Integration Objects'
OPC UA to Azure IoT Hub Solution

Industrial IoT Gateway
Version 1.0 Rev.0

USER GUIDE

OPC Compatibility
OPC Unified Architecture 1.02

Industrial IoT Gateway User Guide Version 1.0 Rev0
Published September 2018

Copyright © 2018 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.

TABLE OF CONTENTS

PREFACE **7**

INTRODUCTION **9**

1. Overview **9**

2. Architecture **9**

3. Features **9**

4. Operating Systems Compatibility **10**

5. OPC Compatibility **10**

6. Minimum Hardware Requirements **10**

GETTING STARTED **12**

1. Pre-Installation Considerations **12**

2. Installing and Running **12**

3. Starting-up **19**

4. Removing the IIoT Gateway **19**

USING INDUSTRIAL IOT GATEWAY **21**

1. User Interface Overview **21**

2. Menu Bar **22**

2.1. Configuration Menu 22

2.2. Application Menu 23

3. OPC UA Connection Management **26**

3.1. Sources Tree View 26

3.2. Add New OPC UA Connection 27

3.3. Edit OPC UA Connections 30

3.4. Change User Identity 31

3.5. Remove an OPC UA Connection 32

4. IoT Hub Agent Management **33**

4.1. Destinations Tree View 33

4.2. Add New Publisher Agent 33

4.3. Remove Agent 36

4.4. Edit Agent Settings 37

5. OPC UA to Azure IoT hub Mapping Management 37

5.1. Configure Mapping 37
5.2. Mappings Grid 39
5.3. Remove Mapping 39
5.4. Add monitored Items 39
5.5. Edit Mapping Settings 40
5.6. Start publishing service 41
5.7. Start All publishing services 42
5.8. Stop publishing service 42
5.9. Stop All publishing services 42

6. Automatic Reconnection 42

7. Automatic Data Recovery 43

IIOT GATEWAY TRACING CAPABILITIES 44

TROUBLESHOOTING 46

TABLE OF FIGURES

Figure 1: IIoT Gateway Architecture 9
Figure 2: Installation Welcome Dialog 12
Figure 3: License Agreement Dialog 13
Figure 4: Customer Information Dialog 13
Figure 5: Setup Type Dialog 14
Figure 6: Features Dialog 14
Figure 7: Deployment Version Dialog Box 15
Figure 8: Destination Folder Dialog 16
Figure 9: Installation Dialog 16
Figure 10: Install OPC Core Components Dialog Box 17
Figure 11: Install OPC UA Local Discovery Server Dialog Box 18
Figure 12: Installation Completed Dialog Box 18
Figure 13: IIoT Gateway Start Menu 19
Figure 14: Uninstall Shortcut in the Start Menu 19
Figure 15: Uninstall the IIoT Gateway 20
Figure 16: Configuration Tool Main View 21
Figure 17: Configuration Menu Bar 22
Figure 18: Application Menu Bar 23
Figure 19: OPC UA General Settings 24
Figure 20: Notification Window 26
Figure 21: Sources Tree View 27
Figure 22: OPC UA Connection Creation Dialog Screen 28
Figure 23: OPC UA Connections Management View 29
Figure 24: OPC UA Connection Settings 30
Figure 25: Change User Identity 32
Figure 26: Destinations Tree View 33
Figure 27: IoT HUB Agent Creation 34
Figure 28: IoT HUB Agents Management View 36
Figure 29: IoT HUB Agent Removal 36
Figure 30: IoT HUB Agent Settings 37
Figure 31: Configuring A New Mapping 38
Figure 32: Alarms & Events 38
Figure 33: Mappings Grid 39
Figure 34: DA Message Attributes Selection 41
Figure 35: Subscription Establishment Notification Management 42
Figure 36: Connection Monitoring 43
Figure 37: License Authorization 46
Figure 38: License Service Port Number Unavailable 47
Figure 39: Certificate Loading Failure 48
Figure 40: Agent Creation Failed 49
Figure 41: Industrial IoT Gateway Service log on 50

TABLE OF TABLES

Table 1: Minimum Hardware Requirements....11
Table 2: OPC UA General Settings....25
Table 3: OPC UA Connection Settings....31
Table 4: IoT HUB Agent Settings....35
Table 5: Log Settings....45

PREFACE

ABOUT THIS USER GUIDE

This guide:

- Describes the main features offered by the Integration Objects' Industrial IoT Gateway.
- Lists the system requirements for installing and running IIoT Gateway,
- Explains how to configure the IIoT Gateway,
- And details how to use and run the IIoT Gateway.

TARGET AUDIENCE

This user guide is intended for users who are looking for applications that can collect data from OPC UA Servers and push those data to the Azure IoT hub.
Knowledge of the basics of OPC Unified Architecture (OPC UA) specification is a prerequisite.
It is also assumed that the user has some prior knowledge of Azure IoT hub.

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' Industrial IoT Gateway is an innovative solution that allows you to collect real time data and alarms & events data from OPC UA servers and publish it to Microsoft Azure IoT HUB.

IoT Hub is a managed service, hosted in the Cloud, that acts as a central message hub for bi-directional communication between cloud services and local devices.

2. Architecture

The following diagram illustrates the Industrial IoT Gateway typical system architecture.

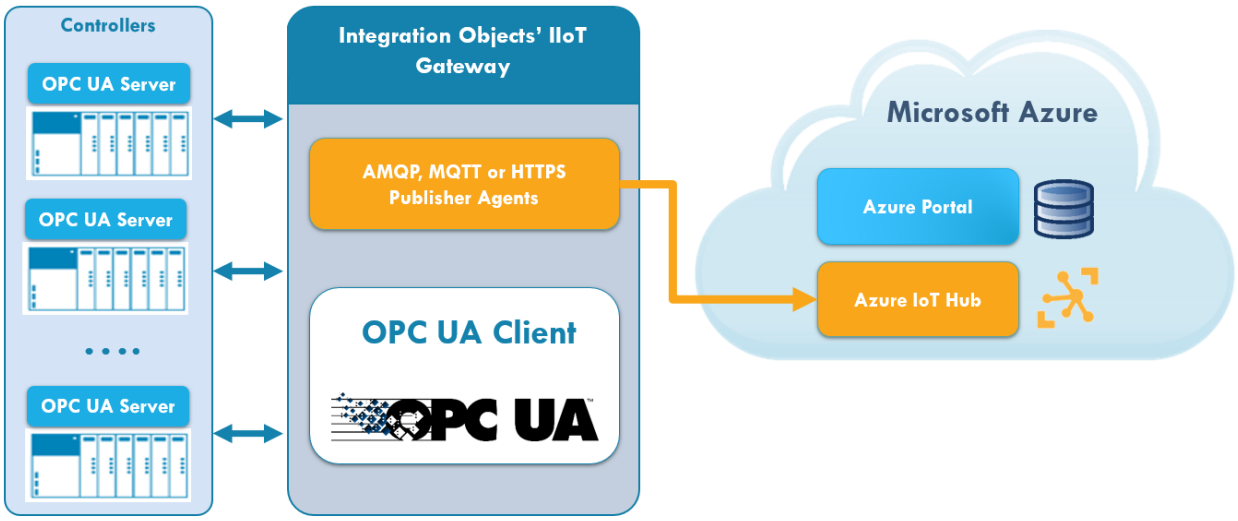


Figure 1: IIoT Gateway Architecture

3. Features

The IIoT Gateway offers the following features:

- Configure multiple publishing agent services through an intuitive Graphical User Interface

- Configure data sources:
    1. Discover local and remote OPC UA servers

2. Establish secure communication sessions with OPC UA servers over TCP HTTP or HTTPS protocols.
3. Browse the address space of any OPC UA compliant server
4. Create subscriptions to items data change events and alarms events
5. Manage OPC UA sessions (edit settings, remove session)
6. Reconnect automatically to OPC UA Servers after recovering from connection losses or network glitches

- Configure data destinations:
  1. Create IoT HUB publisher agents
  2. Establish secure communication channels with the IoT HUB over MQTT, AMQP or REST protocols
  3. Configure IoT HUB message size and send rate
  4. Manage IoT HUB agents (edit settings, remove agent)
- Map OPC items to IoT HUB agents:
  1. Select the monitored Items and the publisher agent to use
  2. Select sent IoT HUB message attributes
- Publish data to IoT HUB:
  a. Start/Stop the publishing services
  b. Reconnect automatically to IoT HUB
  c. Backup data to disk files in case of connection losses
  d. Data recovery from backup disk files after reconnection
  e. Parallel publishing for high number of monitored items

4. Operating Systems Compatibility

IIoT Gateway supports the following operating systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

5. OPC Compatibility

- OPC Unified Architecture 1.02

6. Minimum Hardware Requirements

The following are the minimum hardware requirements to run the Industrial IoT Gateway:

	Description
Processor	2 GHz (higher recommended)
RAM	4 Gb (higher recommended)
Disk Space	200 MB hard disk space for full installation

Table 1: Minimum Hardware Requirements

GETTING STARTED

1. Pre-Installation Considerations

In order to properly run the IIoT Gateway, the following software components on the target system need to be installed:

- .NET framework 4.5.1 or higher.
- 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.
- The OPC UA Discovery Server, which lists the OPC UA endpoints available on a given computer.

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

2. Installing and Running

To install the IIoT Gateway:

1. Run the **Integration Objects' Industrial IoT Gateway** installation package using an administrator account. The installation welcome dialog box will appear.

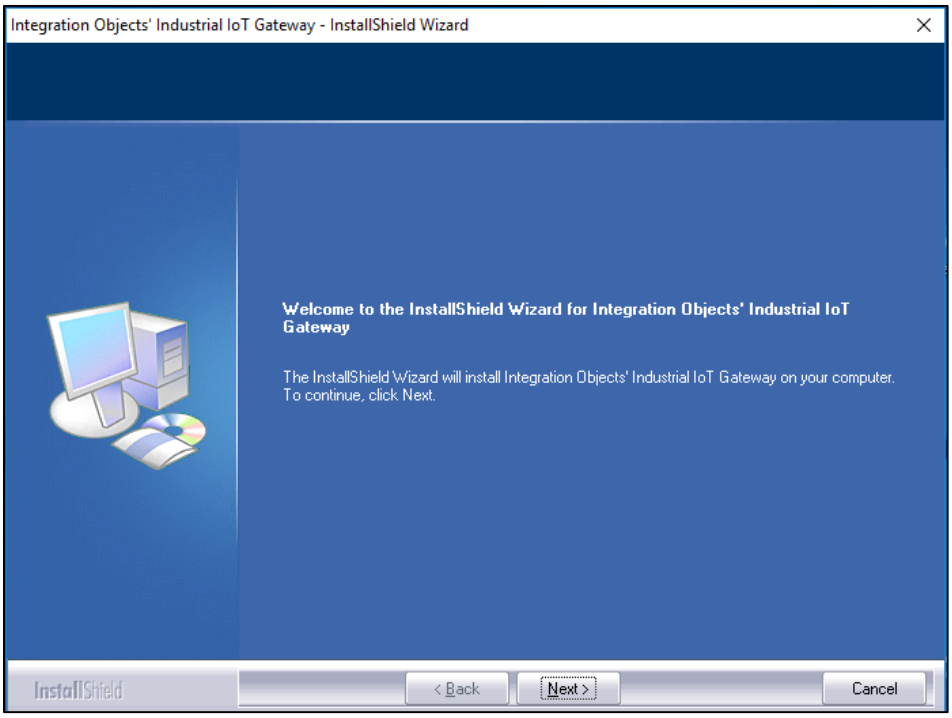


Figure 2: Installation Welcome Dialog

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

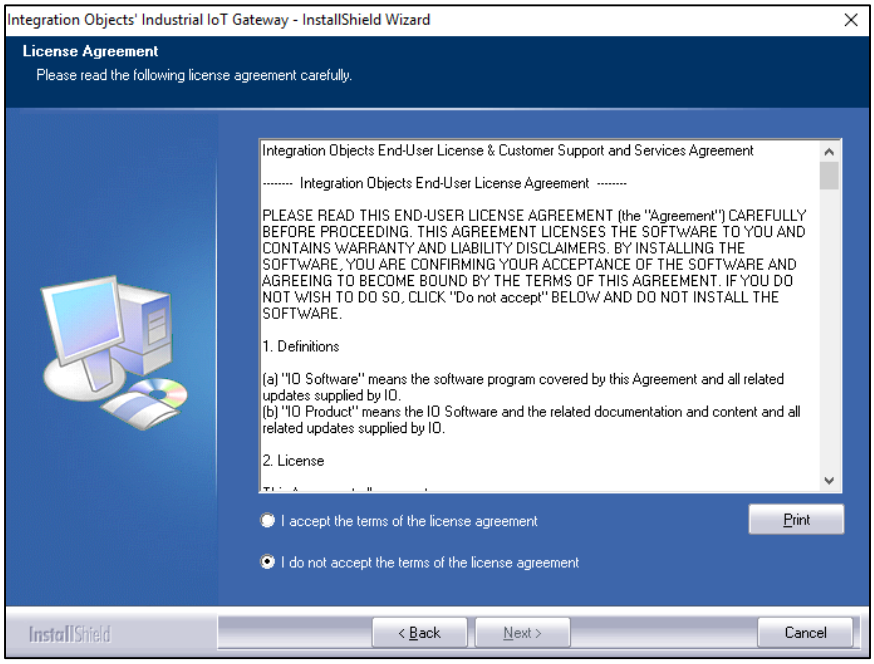


Figure 3: License Agreement Dialog

3. After reading the license agreement, select the first option and click the **Next** button. By proceeding, you are accepting all of the license agreement terms. Otherwise, you can cancel the installation. The customer information dialog box will appear.

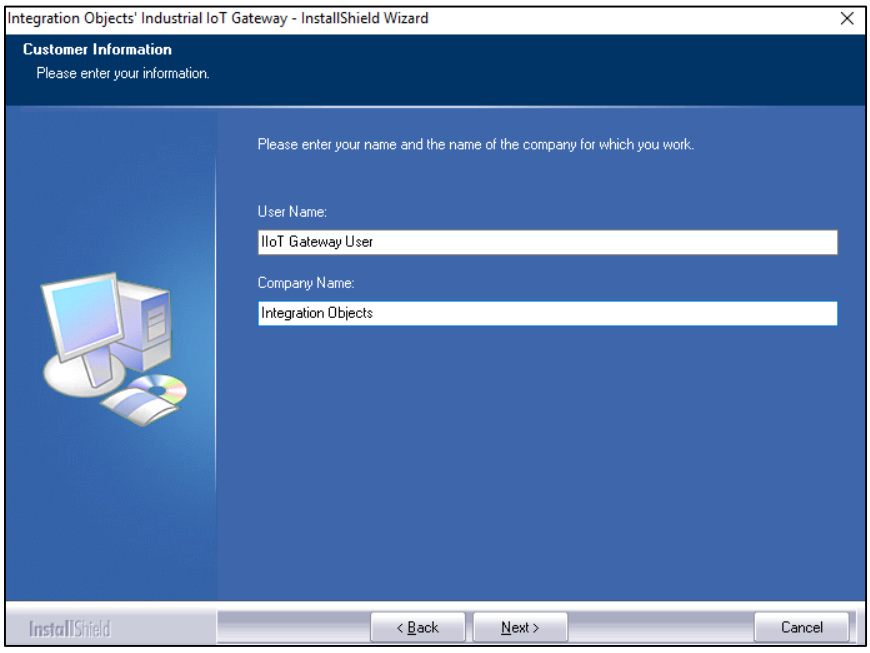


Figure 4: Customer Information Dialog

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

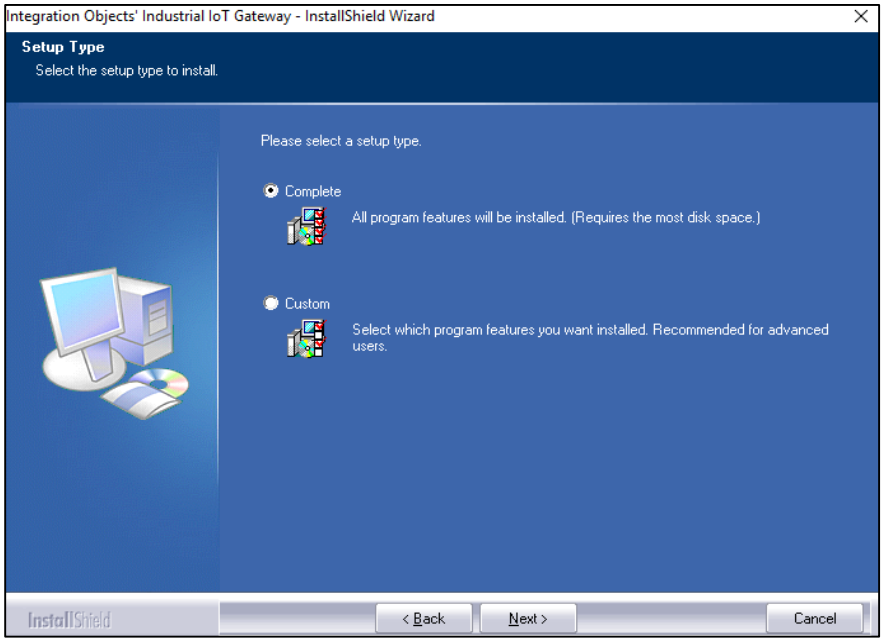


Figure 5: Setup Type Dialog

5. 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 specific features that you want to install:

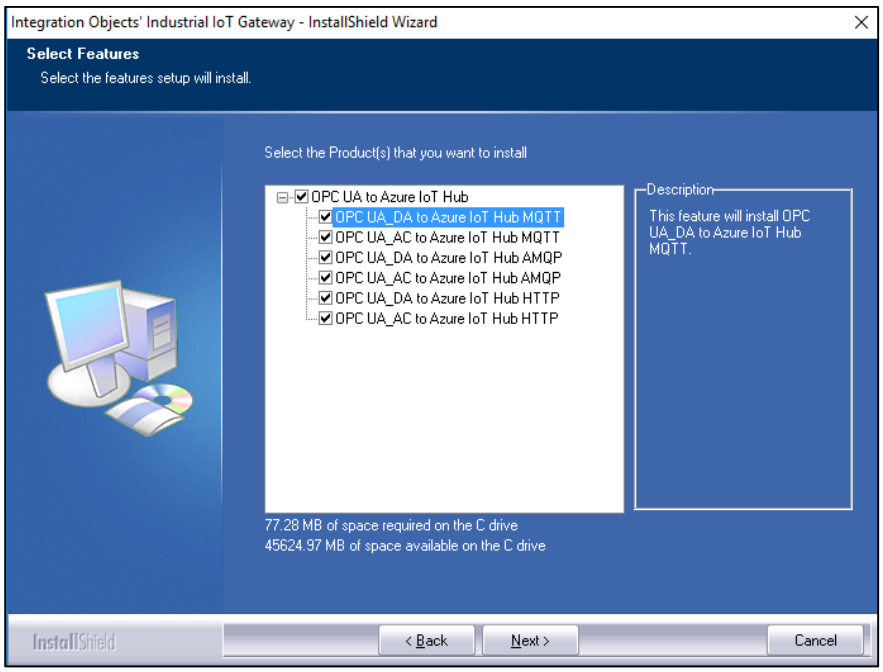


Figure 6: Features Dialog

Based on your requirements, you can activate sending OPC UA Data Access and Alarms and Conditions data to IoT HUB using one of our supported protocols (MQTT, AMQP and HTTP). The features are listed below:

- OPC UA_DA to Azure IoT Hub MQTT: Publish Data Access data using MQTT.
- OPC UA_AC to Azure IoT Hub MQTT: Publish Alarms & Conditions data using MQTT.
- OPC UA_DA to Azure IoT Hub AMQP: Publish Data Access data using AMQP.
- OPC UA_AC to Azure IoT Hub AMQP: Publish Alarms & Conditions data using AMQP.
- OPC UA_DA to Azure IoT Hub HTTP: Publish Data Access data using HTTP.
- OPC UA_AC to Azure IoT Hub HTTP: Publish Alarms & Conditions data using HTTP.

These features can be installed and licensed separately.

6. After selecting the features, you want to install, click the **Next** button. The dialog box of choosing the IIoT Gateway deployment version will be displayed.

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

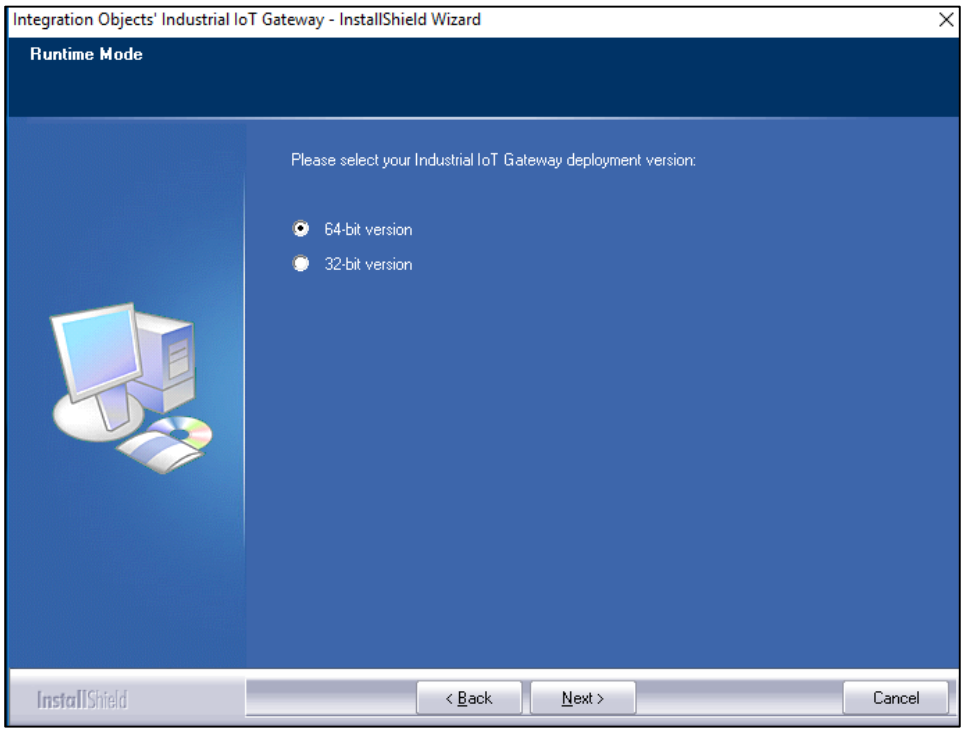


Figure 7: Deployment Version Dialog Box

7. After selecting the IIoT Gateway deployment version, the dialog box for choosing the destination folder will be displayed.

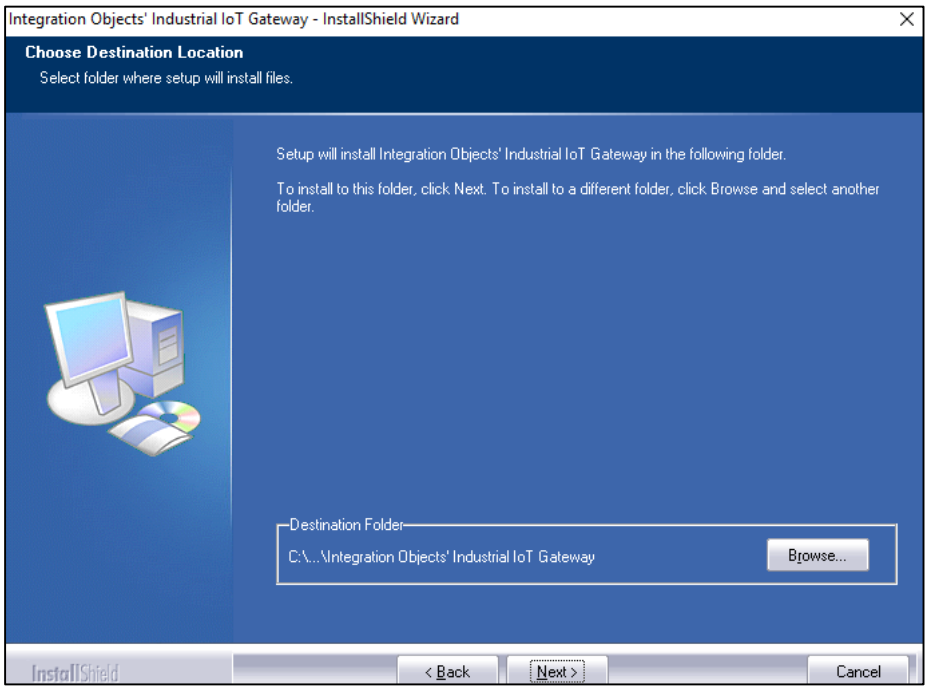


Figure 8: Destination Folder Dialog

8. Click the **Next** button to use the default destination folder and continue the installation, or the **Browse** button to select a different destination folder. The installation dialog box will then appear.

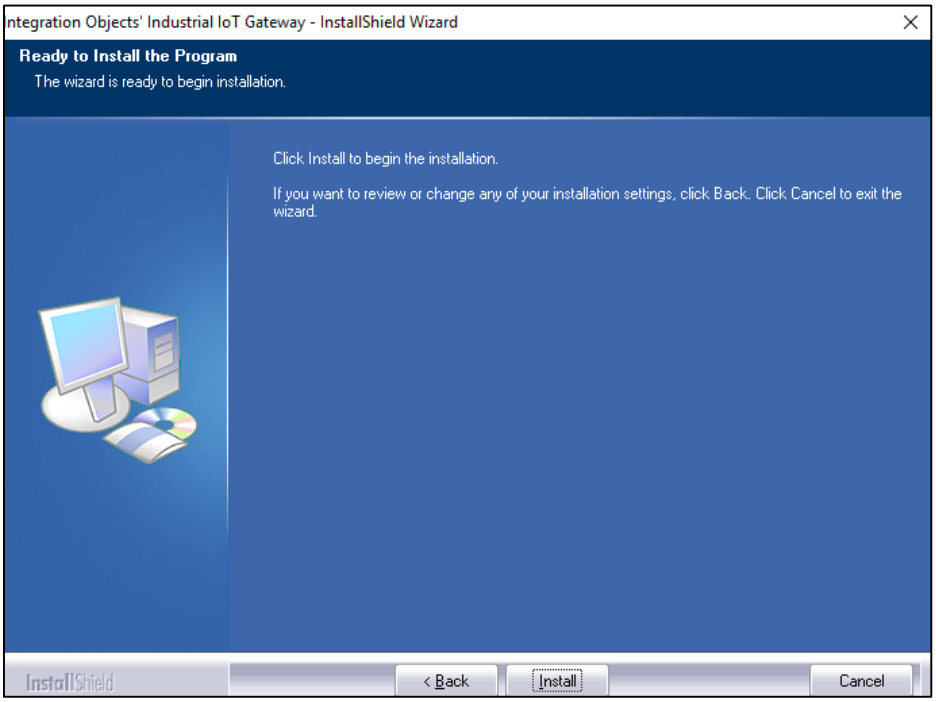


Figure 9: Installation Dialog

9. Click the **Install** button to start installation.
   The setup will then copy the necessary files to the selected destination folder, create shortcut icons to launch the IIoT Gateway and license authorization program from the start menu. It will also make an un-installation entry in the Programs and Features in the Control Panel.

10. 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.

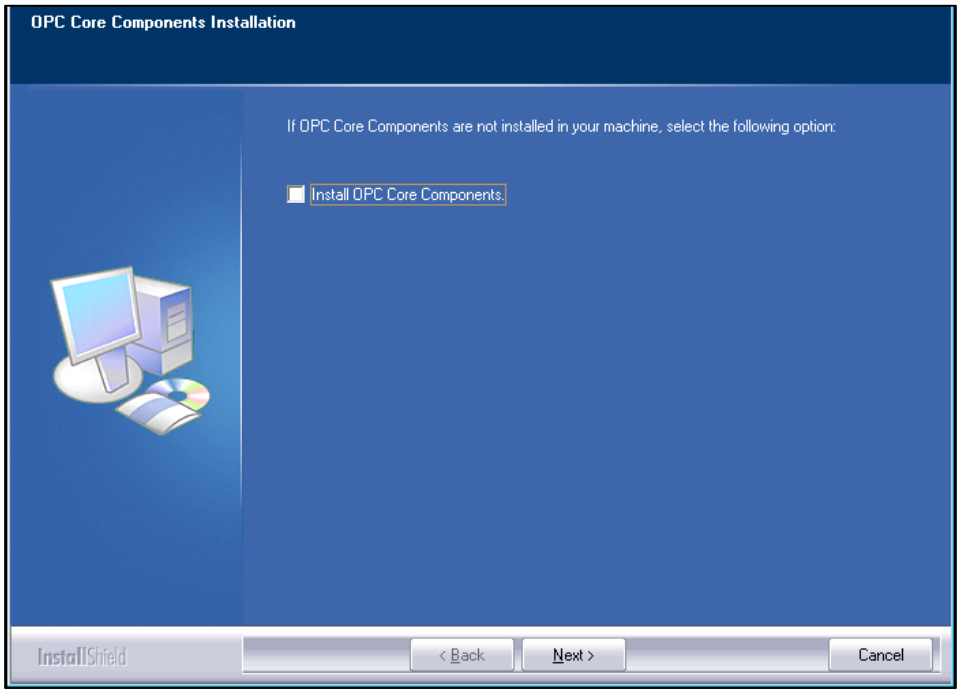


Figure 10: Install OPC Core Components Dialog Box

11. 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.

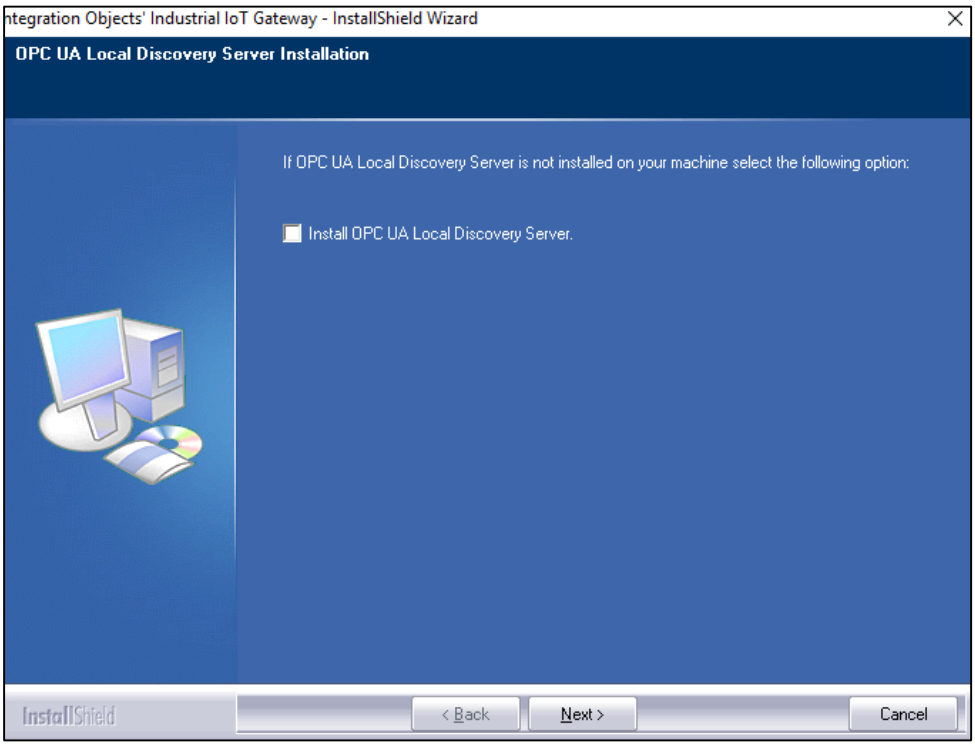


Figure 11: Install OPC UA Local Discovery Server Dialog Box

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

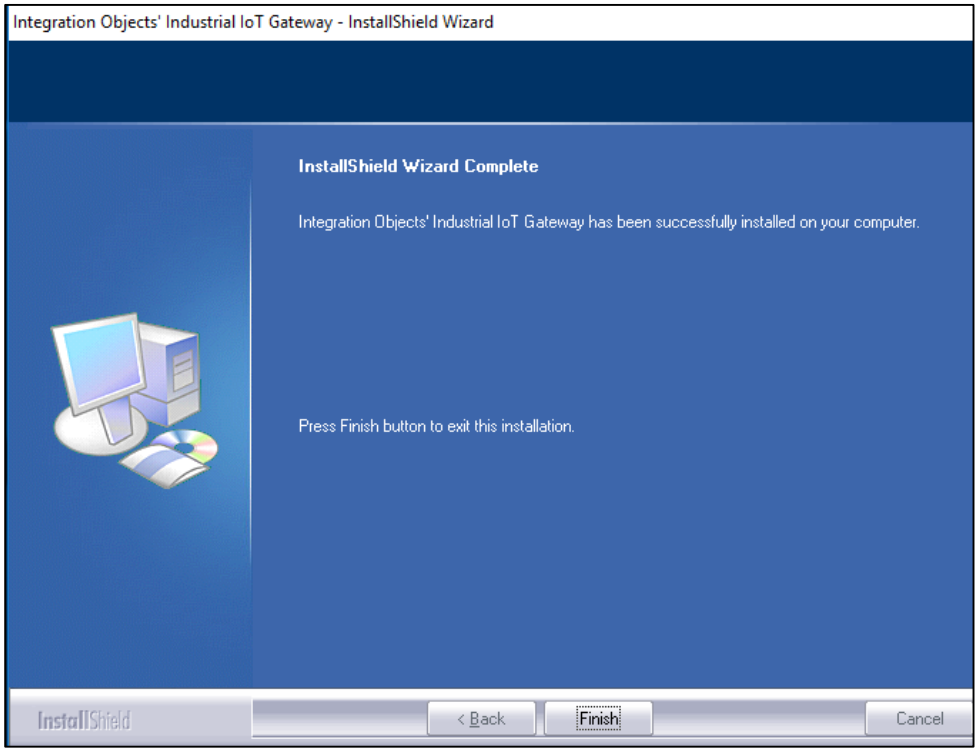


Figure 12: Installation Completed Dialog Box

3. Starting-up

The IIoT Gateway user interface can be launched from the start menu shortcut. To do so, click on **Start ➔ Programs ➔ Integration Objects ➔ IIoT Gateway Config Tool**

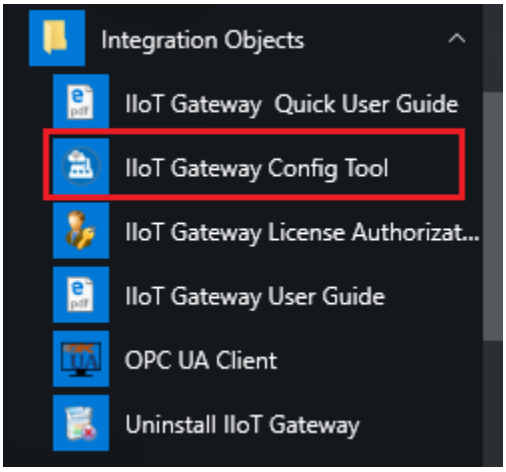


Figure 13: IIoT Gateway Start Menu

4. Removing the IIoT Gateway

Make sure that you are using an administrator account using the uninstallation procedure. To uninstall the IIoT Gateway, follow the steps below:

1. Click the **Uninstall** shortcut available in the start menu, as shown in the figure below:

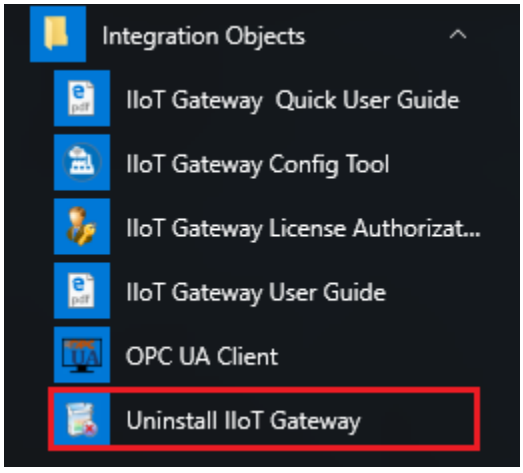


Figure 14: Uninstall Shortcut in the Start Menu

The following dialog box will appear:

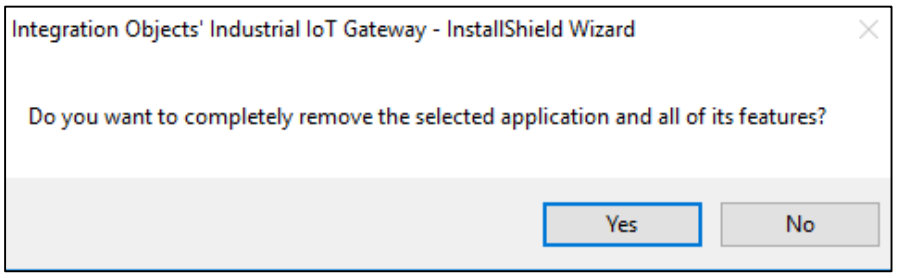


Figure 15: Uninstall the IIoT Gateway

2. Click the **Yes** button to start uninstalling.

3. The wizard will then take you through the removal steps. At the end, click **Finish** when the un-installation is complete.

The IIoT Gateway can be also 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' Industrial IoT Gateway**.
4. Click **Uninstall** then **OK**.

USING INDUSTRIAL IOT GATEWAY

In this section, you will find an overview of the IIoT Gateway user interface as well as the steps required to configure and use the application.

1. User Interface Overview

The Industrial IoT Gateway configuration tool is a user-friendly graphical interface designed to configure and manage OPC UA Sessions, IoT HUB Agents and publisher services.

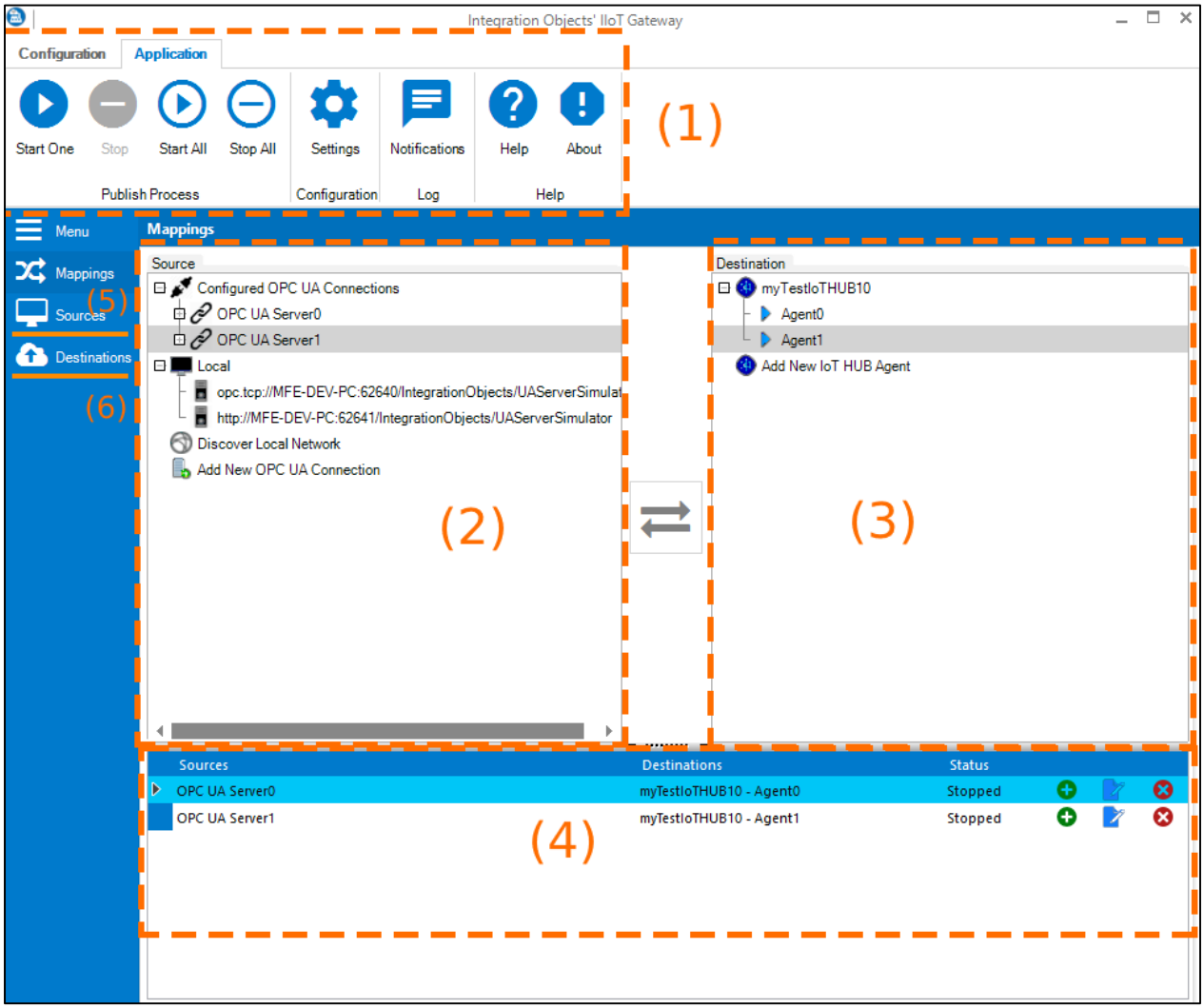


Figure 16: Configuration Tool Main View

There are 6 parts in the configuration tool user interface, as highlighted above:

- Menu bar (1): It contains the configuration and the application menus:
    a. The configuration menu provides configuration related functionalities such as saving to or opening a configuration file and defining a default configuration.
    b. The application menu provides functionalities such as starting/stopping the publisher services, configuring OPC UA general settings, showing log messages and providing help.
- Sources Tree View (2): It contains the configured OPC UA Connections, the discovered local OPC UA Servers. It also provides local network discovery and manual OPC UA connection creation functionalities.
- Destinations Tree View (3): It contains the configured IoT HUB agents and provides the IoT HUB agent creation functionality.
- Mappings Grid (4): The grid contains the configured mappings between OPC UA connections and IoT HUB agents. It also allows users to edit or remove mappings and to add new monitored items.
- Sources Tab (5): The sources tab presents the configured OPC UA Connections in a grid. The grid lists the information about the configured connections. It provides edit/remove functionalities and change user identity feature.
- Destinations Tab (6): The destinations tab presents the configured IoT HUB agents in a grid. The grid lists the information about the configured agents and provides edit/remove functionalities.

2. Menu Bar

2.1. Configuration Menu

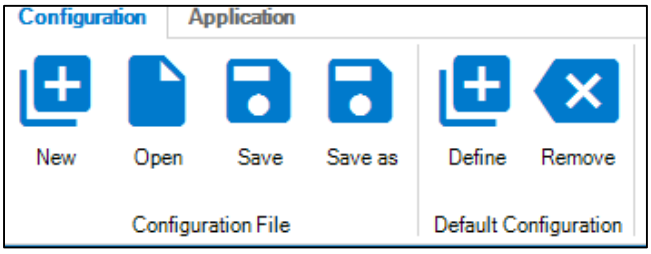


Figure 17: Configuration Menu Bar

Using the Configuration menu, you can**:**

- **New:** Create a new configuration by clicking the **New** button.
- **Open:** Open an existing configuration by clicking **Open** and selecting the appropriate ".iog" configuration file.
- **Save:** Save your current configuration by clicking **Save** or **Save As**.

- **Define:** Click the **Define** button to define the default configuration to be loaded automatically at the application start-up. This will prompt a file dialog screen. Select your saved configuration and then click the **OK** button.
- **Remove**: To remove the default configuration, click the **Remove** button.

2.2. Application Menu

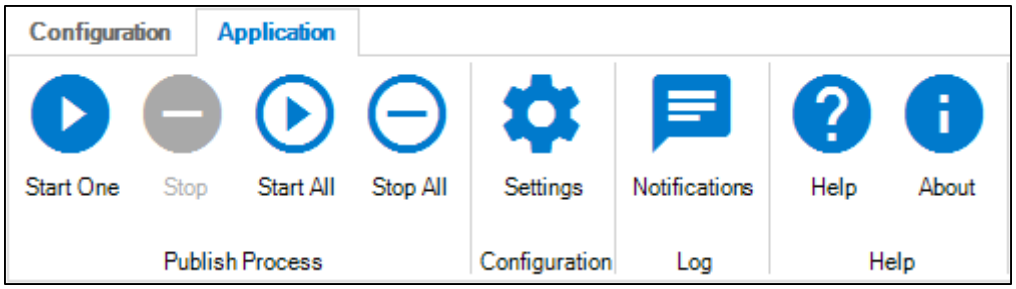


Figure 18: Application Menu Bar

Using the Application menu, you can**:**

1. Control the publish processes:

    - **Start One**: Start one publisher service by clicking the **Start One** button. The button is enabled only if a mapping is selected in the Mappings grid.
    - **Stop**: Stop one publisher service by clicking the **Stop One** button. The button is enabled only if a mapping is selected in the Mappings grid.
    - **Start All**: Start all the configured publishing services.
    - **Stop All**: Stop all the configured publishing services.

2. Configure OPC UA general settings:

    - **Settings:** Edit general OPC UA Settings by clicking the **Settings** button.

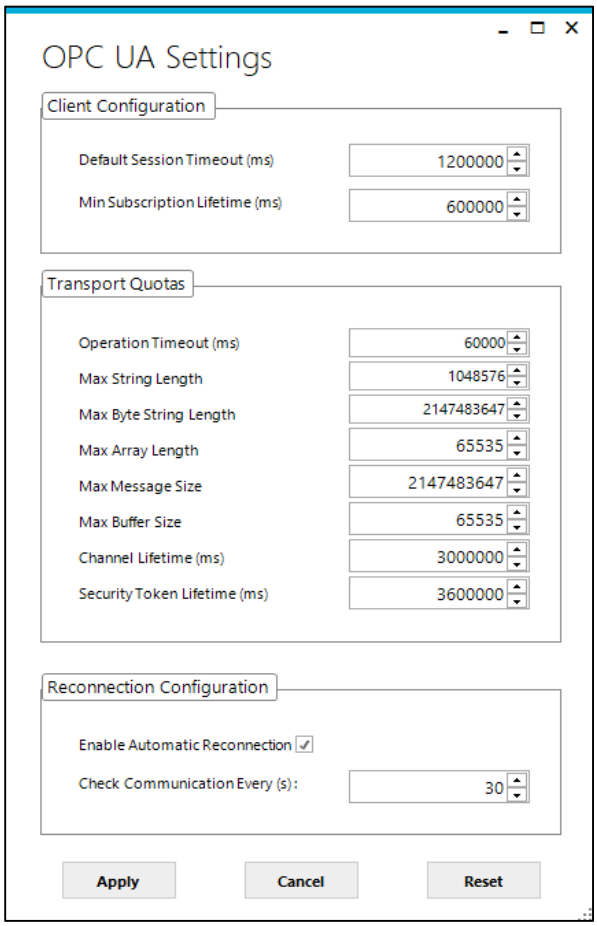


Figure 19: OPC UA General Settings

The default client and transport parameters are listed in the table below:

Setting	Description	Default Value
Default Session Timeout	The default timeout for new sessions in milliseconds.	60000 ms
Min Subscription Lifetime	The minimum subscription lifetime to ensure that subscriptions are not quickly expired in milliseconds.	60000 ms
Operation Timeout	The default timeout for operations in milliseconds.	120000 ms
Max String Length	The maximum length for a string value in any message.	1048576 bytes

Max Byte String Length	The maximum length for a byte string value in any message.	4194304 bytes
Max Array Length	The maximum length for any array in a message. Note that some protocols do not distinguish between bytes and arrays. In these cases, the binding will choose the biggest value between the Max Byte String Length and Max Array Length.	65535 bytes
Max Message Size	The maximum size of any message.	4194304 bytes
Max Buffer Size	The maximum buffer size. This value controls how big a block of memory the transport layer allocates. Setting this value to a large number will reduce the performance and use a lot of memory.	65535 bytes
Channel Lifetime	The lifetime of a Secure Channel in milliseconds. It specifies how long the server will keep a broken channel around while waiting for a client to reconnect. Not used by HTTP or .NET TCP bindings.	300000 ms
Security Token Lifetime	The lifetime of a Security Token in milliseconds. It specifies how long a security token can be used without renewal.	3600000 ms
Check Communication Every(s)	It specifies the connection check period in seconds.	30 s

Table 2: OPC UA General Settings

3. Monitor the application**:**
   - **Notification**: Prompt the message log browser by clicking the **Notification** button. Messages are listed from the most recent one to the least recent one and are highlighted according to the message type:
     - blue for control messages
     - yellow for warning messages
     - and red for error messages

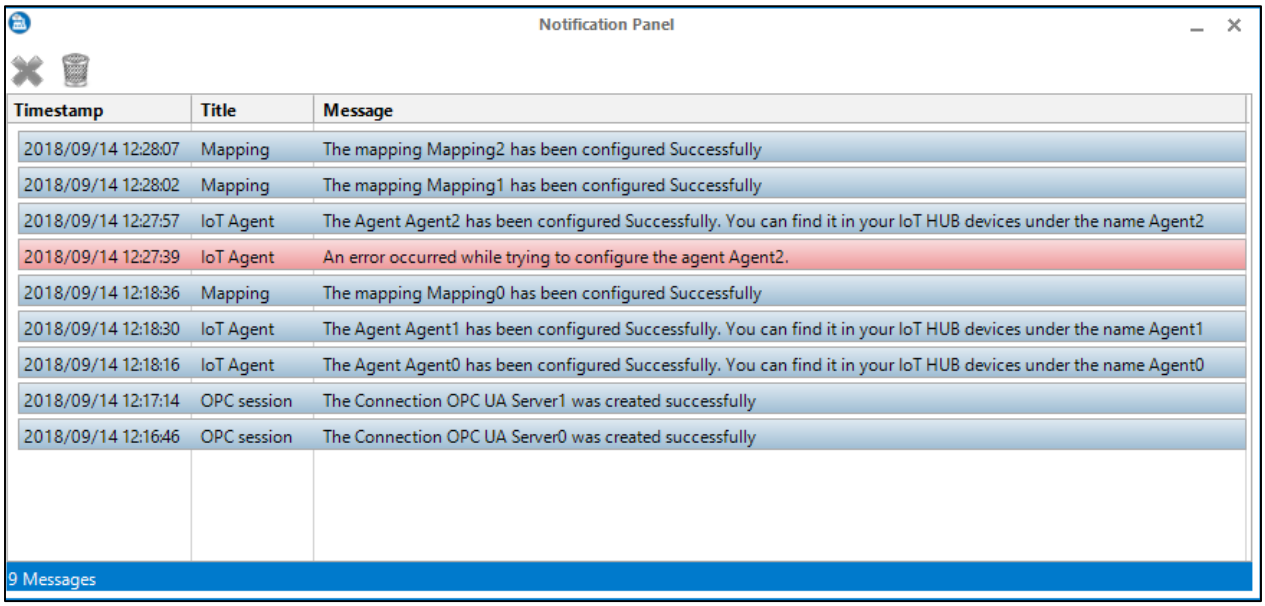


Figure 20: Notification Panel

4. Help**:**
   - **Help**: Open user guide by clicking the **Help** button.
   - **About**: Show product information by clicking the **About** button.

3. OPC UA Connection Management

In this section, we will detail the procedures of creating, editing and removing an OPC UA Connection.

3.1. Sources Tree View

In this tree view, you can find your configured OPC UA Connections and their address spaces.

In addition, the local OPC Servers discovered in your machine and your local network workstations are presented under **Local** and **Discover Local Network** nodes as illustrated below:

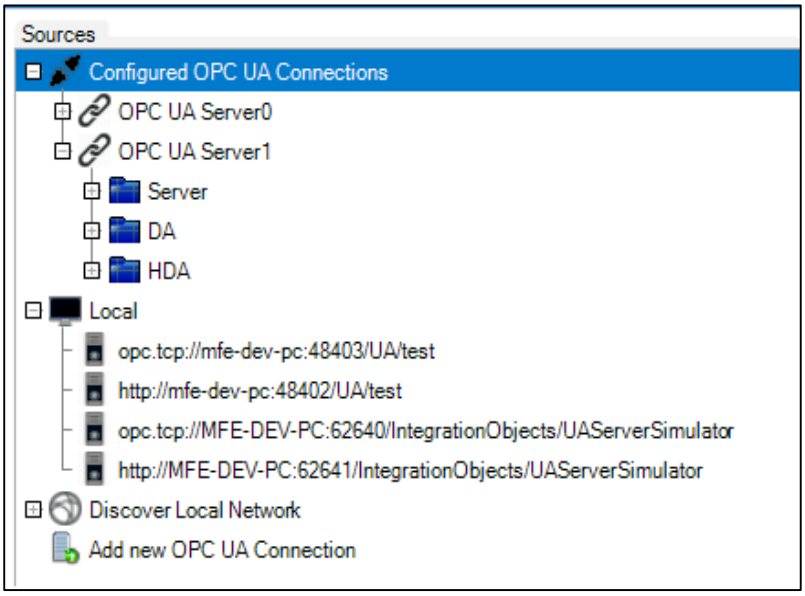


Figure 21: Sources Tree View

3.2. Add New OPC UA Connection

You can configure an OPC UA Connection as follows:

- Double clicking on a discovered OPC UA Server available at the Sources tree view under the Local node.
- Or clicking the Add New OPC UA Connection button available at the Sources Tree View or the Sources tab and type the server URL in the endpoint URL field.

All the settings presented in the following dialog screen are required to open a channel and to establish a session with the selected OPC UA server:

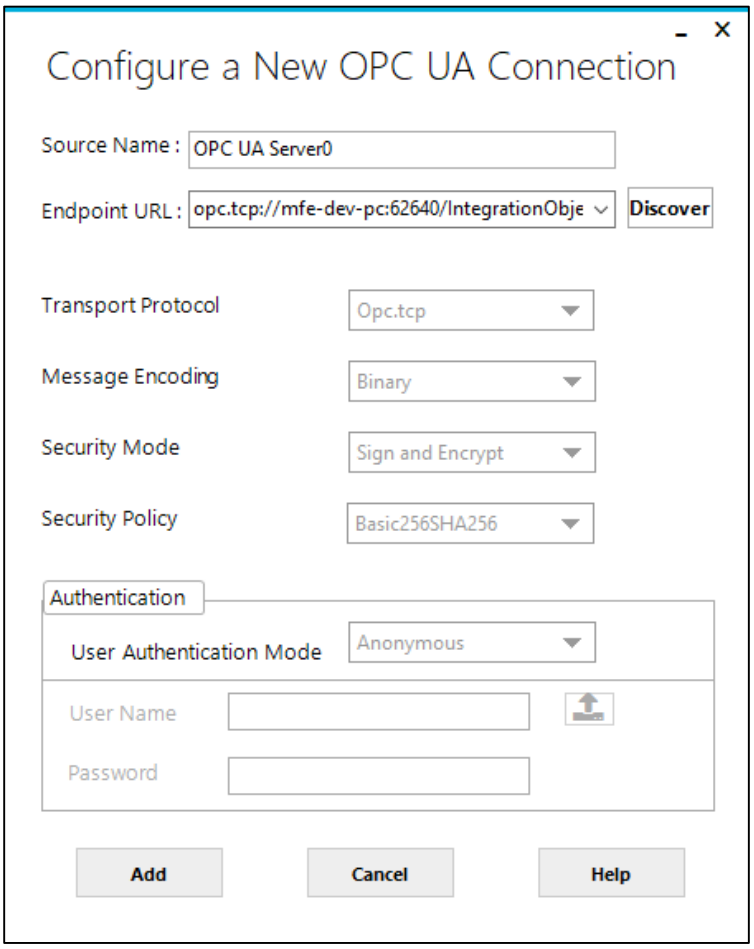


Figure 22: OPC UA Connection Creation Dialog Screen

- **Endpoint settings**

You can type the server URL or select it from the discovered URLs list.
The IIoT Gateway supports "http", "https" and "opc.tcp" transport protocols and detects which of them to use from the specified endpoint URL.

- **Security settings**

You also need to select a Security Mode and Security Policy so that the IIoT Gateway opens a secure channel with the selected endpoint. Only security settings supported by the chosen UA server will be enabled.
Three different security modes are available:

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

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

- None: an algorithm suite that does not provide any security settings.
- Basic128RSA15: an algorithm suite that uses RSA15 as the key wrap algorithm and 128-bit Basic as the message encryption algorithm.
- Basic256: an algorithm suite that uses 256-bit Basic as the message encryption algorithm.

- **Authentication settings**

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

- Anonymous: user identity is not set.
- Username and Password: the user is identified by a User Name/Password combination.
- Certificate: the user is identified by an X509 certificate.

Once the server URL, the security options, the user authentication mode and the session name are entered, you can establish the connection to the server by clicking the **Add** button.
To manage your configured OPC UA Connections, click the "**Sources**" tab in the navigation bar side.

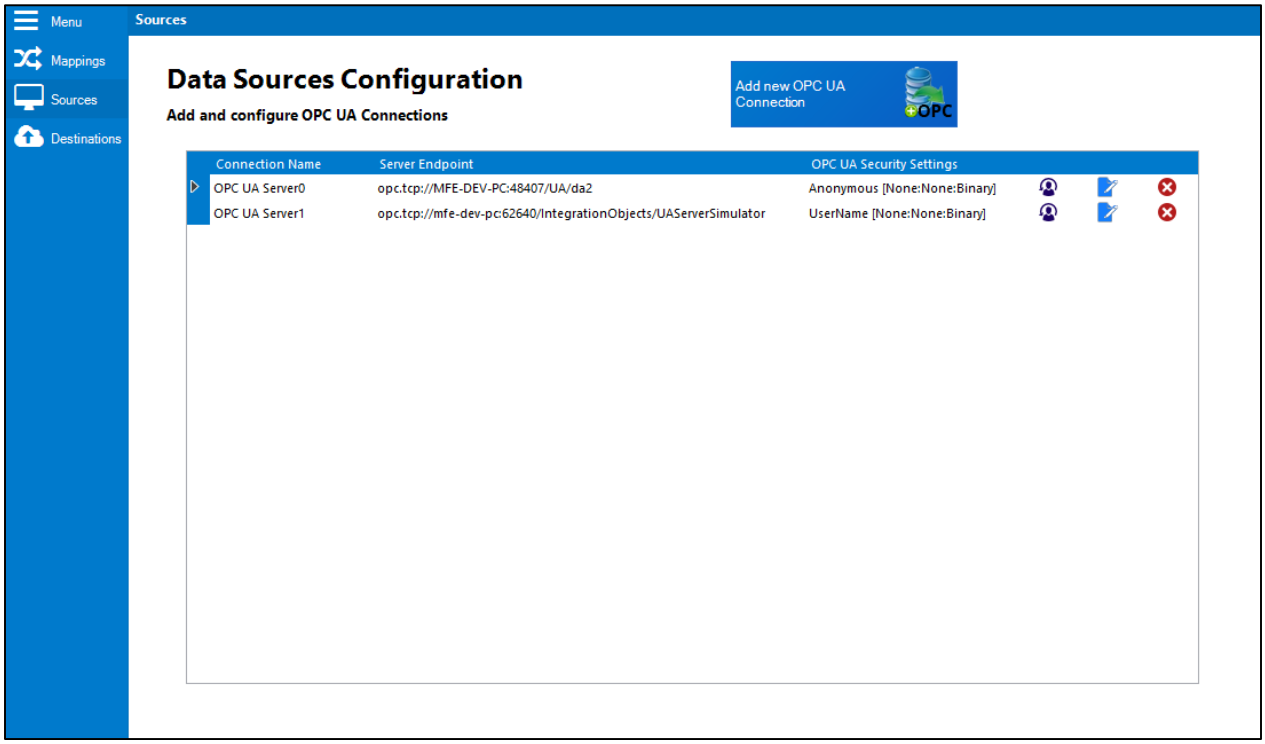


Figure 23: OPC UA Connections Management View

3.3. Edit OPC UA Connection

You can edit the OPC UA Connection settings by clicking on the blue edit icon of a specific row in the grid ( ).
The following dialog screen will be prompted:

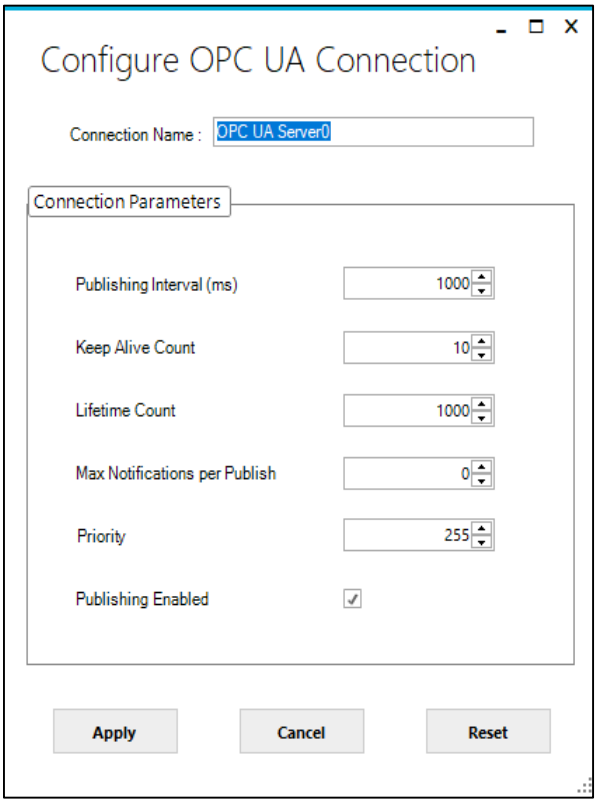


Figure 24: OPC UA Connection Settings

The related settings are detailed in the table below:

Setting	Description	Default Value
Publishing Interval	This interval defines the cyclic rate that the subscription is being requested to return notifications to the client. This interval is in milliseconds.	1000 ms

Keep Alive Count	This setting defines the number of consecutive publishing cycles during which there have been no notifications to report to the client. When the maximum keep-alive count is reached, a publish request is de-queued and used to return a keep alive message. This keep-alive message informs the client that the subscription is still active.	10
Lifetime Count	This setting defines the number of Publishing Intervals without receiving a Publish Request from the client. Once expired, the subscription is then removed by the server.	1000
Max Notifications per Publish	The maximum number of notifications that the client wishes to receive in a single publish response. A value of zero indicates that there is no limit.	0
Priority	This setting indicates the relative priority of the subscription. When more than one subscription needs to send notifications, the server should de-queue a publish request to the subscription with the highest priority number. For subscriptions with equal priority, the server should de-queue publish requests in a round-robin fashion.	255
Publishing Enabled	A Boolean parameter with the following values: • True: publishing is enabled for the subscription. • False: publishing is disabled for the subscription.	True

Table 3: OPC UA Connection Settings

If the OPC UA connection is edited, you need to restart the mapping service, which contains this OPC UA connection as a data source for the changes to take effect.

3.4. Change User Identity

You can change the user identity of your OPC UA session by clicking the blue user icon of a specific row in the grid ( ).
The following dialog screen will be prompted:

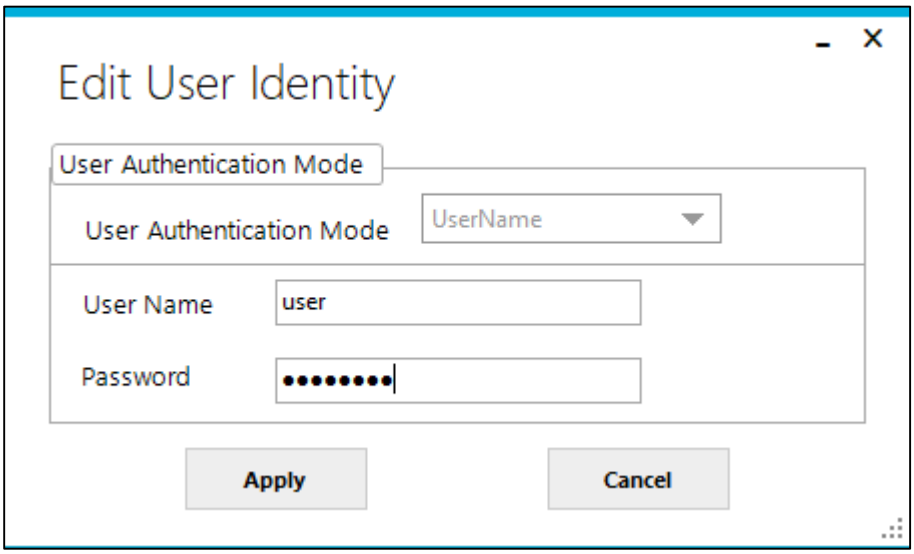


Figure 25: Change User Identity

3.5. Remove an OPC UA Connection

You can remove an OPC UA Connection by clicking the red remove icon of a specific row in the grid ( ) .

Note that you will not be able to remove the connection if it is configured as a data source in a mapping.

4. IoT Hub Agent Management

In this section, we will detail the procedures of creating, editing and removing an IoT HUB agent.

4.1. Destinations Tree View

In this tree view, you will find your configured IoT HUB agents.

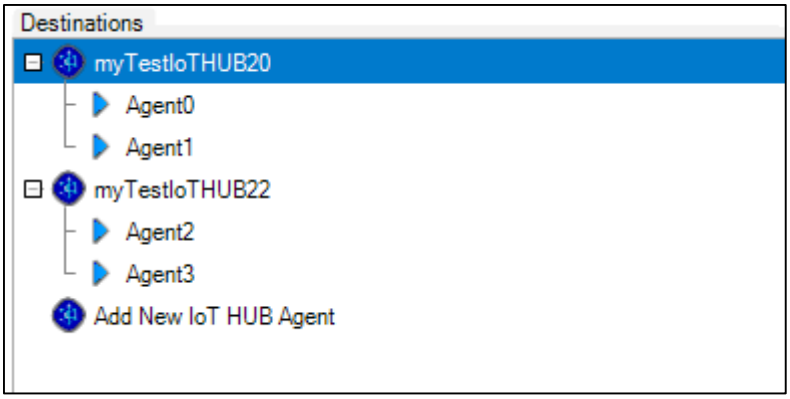


Figure 26: Destinations Tree View

You can create new agents by clicking the **Add new IoT HUB agent** button.

4.2. Add New Publisher Agent

After clicking the **Add new IoT HUB agent** button, the following dialog screen will appear:

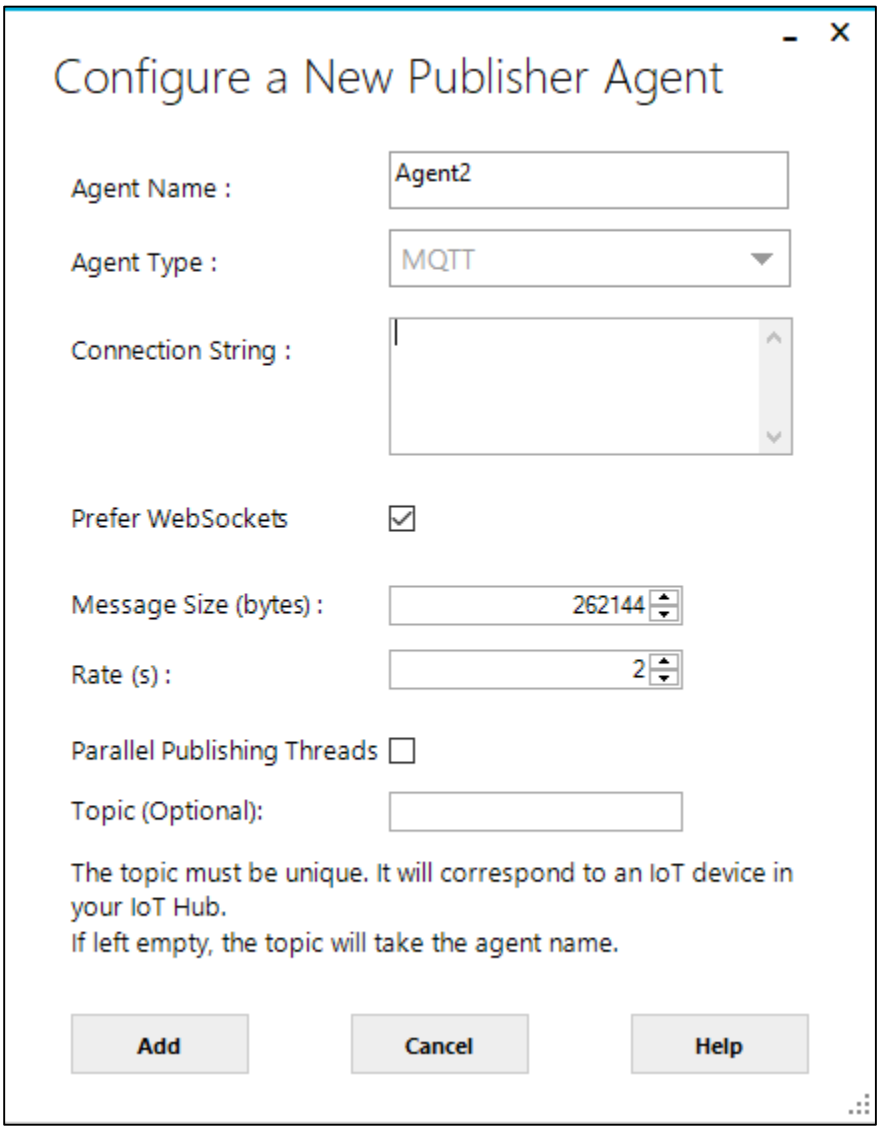


Figure 27: IoT HUB Agent Creation

You can retrieve your IoT HUB connection string as follows:

- Go to your **IoT HUB** page from the **Azure Portal.**
- Click the **Shared access policies** tab (In the side bar) and then choose the **iothubowner** policy.
- A side panel will appear. Copy the **connection string-primary key (Third field)** and paste it in the connection string field of your Publisher Agent Creation form.

Creating an agent in the IIoT Gateway will result in creating an IoT device in your Azure portal. The parameters are detailed in the following table:

Setting	Description	Default Value
Connection String	The connection string is used for authentication.	None
Agent Type	The protocol used to establish secure communication channel with the IoT HUB. The communication protocol can be MQTT, AMQP or REST.	MQTT
Message Size	This setting defines the maximum size of an IoT HUB message. This field has a maximum of 256KB (262144 bytes) and a minimum of zero. If the message size is set to zero, it will be set to the maximum value (256KB).	262144 bytes
Prefer WebSockets	The standard AMQP protocol uses port 5671, and MQTT listens on port 8883. Use of these ports could be restricted in your network configuration. In this case, check the Prefer WebSockets option to use MQTT over WebSockets or AMQP over WebSockets.	True
Rate	This setting defines the interval between two consecutive send attempts. However, if the maximum message size is reached, the message is sent without waiting.	10 s
Parallel publishing threads	This feature can be activated for big address spaces (more than 20000 tags). This will allow the IIoT Gateway to raise its output speed. It is recommended to this feature only if the values publish order is not important.	False
Topic	The topic corresponds to the IoT device name found in your IoT HUB. It must be unique.	None

Table 4: IoT HUB Agent Settings

The message size property value should be relative to the number of OPC UA monitored items. For large number of monitored items, batching will improve the publishing process performance. With a small number of monitored items, waiting for the message size to be reached will, however, introduce some latency. In this case, we recommend decreasing the publishing rate.

To manage your configured IoT HUB Agents, click the **Destinations** Tab in the side navigation bar.
The following figure presents the destinations tab interface:

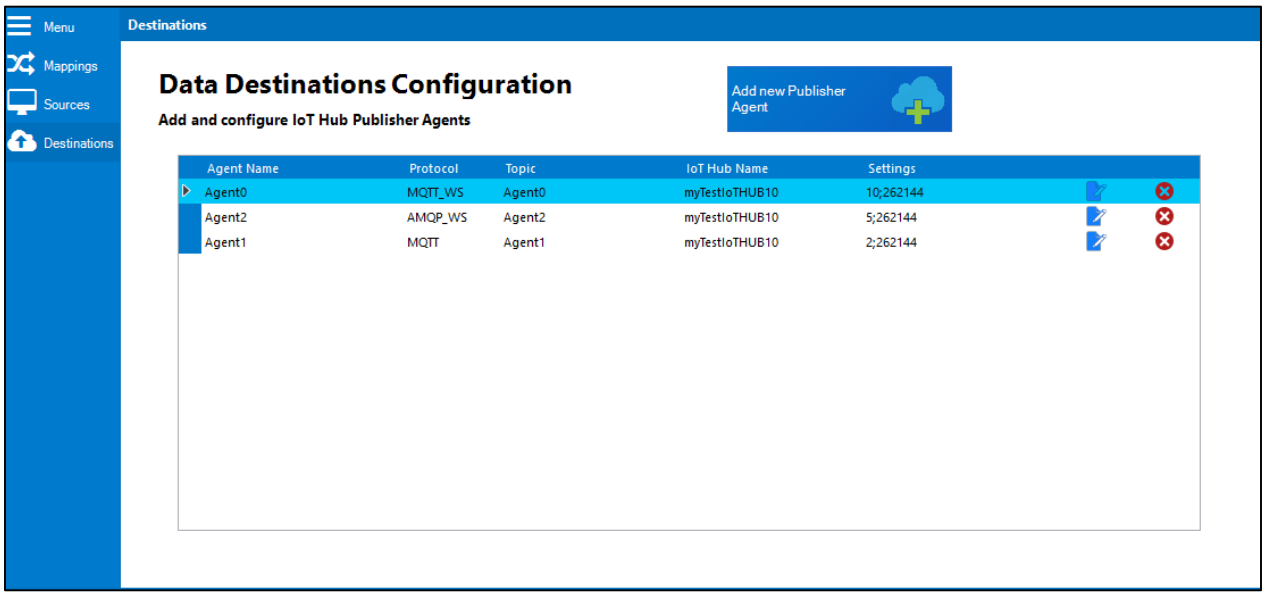


Figure 28: IoT HUB Agents Management View

4.3. Remove Agent

You can remove an IoT HUB Agent by clicking the red remove icon of a specific row in the agents grid ( ) . The following dialog screen will be prompted:

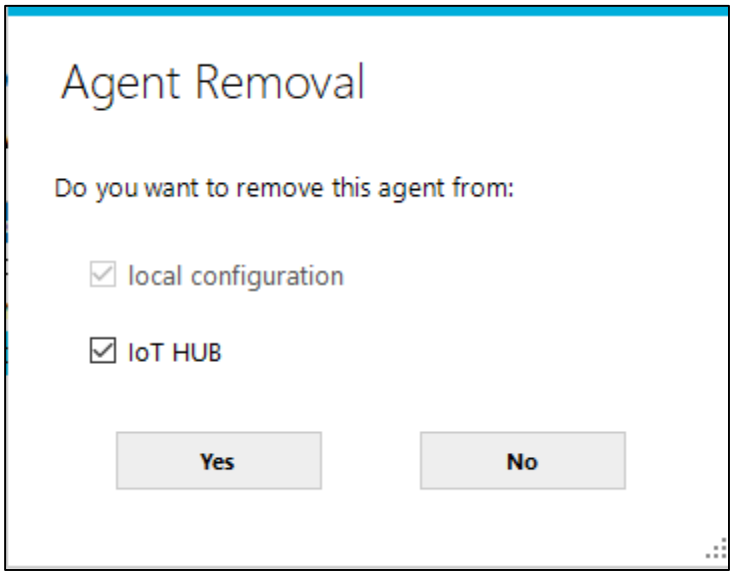


Figure 29: IoT HUB Agent Removal

You will have the choice to remove the corresponding IoT device from his IoT HUB or to keep it.

The agent cannot be removed if it is configured as a data destination in a mapping.

4.4. Edit Agent Settings

You can edit the IoT HUB agent settings by clicking on the blue edit icon of a specific row in the grid ( ) .

You can change the message size and the rate. You can also enable or disable the parallel publishing feature as shown in the figure below.

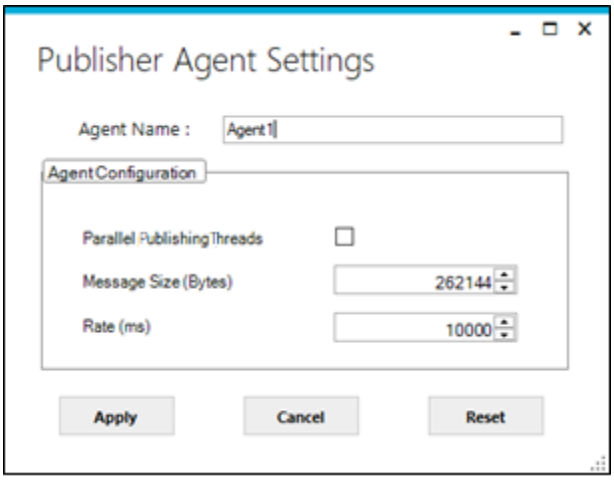


Figure 30: IoT HUB Agent Settings

Make sure to restart the publishing process after editing the publisher agent.

5. OPC UA to Azure IoT Hub Mapping Management

5.1. Configure Mapping

The IIoT Gateway provides an easy way to configure a mapping between a server address space node and an IoT Hub agent. You can configure a mapping by choosing one of the options below:

- Drag an OPC UA Server address space node and drop it on an IoT Hub agent node.
- Drag an OPC UA Server address space node and drop it on the mapping grid. You will be prompted to configure the corresponding IoT HUB Agent.
- Drag an IoT Hub Agent and drop it on the mapping grid. You will be prompted to configure the corresponding OPC UA Server.

- Select an OPC UA address space node and an agent and click the **mapping** button as illustrated in the figure below:

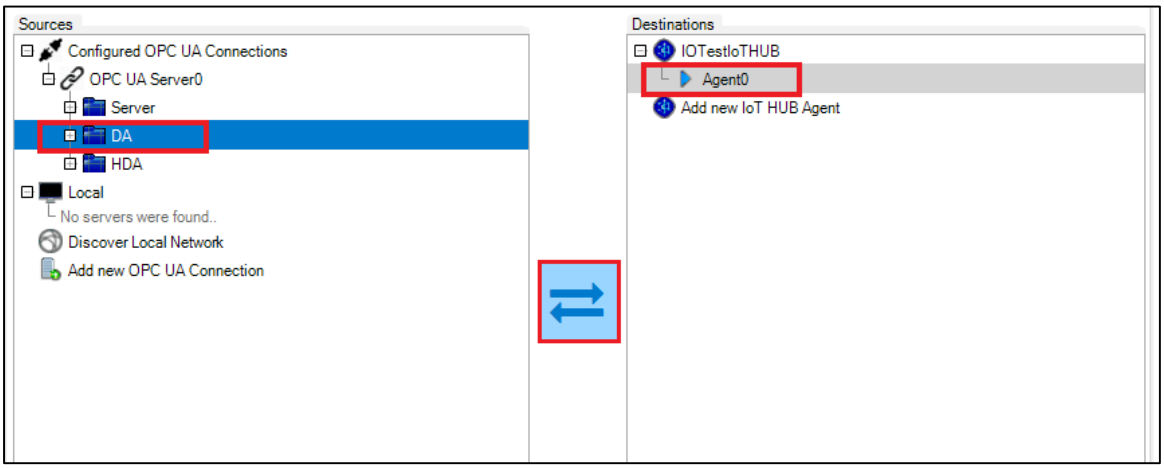


Figure 31: Configuring A New Mapping

Before terminating the mapping configuration, you will be asked whether to send Alarms & Events data along with real time data to the IoT Hub or not.

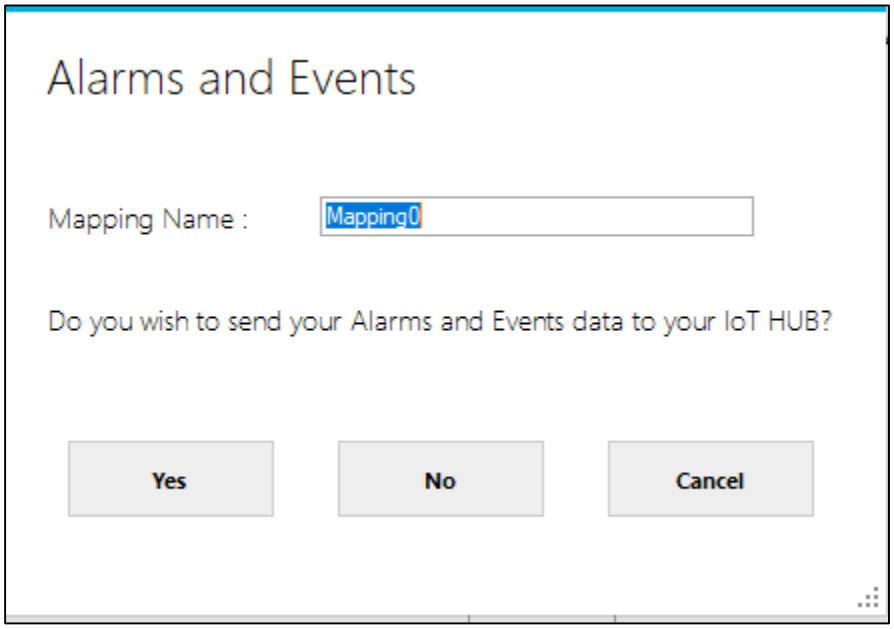


Figure 32: Alarms & Events

The IIoT Gateway will browse all the children tags of the dragged address space node and create a subscription to receive their data changes.

The IIoT Gateway will listen to events emitted by the server dragged address space node.

5.2. Mappings Grid

This grid contains your configured mappings and the status of their corresponding publishing process. You can manage your mappings by clicking the **edit** or **remove** buttons of a specific row in the grid.

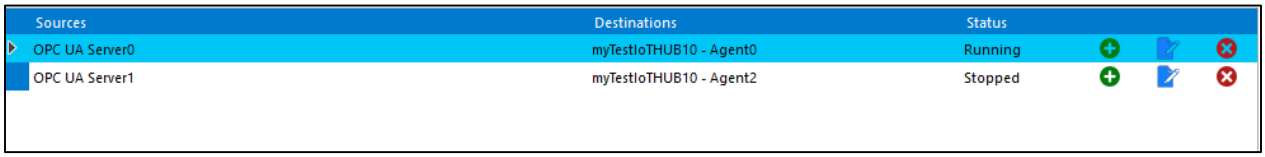


Figure 33: Mappings Grid

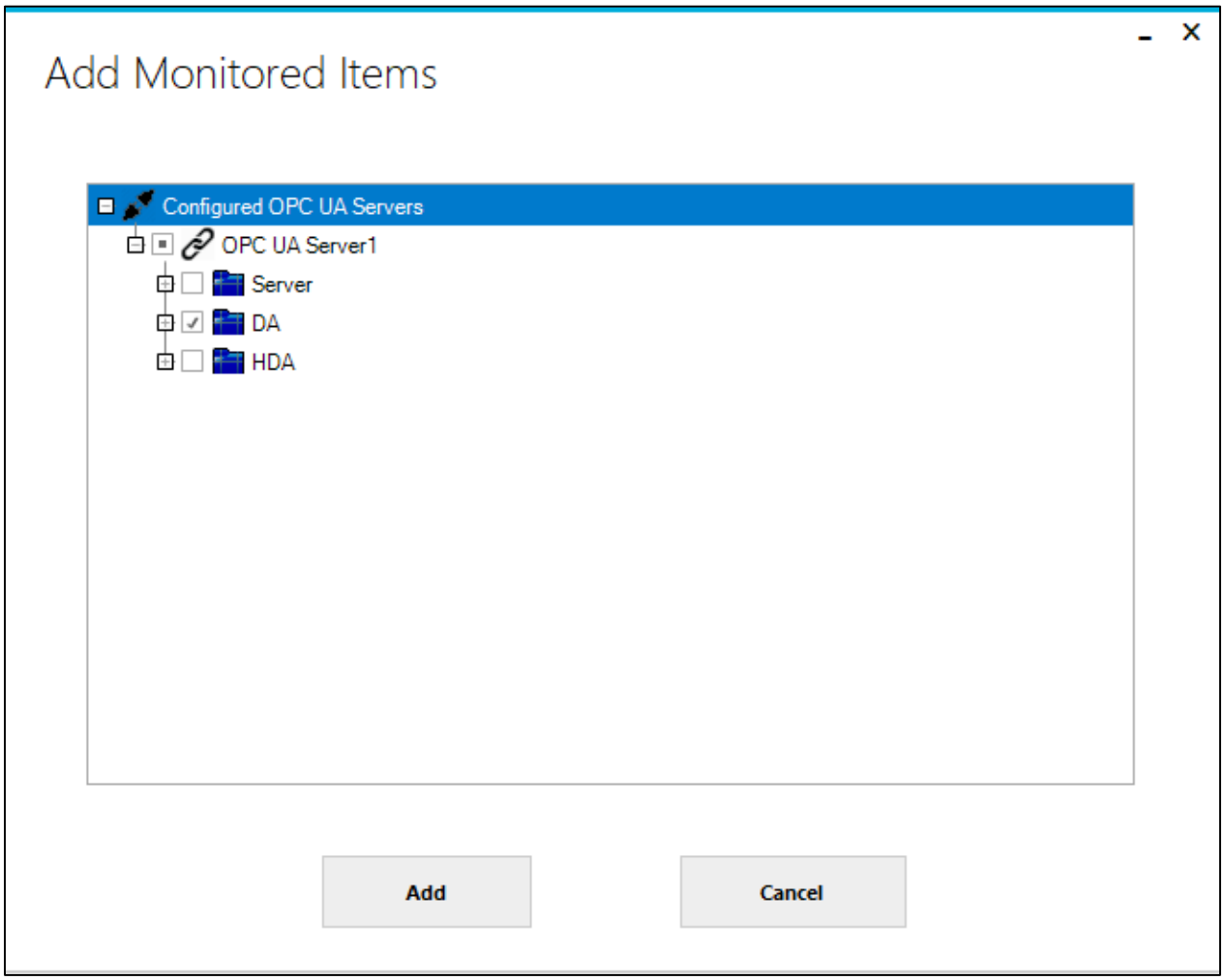
5.3. Remove Mapping

You can remove a configured mapping by clicking the red **Remove** icon of a specific row in the grid ( ).
Removing a mapping will result in uninstalling the corresponding publisher service and deleting its files.

A mapping cannot be removed while it is running.

5.4. Add Monitored Items

You can add new monitored items to the mapping by clicking the green **Add** icon of a specific row in the grid ( ).
The following dialog screen will be prompted and you can check the items that you want to monitor:



Checking an address space folder will result in monitoring all of its children nodes.

You can also add new monitored items using the drag & drop feature.

5.5. Edit Mapping Settings

You can edit a configured mapping by clicking on the blue **Edit** icon in a specific grid row. ( ) This feature allows you to select the OPC UA message attributes that you wish to publish to your IoT Hub.

The following figure presents the attribute selection screen for OPC UA Data Access messages:

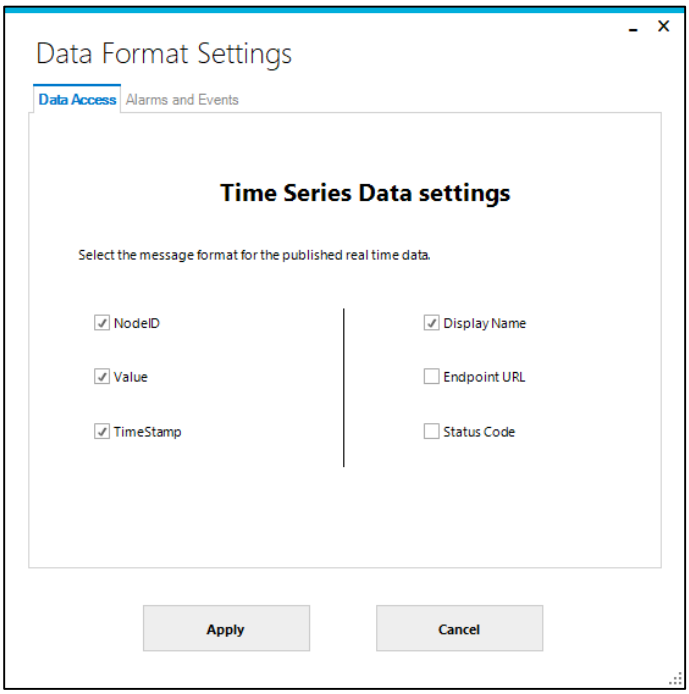


Figure 34: DA Message Attributes Selection

Make sure to restart the publishing process after editing the mapping.

5.6. Start Publishing Service

After configuring the data sources and destinations, you can start sending your DA and AE data to your IoT Hub by selecting a mapping and clicking the **Start One** button available in the Application menu bar. This action will automatically generate a new service executable file and its related configuration files. Once a service is started, the mapping status in the mappings grid will be updated from "Stopped" to "Started".

If the publishing process started correctly, a log message confirming that the subscription to the server was created will be added to the log messages as shown in the figure below.

The subscription creation may take several minutes in case of a big number of monitored items.

You can check the log messages by clicking the **Notifications** button available in the Application menu bar.

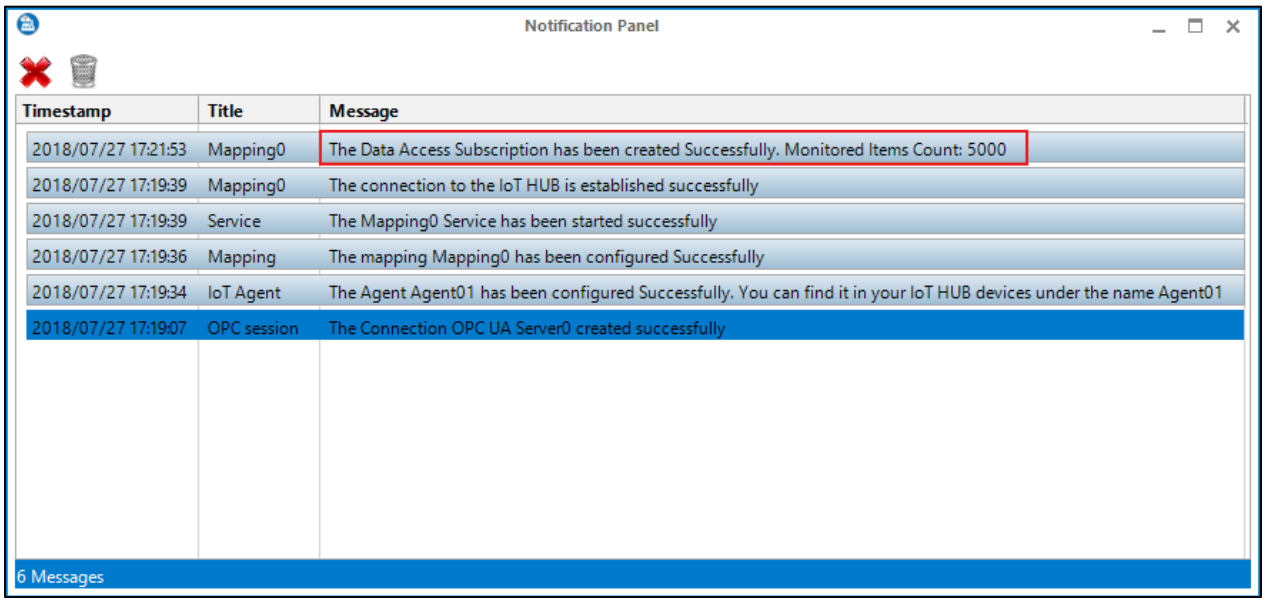


Figure 35: Subscription Establishment Notification Management

5.7. Start All Publishing Services

You can start all your configured publishing services by clicking the **Start All** button.

5.8. Stop Publishing Service

You can stop a publishing service by selecting a mapping in the mappings grid and clicking the **Stop One** button.

5.9. Stop All Publishing Services

You can stop all running publishing services by clicking the **Stop All** button.

6. Automatic Reconnection

The industrial IoT Gateway offers an automatic reconnection feature for both connections to the OPC UA Server and to Azure IoT Hub.

The industrial IoT Gateway automatically detects a connection loss with an OPC UA Server and will start the reconnection process automatically.
This feature is enabled by default but it can be disabled by unchecking the **Enable Automatic Reconnection** checkbox in the **OPC UA General Settings** window. The connection check interval is also editable in the same window.

The industrial IoT Gateway will also detect a connection failure with the IoT Hub and will start the reconnection and backup process. The backup process consists of storing the incoming data from the OPC UA Server into backup files. This process will stop once the connection is re-established successfully and the recovery process will then take place.

The connection status changes are logged in the notification panel as shown in the following figure:

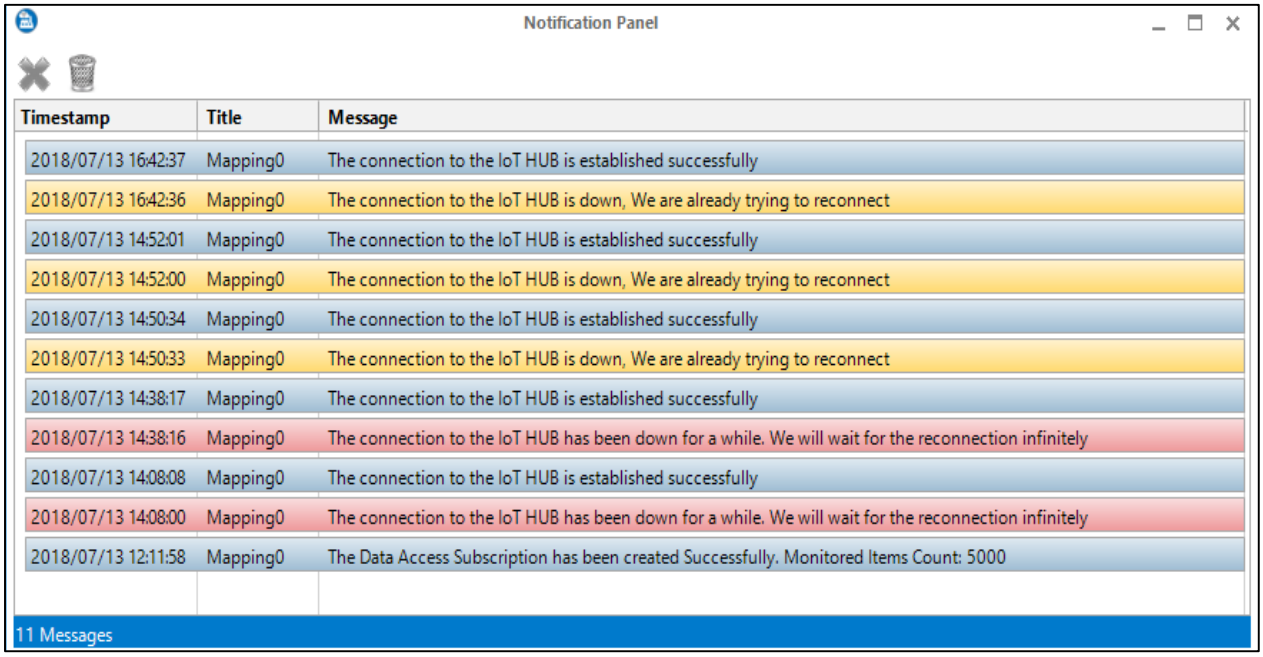


Figure 36: Connection Monitoring

The connection to the IoT Hub has 3 states:

- Connected
- Disconnected and Retrying (yellow notification)
- Disabled (Red notification)

7. Automatic Data Recovery

The automatic recovery process consists of resending OPC UA data after a connection failure with IoT Hub after a reconnection success. This feature ensures the publishing of the backup files messages and deleting those files from the local disk afterwards.

IIOT GATEWAY TRACING CAPABILITIES

The IIoT Gateway has event tracing capabilities and produces 3 types of log files named as follows:

- The `IoTGatewayGUILog.log` that records errors and debugging information generated by the user Interface.
- The `IOTGatewayLicenseServiceLog.log` that records errors and information generated by the Integration Objects' Industrial IoT Gateway license service.
- The `IO Industrial IoT Gateway [Mapping Name] Service.log` that records errors and debugging information generated by the related publishing service.

If difficulties occur with the Industrial IoT Gateway, the log files can be extremely valuable for troubleshooting. Under normal operation, the client logs contain very little information. These log files are generated at start-up under the installation folder.

The Industrial IoT Gateway incorporates 2 configuration files: `Config.ini` and `Services/Config.ini`. These files include several logging parameters. All these parameters have default settings and can be changed by editing the configuration files. The logging parameters are detailed in the following table.

Log Settings	Description	Default Value
AutoAppend	Set to true to continue writing log messages in the existed log file or to false to create a new file.	True
BufferSize	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 messages
FileName	The Industrial IoT Gateway log file name	IoTGatewayGUILog
MaximumFiles	Set to 0 means that log files will be created in an unlimited way.	0
Level	There are five log levels: 1. Control: Logs only control messages. 2. Error: Logs error and control messages. 3. Warning: Logs warning, error and control. 4. Inform: Logs information, warning, error and control messages The higher the log level, the more information is recorded. We recommend using level "Error" for a better performance of the service.	Error

	The other levels are dedicated for troubleshooting purposes.	
AutoSaveTimeOut	The time to wait to read all messages from the buffer and write them to the hard disk. The minimum value is 10s.	10 seconds

Table 5: Log Settings

TROUBLESHOOTING

Case 1: Cannot launch the Industrial IoT Gateway (Evaluation License expired)

If your evaluation license has expired, the License authorization tool will be prompted on application startup as shown below:

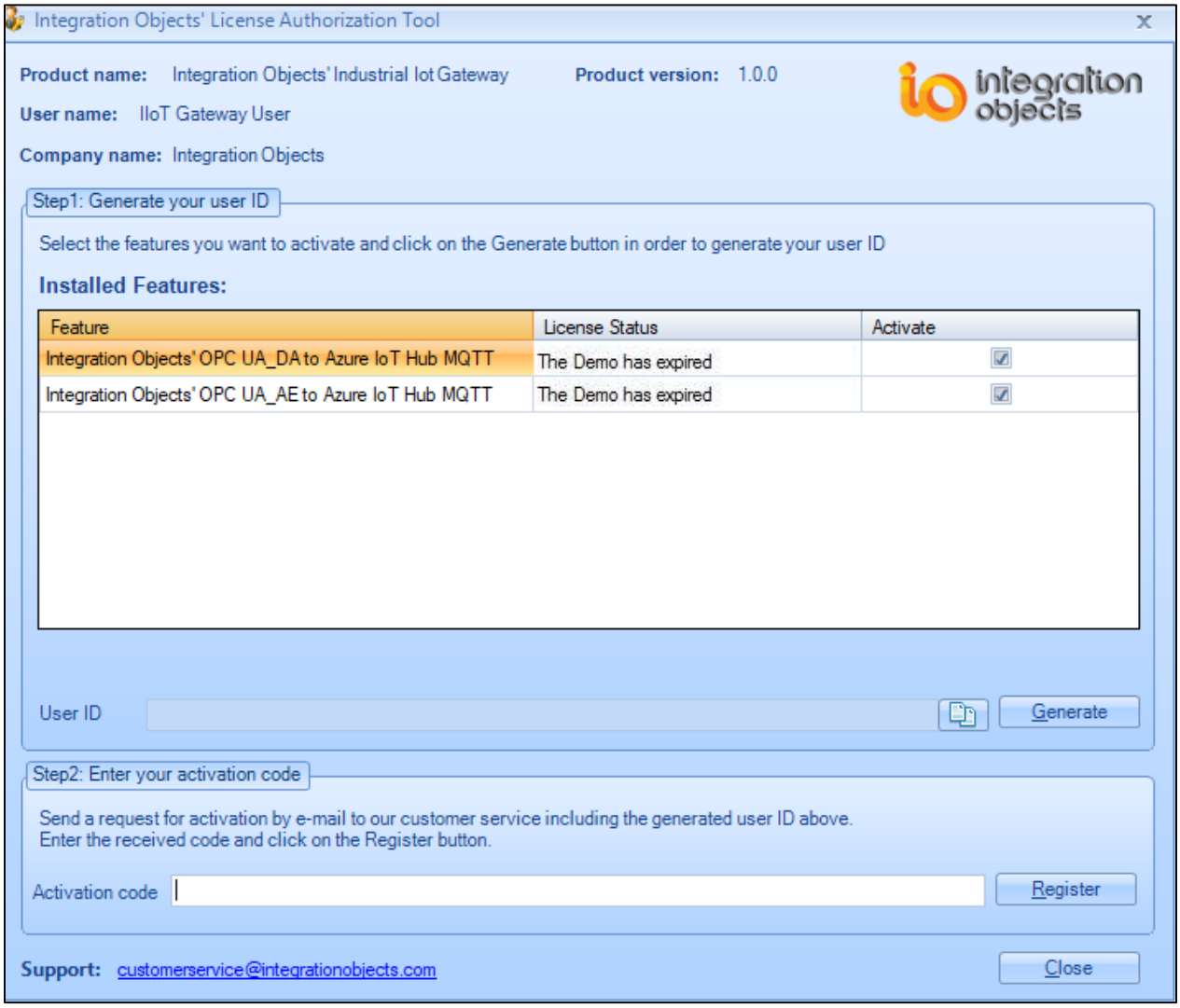


Figure 37: License Authorization

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

1. Run the License Authorization tool using an administrator account.

2. Choose the features you want to activate.
3. Click the **Generate** button.
4. Copy and send the **User ID** to the sales team {sales@integrationobjects.com} along with your license ID, which is the identifier delivered after your product license purchase, so they can generate your activation code.
5. Enter the given **Activation code.**
6. Click the **Register** button.

Case 2: Cannot launch the Industrial IoT Gateway (License service Failure)

On application startup, the IIoT Gateway connects to the license service to identify the user license status. If the license service port is used in your machine by another process, the following error message will be prompted.

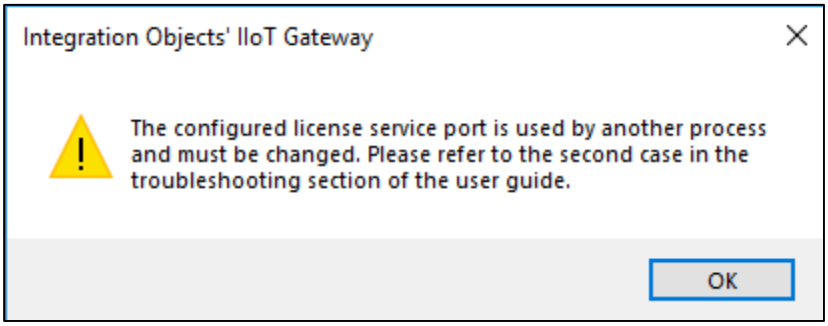


Figure 38: License Service Port Number Unavailable

In this case, you need to:

1. Stop the license service as follows:
   - Open the Windows service manager.
   - Locate the **Integration Objects' Industrial IoT Gateway License Service.**
   - Click on **Stop** the service
2. Change the service port in the `Config.ini` files available under the installation folder as follows:
   - Locate and open the `Config.ini` file
   - Change the property **PortNumber** to indicate a port number that is not used
   - Open the services folder
   - Locate and open the `Config.ini` file under the services folder
   - Change the property **PortNumber** to indicate a port number that is not used
3. Restart the license service
4. Start the IIoT Gateway application

Case 3: Cannot launch the Industrial IoT Gateway (Certificate Loading Failure)

The Industrial IoT Gateway embeds an OPC UA Client application that requires a certificate to connect to OPC UA Servers. If the certificate generator tool is not installed in your machine, the following error message will be prompted.

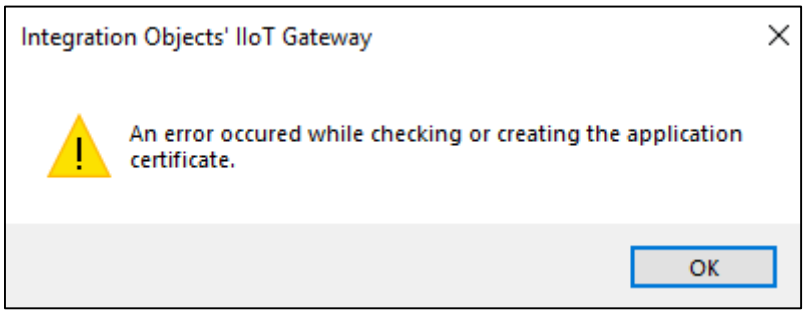


Figure 39: Certificate Loading Failure

The certificate generator tool installation is included in the OPC UA Local discovery server setup available under "Installation Folder\Components".

In this case, you need to check if the OPC UA Local discovery server is installed as follows:

- Open the control panel.
- Open Programs.
- Locate the OPC UA Local Discovery Server 1.03

If not found, you should install the Local Discovery Server (UALDS) available under "Installation Folder\Components".

Case 4: The industrial IoT Gateway fails to load the default configuration

On application start-up, the IIoT Gateway tries to connect to the configured OPC UA Server and to check IoT Hub agents' availability.
If you have defined a default configuration and the application fails to load it, you need to check:

- If the configured OPC UA Servers are still up and running.
- If the internet connection is up and running.

Case 5: I cannot discover OPC UA Servers

If you are not able to discover any OPC UA Server but you can directly connect to an endpoint using its URL, you should install the Local Discovery Server (UALDS) available under "Installation Folder\Components". The UALDS will list the OPC UA servers and wrapper endpoints available on a given computer.

Case 6: I cannot connect to an OPC UA Server

If you cannot connect to your OPC UA Server, you may be facing one of the situations below:

- You are trying to open a session with an unsupported security policy. In this case, you can establish a session with none security, or configure the security modes of the UA server to include the desired security mode.

- The user token policy is not supported by the UA server. In this case, you have to configure the session using the identity settings enabled in your server configuration.
- The username and/or the password are incorrect. In this case, you should set the username/password configured in your server.
- You can connect to an OPC UA Server locally but not remotely. In this case, you should check if the host machine is reachable via the network or if there is an antivirus or a firewall blocking the communication.

Case 7: I cannot create an IoT HUB agent

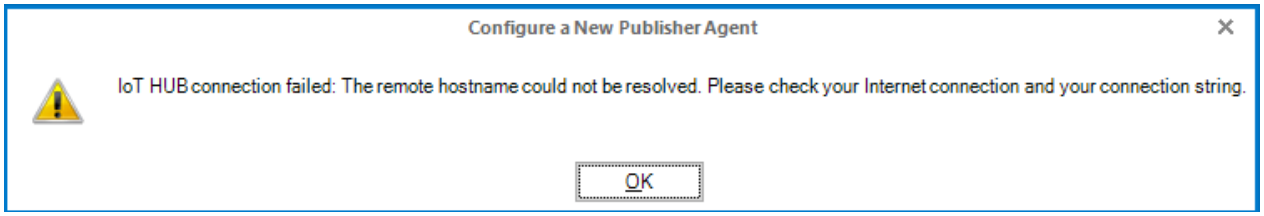


Figure 40: Agent Creation Failed

If the dialog box above is prompted, you should check:

- Your Internet connection.
- Your connection string.
- Your firewall settings. (Allow outbound traffic on port 8883 for MQTT and 5671 for AMQP). Otherwise, use WebSockets or HTTPS.

You can use WebSockets over MQTT or AMQP by checking the Prefer WebSockets option in the add new agent form.

Case 8: Cannot start the Industrial IoT Gateway Service

If you are using an evaluation license, you should check:

- The license is still valid. (Refer to case 1)
- The user has the correct privileges to run the service.
  In order to change the user account used to run the Industrial IoT Gateway service, proceed as follows:

  1. Open Windows service manager.
  2. Right click on **Integration Objects' IIoT Gateway [Your Mapping Name] service** and select **Properties.**
  3. Go to the **Log on** tab.
  4. Check **This account** and enter the user credentials for the service as illustrated in the figure below:

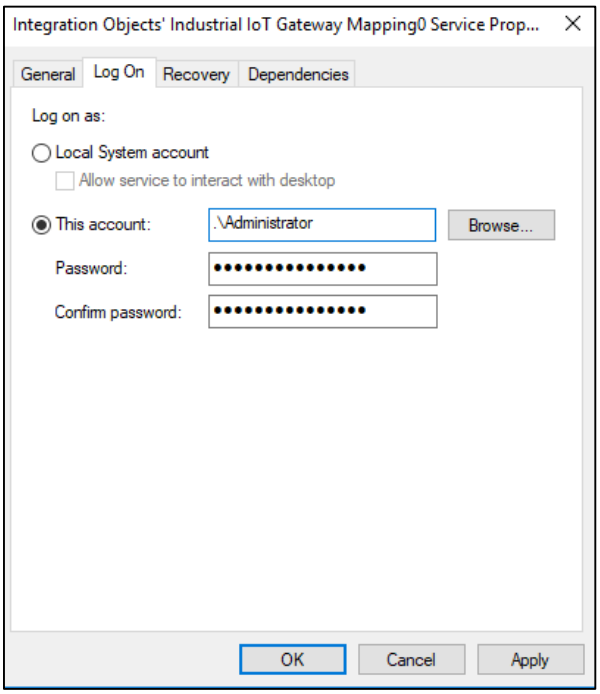


Figure 41: Industrial IoT Gateway Service log on

- The service name is not already used.
  In order to check the installed services, proceed as follows:
  1. Open Windows service manager.
  2. Check services with **Integration Objects' IIoT Gateway [Mapping Name] service** as a name.
  3. If you have an old installed service that is using your service name, you can uninstall it by:
     a. Double click the installed service.
     b. Copy the displayed service Name.
     c. Open a command prompt as administrator.
     d. Execute the following command: **sc delete "[Service Name]"**

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, visit our website www.integrationobjects.com.