Integration Objects'
SNMP to OPC Driver

OPC Server for SNMP
Version 1.2 Rev. 1

USER GUIDE

OPC Compatibility
OPC Data Access 3.00
OPC Data Access 2.05a
OPC Data Access 2.0
OPC Data Access 1.0

OPC Server for SNMP User's Guide Version 1.2 Rev .1
January 2020

TABLE OF CONTENTS

Table of Figures

Table of Tables

PREFACE

About this User Guide

This guide:

- Describes the main features of Integration Objects' OPC Server for SNMP.
- Lists the system requirements for installing and running the OPC Server for SNMP.
- And explains how to use and run this OPC server.

Target Audience

This document is intended for users that are looking for applications providing standard OPC DA (Data Access) connectivity to SNMP enabled devices. Knowledge of the basics of OPC DA specification is assumed. It is also expected that you have some prior knowledge of the SNMP protocol.

Document Conventions

Convention	Description
Bold	Click/selection action required
	Information to be noted
Blue bold italics	Reference to other sections, or to other Integration Objects user guides

Customer Support Services

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

INTRODUCTION

1. Overview

Integration Objects' OPC Server for SNMP is an OPC Server software designed to provide an OPC DA standard interface to SNMP enabled devices such as network routers, switches, firewalls, UPS (Uninterrupted Power Supply) systems, PLCs and other network devices. It establishes connection with one or more SNMP enabled devices via TCP/IP protocol in order to collect data in real-time and provide monitoring features for these devices to OPC compliant client applications.

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

The OPC Server for SNMP helps in reducing the gap between the plant-floor operation and the IT operation as both parties have the information they need to monitor equipment and diagnose problems.

2. System Architecture

This OPC Server reads and updates data from/to devices such as routers, PLCs and firewalls. It can be accessed locally or remotely via DCOM by any OPC DA compliant client.

The following figure illustrates the client/server architecture and demonstrates the interaction between the OPC DA clients, the OPC Server for SNMP and the various SNMP enabled devices.

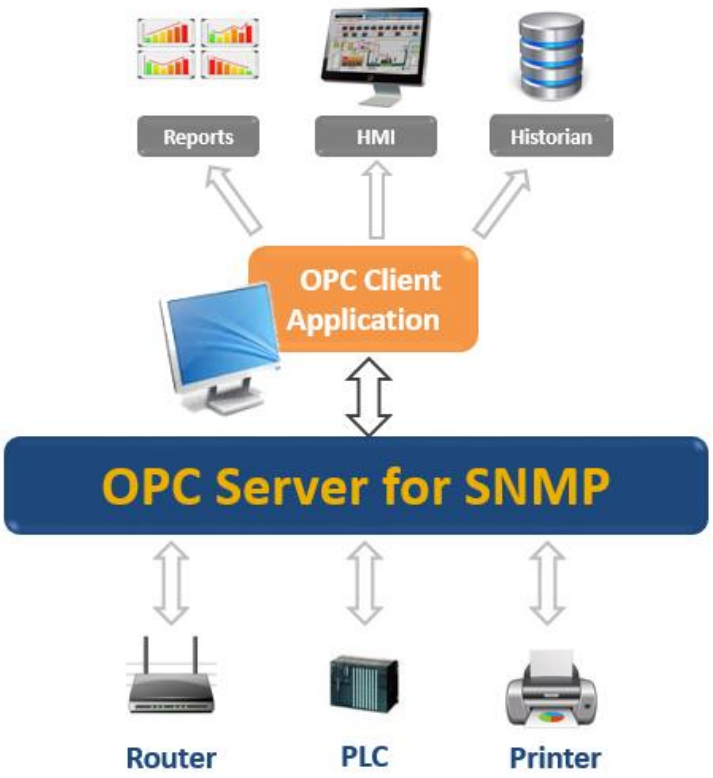

Figure 1: System Architecture

3. Features

The OPC Server for SNMP offers the following features:

- **Devices monitoring**: This server offers the possibility to manage and monitor unlimited number of devices and servers of different vendors using the SNMP protocol.
- **Network discovery**: The server discovers all the devices present within a provided IP range using both SNMP (version1, version2 and version3) and ICMP methods to discover SNMP or non-SNMP enabled devices in the network.
- **Trap recognition**: The user can manage all the agents he wants in order to receive their SNMP traps messages. The server then will process the received messages and expose them in OPC DA tags format.
- **Intuitive user interface**: The end user has access to a configuration tool allowing him to easily set-up the network equipment, machines and properties to be monitored.
- **Support of multiple client connections**: Any compliant OPC DA client can easily connect to the OPC Server and get different tags' values. The server also supports multiple OPC DA client connections.
- **Traceability of events**: The server contains log capabilities to log different events in text files.

The following table lists the supported OPC DA interfaces:

Object	Interface	Supported
OPC DA Server	IUnknown	Yes
	IOPCCommon	Yes
	IOPCServer	Yes
	IConnectionPointContainer	Yes
	IOPCBrowseServerAddressSpace (Optional)	Yes
	IOPCItemProperties	Yes
OPC DA Group	IUnknown	Yes
	IOPCItemMgt	Yes
	IOPCGroupStateMgt	Yes
	IOPCPublicGroupStateMgt (Optional)	Yes
	IOPCSyncIO	Yes
	IOPCAsyncIO	Yes

Table 1: Supported OPC DA Interfaces

4. OPC Compatibility

Integration Objects' OPC Server for SNMP implements OPC Data Access specification version 1.0, 2.05 and 3.0.

5. Operating Systems Compatibility

This OPC Server was successfully installed and executed under the following operating systems:

- Windows XP SP3
- Windows 7
- Windows 8
- Windows 10
- Windows Server 2003 SP2
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019

6. System Requirements

The following table summarizes the minimum requirements to run the OPC Server for SNMP:

	Description
Processor	1 GHz (higher recommended)
RAM	1 Gb (higher recommended)
Disk Space	100 Mb hard disk space for full installation

Table 2: Minimum System Requirements

Also, refer to the next section for more details about installation pre-requisites.

GETTING STARTED

1. Pre-Installation Considerations

In order to properly run the OPC Server for SNMP, the following software components need to be installed on the target system:

- The **OPC core components 3.00** which consists 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.

Make sure there is no firewall or antivirus blocking the application.

2. Installing OPC Server

To install the OPC Server for SNMP:

1. Double-click on the **Integration Objects' OPC Server for SNMP** installation package. The installation welcome dialog box will appear.

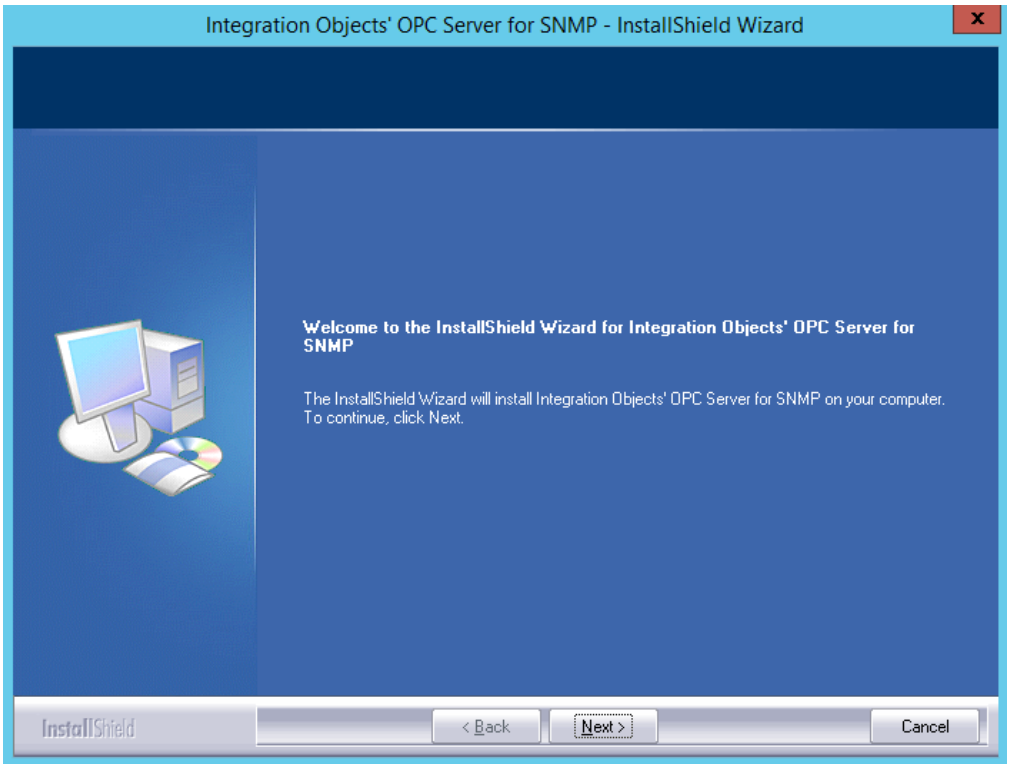

Figure 2: Installation Welcome Dialog

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

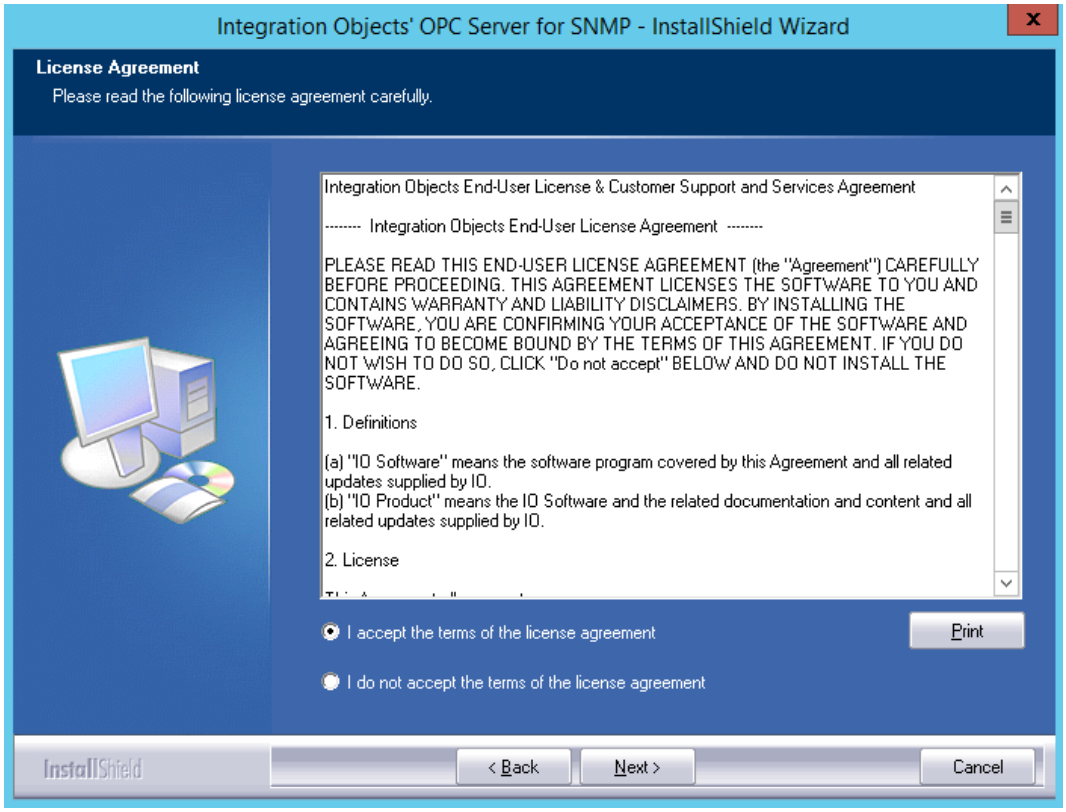

Figure 3: License Agreement Dialog

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. If you choose the first option, the customer information dialog will then appear.

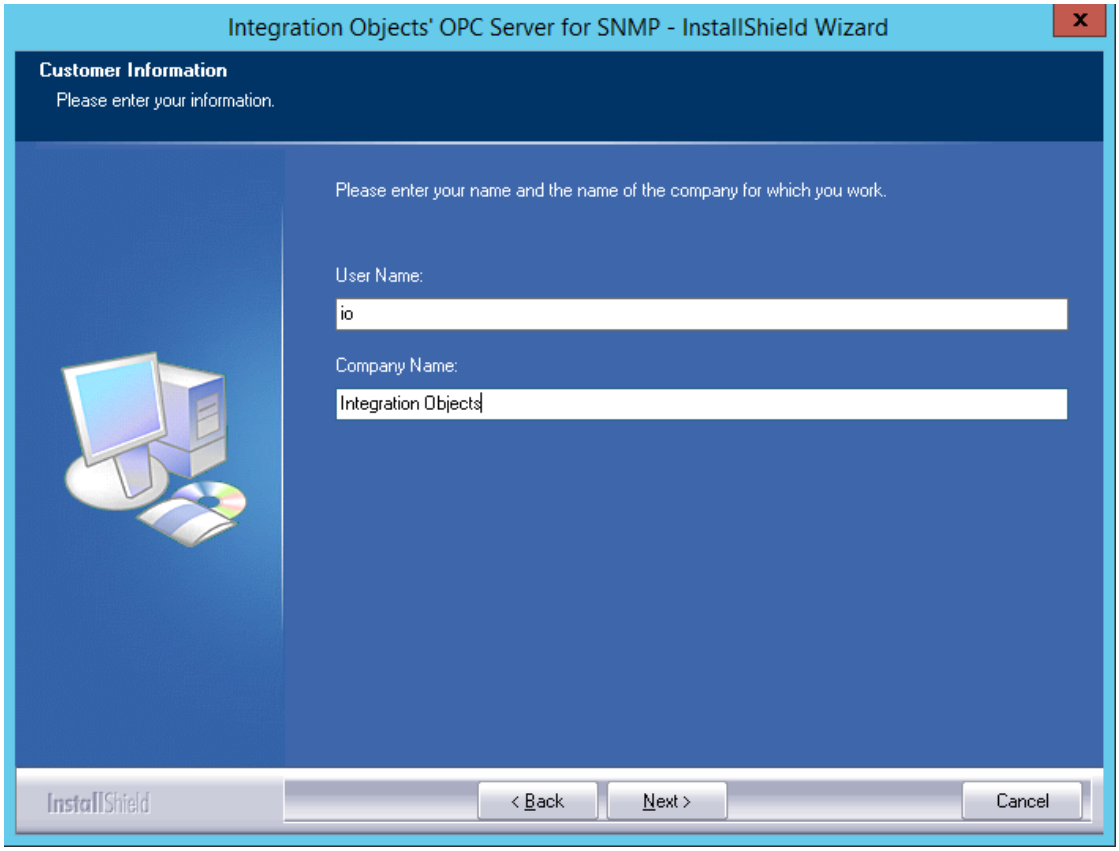

Figure 4: Customer Information Dialog

4. Enter the user name and the company name and then click the **Next** button. The dialog box for selecting the destination folder will be displayed.

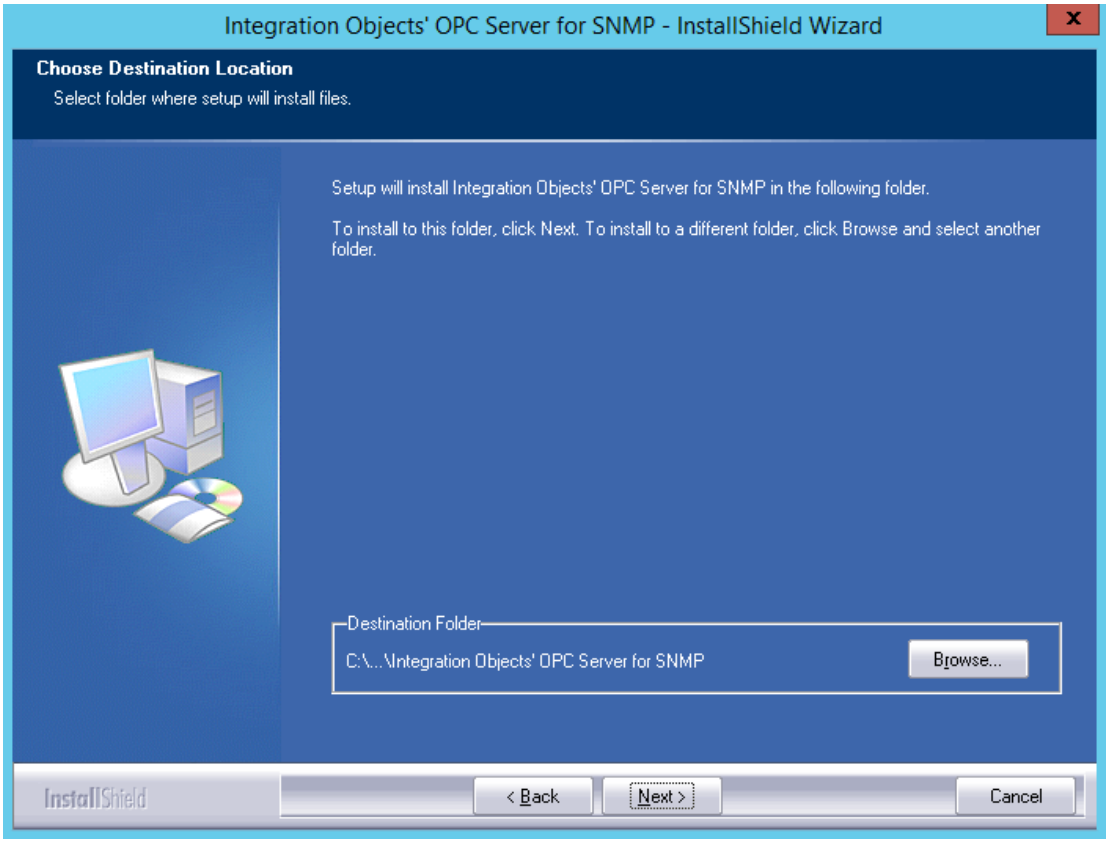

Figure 5: Choose Destination Folder Dialog

5. Click the **Next** button to continue the installation, or the **Browse** button to choose a different destination folder. The installation dialog box will then appear.

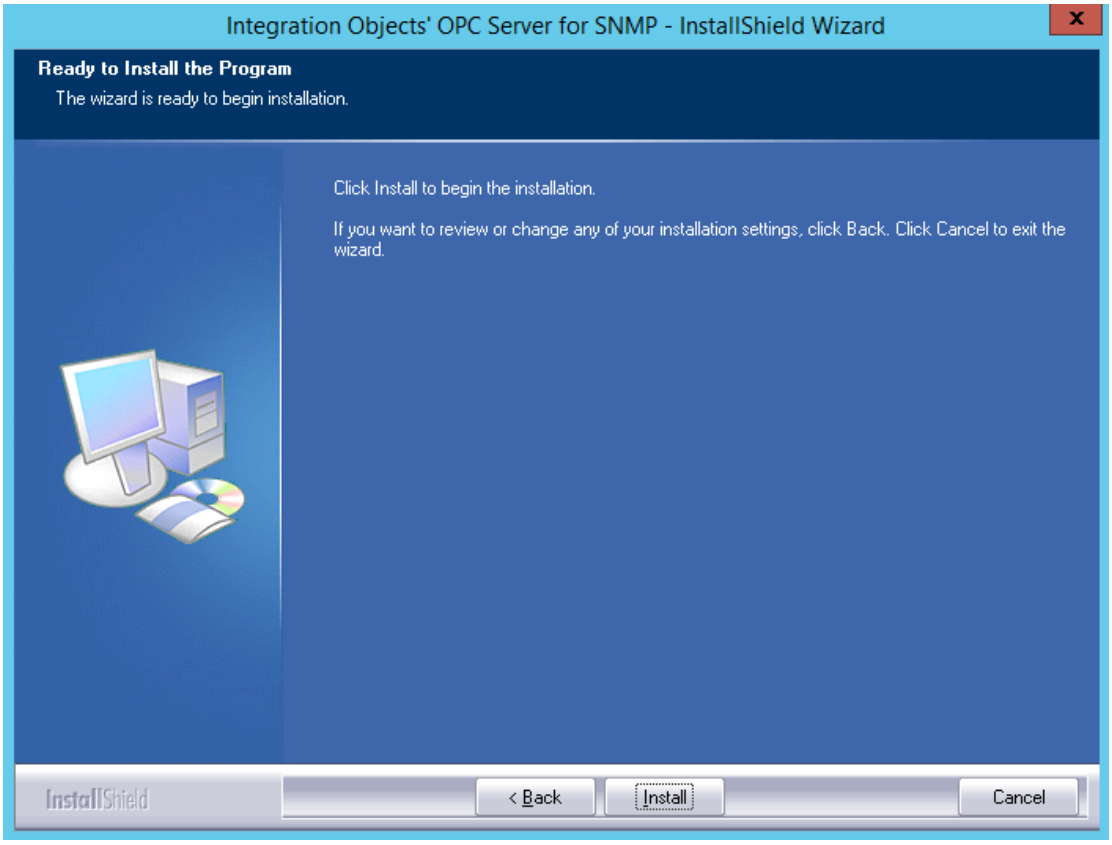

Figure 6: Installation Dialog

6. Click the **Install** button to start installation. The setup will then:
   - Copy the necessary files to the selected target folder,
   - Create shortcut icons to launch the OPC Server for SNMP and license authorization program from the start menu and the desktop,
   - Make an un-installation entry in the Programs and Features in the Control Panel.

7. Click the **Finish** button.

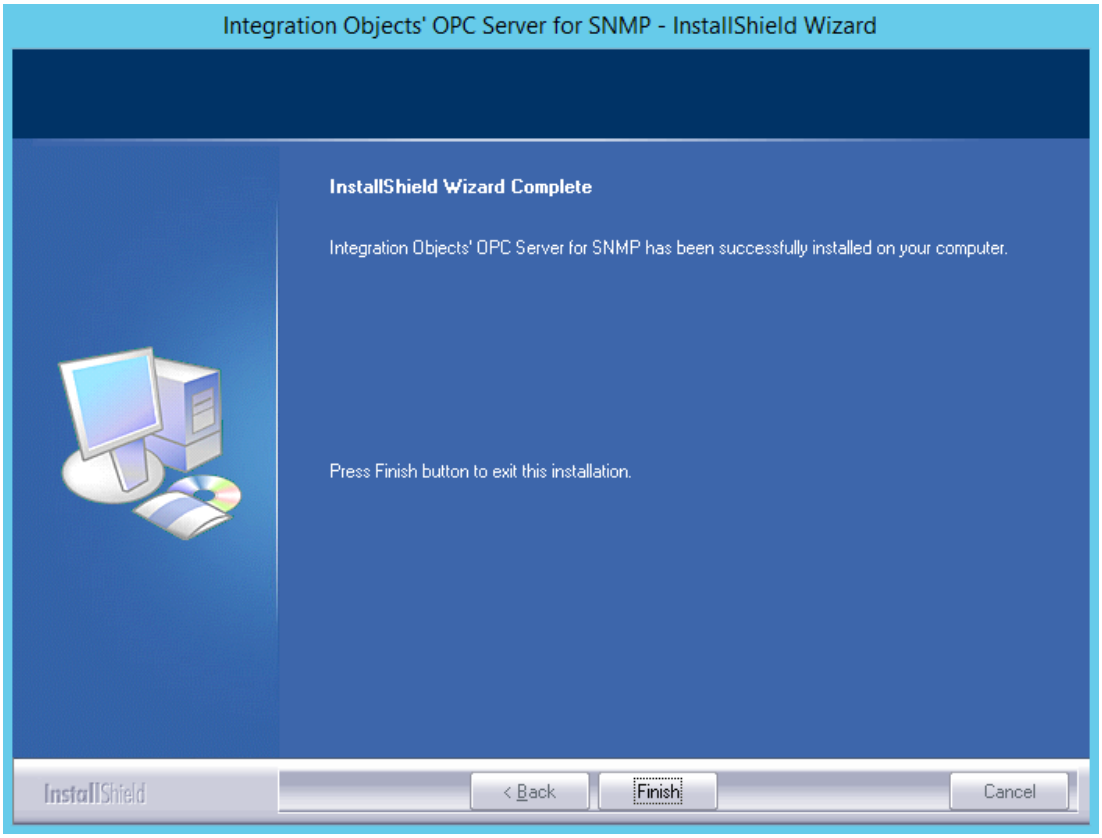

Figure 7: Installation Completed Dialog

3. Starting-up

The OPC Server for SNMP service is started automatically with the host machine restart. It can be started and stopped manually from the Windows services manager. The user interface can be launched from the start menu shortcut.

To do so, click on **Start ➔ Programs ➔ Integration Objects ➔ OPC Server for SNMP**

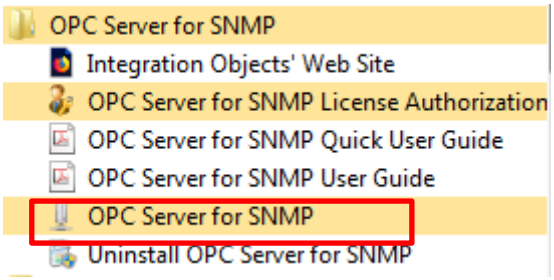

Figure 8: OPC Server for SNMP Start Menu

The server can also be launched automatically when the first OPC DA client connects to it.

4. Server Registration

In compliance with the OPC and COM specifications, the OPC Server for SNMP creates the following registry entries under HKEY_CLASSES_ROOT when installed on the target system. These entries will be removed when the server is uninstalled.

Registry Entry	Description
IntegrationObjects.OPC.SNMP.1	Integration Objects' OPC Server for SNMP; http://www.integrationobjects.com
IntegrationObjects.OPC.SNMP.1\CLSID	{***CLSID***} = {81A0F806-9F39-4776-845E-0AD85AB3306B}
CLSID\{***CLSID***}	Integration Objects' OPC Server for SNMP; http://www.integrationobjects.com
CLSID\{***CLSID***}\AppID	{***CLSID***}
CLSID\{***CLSID***}\ProgID	IntegrationObjects.OPC.SNMP.1

Table 3: OPC Server for SNMP Registry Entries

5. Removing the OPC Server

You can remove the server from your machine by clicking the **Uninstall OPC Server for SNMP** shortcut from the start menu.

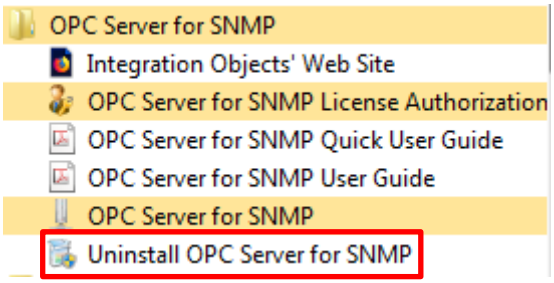

Figure 9: Uninstaller Shortcut

This OPC Server can also be removed manually as follows:

1. Click on the **Start Menu.**
2. Go to **the Control panel.**
3. Click **Programs and Features**.
4. In the **Programs and Features** dialog screen, select "**Integration Objects' OPC Server for SNMP**".
1. Click **Uninstall** then **OK**.

USING OPC SERVER FOR SNMP

In this section, you will find an overview of the OPC Server for SNMP user interface as well as the steps required to configure and use the application.

1. User Interface Overview

Users can configure the OPC Server for SNMP with an intuitive graphical user Interface. The following figure illustrates the main user interface.

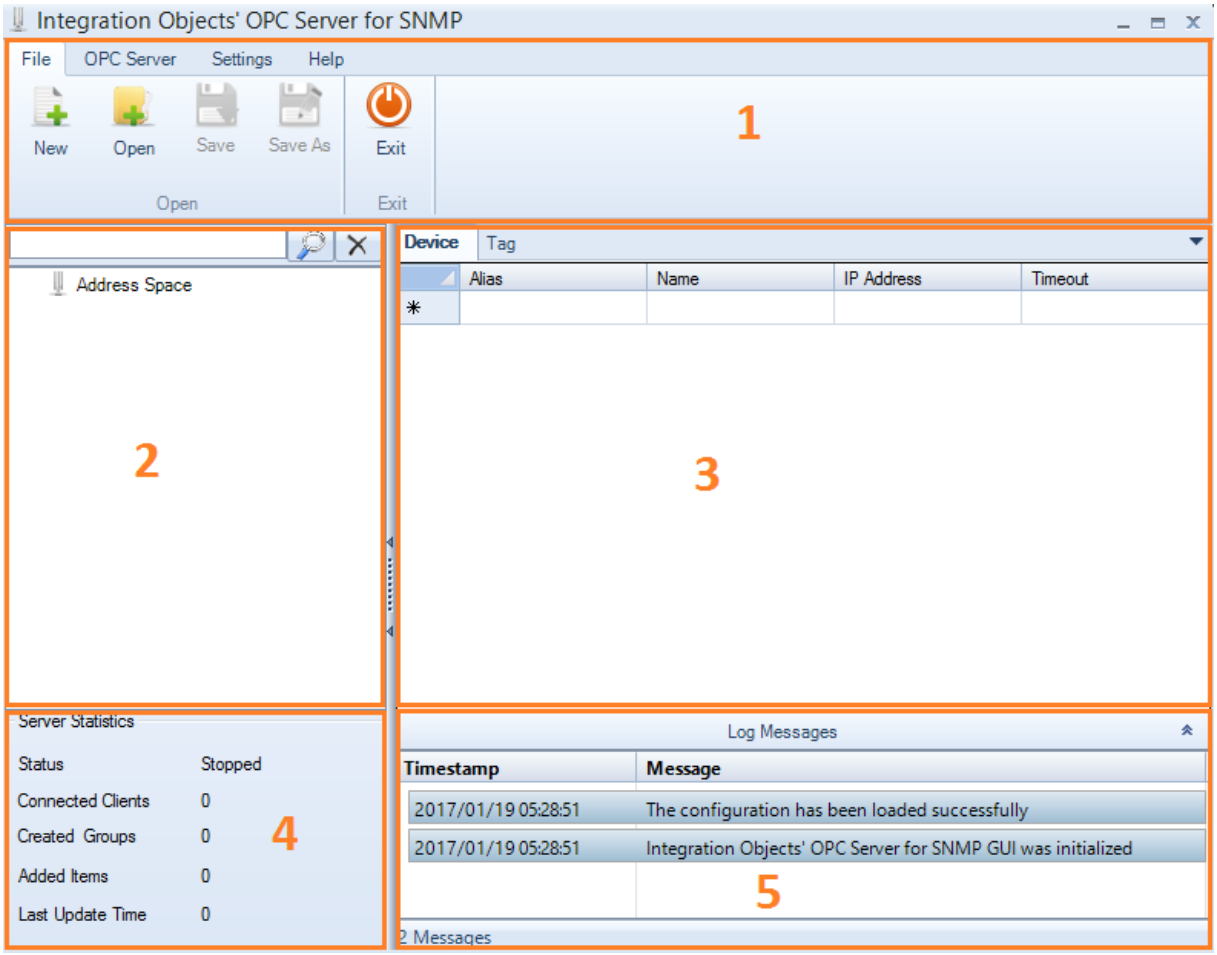

Figure 10: Main User Interface

The main user interface includes four main sections:

- Menu bar (1): This part contains the File menu, the OPC Server menu, the Settings menu and the Help menu. These menus provide access to functions that help the user interact with the application.
- Server address space tree view (2): allows configuring the OPC Server address space. All added devices and tags will be displayed in this tree view.
- Tag & Device data grid (3): The Tag Tab displays the properties of the selected tag and the device tab displays the properties of the selected device in the tree view.
- Server statistics summary (4): displays server status (running or suspended…), the number of connected clients, the number of created groups, the number of created items and the last updated time.
- Log messages (5): displays the different log messages.

2. File Menu

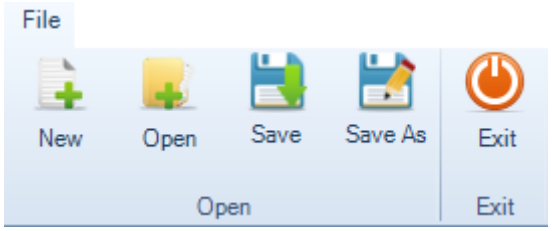

Figure 11: File Menu

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

- Create new configuration by clicking on **New**,
- Open an existing configuration by clicking on **Open** and selecting the appropriate XML configuration file,
- Save your current configuration by clicking on **Save** or **Save As**,
- Close the application by clicking the **Exit** button.

3. OPC Server Menu

The OPC Server is registered automatically during the installation. The end user can also use the OPC Server menu to manually **register** and **unregister** the server.

Make sure to run the OPC Server for SNMP configuration tool as administrator when registering or unregistering the server.

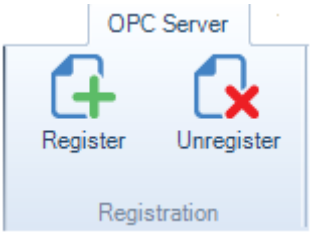

Figure 12: OPC Server Menu

4. Settings Menu

Using the Settings menu, you can:

- **Define** the default configuration that will be loaded automatically when you restart the server.
- **Remove** the default configuration.
- Select the style of the graphical user interface, which is set by default to "**Windows7Blue**".
- Configure the server setting when clicking the **Configure** button.

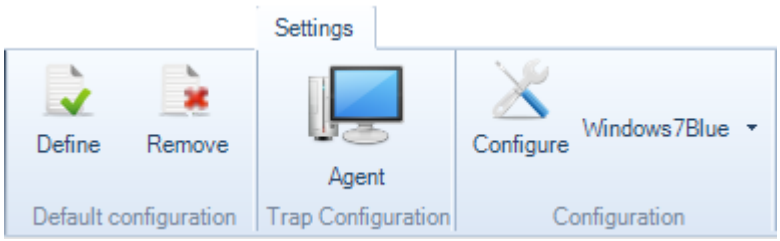

Figure 13: Settings Menu

When the user clicks the **Configure** button, the window below will be prompted:

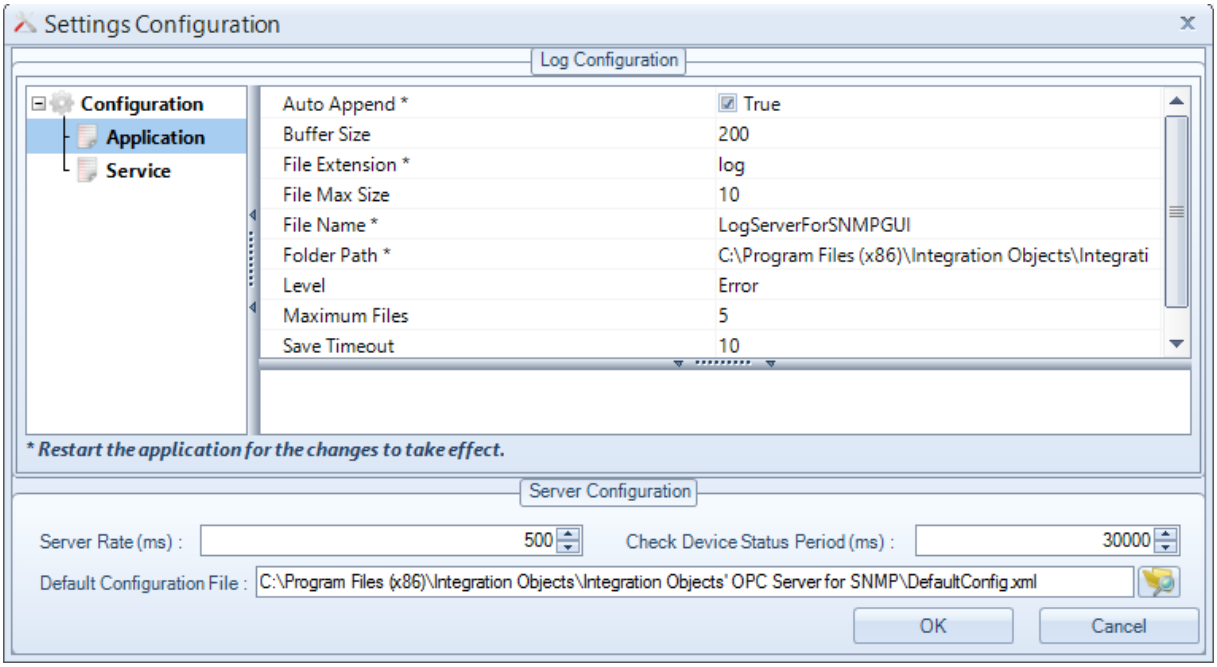

Figure 14: Settings Configuration Window

In this window, you can configure the following parameters:

- For the server configuration, you can update the following parameters:

Parameter	Description	Default Value
Server Rate	The frequency at which the server handles the asynchronous reads/updates	500 milliseconds
Check Device Status Period	The frequency at which the server will check the device connection status	60 000 milliseconds
Default Configuration File	The full path of the server XML configuration file	C:\ProgramFiles(x86)\IntegrationObjects\IntegrationObjects' OPCServerforSNMP\DefaultConfig.xml

Table 4: Server Configuration Parameters

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	200

	runtime memory before launching writes action in the hard disk. It must be greater than 100.	
File extension	The log file extension	log
File max size	The maximum size of the log file (in Mb)	10 Mb
File name	The log file name	• LogServerforSNMPGUI: log file of the configuration user interface • LogServerforSNMPService: log file of the service
Folder path	The application folder path	Installation Folder
Level	The type of log messages to be logged. The value can be Control, Error, Warning, Inform, and Debug.	Error
Maximum files	Maximum number of files	5
Auto save timeout	Time to wait to read all messages from the buffer	10

Table 5: Log Settings

When the user clicks the **Agent** button, the window below will be prompted:

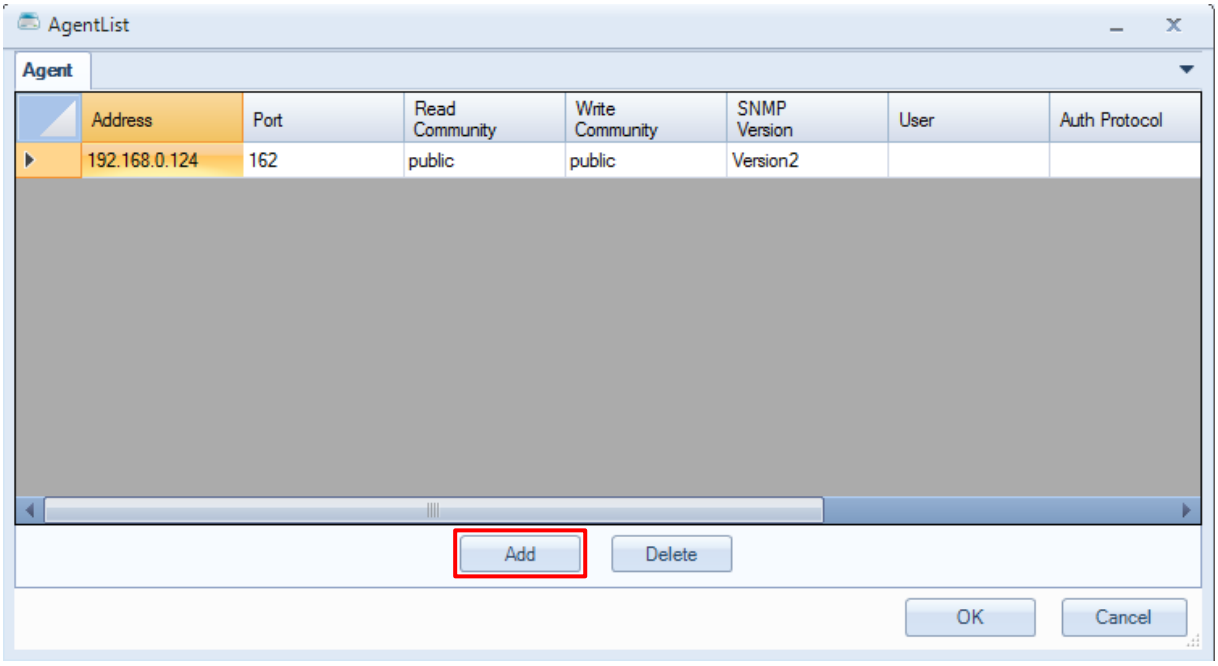

Figure 15: Agent Dialog Box

In the agent dialog box, the user can either add or delete agent (equipment) from the list. The user can only receive trap messages from the agent added to this list.
After clicking on the **Add** button, the next dialog box will be displayed.

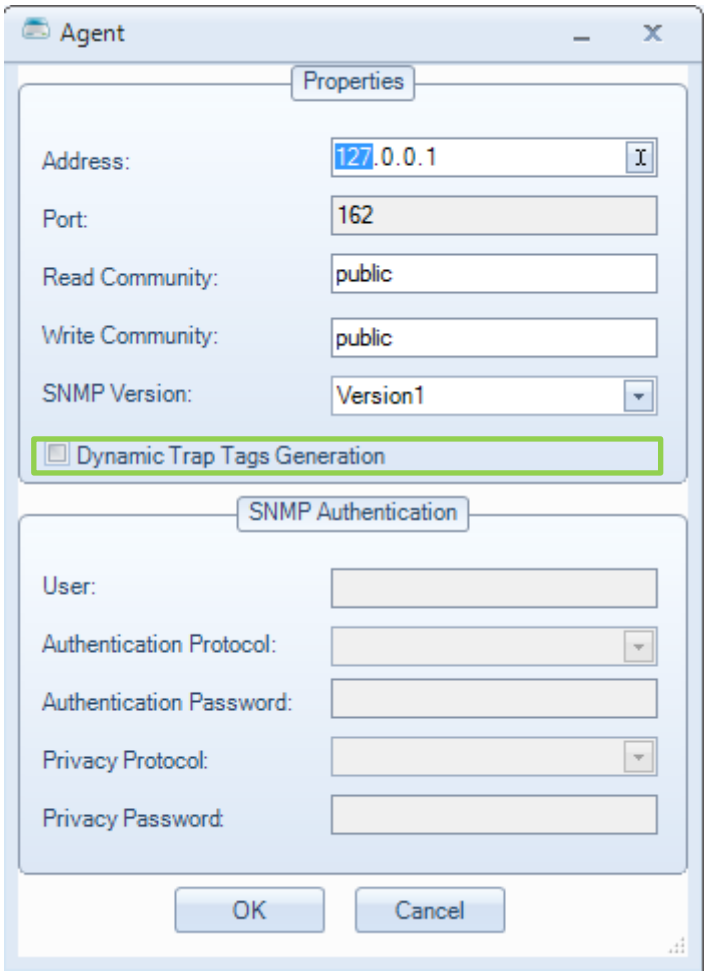

Figure 16: Add Agent Dialog Box

In this window, you can configure the following parameters:

Parameter	Description
Address	The SNMP enabled device IP address.
Port	The server will listen to trap messages that will come through this port.
Connection Timeout	The waiting period for an unresponsive server.
Read community	The SNMP read Community string is a user Id or password that allows access to device's information.

Write community	The SNMP write Community string is a user Id or password that allows access to device's information.
SNMP version	The SNMP version of the device (Version1 or Version2 or Version3).
Dynamic Trap Tags Generation	If checked, all of the variables contained in the trap message are created and added to server address space dynamically. If not checked, the server will only update the value of existing tags.
SNMP Authentication	SNMP version3 requires user credentials to be passed on within each SNMP request. Three attributes are associated to this parameter: • User: user name • Authentication Password: private key name if the agent requires SHA or MD5 authentication. • Authentication Protocol: MD5 or SHA. • Privacy Password: a unique password if the agent requires privacy (DES or AES) protection. • Privacy Protocol: DES or AES.

Table 6: Added Agent Parameters

5. Address Space Configuration

The OPC Server address space can be configured from the tree view at the left side of the main user interface.

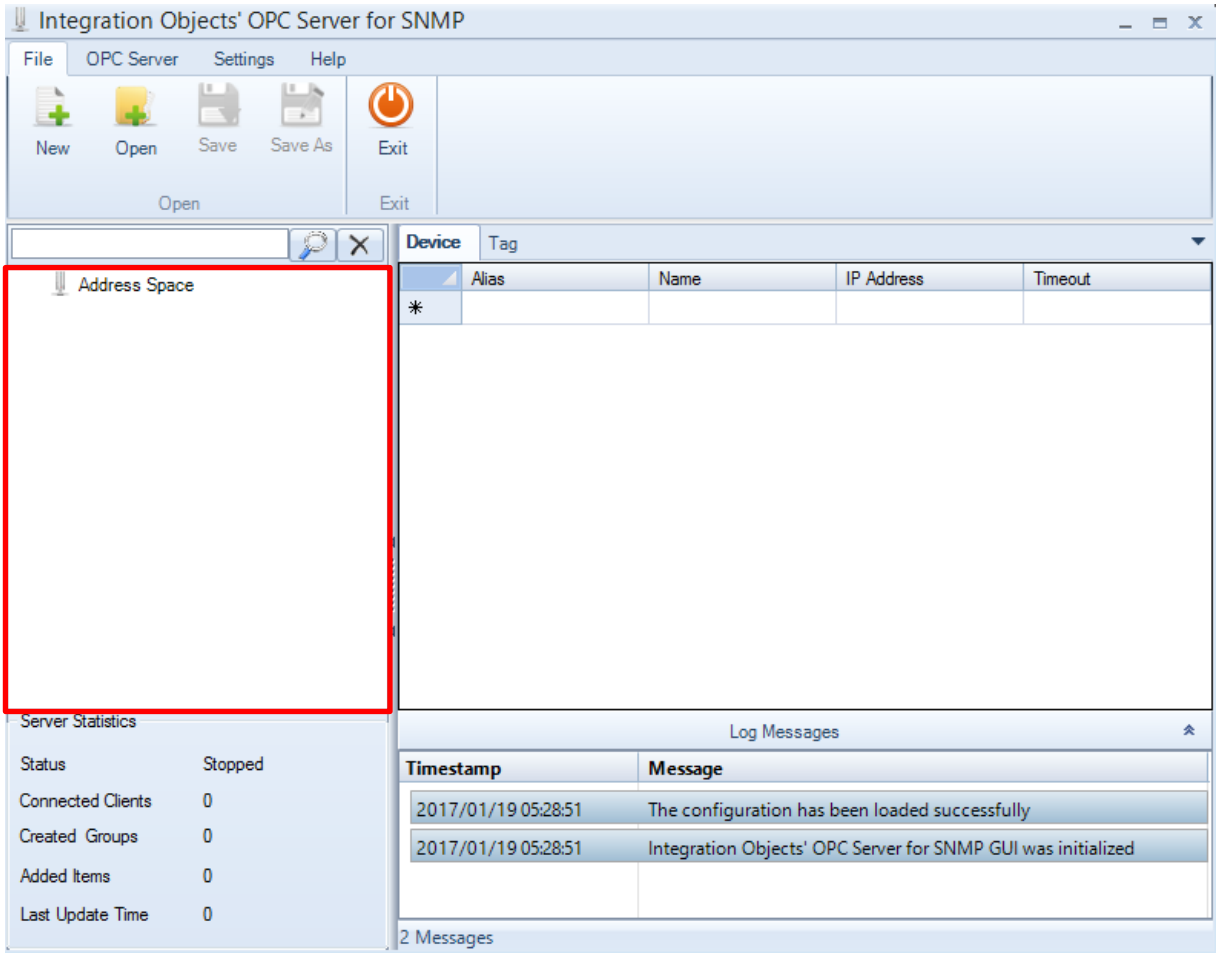

Figure 17: OPC Server SNMP Address Space Tree View

The sections below describe how to add, edit and delete SNMP devices and tags.

5.1. ADD DEVICE

Right click on the **Address Space** node, select **Add Device** from the displayed menu as illustrated below.

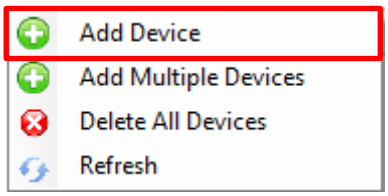

Figure 18: New Device Dialog

Then, the New Device dialog will be displayed as shown below:

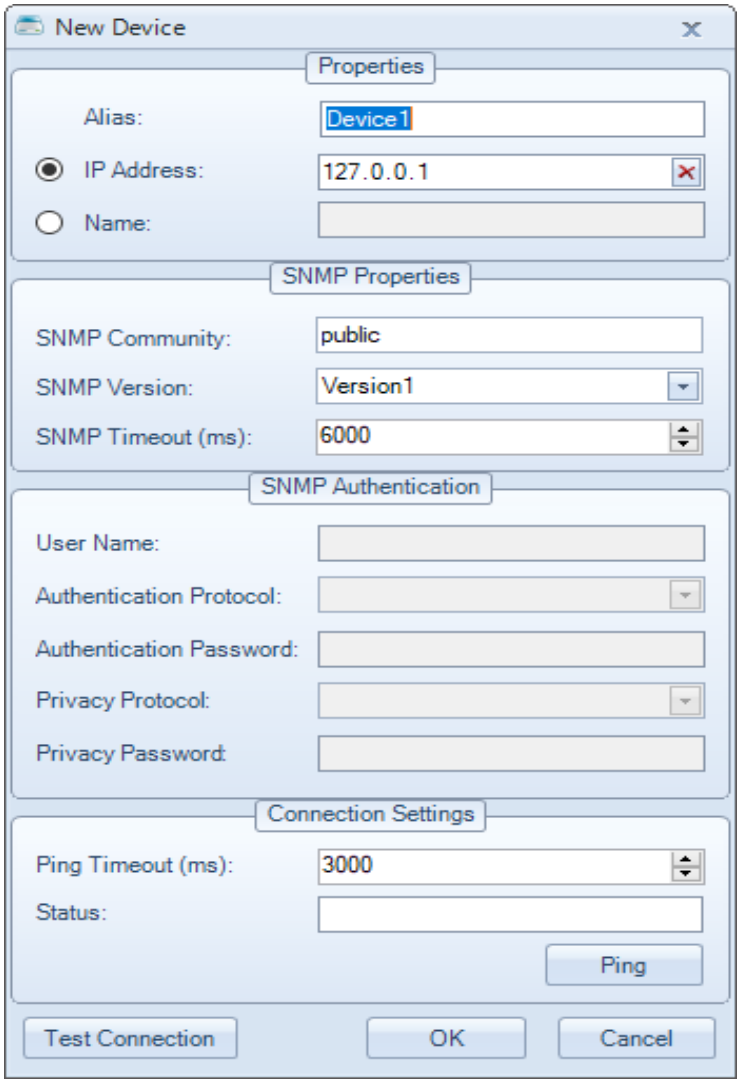

Figure 19: New Device Dialog

The table below summarizes the parameters to configure your SNMP device:

Parameter	Description
Alias	The device name to be used to manipulate the device
IP Address	The SNMP enabled device IP address
Name	The device name in the network
Ping Timeout	The time to wait before flagging the device as unresponsive to ICMP request
SNMP community	The SNMP Community string is a user Id or password that allows access to device's statistics

SNMP version	The SNMP version of the device (Version1 or Version2 or Version3)
SNMP Timeout	The time to wait before flagging the SNMP enabled device as unresponsive.
SNMP Authentication	SNMP version3 requires user credentials to be passed on within each SNMP request. Three attributes are associated to this parameter: • Use name: user name • Authentication Password: private key name if the agent requires SHA or MD5 authentication. • Authentication Protocol: MD5 or SHA. • Privacy Password: a unique password if the agent requires privacy (DES or AES) protection. • Privacy Protocol: DES or AES.

Table 7: Device Parameters

You can ping the device by clicking on the **Ping** button. The status of the connection to the device (success, destination unreachable, etc.) will be displayed in the filed Status.

You can test the connection of the device by clicking on the **Test Connection** button. The connection status will be displayed in a message box.

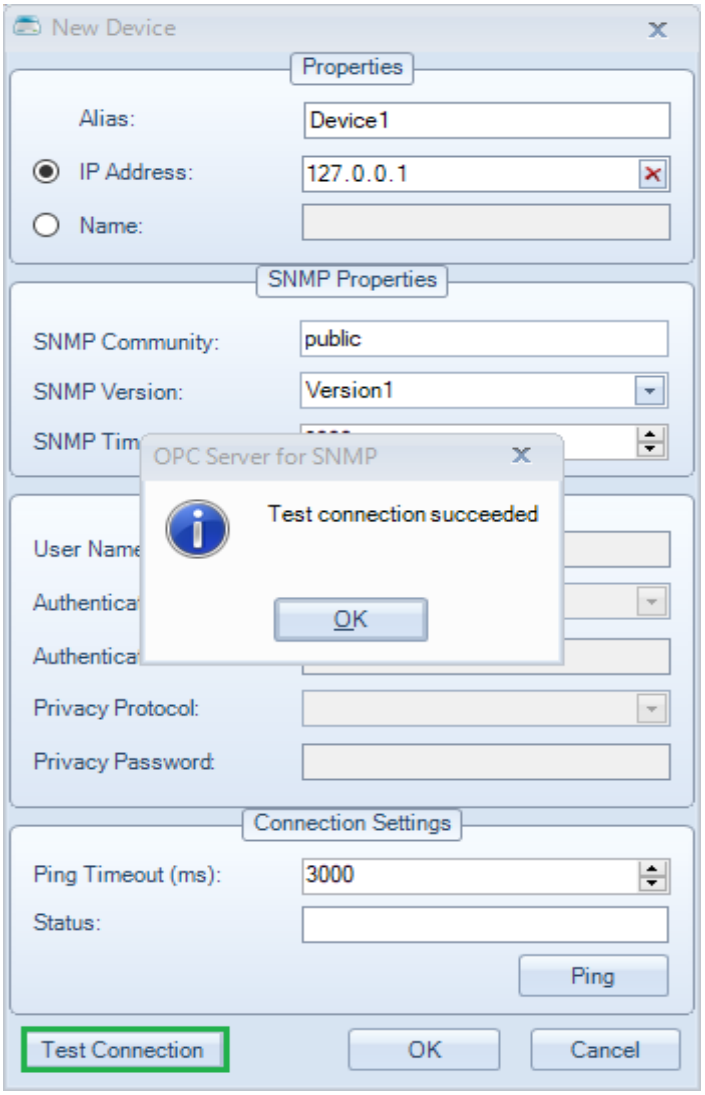

Figure 20: Test Device Connection

5.2. ADD MULTIPLE DEVICES

You can add multiple devices available within a certain IP range by right clicking on the **Address Space** node and selecting **Add Multiple Devices** option from the displayed menu.

Figure 21: Add Multiple Devices

Then, the Add Multiple Devices dialog will be displayed as illustrated below:

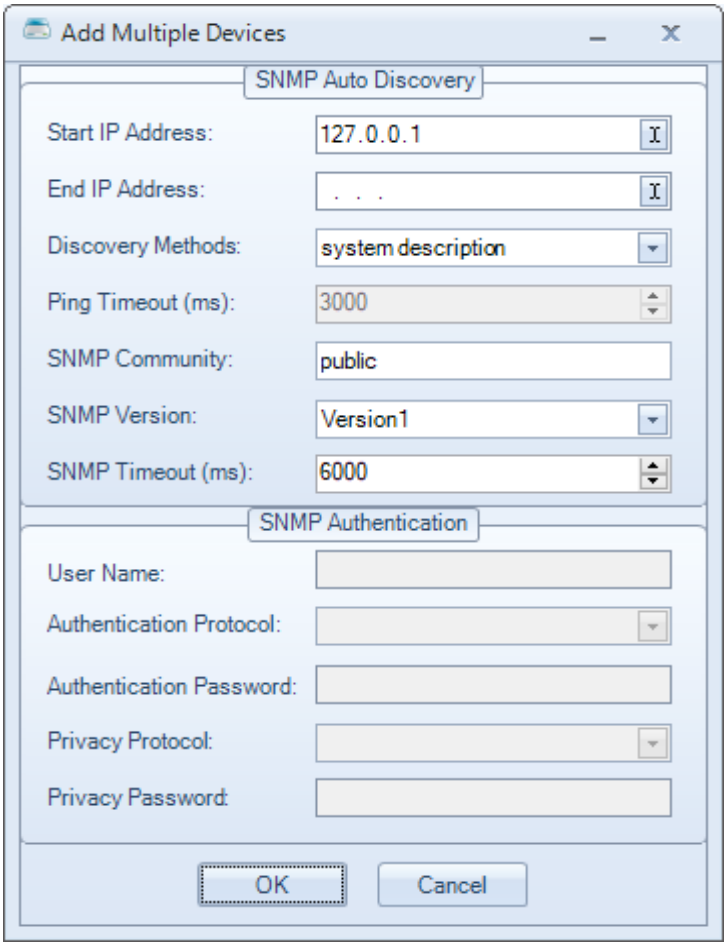

Figure 22: Add Multiple Devices Dialog

The table below summarizes the configuration parameters for the discovery of multiple devices to be added:

Parameter	Description
Start IP Address	The first IP address in the IP address range
End IP Address	The last IP address in the IP address range
Discovery Methods	The method that the server will use to discover devices. Two methods are available: • system description: SNMP method (Discovers only SNMP enabled devices) • ping: ICMP method (Discovers SNMP and non SNMP enabled devices)

Ping Timeout	If the chosen discovery method is ping, the user will need to enter the ping timeout parameter, which is the time to wait before flagging the server as unresponsive.
SNMP Community	The SNMP Community string is a user id or password that allows access to device's statistics
SNMP Version	The SNMP version supported by the device (Version1 or Version2 or Version3)
SNMP Timeout	The time to wait before flagging the SNMP enabled device as unresponsive.
SNMP Authentication	SNMP version3 requires user credentials to be passed on within each request. Three attributes are associated to this parameter: • Use name: user name • Authentication Password: private key name if the agent requires SHA or MD5 authentication. • Authentication Protocol: MD5 or SHA. • Privacy Password: a unique password if the agent requires privacy (DES or AES) protection. • Privacy Protocol: DES or AES.

Table 8: Multiple Devices Parameters

5.3. Refresh Address Space

You can refresh the address space to update the tag list by right clicking on the Address Space node and selecting the **Refresh** option from the displayed menu. Or you can simply select the Address space node and press F5 in your keyboard.

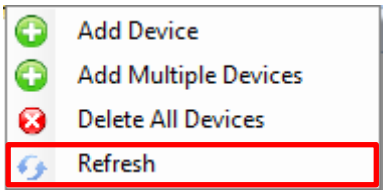

Figure 23: Refresh Address Space

5.4. Edit Device

You can edit the device configuration parameters by right clicking on its node and selecting the **Edit Device** option from the displayed menu.

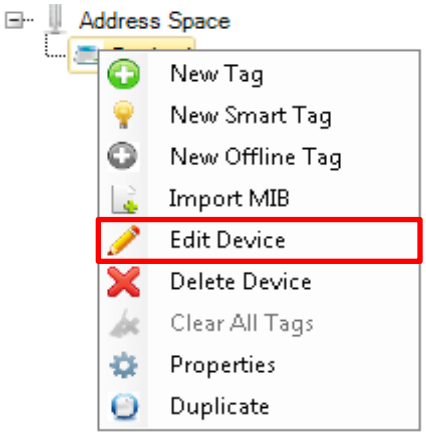

Figure 24: Edit Device

The "Edit Device" dialog will then be displayed as illustrated below:
You can edit the IP address, name, the SNMP properties and connection settings.

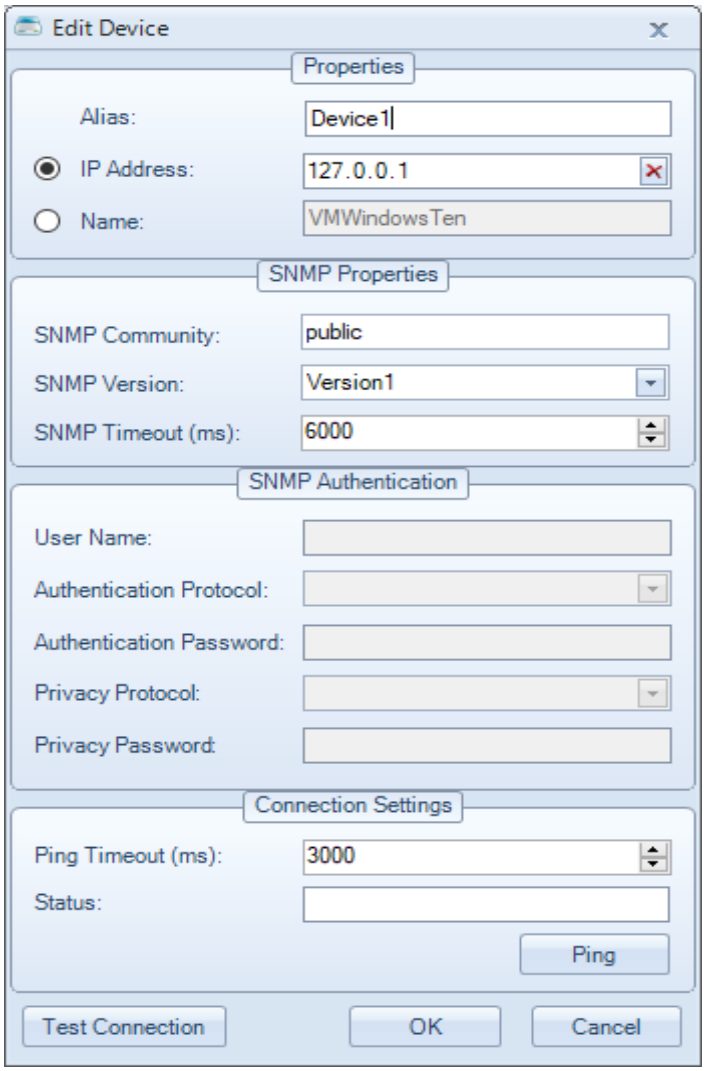

Figure 25: Edit Device Dialog

5.5. DELETE DEVICE

You can remove a device by right clicking on its name in the tree and selecting the **Delete Device** option from the displayed menu.

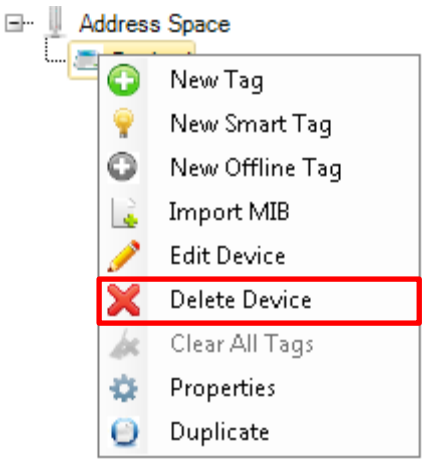

Figure 26: Delete Device

5.6. DUPLICATE DEVICE

You can duplicate an existing device configuration to multiple devices by right clicking on the device name and choosing the **Duplicate** option from the displayed menu.

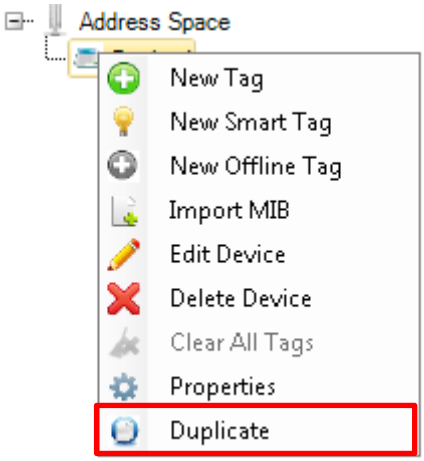

Figure 27: Duplicate Device

A dialog box will be displayed allowing the user to add list of the IP addresses separated with semicolon.

.

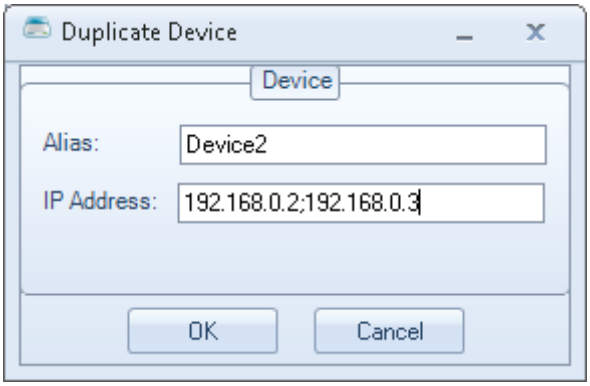

Figure 28: Duplicate Device Dialog

5.7. IMPORT MIB

You can import a MIB file by right clicking on a device name from the tree and choosing the **Import MIB** option from the displayed menu.

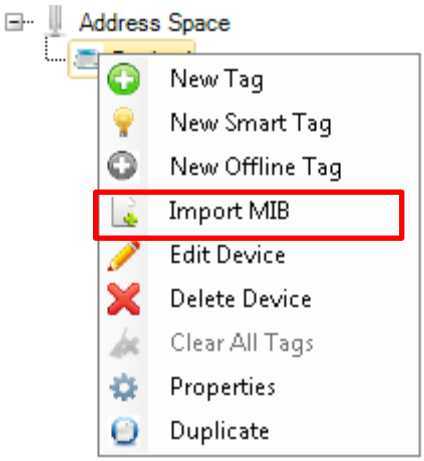

Figure 29: Import MIB

A dialog box will be displayed allowing the user to add his MIB file.

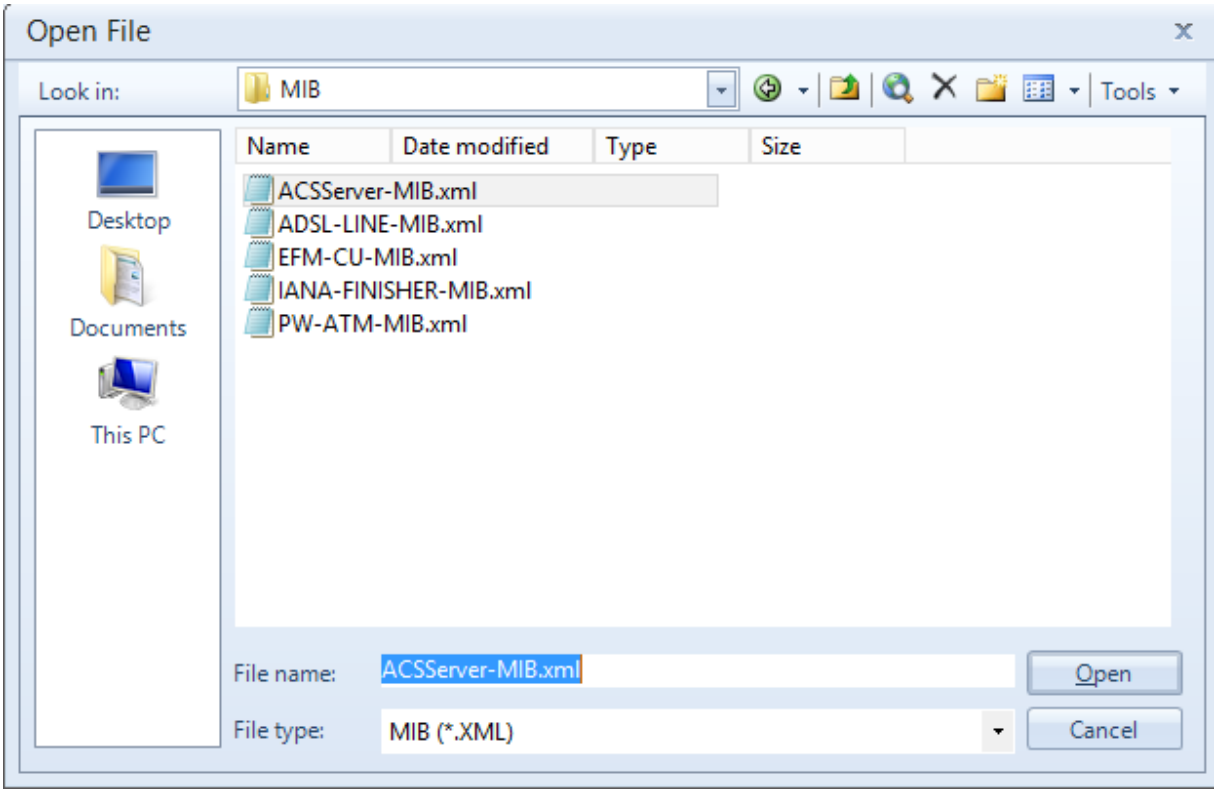

Figure 30: Choose a MIB file Dialog

After choosing a specific MIB file, the user can then visualize the content of the chosen file.

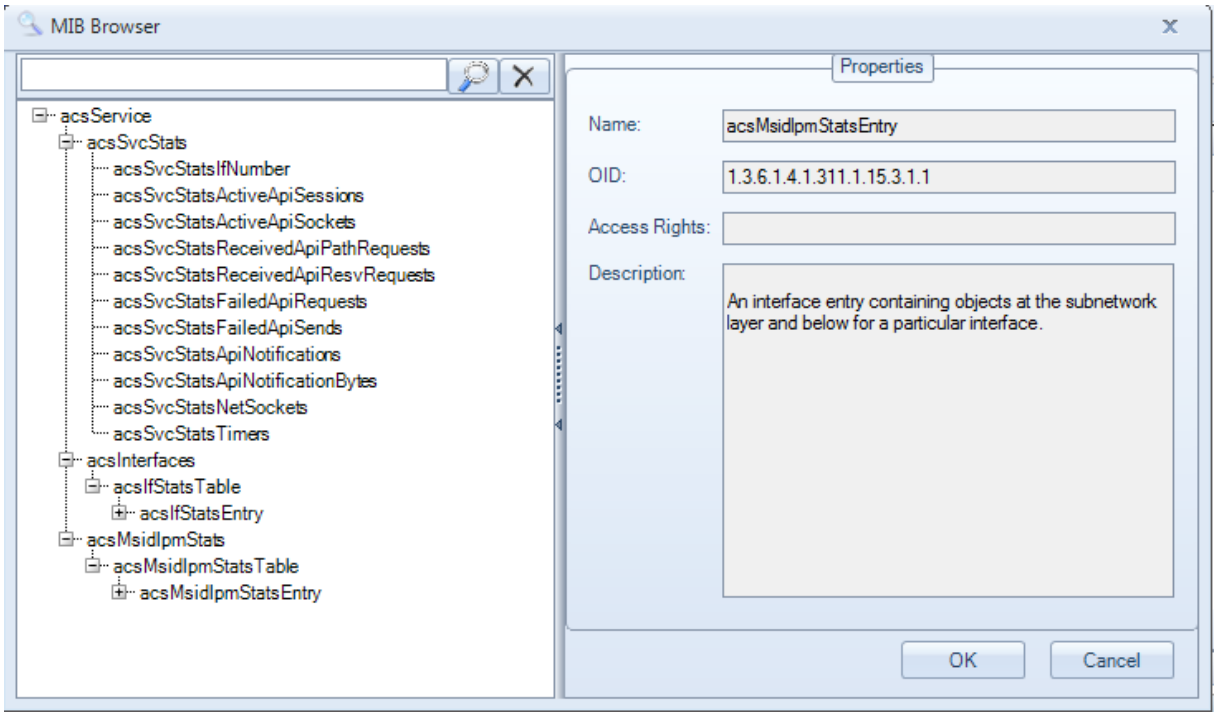

Figure 31: MIB Browser

5.8. VIEW DEVICE PROPERTIES

The OPC Server for SNMP offers two ways for the user to check the device properties.

1. After selecting a device in the tree, the user can visualize the selected device properties in the grid view on the right side.

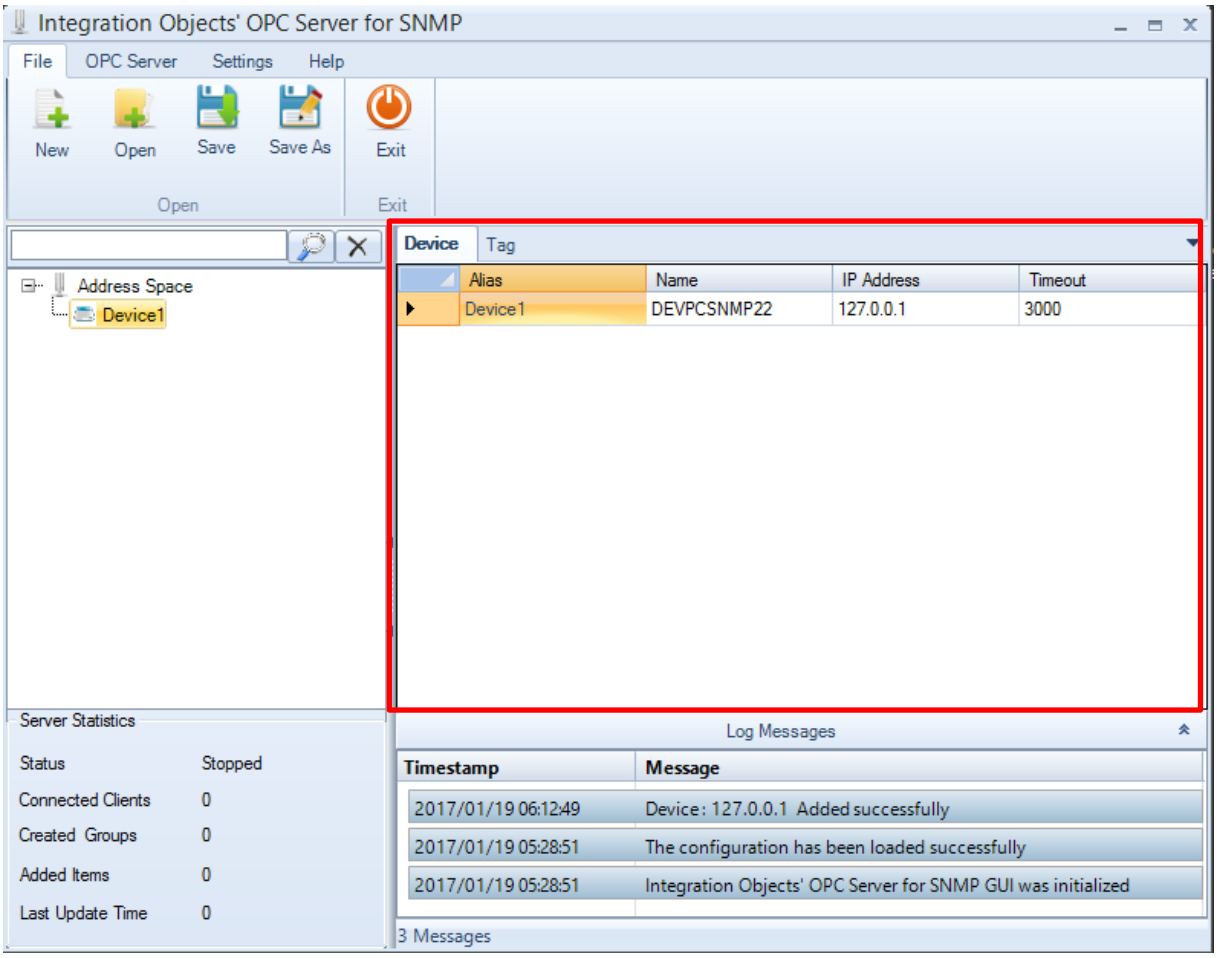

Figure 32: Visualize Device Properties

2. The user can also check the properties of a device by right clicking on a device name from the tree and choosing the **Properties** option from the displayed menu.

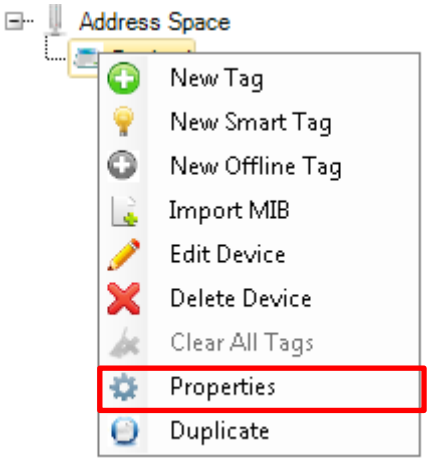

Figure 33: Device Properties

Then, the "Device Properties" dialog will be displayed.

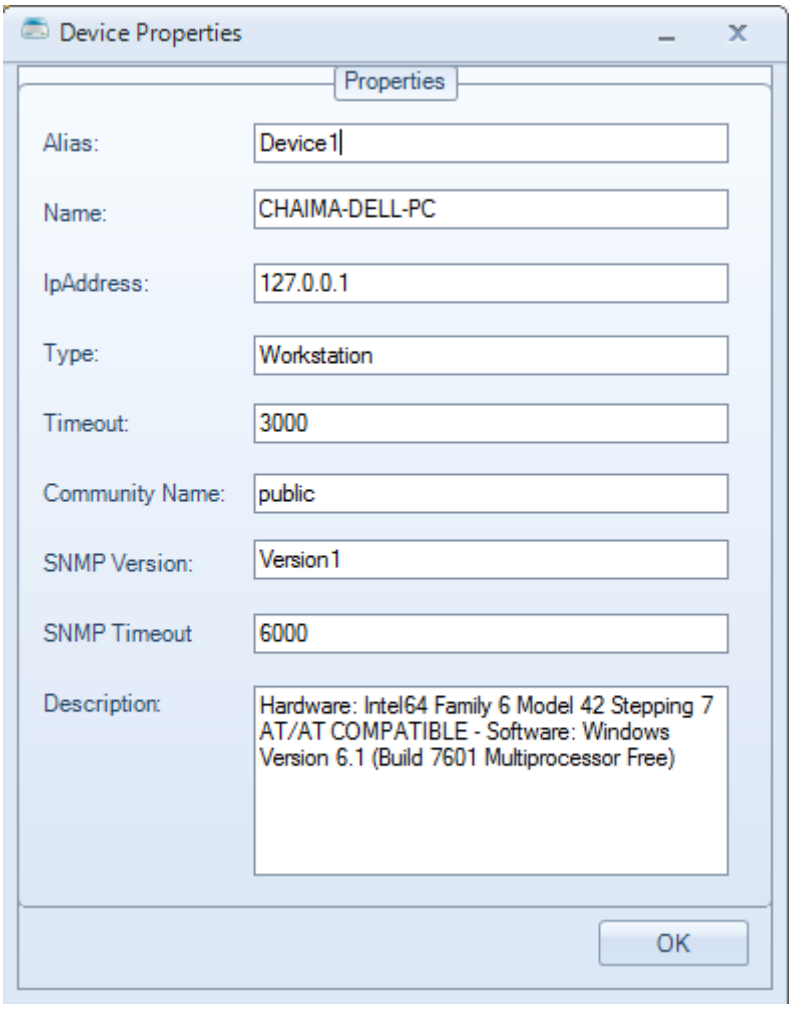

Figure 34: Device Properties Dialog

5.9. ADD TAG

The figure below shows how to add a new tag to a device.

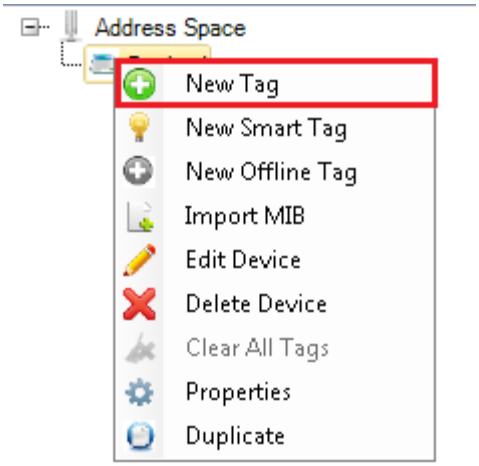

Figure 35: New Tag

Once the **New Tag** option is selected, a dialog will be displayed allowing the user to configure the tag parameters.

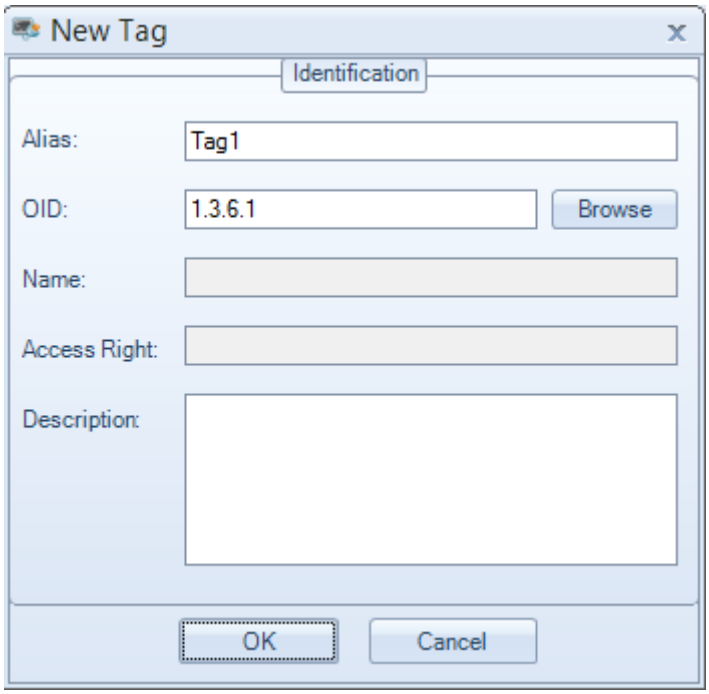

Figure 36: New Tag Dialog

The table below summarizes the tag configuration parameters:

Parameter	Description
Alias	The name used to manipulate the tag.
OID	Object Identifier (OID): it is the unique identifier of each tag.
Name	The associated name of the OID in the MIB file. This name is not editable.
Access Right	Each tag has an access right. It could be: Read, Write, or Read/Write. This property is not editable.
Description	Textual description of the tag.

Table 9: Tag Parameters

The user can either add a specific OID manually or a click on the **Browse** button to search for a tag. The Browse button will perform a SNMP Walk starting from the entered OID and the" Tag Browser" dialog will be displayed. You can choose one or many tags from the list of tags. Besides, you can access the different properties by selecting the tag.

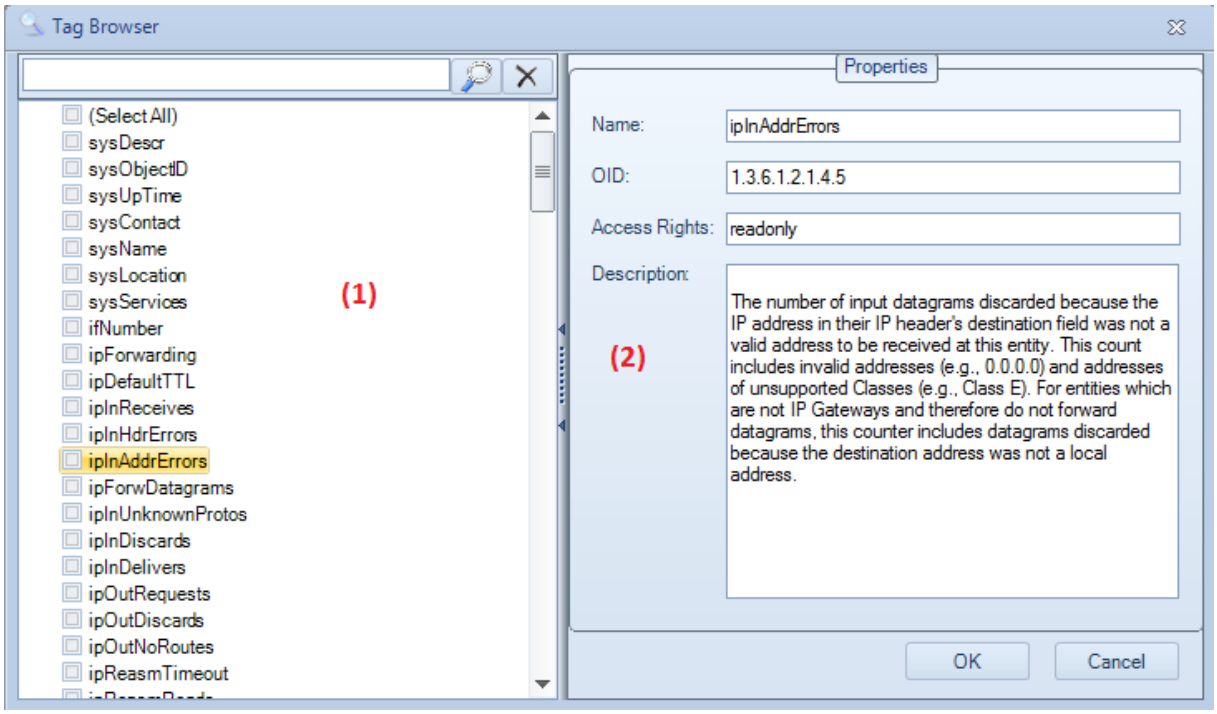

Figure 37: Tag Browser Dialog

- **List of tags (1):** This is where all the available tags of a device are displayed. To add a tag, check the related box. If you wish to add all tags you will need to check the **Select All** node.

- **Tag properties (2):** When selecting a tag in the list, you can visualize its properties: name, OID, access rights and description.

5.10. ADD SMART TAG

A smart tag is a predefined and calculated tag based on a combination of different tags. The list of available smart tags is in the following table:

Smart Tag	Description
Used Memory	The total amount of real system memory allocated to all active process in Gbyte
CPU Usage	The average of percentage of time over the last minute when CPU was not idle
Core Usage	The average amount of percentage of time over the last minute where the CPU is not idle
Network Interface 's Input Utilization	The interface's input utilization in Mbps
Network Interface 's Output Utilization	The interface 's output utilization in Mbps
Network Interface 's Status	The interface's status. It can be: • up • down • testing • unknown • dormant • notPresent • loweLayerDown
Disks' Volume Used	The volume used of a disk in GB
Disks' Size	The volume size of a disk in GB
Disks' Available Space	The available space of a disk in GB
Status	The status of the device on the network based on the device response to ping requests: • Available • Not Available
Ping Timeout	The number of milliseconds taken to send an ICMP echo request and receive a reply in milliseconds

Table 10: Smart Tag List

You can add a smart tag by clicking on the **New Smart Tag** option in the displayed menu of a device.

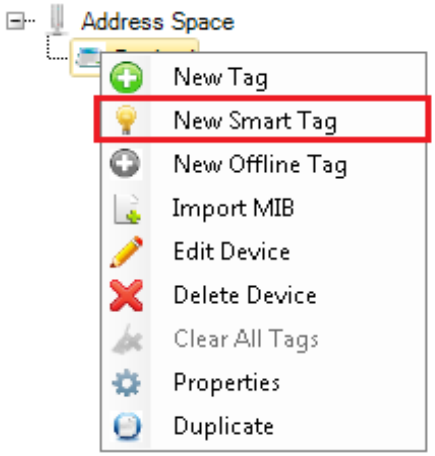

Figure 38: New Smart Tag

After clicking on **New Smart Tag**, the following dialog will be displayed.

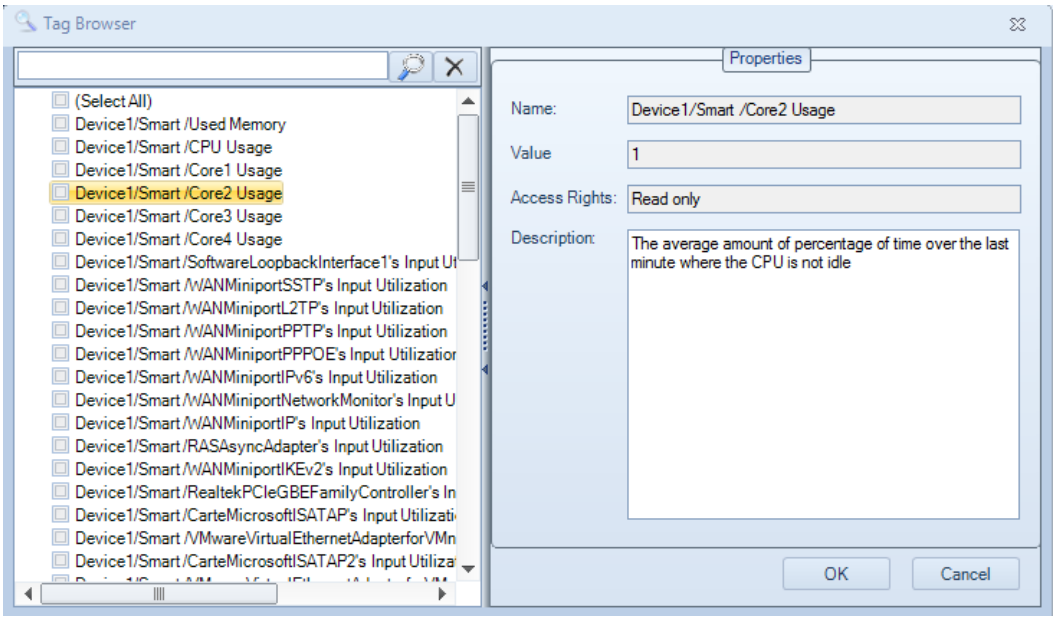

Figure 39: Add Smart Tag Dialog

5.11. ADD OFFLINE TAG

You can add one or multiple offline tags even when the device doesn't response to SNMP request.

The figure below shows how to add an offline tag to the device

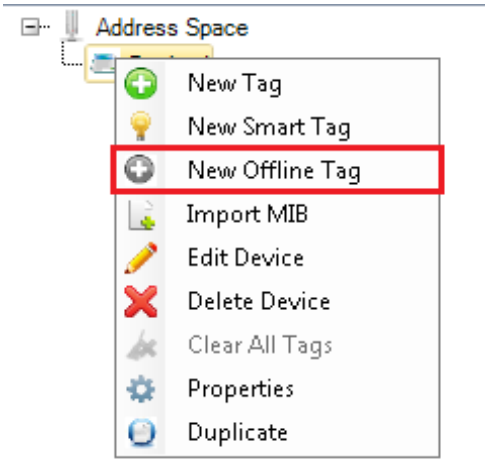

Figure 40: Add Offline Tag

After clicking on **New Offline Tag**, the following dialog will be displayed.

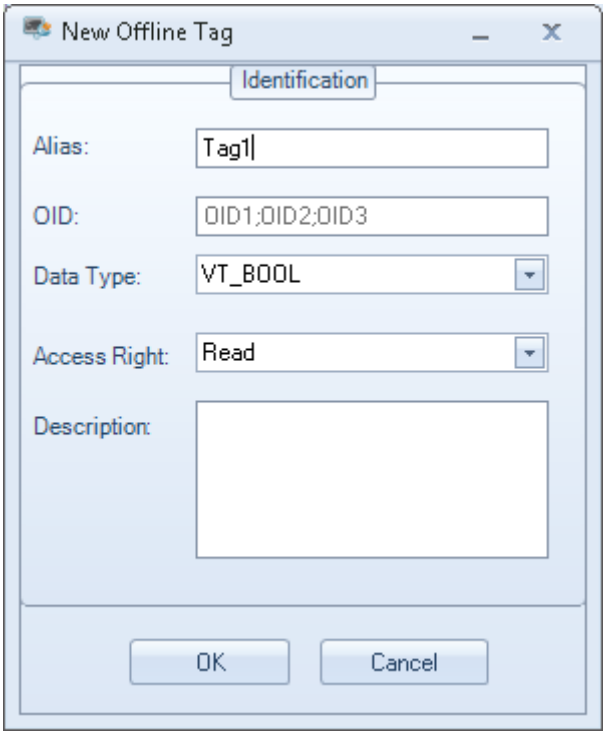

Figure 41: New Offline Tag Dialog

The table below summarizes the tag configuration parameters:

Parameter	Description
Alias	The name used to manipulate the tag.
OID	Object Identifier (OID): it is the unique identifier of each tag.
Data Type	The type of data, which can be: • VT_I2 • VT_I4 • VT_R4 • VT_UI2 • VT_UI4 • VT_BSTR • VT_BOOL
Access Right	Each tag has an access right. It could be: Read, Write, or Read/Write. This property is not editable.
Description	Textual description of the tag.

Table 11: Offline Tag Parameters

5.12. EDIT TAG

You can update a tag configuration by clicking on the **Edit Tag** option in the right click menu.

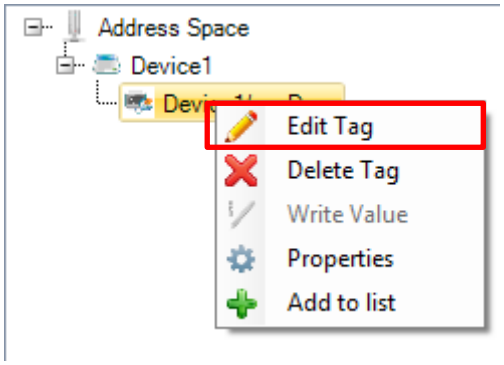

Figure 42: Edit Tag

The" Edit Tag "dialog will be displayed as illustrated below: the user is able to edit only the OID or the description of the tag.

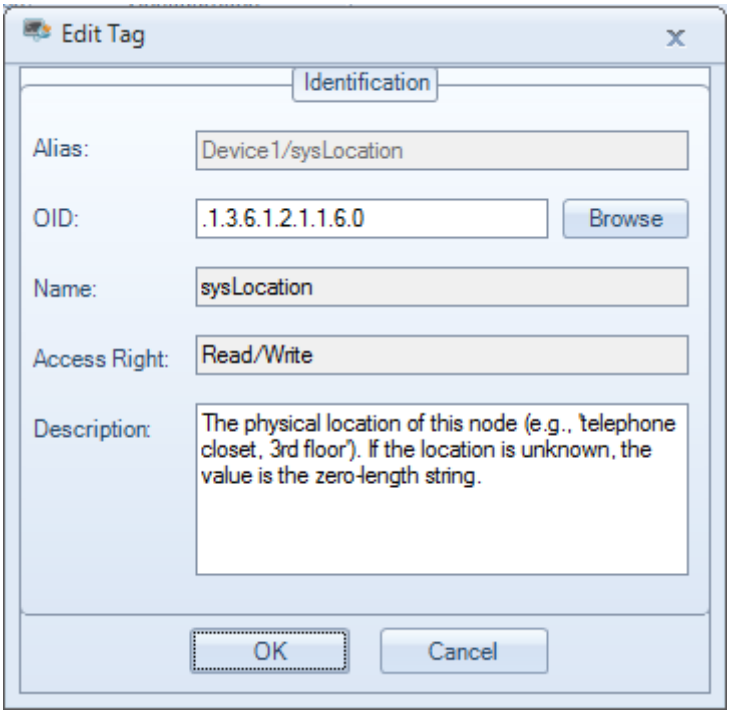

Figure 43: Edit Tag Dialog

5.13. DELETE TAG

You can delete a tag from the address space by clicking the **Delete Tag** option in the right click menu.

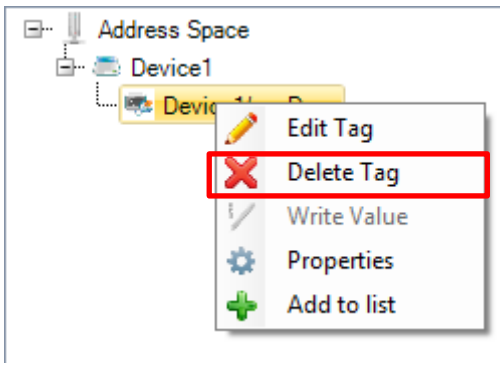

Figure 44: Delete Tag

You can delete all the tags of a device by selecting the **Clear All Tags** option in the right click menu of the device.

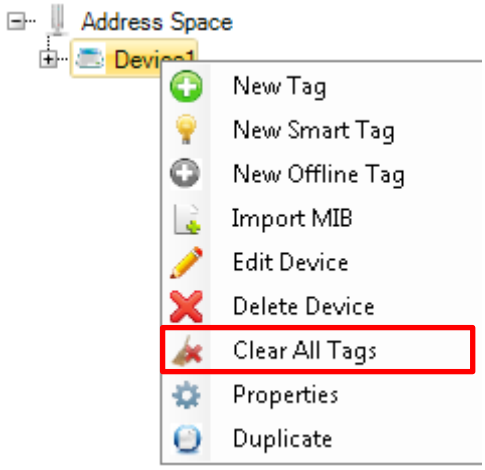

Figure 45: Delete All Tags

You can also delete multiple tags by selecting multiple tags and right clicking on them. Then, choose the delete option from the displayed menu.

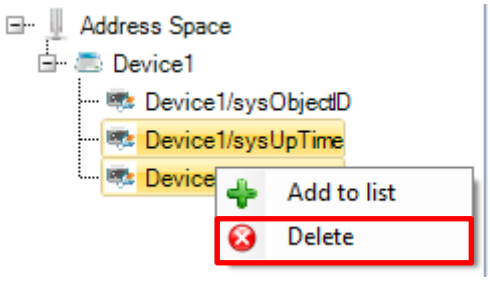

Figure 46: Delete Multiple Tags

5.14. WRITE TAG VALUE

You can change the value of a tag if it has a read/write or write access by clicking the **Write Value** option in the right click menu of the tag.

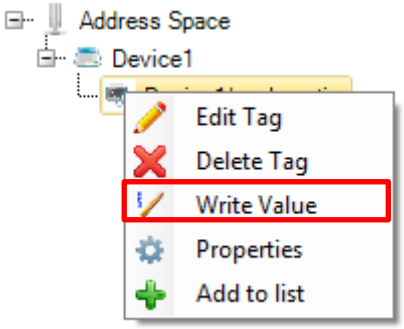

Figure 47: Write Value

When selecting the **Write Value** option, the following dialog will be displayed.

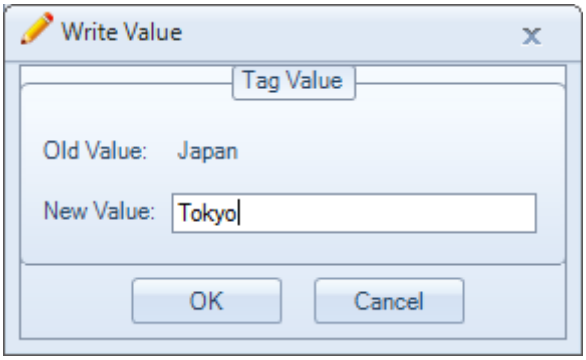

Figure 48: Write Value Dialog

5.15. VIEW TAGS PROPERTIES

Select multiple tags and right click, then choose **Add to list** option. The tags properties will be displayed in the grid view on the right side of the main user interface.

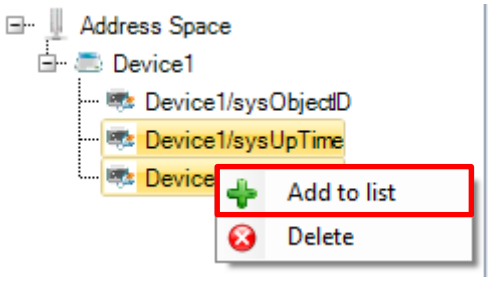

Figure 49: Add to List

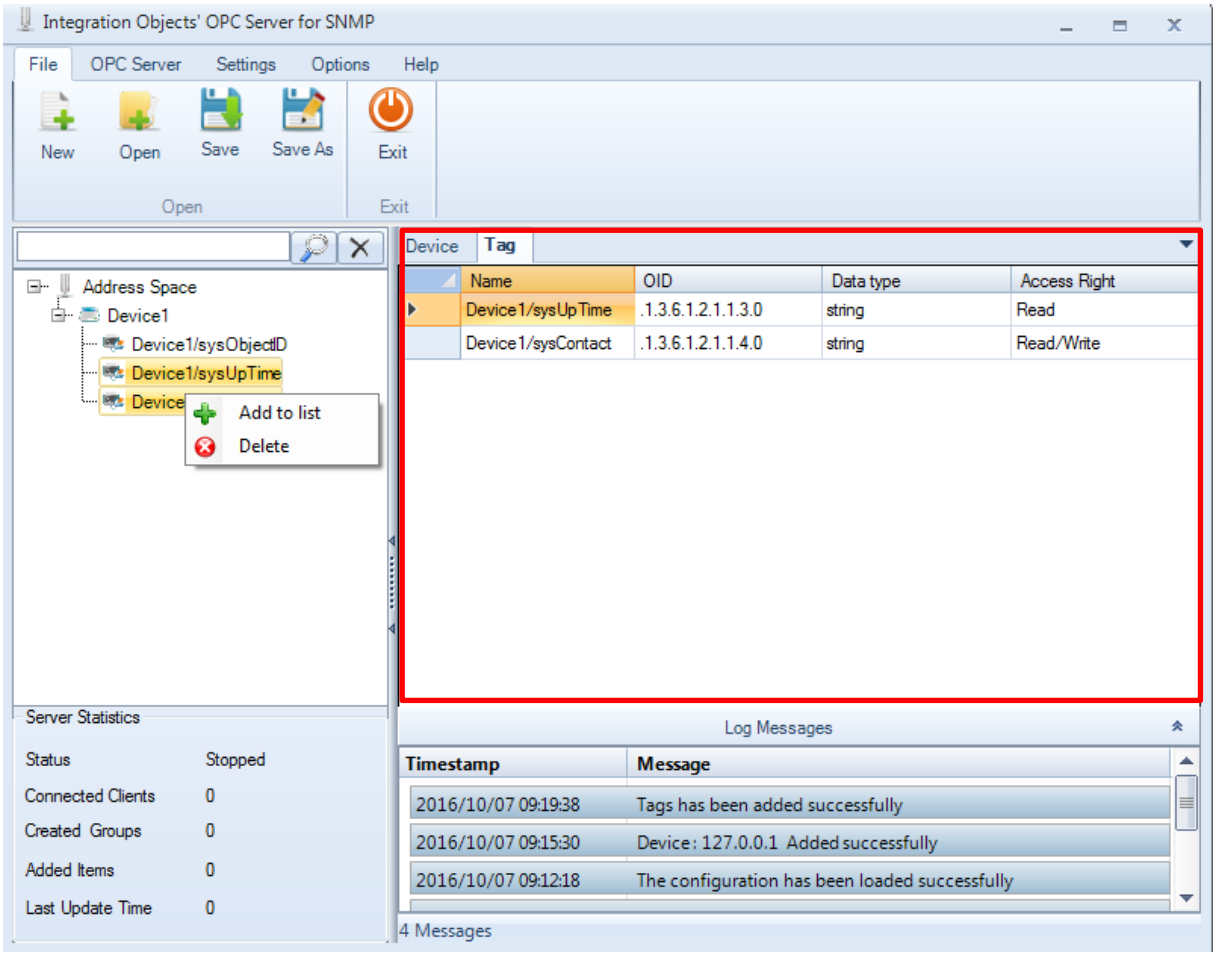

Figure 50: Display Selected Tag Properties

You can also visualize the tag properties by right clicking a specific tag and choosing the **Properties** option from the displayed menu.

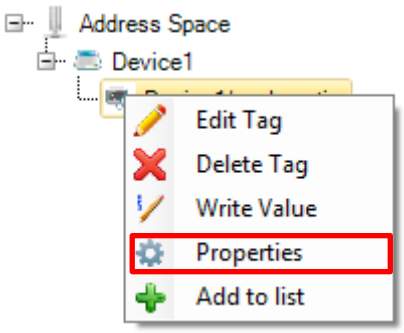

Figure 51: Tag Properties

The “Tag Properties” dialog will then be prompted.

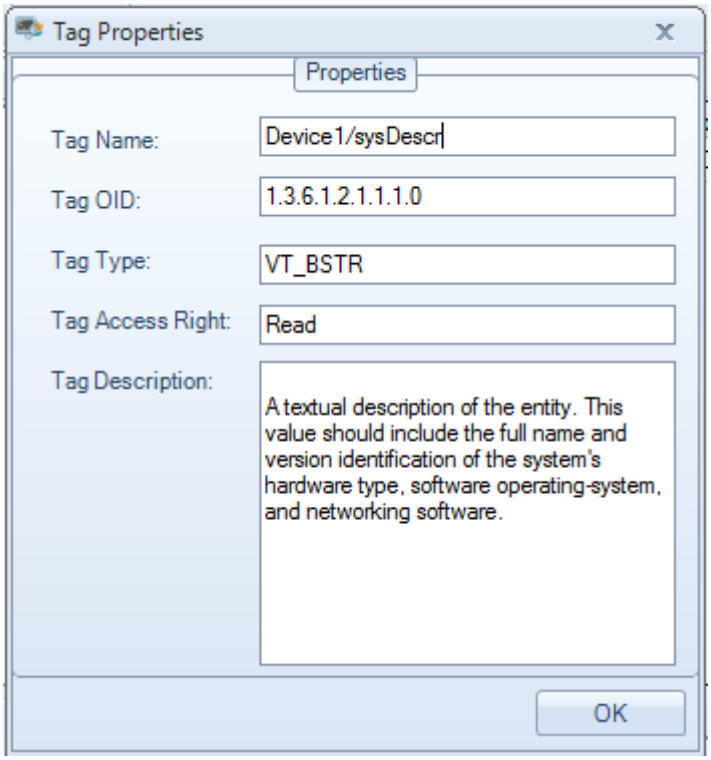

Figure 52: Tag Properties Dialog

5.16. SAVE CONFIGURATION

Save your configuration using the **Save As** or **Save** button available in the file menu.

The" Save File As" dialog illustrate in the figure below is used to choose the path where the configuration will be saved.

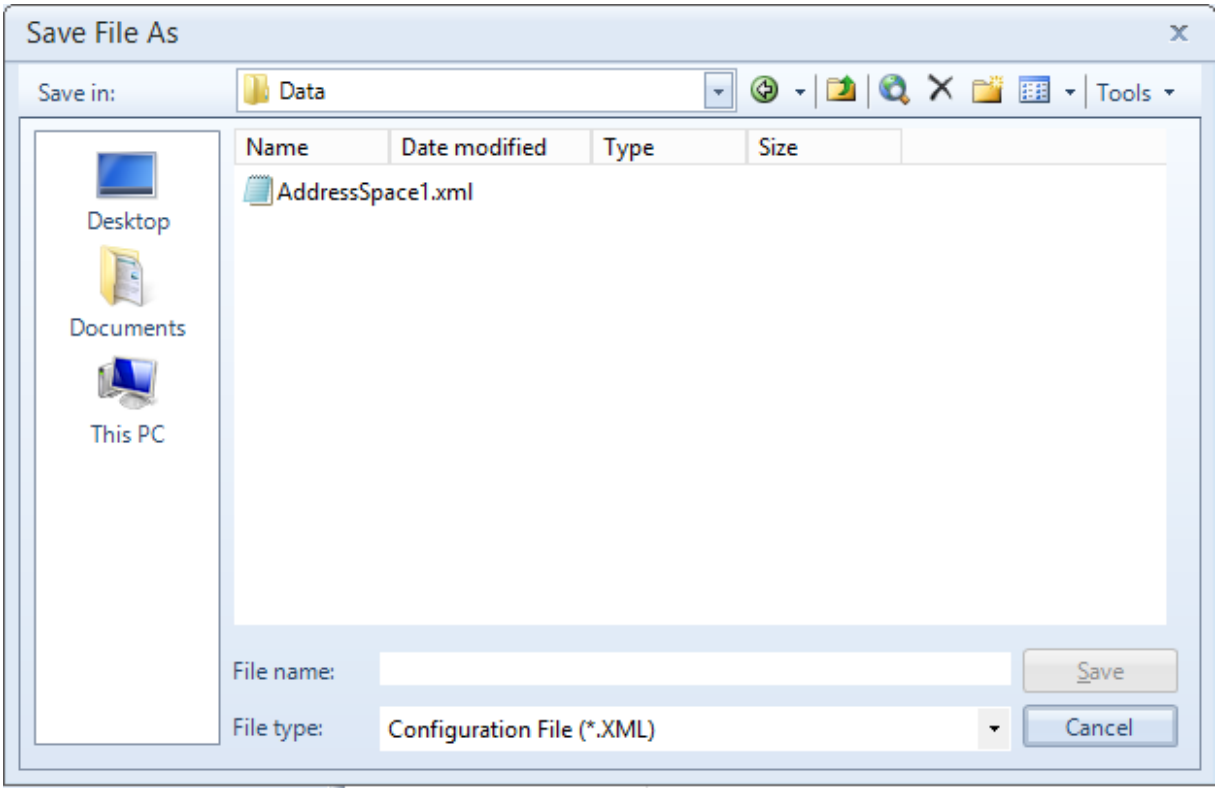

Figure 53: Save File as Dialog

The configuration will be then saved in XML file format. The configuration is divided into devices sections, and each device section contain tag list section that holds all the SNMP tags and their associated parameters.
The table below describes the 18 attributes of the devices configuration section.

#	Field	Description
1	**strName**	The device name
2	**strAlias**	The device alias
3	**deviceIPAddress**	The device IP address
4	**ConfgWith**	ConfgWith will indicate if the device was configured with its IP address or with its name
5	**intTimeout**	The timeout of the ping request
6	**strSNMPV**	The SNMP version of the device(Version1 or Version2 or Version3)
7	**strCommunity**	The SNMP community name of the device
8	**strUserName**	The user name used for the authentication if the device supports SNMP version3

9	**strAuthProtocol**	The authentication protocol used for the authentication if the device supports SNMP version3
10	**strPrivProtocol**	The privacy protocol used for the authentication if the device supports SNMP version3
11	**strAuth**	The authentication password used for the authentication if the device supports SNMP version3
12	**strPwd**	The privacy password used for the authentication if the device supports SNMP version3
13	**tagList**	This parameter lists the different SNMP tags.

Table 12: Devices Configuration Section

The tagList section holds the different SNMP tags. We will detail in the table below the different attributes of a SNMP tag.

#	Field	Description
1	**strTagName**	The tag name
2	**strTagDescrp**	The tag description
3	**uiAccessRight**	The access rights of a tag
4	**strTagOID**	The tag Object Identifier (OID) is a unique identifier associated to each tag
5	**DataType**	The type of data, which can be: • VT_I2 • VT_I4 • VT_R4 • VT_UI2 • VT_UI4 • VT_BSTR • VT_BOOL
6	**bIsTrap**	If bIsTrap is equal: • True: The tag was dynamically created after receiving a trap message. • False: The tag was added from the configuration tool.

Table 13: Tags Configuration Section

```
<?xml version="1.0" encoding="utf-8"?>
<Devices>
    <SNMPDevice>
        <DeviceName>
            <string>Device1</string>
        </DeviceName>
        <DeviceConfiguration>
            <Device xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
                <strName>VMWindowsTen</strName>
                <strAlias>Device2</strAlias>
                <deviceIPAddress>127.0.0.1</deviceIPAddress>
                <deviceType>Workstation</deviceType>
                <intSNMPTimeout>6000</intSNMPTimeout>
                <ConfgWith>withIp</ConfgWith>
                <intTimeout>3000</intTimeout>
                <strSNMPV>Version1</strSNMPV>
                <strCommunity>public</strCommunity>
                <strUserName />
                <SNMPTimeout>6000</SNMPTimeout>
                <strAuthProtocol />
                <strPrivProtocol />
                <tagList>
                    <SNMPTag>
                        <strTagName>Device2/sysDescr</strTagName>
                        <strTagOID>1.3.6.1.2.1.1.1.0</strTagOID>
                        <strTagDescrp>
A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software.
</strTagDescrp>
                        <strtagMibName>sysDescr</strtagMibName>
                        <bOfflineTag>false</bOfflineTag>
                        <uiAccessRight>1</uiAccessRight>
                        <DataType>8</DataType>
                        <DependencyList />
                        <bIsTrap>false</bIsTrap>
                    </SNMPTag>
                </tagList>
                <strAuthenticationPassword />
                <strPrivacyPassword />
            </Device>
        </DeviceConfiguration>
    </SNMPDevice>
</Devices>
```

Figure 54: Configuration File Example

After saving your configuration, you need to set the default configuration, which will be loaded automatically at the OPC Server for SNMP Service start-up. To define a default configuration, click the Define button available in the Settings Menu.

6. Connection to the OPC Server

Once the OPC Server is configured, the next step will be to connect to it using an OPC Client and read/write data. To do so, you only need to:

1. Launch your OPC DA Client.
2. Enter the IP address of the machine where the OPC Server is installed
3. Connect to the OPC Server with the following progID: "IntegrationObjects.OPC.SNMP.1".

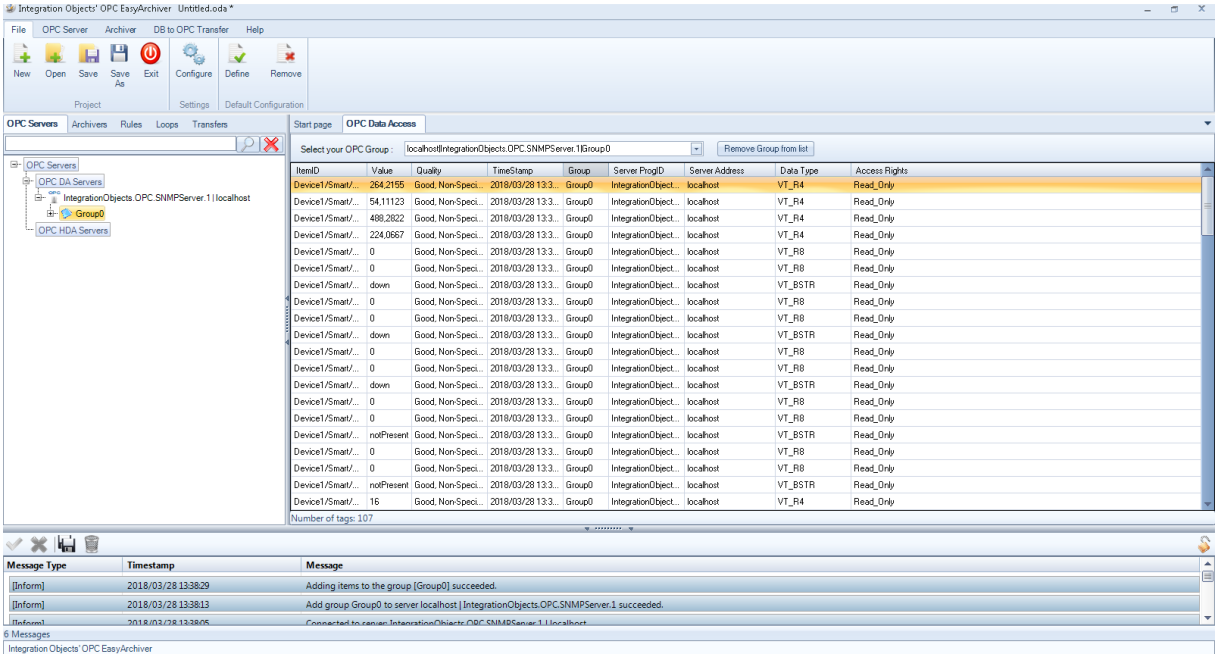

Figure 55: OPC DA Client - Connect to OPC Server for SNMP

Add a group and select the items to be read.

TRACING CAPABILITIES

The OPC server creates two log files named "LogServerForSNMPGUI.LOG" and "LogServerforSNMPService.LOG" that record errors and debugging information for the server configuration and runtime execution. This server also generates a separate log file dedicated to the details of operations of the OPC interfaces: "SrvToolkit_LogEvent.log" log file to easily diagnose the occurred problems and it can be extremely valuable for troubleshooting. Under normal operations, the server logs very little information.
These log files are generated at start-up under the installation folder where the executable file is located.
The OPC Server for SNMP settings are based on two configuration files:

- "SrvToolkit_CfgFile.ini"
- "OPCSNMPConfig.ini"

These files include several logging parameters. To change the default configuration:
Open "OPCSNMPConfig.ini" or "SrvToolkit_CfgFile.ini" in a text editor.
Edit any of the parameters listed in the following tables:

The following table describes the logging parameters saved on "SrvToolkit_CfgFile.ini":

Log Setting	Description	Default Value
LogFileName	The log file name	SrvToolkit_LogEvent
LogFileMaxSize	The maximum log file size, in bytes. Once this size is reached during runtime, the log file will be overwritten.	2097152
LogLevel	The log level. Possible values are: **Control (-1):** It is the lowest level. This log file contains at least a description of succeeded methods. **Fatal (0):** Only fatal error messages are logged. **Critical (1):** All critical error messages are logged. **Error (2):** All errors are logged. **Warning (3):** All warnings are logged. **Info (4):** All information is logged. **Debug (5):** For Debug information. The higher the log level, the more information is recorded. We recommend using the default level for a better performance of the server.	Error

ArchiveLastLog	TRUE: Old file is copied to an intermediate file with incremental extension, before being overwritten. FALSE: Any pre-existing log file is erased and overwritten at start-up.	FALSE

Table 14: Log Settings of the "SrvToolkit_CfgFile.ini"

The following table describes the log parameters of "OPCSNMPConfig.ini" configuration file:

Setting	Description	Default Value
AppConfiguration / ServiceConfiguration		
AutoAppend	Set to true to continue writing log messages in the existing 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 writes action in the hard disk. It must be greater than 100.	200
FileExtension	The log file extension	Log
MaxSize	The maximum size of the log file (in Mb)	10
FileName	The log file name	• LogServerforSNMPGUI: log file of the configuration user interface • LogServerforSNMPService: log file of the service
FilePath	Used to save the full installation directory path	Installation Folder
MaximumFiles	Set to 0 means that log files will be created in an unlimited way.	5
Level	The type of log messages to be logged. The value can be Control, Error, Warning, Inform, and Debug.	Error
AutoSaveTimeOut	Time to wait to read all messages from the buffer	10

ConfigSetting		
ConfigFilePath	Used to save the default configuration file path	OPCSNMPServiceConfig.xml
ServerRate	This parameter is the frequency at which the server handles the asynchronous reads/updates.	500 ms
CheckDeviceStatusPeriod	The period between two checks of the devices status in milliseconds	60000 ms
Style	The style of the GUI	Windows7Blue
StrSeparator	OPC Item Delimiter	/
UpdateAddressSpaceRate	The period between two updates of the Address Space	500 ms
UpdateTagRate	The period between two updates of tags	0 ms
ListenTrapPeriod	The period between listening to two trap messages	500ms
CheckDeviceConnectivity	If True: The server will check the device connectivity periodically using SNMP request. If False: the server will not check the device connectivity.	True
CheckValidationTag	If True: The server will validate each item before adding the item to the group If False: The item validation is ignored	True
UpdateOnlyOnTrapReceive	If True: the trap tag will only be updated when a trap message arrives If False: an SNMP Get will be performed to et the value of the trap tag	True

Table 15: Configuration Settings of "OPCSNMPConfig.ini"

1. Save the file and restart the server for the changes to take effect.

SrvToolkit_CfgFile.ini Configuration File

```
[LogSetting]
LogFileName=SrvToolkit_LogEvent
LogFileMaxSize=2097152
LogLevel=5
ArchiveLastLog=false
```

Figure 56: "SrvToolkit_CfgFile.ini" File

OPCSNMPConfig.ini Configuration File:

```
[AppConfiguration]
AutoAppend=true
BufferSize=200
FileExtension=log
MaxSize=10
FileName=LogServerForSNMPGUI
FilePath=C:\Program Files (x86)\Integration Objects\Integration Objects' OPC Server for SNMP\LogFiles\
MaximumFiles=5
Level=Error
AutoSaveTimeOut=10
[ServiceConfiguration]
AutoAppend=true
BufferSize=200
FileExtension=log
MaxSize=10
FileName=LogServerforSNMPService
FilePath=C:\Program Files (x86)\Integration Objects\Integration Objects' OPC Server for SNMP\LogFiles\
MaximumFiles=5
Level=Error
AutoSaveTimeOut=10
[ConfigSetting]
ConfigFilePath=C:\Program Files (x86)\Integration Objects\Integration Objects' OPC Server for SNMP\OPCSNMPServiceConfig.xml
ServerRate=500
UpdateAddressSpaceRate=500
UpdateTagRate=0
CheckDeviceStatusPeriod=30000
ListenTrapPeriod=500
CheckServerStaticticsPeriod=4000
Style=Windows7Blue
StrSeparator=/
CheckDeviceConnectivity=true
CheckValidationTag=true
UpdateOnlyOnTrapReceive=true
```

Figure 57: "OPCSNMPConfig.ini" File

You can also update these parameters through the OPC Server for SNMP user interface.

TROUBLESHOOTING

Case 1: Cannot launch the OPC Server for SNMP?

You should check the license validity by launching the License Authorization tool existing under the OPC Server for SNMP installation folder, or start it directly from the start up menu:

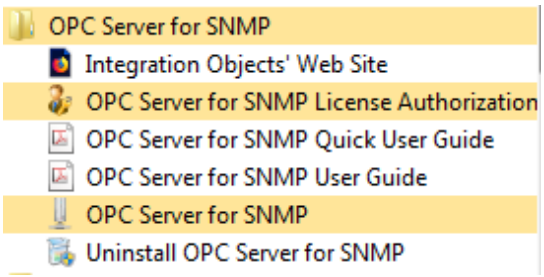

Figure 58: OPC Server for SNMP Start Menu

If the License Authorization tool shows that the demo has expired and you want to activate it using your full activation license, you should follow the following steps:

1. Open the License Authorization tool and click on the **Register** button.

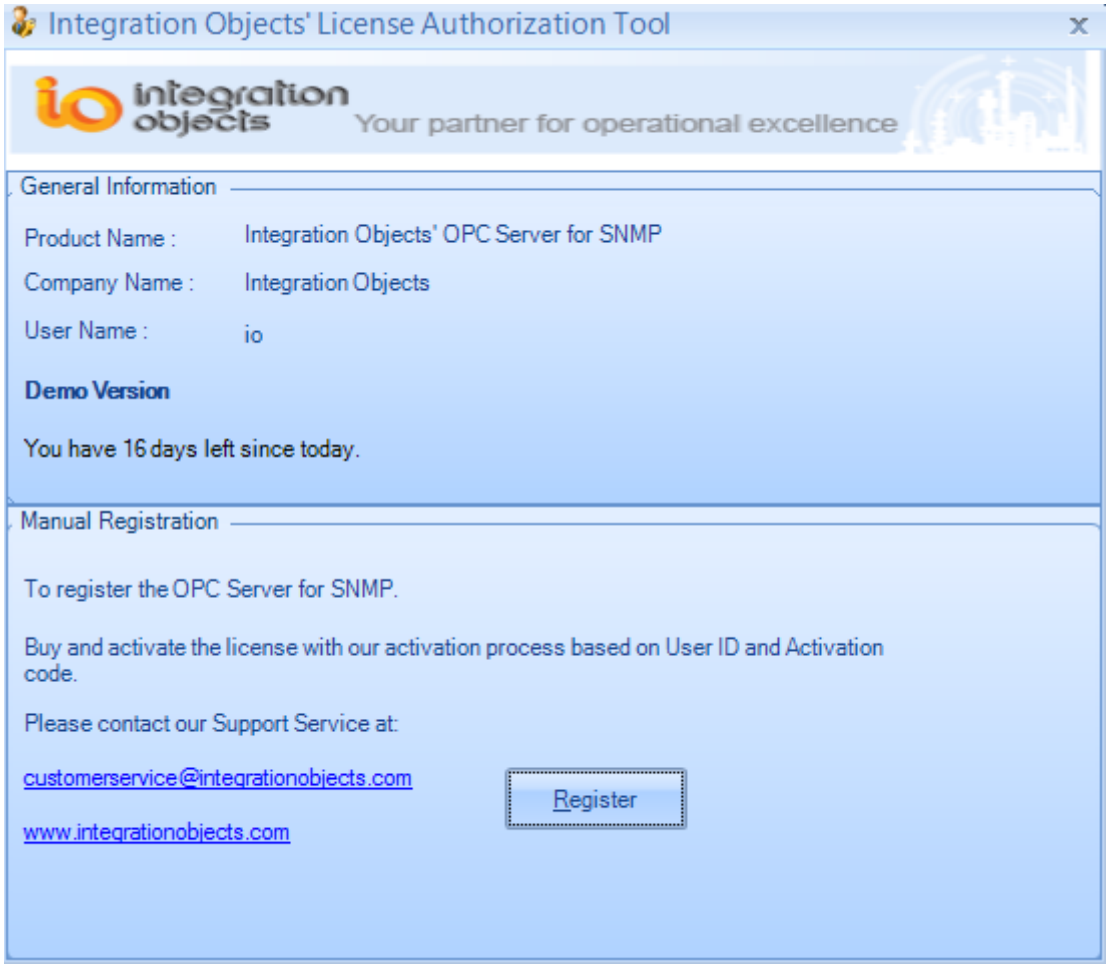

Figure 59: License Authorization

1. Copy and send the User ID to the sales team so they can generate the dedicated activation code.

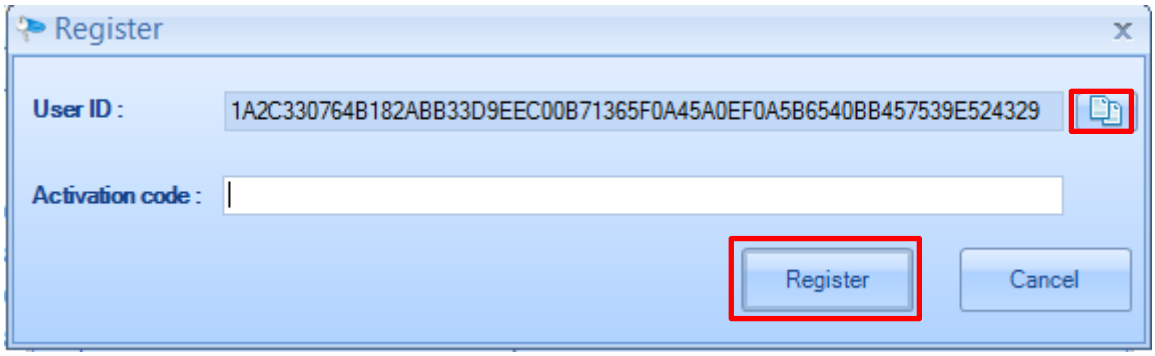

Figure 60: License Registration

2. Copy and paste the received activation code and click on the **Register** button.

Case 2: Cannot start the OPC Server for SNMP Service?

In case the local connection to the OPC Server for SNMP failed due to an access deny you need to follow the steps below:

1. Open the windows service manager
2. Select the Integration Objects' OPC Server for SNMP Service.
3. Right click and select the Log on tab.
4. Check the "This account" radio button.
5. Enter your administrator account credentials as shown in the following figure:
6. Click the OK button.

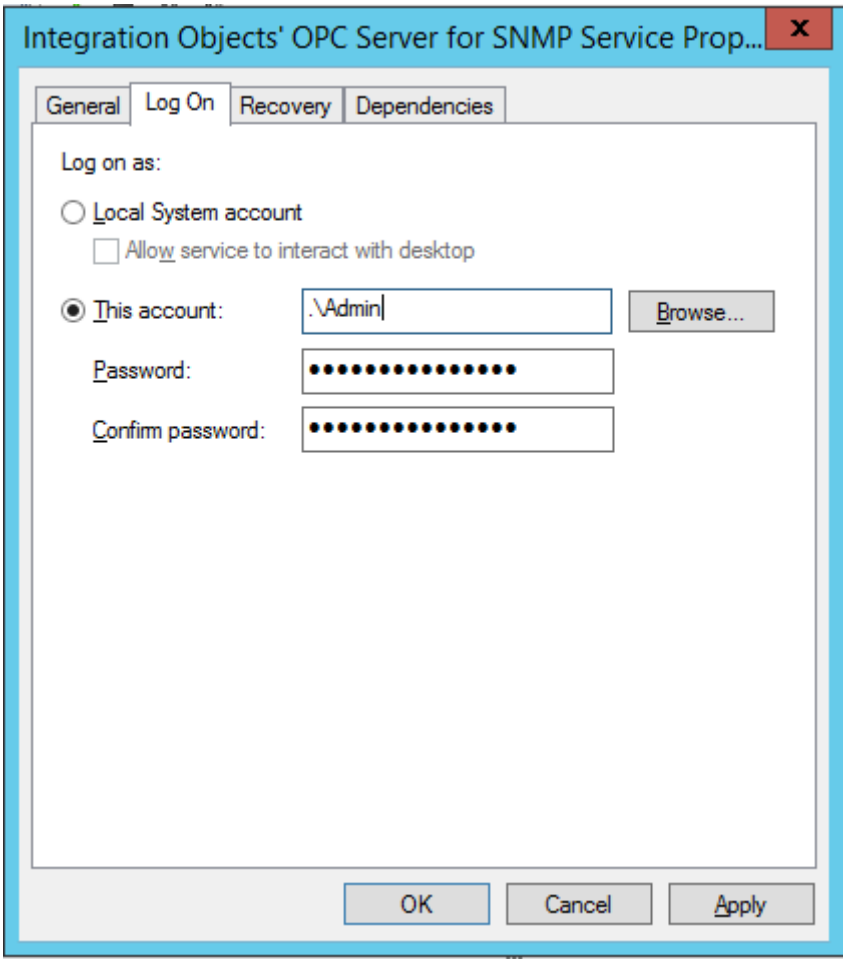

Figure 61: OPC Server for SNMP Service Properties

Case 3: Why the Smart tag CPU Usage does not update more often?

The CPU Usage Tag is a smart tag that describes the average of percentage of time over the last minute when CPU was not idle. Thus the value is expected to change every one minute.

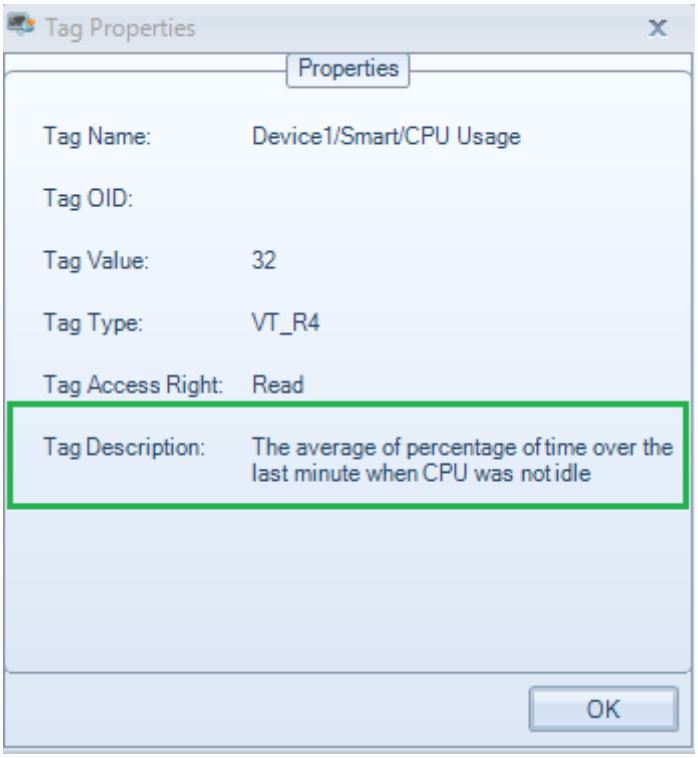

Figure 62: CPU Usage Tag Properties

Case 4: Why do I get the SNMP timeout exception?

SNMP requests are timed out for many reasons such as:

- Incorrect agent configuration: The community name may be different. SNMP mandates that the agents should accept requests only if the community string in the message matches its community name.
- The listening port of the agent might be different. Management applications communicate with the SNMP agents in the managed node on a particular port number. This remote port number is the UDP port 161.
- The agent may be slow in responding to the request. To solve this problem, you must increase the timeout value.
  The SNMP properties can be configured when adding a new device. You can edit the SNMP timeout and the community name of a device.

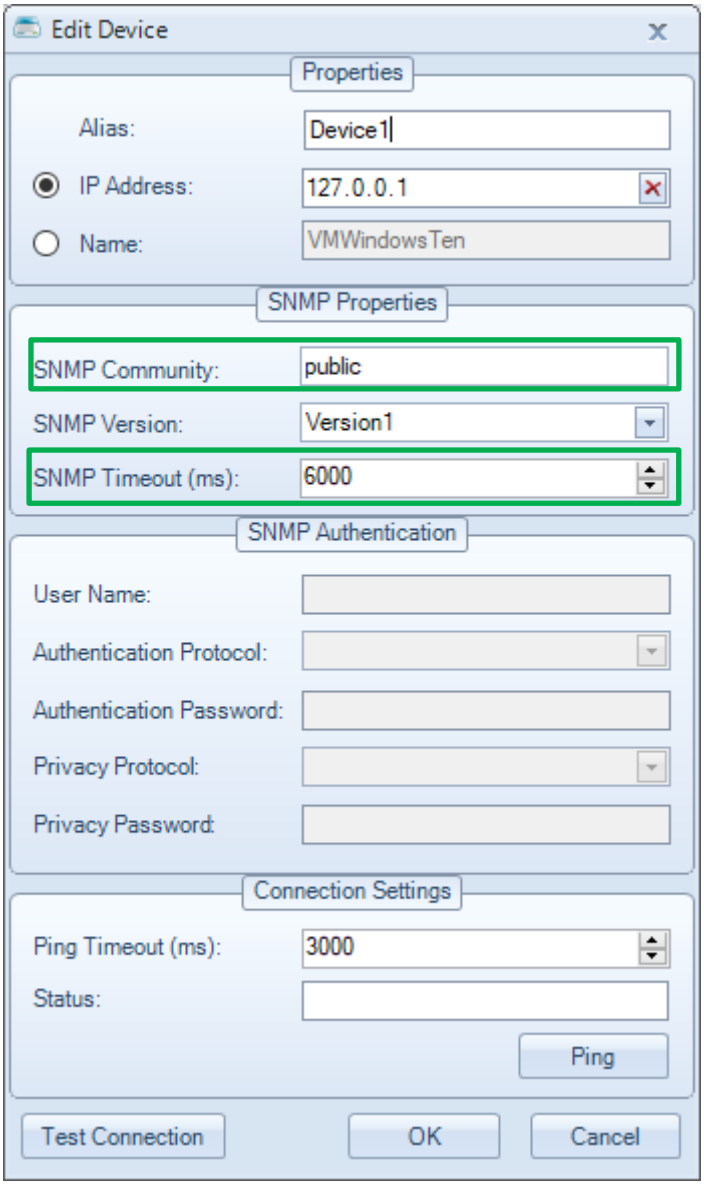

Figure 63: Edit Device Properties

Case 5: Why I am not getting trap tags?

To be able to receive trap messages, you need to add first the trap sender address and other parameters correctly in the list of agent down below. You also need to make sure to check the "Dynamic Trap Tags Generation" option.
When you enable this option the server will create dynamically the tags associated to the trap message (Please refer to the section Setting Menu for more details).

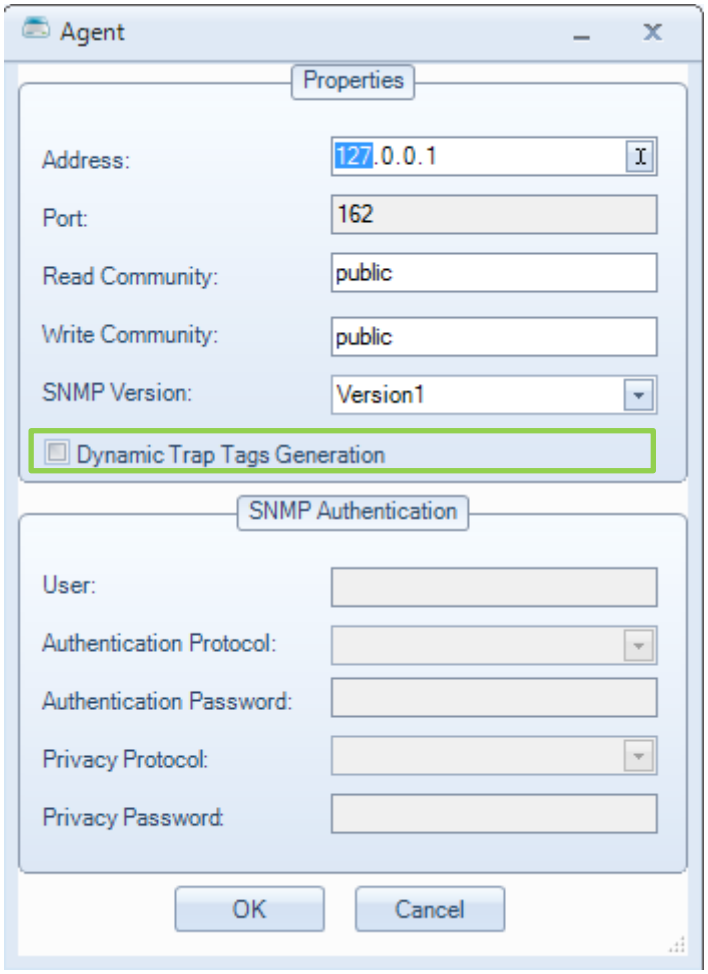

Figure 64: Agent properties

Case 6: The trap tags are not visible in the OPC Server for SNMP GUI.

In order to see the trap tag, you need to click the **Refresh** option available in the context menu of the "Address Space" node.

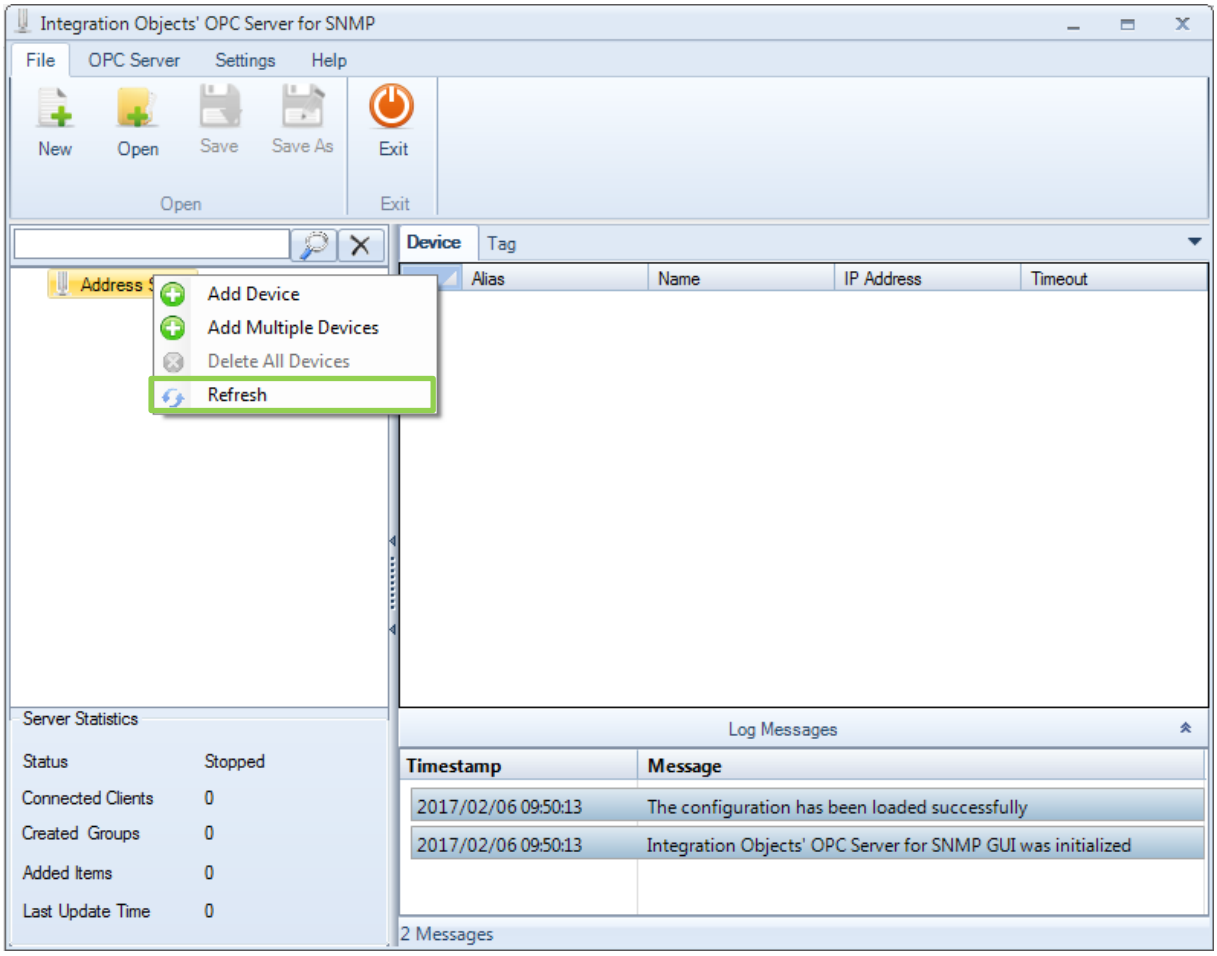

Figure 65: Refresh Option

SET UP WINDOWS SNMP SERVICE

1. Install SNMP Service

To install SNMP on Windows 7, follow the steps given below:

1. Click **Start** and go to the **Control Panel**, double-click **Programs and Features.**
2. Click **Turn Windows features on or off** in the left-hand side of the page.
3. Select the **Simple Network Management Protocol** check box, and click **OK.**

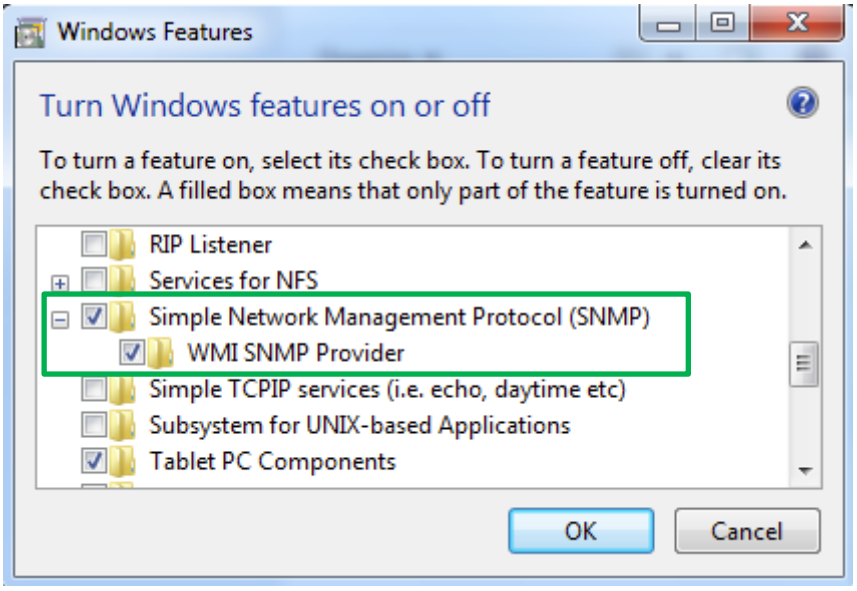

Figure 66: : Adding SNMP Feature

2. Configure SNMP Service

To configure SNMP agent, follow the steps below:

1. **Click on Start ➔ Control Panel ➔ System and Security ➔ Administrative Tools ➔ Services.**

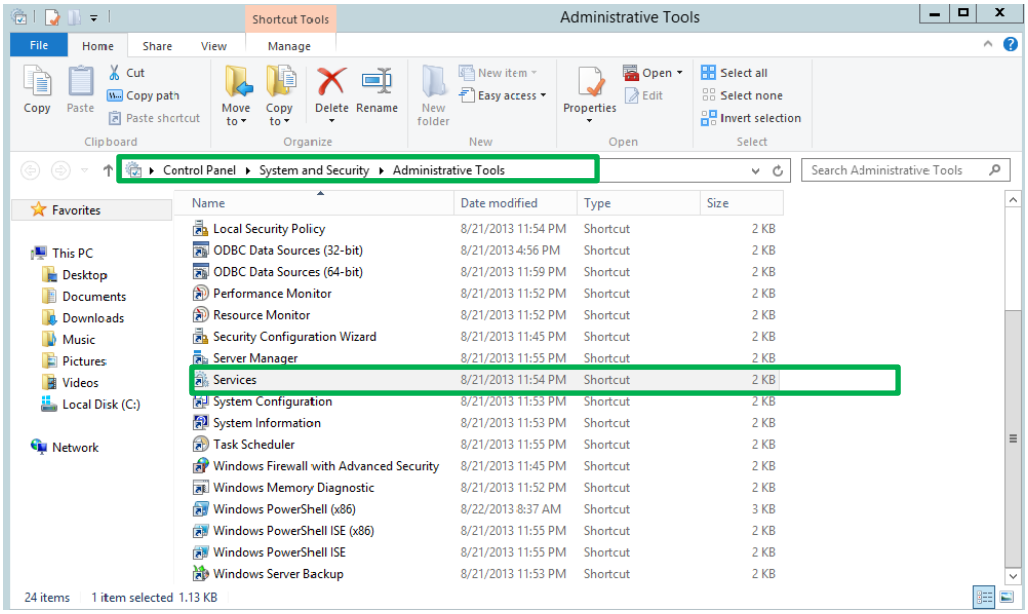

Figure 67: Windows Services

2. In the details pane, scroll down and click **SNMP Service**.
3. On the action menu, click **Properties**.

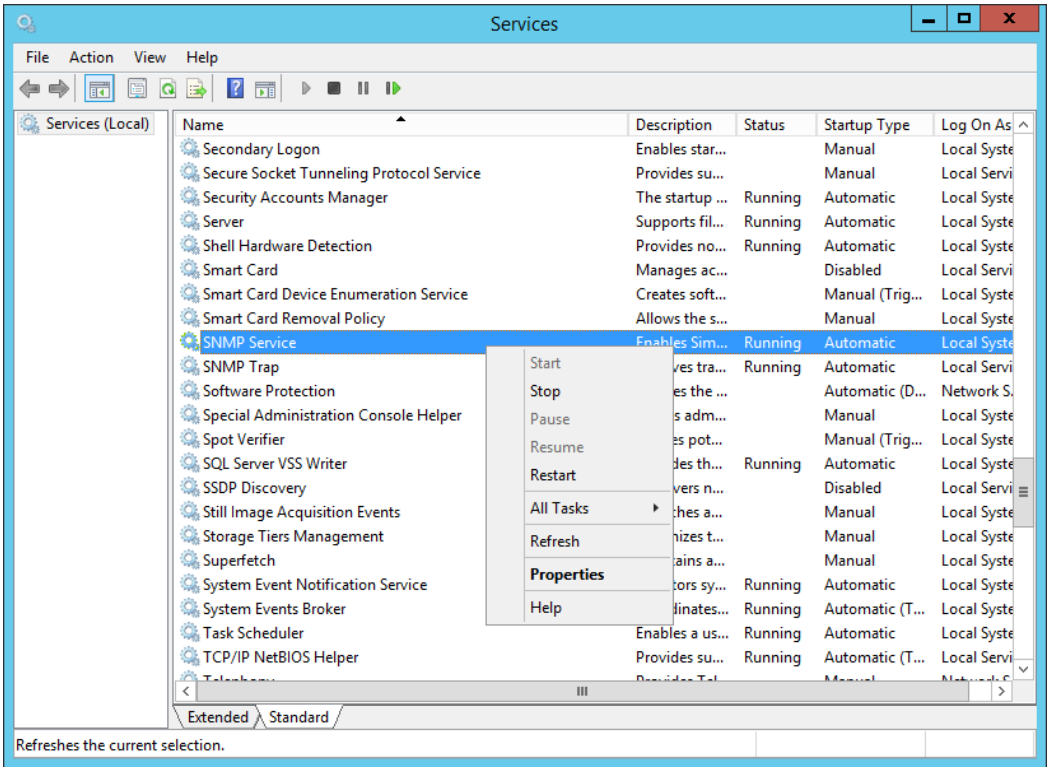

Figure 68: SNMP Service Action List

4. On the **Security** tab, select Send authentication trap if you want a trap message to be sent whenever authentication fails.

5. Under Accepted community names, click **Add**.
6. Under Community Rights, select a permission level for this host to process SNMP requests from the selected community.
7. In Community Name, type a case-sensitive community name, and then click **Add**.
8. Specify whether or not to accept SNMP packets from a host:
9. To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.
10. To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name and IP or IPX address, and then click **Add** again.
11. Click **Apply** to apply the changes, and restart the service.

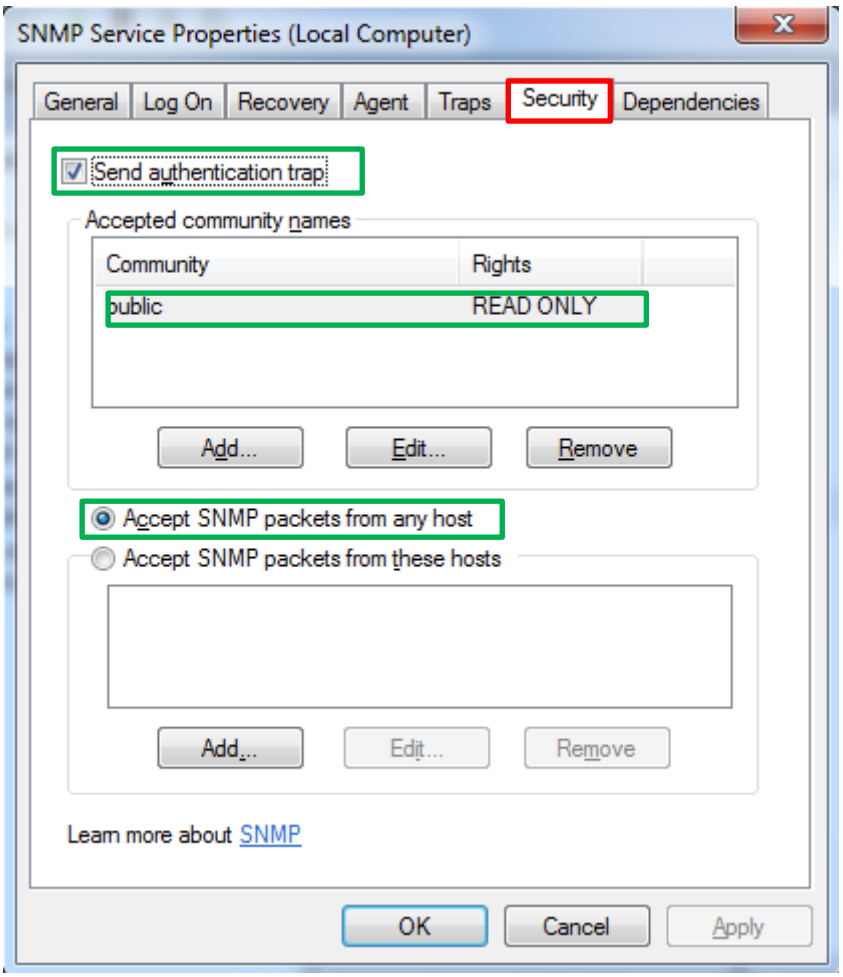

Figure 69: SNMP Service Properties

You must be logged in as an administrator or a member of the Administrators group to complete this procedure. If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

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