3. Certificates Management

Using the Certificates Management tab, you can:

- List the certificates: this option displays the list of the trusted, the rejected and the wrapper certificates.. Users can trust a rejected certificate by right clicking on it and selecting **Trust** as shown in the figure below. They can also reject a trusted certificate.
- Import certificate: this option allows users to select a certificate and add it to the list of the trusted ones.
- Remove certificate: this option allows users to remove the selected certificates from the trusted or rejected list.
- Assign Wrapper Certificate: this option allows the user to select a certificate from a .PFX file stored on disk and assign it to the wrapper.

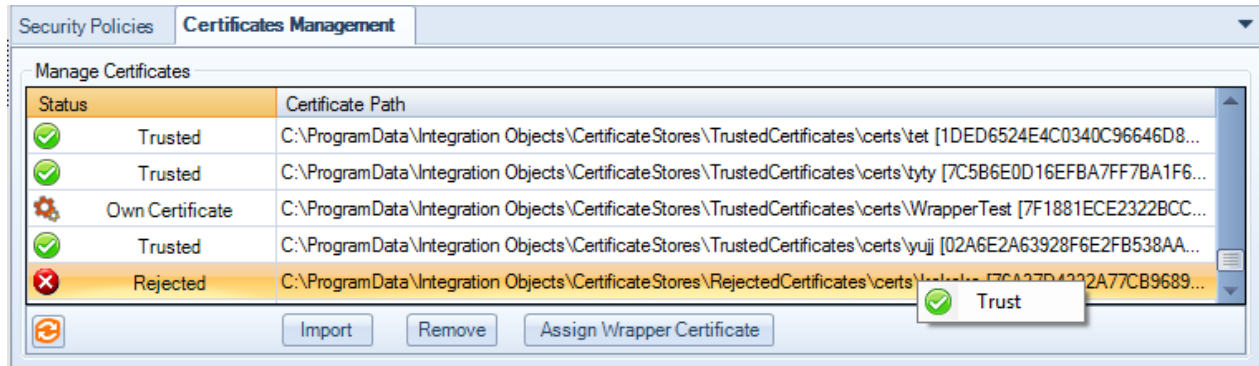


Figure 33: Wrapper Certificates Management

3. OPC UA to OPC COM Proxy

3.1. Proxies Management

3.1.1. Add a Proxy

You can add a proxy by clicking the **Add** button available in the Home menu or by right clicking the UA to COM root node and selecting **Add Proxy** as shown below.

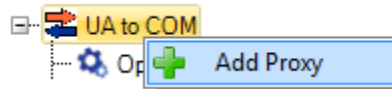


Figure 34: Add Proxy

The UA endpoint configuration dialog screen will appear:

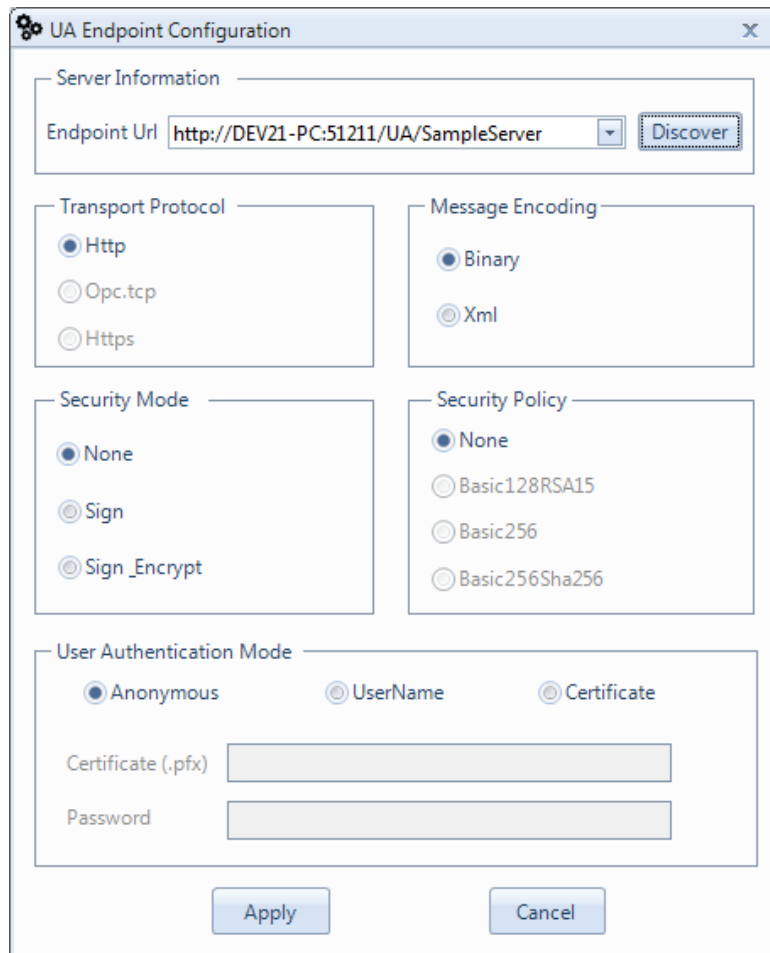


Figure 35: UA Endpoint Configuration Dialog

All the settings presented in this dialog screen are required to create an UA endpoint from the selected OPC UA server.

iii. Endpoint settings

The user can either type the server URL or select it from the URL list discovered by the OPC UA Wrapper. Our OPC UA Wrapper supports http, https and opc.tcp transport protocols and detects which one to use from the specified endpoint URL.

iv. Security settings

The user should also select a Security Mode and Security Policy in order to open a secure channel with the selected endpoint. Only security settings supported by the chosen UA server will be enabled.

There are three different Security Modes available:

- None: the channel is not secured.
- Sign: the message is signed with the associated Private Key of the Application Instance Certificate of the OPC UA Proxy.
- Sign & Encrypt: the message is also encrypted with the Public Key of the server's

Application Instance Certificate.

There are three security policies supported which determine the algorithm for signing and encrypting:

- None: an algorithm suite that does not provide any security settings.
- Basic256: an algorithm suite that uses 256-bit Basic as the message encryption algorithm.
- Basic128RSA15: an algorithm suite that uses 128-bit Basic as the message encryption algorithm.

v. *Authentication settings*

On the session establishment step, it is required to choose the user authentication mode. There are two options available:

- Anonymous: user identity is not set.
- Username and Password: the user is identified by a User Name/Password combination.



The certificate identity token is not supported in this version.

When the server URL, the security options and the user authentication mode are set, the UA endpoint configuration is done and we can proceed to the COM configuration by clicking the **Apply** button.

The COM Server Configuration dialog will be displayed:

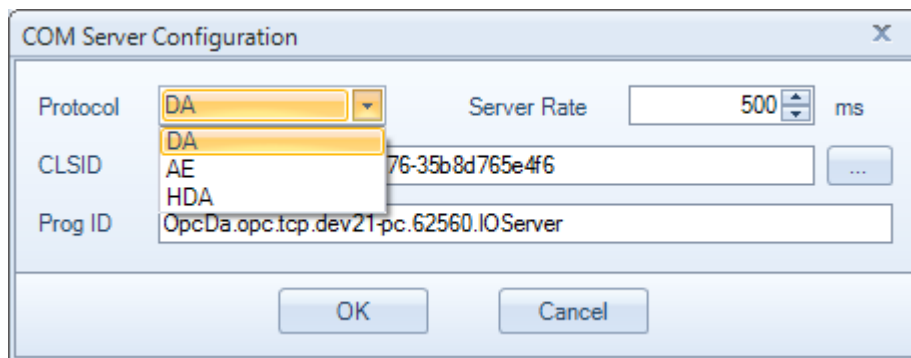


Figure 36: COM Server Configuration Dialog

There are four parameters that should be configured:

- Protocol: The user can choose between DA (Data Access), AE (Alarms & Events) and HDA (Historical Data Access) protocol.
- CLSID: A new CLSID is generated to be assigned to the server.
- Prog ID: The Prog ID is generated from the configured UA endpoint and can be edited by the user.
- Server Rate: the server scan rate of the created DA server.

After clicking the **OK** button, a new node will be added to the UA to COM root node as shown below:

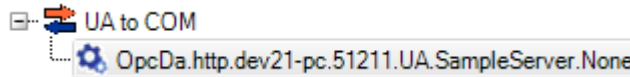


Figure 37: UA to COM Proxies List

3.1.2. Remove a Proxy

In order to remove the proxy and unregister it from the machine, click the **Remove** button available in the Home menu or select **Remove Proxy** from the proxy context menu as illustrated in the figure below.

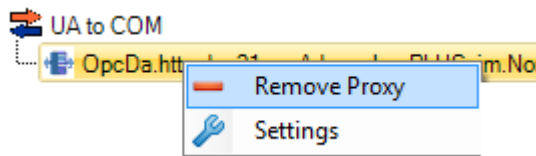


Figure 38: Remove Proxy

You can check that the server was removed from the registered servers.

3.1.3. Edit Proxy Settings

The OPC UA Wrapper comes with default settings for the proxy. These settings can be easily edited using the Proxy Settings dialog presented below.

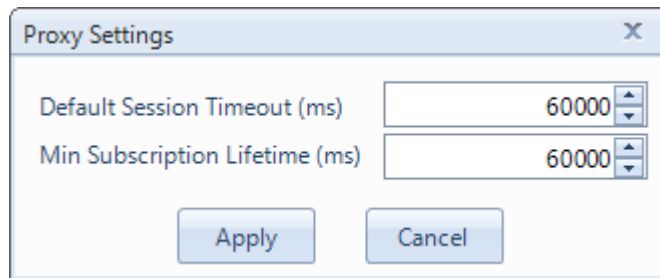


Figure 39: Proxy Settings Dialog

The following table describes the proxy settings:

Setting	Description	Default Value
Default Session Timeout	The default timeout for new sessions (in milliseconds).	60000
Min Subscription Lifetime	The minimum subscription lifetime, that ensures subscriptions are not set to expire too quickly (in milliseconds).	60000

Table 3: Proxy Parameters

3.2. View Proxy Configuration Details

Once you are done with adding the proxy, you can configure its Prog ID, UA endpoint settings and certificates. Clicking on the proxy node will display the configuration tab as illustrated in the figure below:

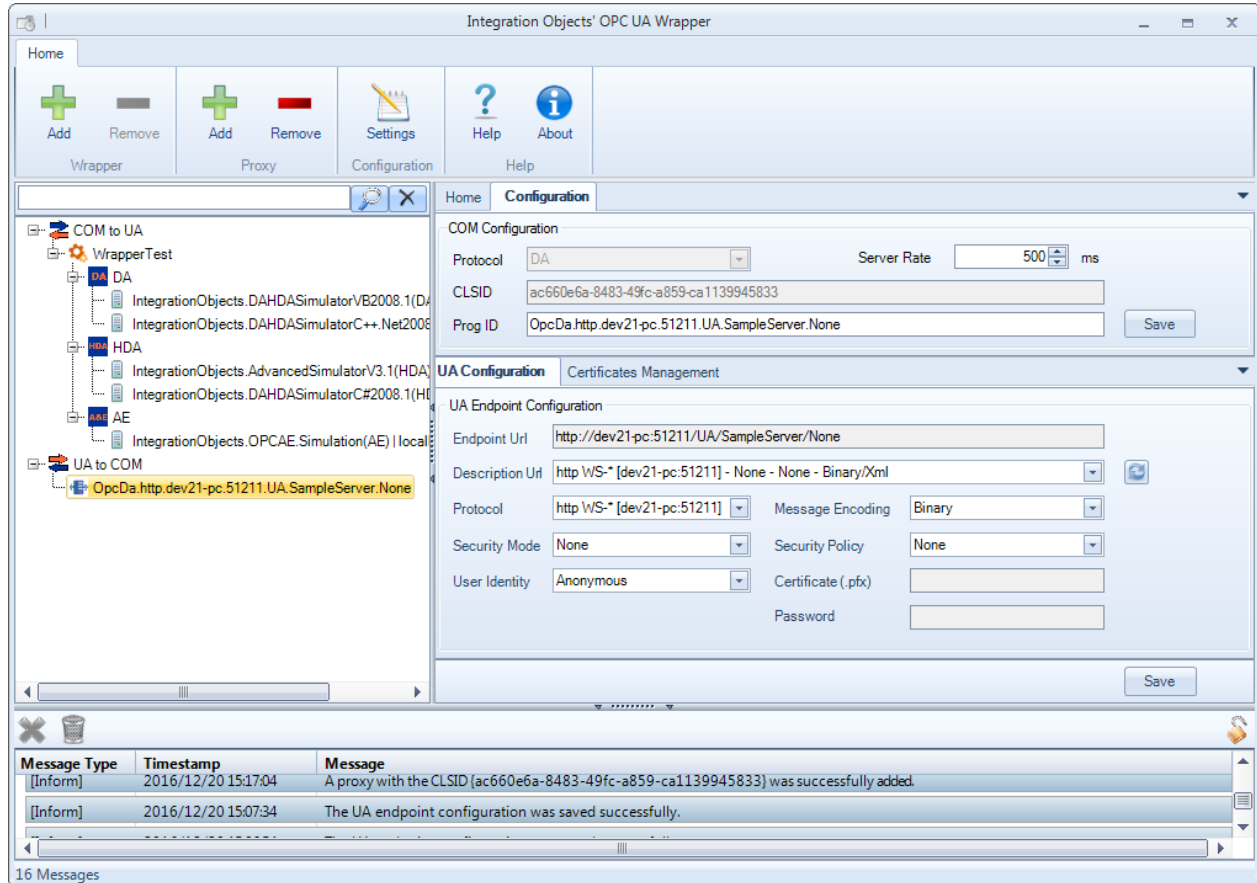
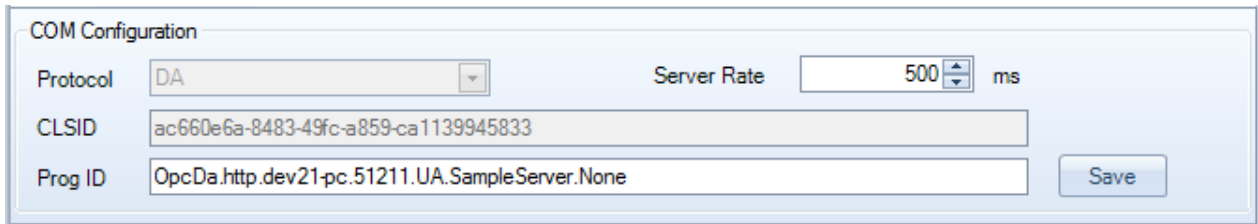


Figure 40: Proxy Configuration Details View

3.2.1. COM Configuration

The COM Configuration section displays the following general information:

- Protocol: the COM protocol associated to the server.
- CLSID: the CLSID of the created server.
- Prog ID: the prog ID of the created server which can be edited by the user.
- Server Rate: the server scan rate of the DA created server which can be edited by the user.



COM Configuration

Protocol: DA Server Rate: 500 ms

CLSID: ac660e6a-8483-49fc-a859-ca1139945833

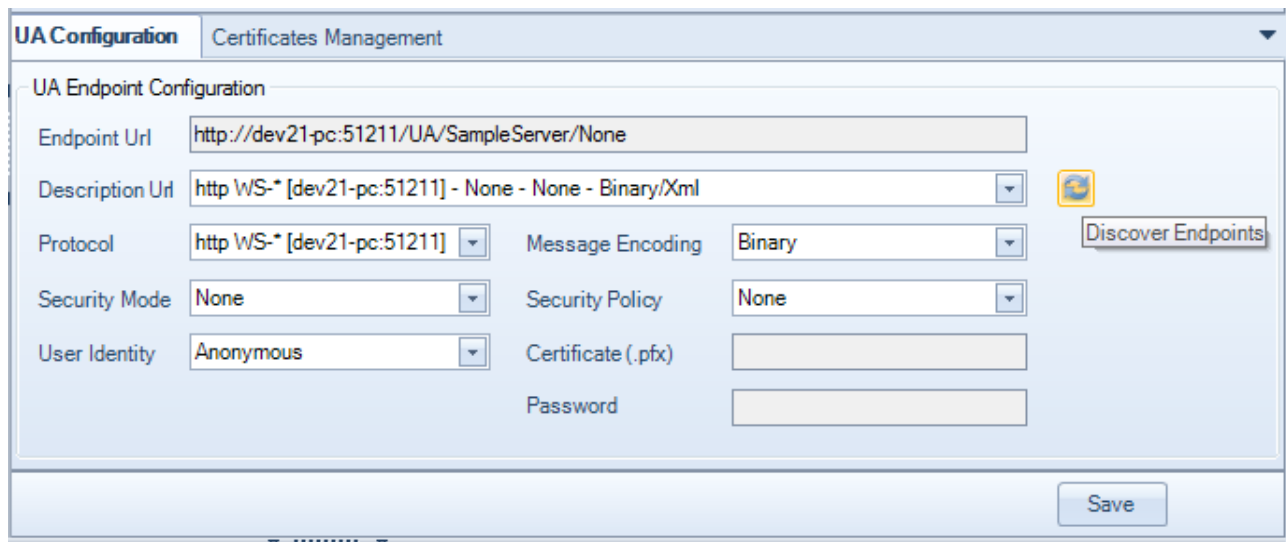
Prog ID: OpcDa.http.dev21-pc.51211.UA.SampleServer.None

Save

Figure 41: COM Configuration

3.2.2. UA Configuration

The user can edit the UA endpoint settings by discovering the endpoints urls, configuring the desired protocol, the security settings and the user identity settings and clicking **Save** button as illustrated in the figure below:



UA Configuration Certificates Management

UA Endpoint Configuration

Endpoint Url: http://dev21-pc:51211/UA/SampleServer/None

Description Url: http WS-* [dev21-pc:51211] - None - None - Binary/XML Discover Endpoints

Protocol: http WS-* [dev21-pc:51211] Message Encoding: Binary

Security Mode: None Security Policy: None

User Identity: Anonymous Certificate (.pfx):

 Password:

Save

Figure 42: UA Configuration

3.2.3. Alias Configuration

The Alias functionality allows to the end user to add a comprehensive identification to the NodeId. To use this functionality, the « Use Alias » checkbox should be enabled and should be saved by clicking the Save button as illustrated in the figure below:

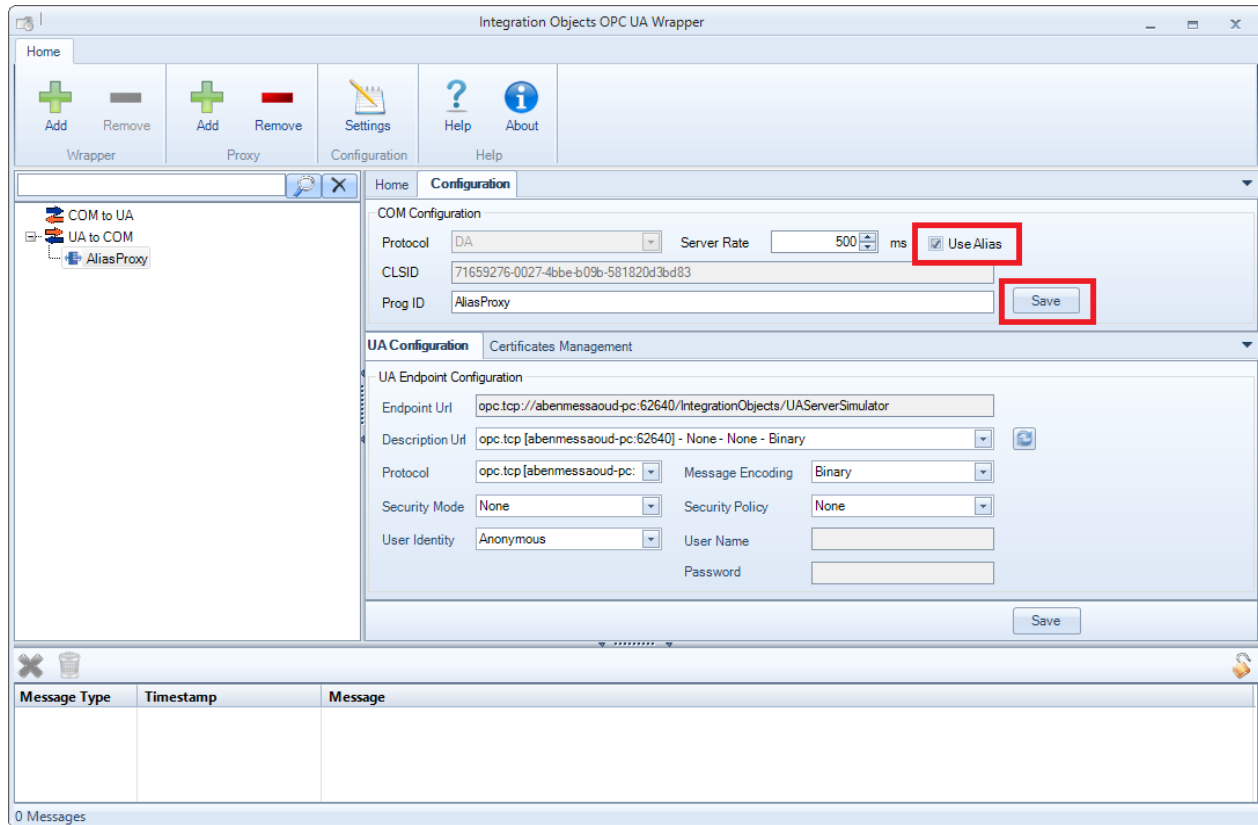


Figure 43: Alias Configuration

Using the Alias Configuration, you can :

- Export Alias to a CSV File : You can export the list of tags into a csv file using the **Export Alias**.
- Import Alias by selecting a CSV File : You can import a tags configuration using the **Import Alias** option.

The figure below shows the export and import features of an alias :

3.2.4. Certificates Management

Using the Certificates Management tab, you can:

- List the certificates: this option displays the list of the trusted, the rejected and the proxy certificates. The user can trust a rejected certificate by right clicking the certificate and selecting **Trust** as shown in the figure below and can also reject a trusted certificate.
- Import certificate: this option allows the user to select a certificate and add it to the list of trusted certificates.
- Remove certificate: this option allows the user to remove the selected certificates from the trust or reject list.

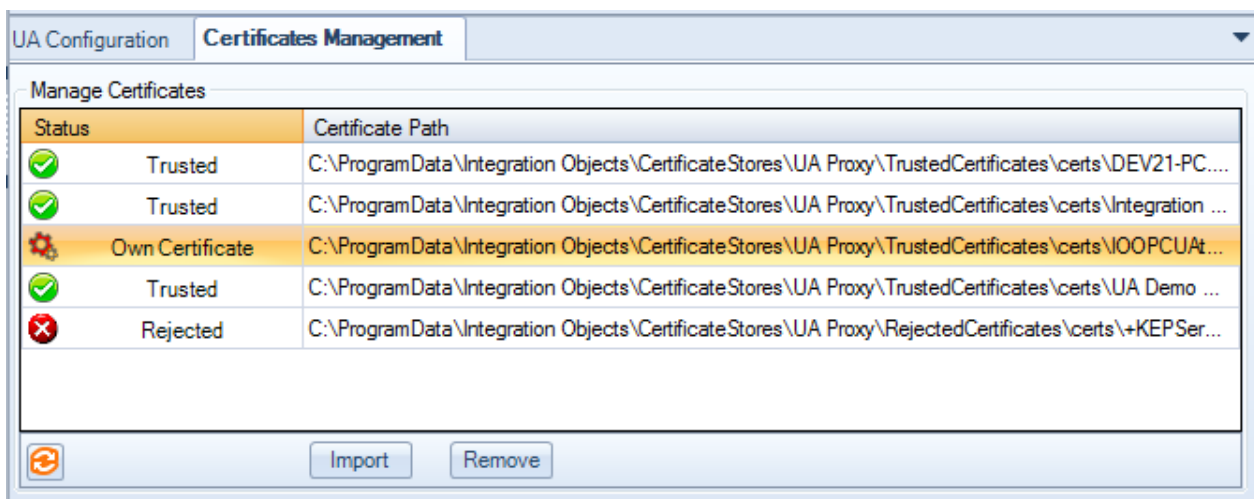


Figure 43: Proxy Certificates Management

3.3. Automatic Reconnection

To configure the reconnection settings, select the **Settings** button available in the home menu bar, navigate to Proxy Configuration tab and you will get the following dialog screen:

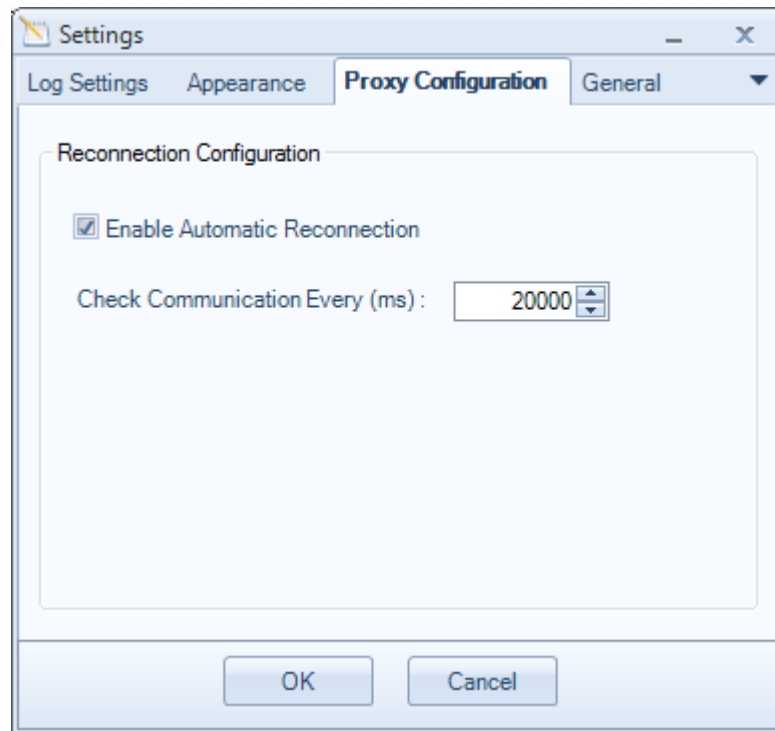


Figure 44: Proxy Reconnection Configuration

You can check the **Enable Automatic Reconnection** box and configure the period separating two reconnection attempts.

OPC UA WRAPPER TRACING CAPABILITIES

The OPC UA Wrapper generates 3 types of log files:

- The “OPCUAConfigurationToolLog.log” that records errors and debug information of the graphical user interface.
- The “ServiceNameLog.log” that records errors and debug information of the given wrapper service.
- The “IOOPCUAtoDAProxyLog.log”, “IOOPCUAtoHDAProxyLog.log” and “IOOPCUAtoAEPProxyLog.log” that record errors and debug information of the OPC UAtoDA Proxy server, UAtoHDA Proxy server and the OPC UAtoAE Proxy server.

The log files can be extremely valuable for troubleshooting. Under normal operations, the logs contain very little information.

The log file for the configuration tool is generated at start-up under the installation folder of the OPC UA Wrapper while services logs can be found in ServiceLogs folder in the Wrappers folder and proxies' logs can be found in ProxyLogs folder in the Proxy folder.

The OPC UA Wrapper comes with default log settings for the wrappers, the proxies and the configuration tool. These settings can be easily edited using the Log settings dialog presented below.

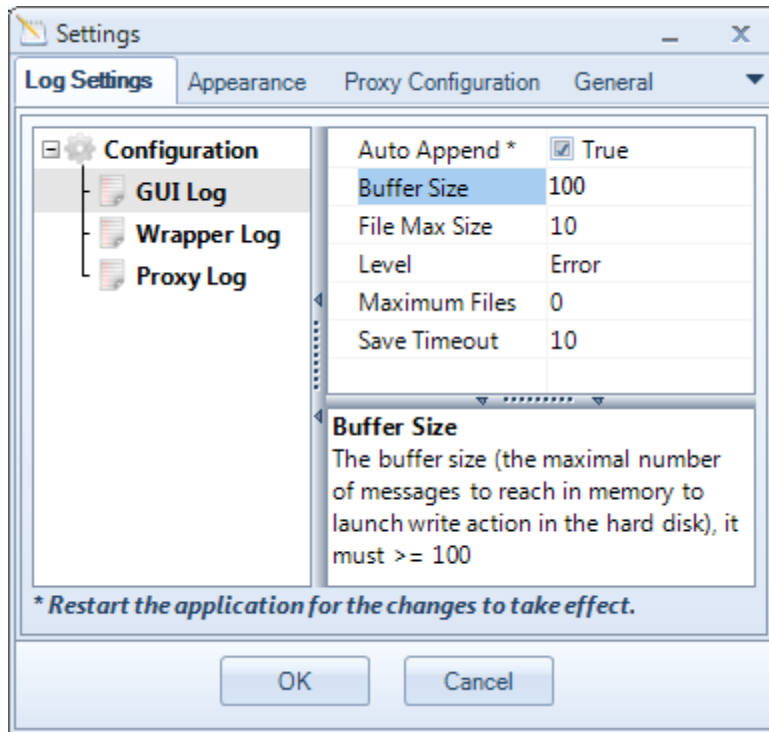


Figure 45: Log Settings Dialog

The following table describes the log settings:

Log Setting	Description	Default Value
Auto Append	Set to true to continue writing log messages in the existed log file or to false to create a new file.	True
Buffer Size	The maximum number of messages to be stored in the runtime memory before launching a write action in the hard disk. The specified value must be greater than 100.	100
File Max Size	This is the maximum log file size, in Mega-Bit. Once it is reached the OPC UA wrapper will automatically create a new log file and archive the last one.	10MB

Level	<p>There are five log levels:</p> <ol style="list-style-type: none"> 1. Control: Logs only control messages. This log level is the lowest level. 2. Error: Logs error and control messages. 3. Warning: Logs warning, error and control messages 4. Inform: Logs information, warning, error and control messages. 5. Debug: Logs all messages. This is the highest level. <p>The higher the log level, the more information are recorded.</p>	Error
Maximum Files	Set to 0 means that log files will be created in an unlimited way.	0
Save Timeout	Specifies the time period to wait before writing the log messages stored in the in-memory buffer to the hard disk. Note that the minimum value is 10 seconds.	10s

Table 4: Log Settings

FREQUENTLY ASKED QUESTIONS

How can I identify my wrapper URL?

To get the wrapper URL, select the wrapper node in the configuration tool and copy the UA endpoint URL. You can choose between TCP and HTTP transport protocol.

How can I purchase an SSL certificate?

The SSL (Secure Sockets Layer) certificates provide secure and encrypted communications between two intended parties. They are issued by any Certificate Authority (organization that is trusted to verify the identity and legitimacy of any entity requesting a certificate)

How can I use my certificate?

Using the configuration tool, you can select your SSL certificate from a .PFX file stored on your disk and assign it to the UA wrapper.

I cannot launch the OPC UA Wrapper Service

If you are using an evaluation license, you should first check the license validity using the License Authorization tool. You can start this tool from the startup menu as illustrated below:

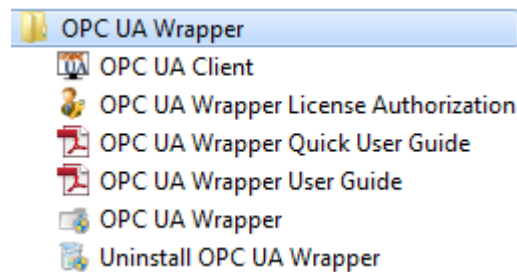


Figure 46: License Authorization

If the License Authorization tool shows that the demo has expired and you want to activate it using an already purchased full license, you should, in this case, follow the steps below:

- Select the feature(s) to be activated
- Click **Generate** button to generate the user ID
- Copy and send the User ID to the sales team { sales@integrationobjects.com } so they can generate the dedicated activation code.

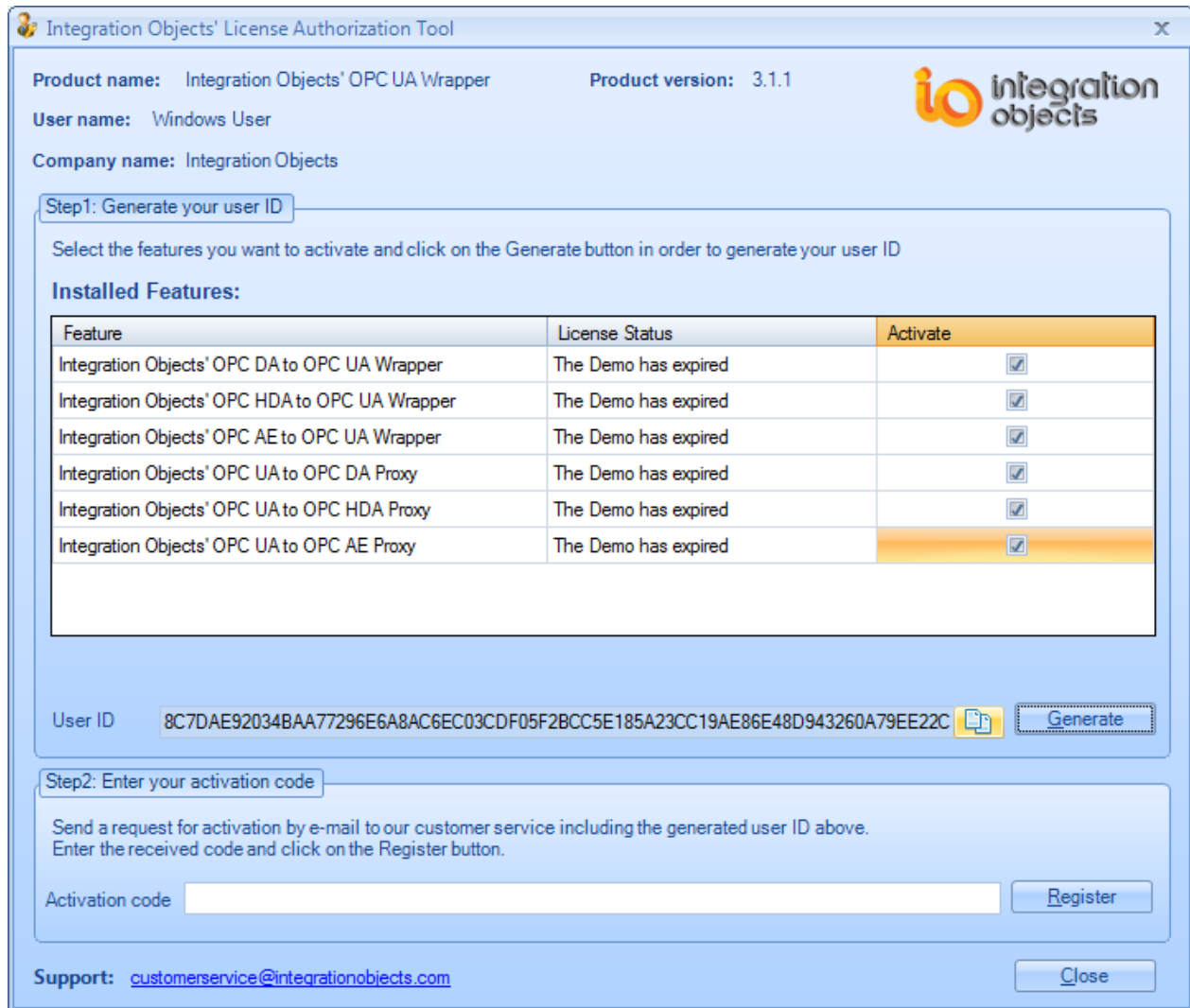


Figure 47: License Authorization (Demo Expired Case)

- Enter the received code in the Activation code field and click the **Register** button.

I cannot connect to a remote OPC Server

If you are not able to connect to a remote OPC server, you should:

- Check if your firewall settings are correct.
- Make sure you have the correct DCOM settings on both computers. Refer to the DCOM configuration guideline documents available under "Installation Folder\Documents".

I cannot connect to a local OPC Server

You should check whether the OPC Core Components are installed in your machine or not.

If they are already installed, you should use the regsvr32 command as shown below to register them again:

1. Example (Windows 7, 64 bit, System Drive "C :"):

```
regsvr32 C:\Windows\SysWOW64\opcproxy.dll
```

```
regsvr32 C:\Windows\SysWOW64\opccomn_ps.dll
```

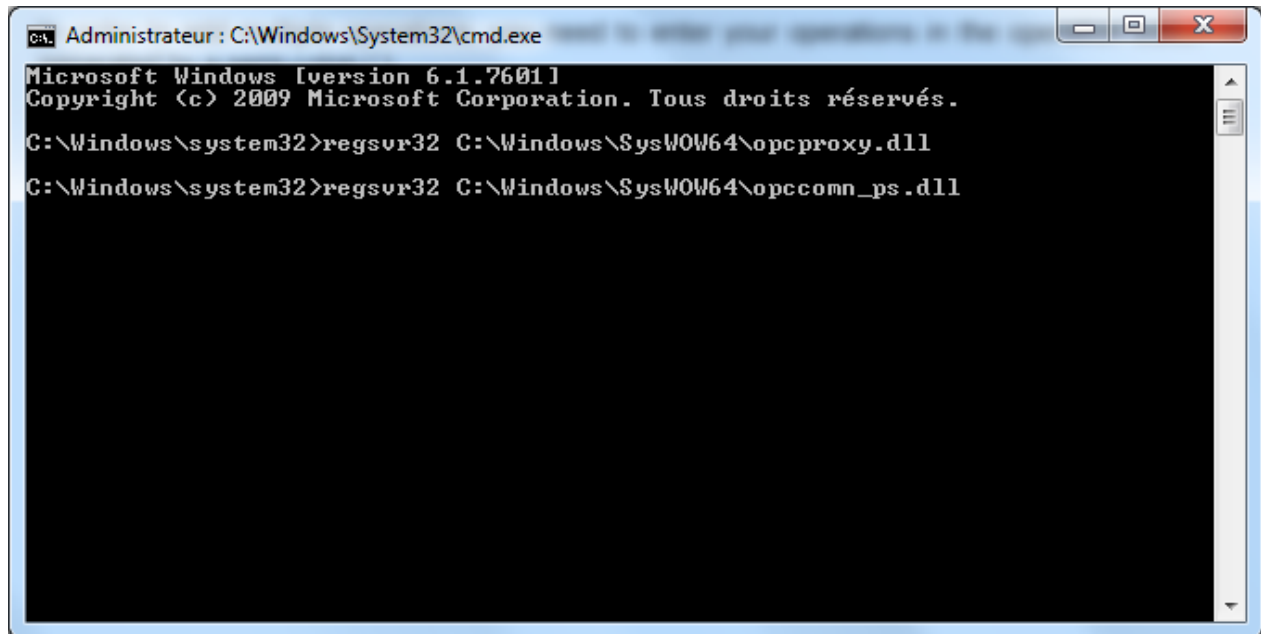
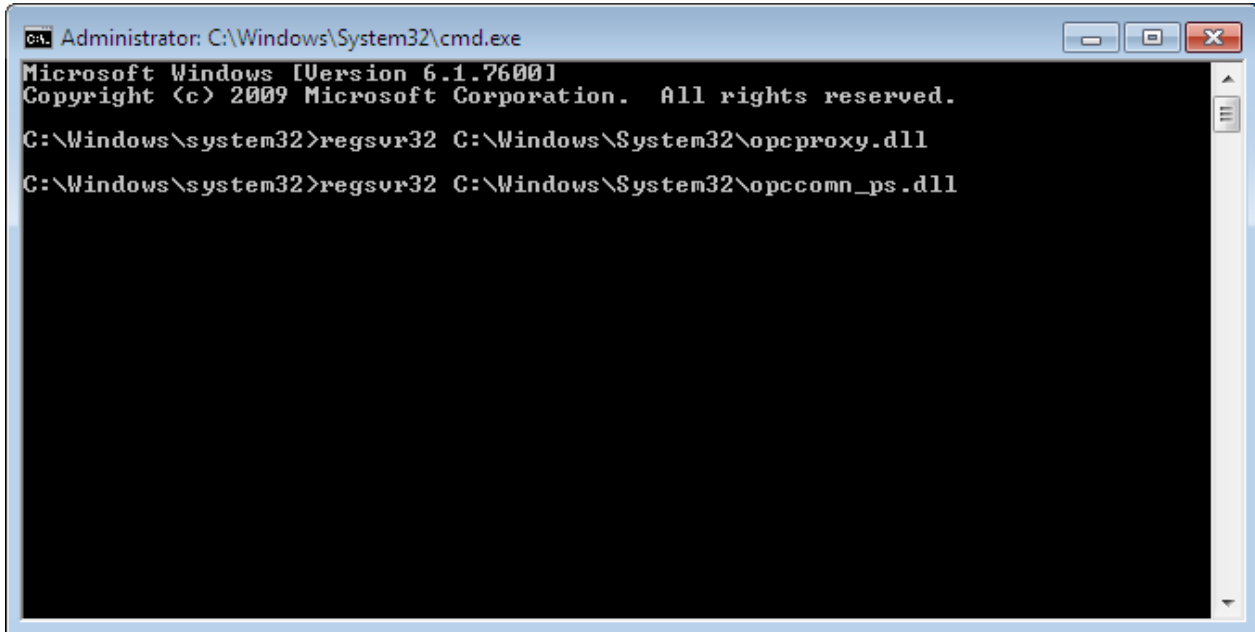


Figure 48: Register OPC Core Components on Windows 7 64 bit

2. Example (Windows 7, 32 bit, System Drive "C :"):

```
regsvr32 "C:\WINDOWS\system32\opcproxy.dll"
```

```
regsvr32 "C:\WINDOWS\system32\opccomn_ps.dll"
```



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>regsvr32 C:\Windows\System32\opcproxy.dll

C:\Windows\system32>regsvr32 C:\Windows\System32\opccomm_ps.dll
```

Figure 49: Register OPC Core Components on Windows 7 32 bit

I cannot discover the OPC UA Wrapper

If you are not able to discover the OPC UA Wrapper from your UA client but you can directly connect to its endpoint using its URL, you should install the Local Discovery Server (LDS), available under “Installation Folder\Components”, which lists the OPC UA servers and wrappers endpoints available on a given computer.

I cannot connect to the OPC UA Wrapper

The list below presents the causes preventing a successful connection to the OPC UA Wrapper:

- Your UA client does not trust the wrapper certificate. In this case, you should trust or trust temporarily the certificate from the client side.
- You are trying to open a session with unsupported security policy. In this case, you can either establish a session with none security, or configure the security modes of the UA wrapper from the configuration tool.
- The user token policy is not supported by the UA wrapper. In this case, you have to configure the session using the identity settings enabled in your wrapper configuration.
- The username and/or the password are incorrect. In this case, you should set the username/password configured in your wrapper.
- You can connect the UA wrapper locally but not remotely. In this case, you should check if the host machine is reachable and if there is an antivirus or a firewall blocking the communication.

How can I fix the missing DLLs error?

When launching the product OPC UA Wrapper, If you get a message box indicating that there is a missing DLL "VCRUNTIME140.dll", you should install visual c++ 2015 redistributable if not installed or reinstall it.

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 our website www.integrationobjects.com.