42. IIoT

This chapter explains how to use IIoT protocols.

42.1. MQTT

42.1.1. Overview

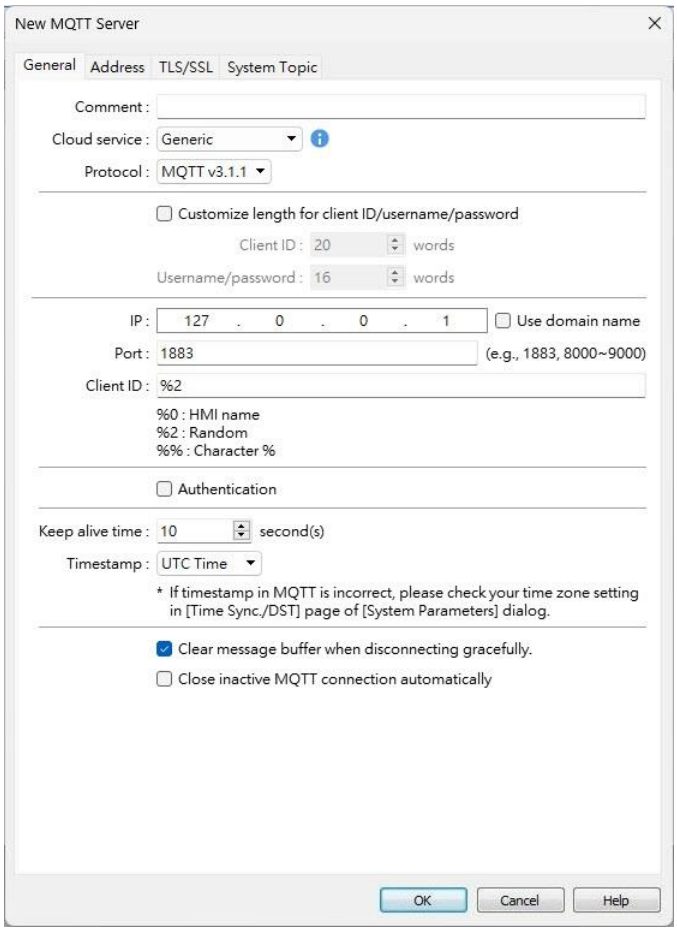
MQTT object can publish messages to an MQTT server, or subscribe to topics to receive messages from an MQTT server. HMI can serve as an MQTT server as well. When HMI serves as an MQTT server, it does not send message to another MQTT server.

42.1.2. Configuration

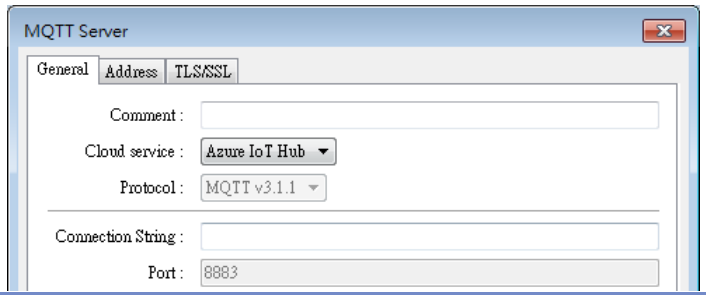
Click [Object] » [IIoT] » [MQTT] in the menu to open the settings dialog box.

42.1.2.1. Server Settings

General Tab

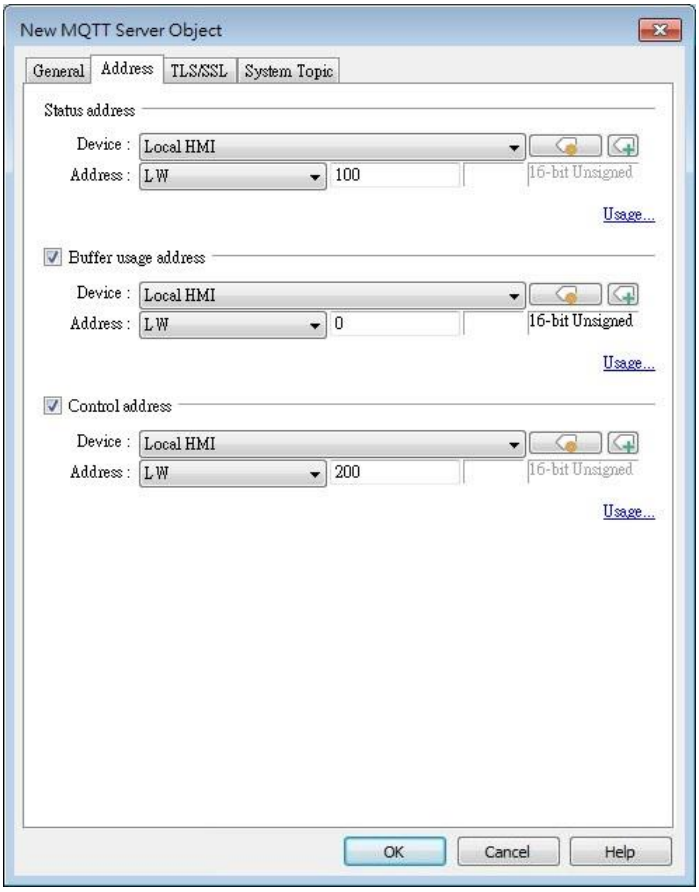


Setting	Description
Cloud service	**Generic** Use general MQTT publish-subscribe service. **AWS IoT** Use AWS IoT as a Broker, and use Thing Shadows service. For more information, please find “AWS IoT User Manual”. **Sparkplug B** Sparkplug B is a specification designed based on the characteristic features of IoT applications. It helps define topics and messages that are not specified by standard MQTT, and allows non-MQTT terminal devices to transfer data with MQTT Server through Edge of Network, which can be HMIs in this architecture. Please see “Sparkplug B Quick Start Guide” for more information.

	Azure IoT Hub Use Microsoft Azure IoT Hub as a Broker. Using this service can simplify setting step to entering a Connection String. The Connection String can be found in Microsoft Azure > IoT devices. 
Protocol	Supports MQTT v3.1, v3.1.1, and v5. (v5 is supported only for cMT / cMT X Series)
Customize length for Client ID/ username/password	Client ID: The upper limit is 128 words. Username/Password: The upper limit is 256 words.
IP	Enter the MQTT Server IP address for receiving the message. If 127.0.0.1 is entered, HMI will run a MQTT server locally.
Use domain name	A domain name can be used as MQTT server's IP address.
Port	Enter the MQTT Server port number for receiving the message.
Client ID	Enter the Client ID. Variables can be used for Client ID, for example, entering %0 will make the HMI Name to be the Client ID.
Authentication	If selected, connecting MQTT Server will require [Username] and [Password].
Username	Enter the username for connecting MQTT Server.
Password	Enter the password for connecting MQTT Server.
Keep alive time	When MQTT Server does not receive the message from HMI passing the specified time, the HMI will be identified as disconnected. Note: When running simulation, the message may be delayed, but the delay will not exceed the [Keep alive time]. The message from the HMI will be sent immediately.
Timestamp	**Local time**

	Use local HMI time for timestamp. **UTC time** Use UTC+0 (coordinated universal time) for timestamp. When the timestamp is shown incorrectly, please go to [System Parameters] » [Time Sync. / DST] tab to set the time zone.
Clear message buffer when disconnecting gracefully	This option is selected by default. With it selected, when disconnecting gracefully (by entering 2 for the command in MQTT's control addresses), message buffer will be cleared. Messages in the buffer will be retained when this option is not selected.
Close inactive MQTT connection automatically	In this mode, the connection will be automatically terminated if there's no data update for a specified period of time. The connection will resume once any data update occurs. The user can choose to publish initial values / topic list only at the first connection. In this mode, the start and stop commands are disabled.

Address Tab



Setting	Description
Status address	LW-n: Displays the connection status to MQTT Server.

Value	Description
0	Not attempting to connect to MQTT Server.
1	Disconnected and can’t connect to MQTT Server.
2	Connection succeeded.

LW-n+1: Error indicator.

Value	Description
0	No error
1	Unknown error
2	Failed to connect
3	Access denied
4	Not allowed port number for built-in MQTT server

5	Unresolvable domain name
6	Buffer overflowed
32	Incorrect client ID
48	Failed to verify certificate
256	Still connecting

Buffer usage address

Messages that have not been sent are stored in the buffer. The maximum buffer capacity is 10000 messages. The buffer capacity is measured in percentage (%), rounded up.

LW-n: Shows buffer usage.

Control address

LW-n: Controls the operation of MQTT Server.

Value	Description
0	Ready
1	Start
2	Stop
3	Update

LW-n+1: Sets the IP address of MQTT Server.

LW-n+5: Sets the port number of MQTT Server.

LW-n+6: Sets the Client ID for connecting MQTT Server.

LW-n+26: Enables / Disables authentication.

Value	Description
0	Disable
1	Enable

LW-n+27: Sets the username for connecting MQTT Server.

LW-n+43: Sets the password for connecting MQTT Server.

LW-n+59: Sets the domain name for connecting MQTT Server.

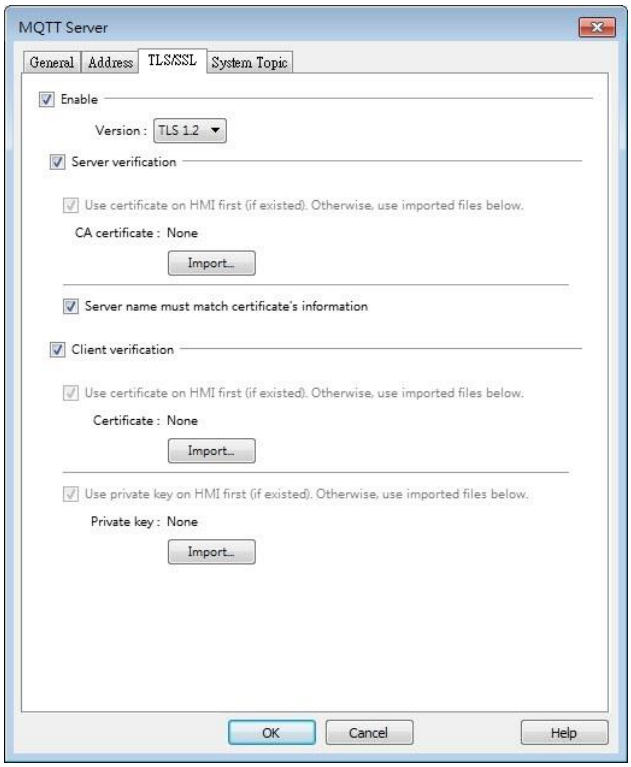
When Azure IoT Hub is used, the control addresses are as below:

LW-n: Controls the operation of MQTT Server.

Value	Description
0	Ready
1	Start
2	Stop
3	Update

	LW-n+1: Sets the Connection String (128 words).

TLS/SSL Tab

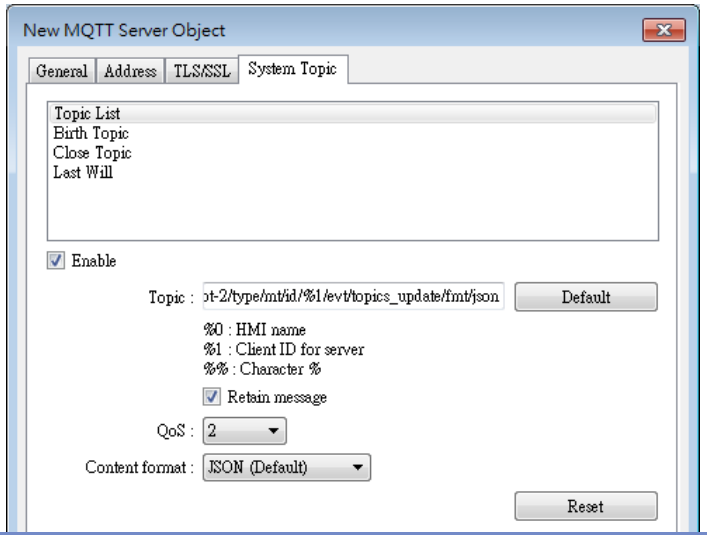


Setting	Description
Enable	Enable TLS/SSL authentication. TLS version can be selected from: TLS 1.0, TLS 1.1, and TLS 1.2. To use TLS 1.1 and TLS 1.2, HMI OS version must be 20180323 or later.
Server verification	**Enable** Verify whether the server certificate is signed by CA (Certificate Authority). Server certificate is sent from server during connection. **Server name must match certificate's information** Verify whether the server's domain name or IP matches the records in the server certificate. Domain name and IP records are stored in Subject Alternative Name of the certificate.
Client verification	Private key and client certificate is required for server to authenticate the client.

System Topic

Several system topics can be enabled for HMI to publish. When a system topic is enabled for an

HMI, the subscribers of that topic can view the list of available topics and connection status of that HMI.



Setting	Description
Topic List	List of topic sent from HMI to the server upon connection.
Birth Topic	The message sent from the HMI after it is connected to the server.
Close Topic	The last message sent from the HMI before it disconnects knowingly from the server.
Last Will	The message received by the subscriber to Last Will when connection between HMI and server is lost ungracefully. HMI updates its Last Will message when it connects to the server.
Topic	The actual topic name of the system topic.
Retain Message	When this checkbox is selected, the MQTT server will save the latest message.
QoS	MQTT provides three levels of reliability, which are known as quality of service (QoS). The reliability of the message determines the persistence of the message. QoS 0: At most once, messages are not persistent. QoS 1: At least once. QoS 2: Exactly once.
Content Format	JSON (Default): Use default content. The following are the defaults of each system topic. Actual context-dependent values are shown in red:

Topic list:

```
{
    "d" : {
        "topics" : [
            {
                "compression" : "Compression Type",
                "nickname" : "Topic Name",
                "topic" : "Topic"
            },
            {
                "compression" : "Compression Type",
                "nickname" : "Topic Name",
                "topic" : "Topic"
            }
        ]
    },
    "ts" : " Current Time "
}
```

Contents in the topics vary according to the actual topic settings. The above is an example for the case of two topics.

Birth Topic:

```
{
    "d":{
        "connected":true
    },
    "ts":"Current Timestamp"
}
```

Close Topic:

```
{
    "d":{
        "connected":false
    },
    "ts":" Current Timestamp"
```

```
}

Last Will:
{
    "d":{
        "connected":false
    }
}
```

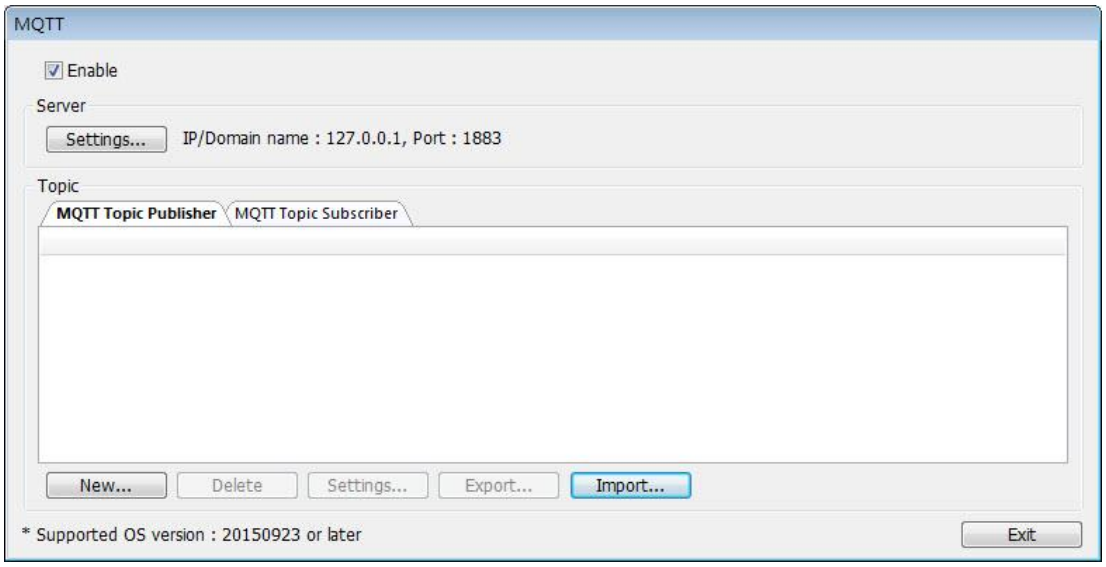
JSON (Advanced): Use user-defined content.

Note

- Please note that System Topics tab is not supported when using Sparkplug B and Azure IoT Hub cloud services.

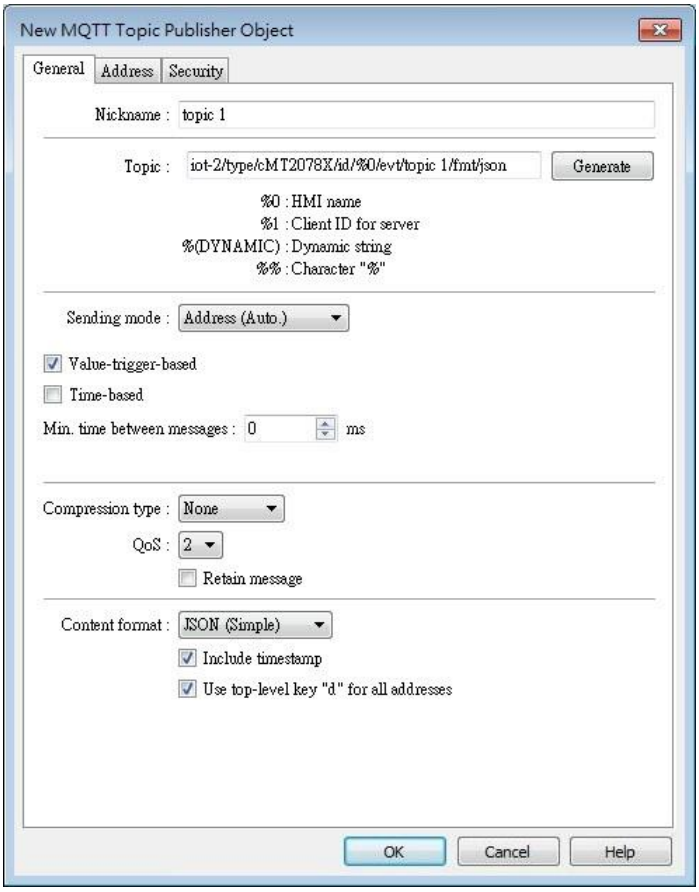
Click the icon to watch the demonstration film. Please confirm your internet connection before playing the film.

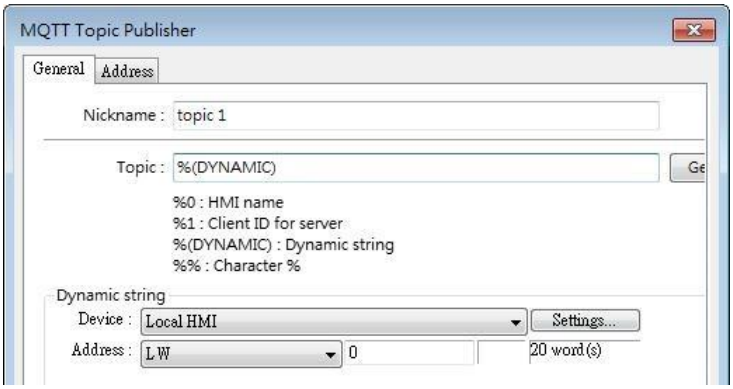
42.1.2.2. MQTT Topic Publisher

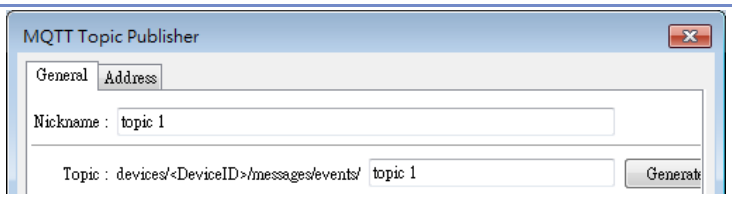


Click [New] to open General and Address settings, or click [Import] / [Export] to import or export an existing *.csv file. The maximum allowable number of topics is 255.

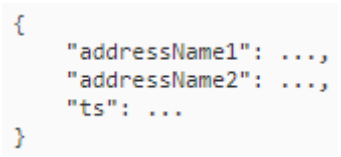
General Tab



Setting	Description
Nickname	Enter the nickname of the MQTT Topic for easier reference.
Topic	Specify the format of the message topic sent to MQTT Server. Variables can be used for Topic. Entering %(DYNAMIC) in the Topic field opens Dyanmic String group box for designating a word address. %(DYNAMIC) can include multiple topic levels. For example: myhome/groundfloor.  When Azure IoT Hub is used, users can only specify the last topic level.

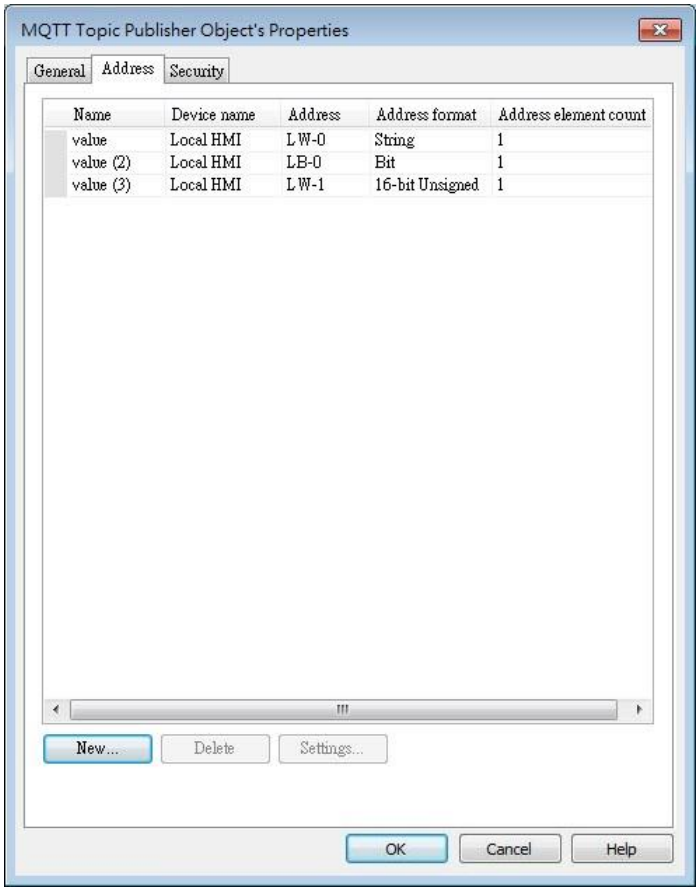


Sending mode	**Address (Auto.)** Value-trigger-based: Sends MQTT message when any value changes. Time-based: Sends MQTT message in a time-based manner. Min. time between messages: Sends MQTT message in a specified time interval. When the value changes within a period of time shorter than the specified time interval, the message will be stored in the buffer and then sent after the set wait time. This prevents the publisher from sending messages too frequently. **Address (Bit trigger)** Sends MQTT message when a designated bit is triggered. **Event (Alarm) Log** The topic source can be an Event Log. MQTT message can be sent when a single event or any event in a specific category occurs.
Compression type	The message will be compressed before being sent, and decompression is needed before reading the message. Messages in MQTT can be compressed / decompressed in zlib, gzip, or with DEFLATE algorithm.
Retain message	If selected, the MQTT server will save the latest message.
Include timestamp	This option is available only when the format used is [JSON (simple)]. Selecting this option can include timestamp in the message.
Use top-level key “d” for all addresses	This option is available only when the format used is [JSON (simple)]. When selected, the message format is as below: `{ "d": { "addressName1": ..., "addressName2": ... }, "ts": ... }` When not selected, the message format is as below:

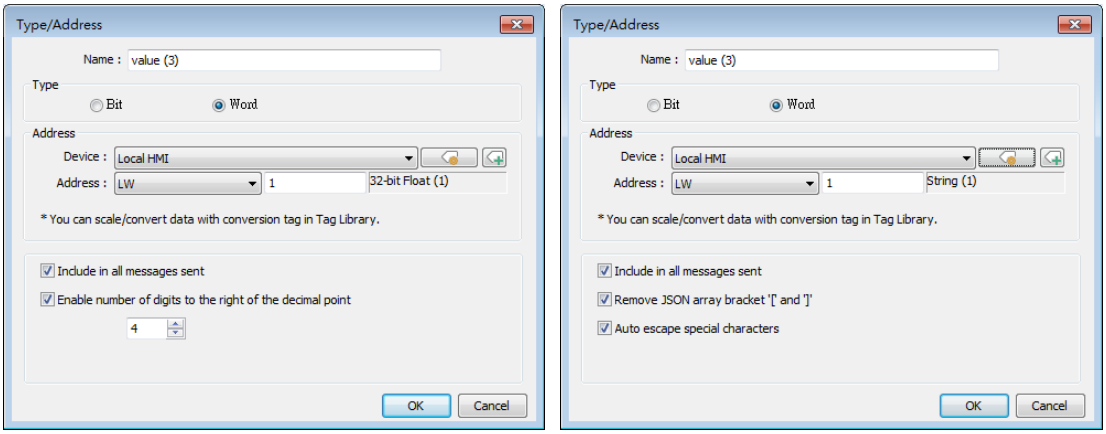
	 As shown in the above figure, when this option is not selected, ts and address names become keys of the same level. Therefore, please avoid using ts as an address name in this case.
QoS	MQTT provides three levels of reliability, which are known as quality of service (QoS). The reliability of the message determines the persistence of the message. 0: At most once, messages are not persistent. 1: At least once. 2: Exactly once.
Content Format	The supported formats are: Raw Data: Data in bytes. JSON (Simple): JSON format with all data put in JSON member “d”. JSON (Advanced): JSON format with flexible JSON structure.

Address Tab

The following explains the address settings for [Raw Data] and [JSON (Simple)] content formats.



Setting	Description
New	Add the source of the topic. The length of each address can be specified respectively.
Delete	Delete the address.
Setting	Change the name and address.



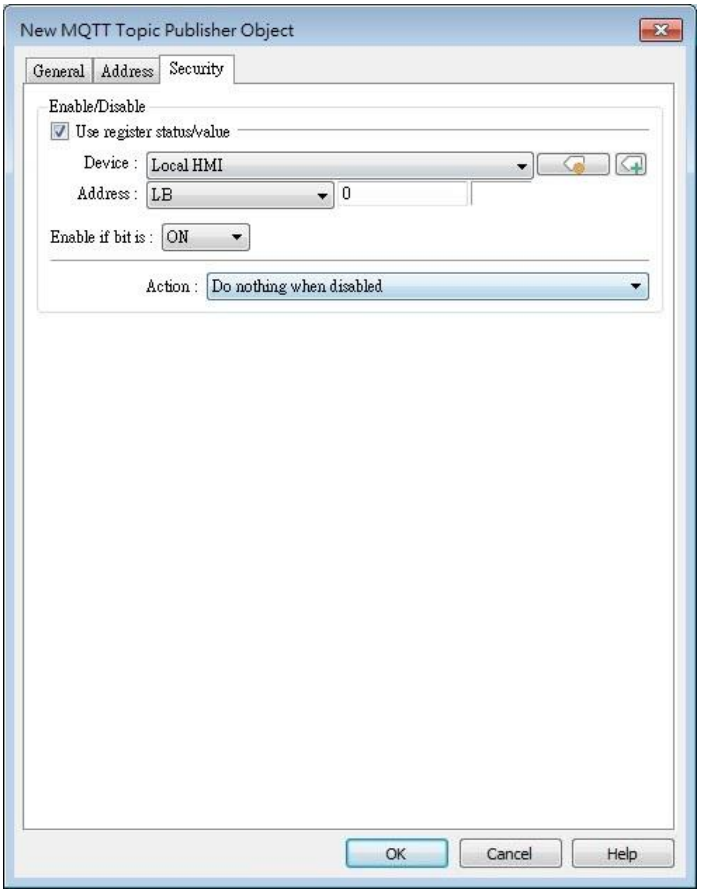
Setting	Description
Include in all messages sent	When the value from one of the source addresses changes, the data in this address can be included in

	all the messages sent. This option is available when the content format is [JSON (Simple)] or [JSON (Advanced)].
Remove JSON array bracket "[" and "]"	For JSON formatted messages, selecting this option can remove bracket "[" and "]". This option is available when the content format is [JSON (Simple)].
Enable number of digits to the right of the decimal point	When data type is Float, the number of digits after the decimal point can be specified. This option is available when the content format is [JSON (Simple)] or [JSON (Advanced)].
Auto escape special characters (cMT / cMT X Series)	This option is available when the data type is String, and the content format is [JSON (Simple)]. JSON formatted messages may contain special characters (e.g. " and \) which can lead to JSON parsing errors. With this option selected, special characters in a string can be escaped (e.g. change from " to \" and change from \ to \\) for successful message parsing.

Note

- Maximum tag length: 255 words.

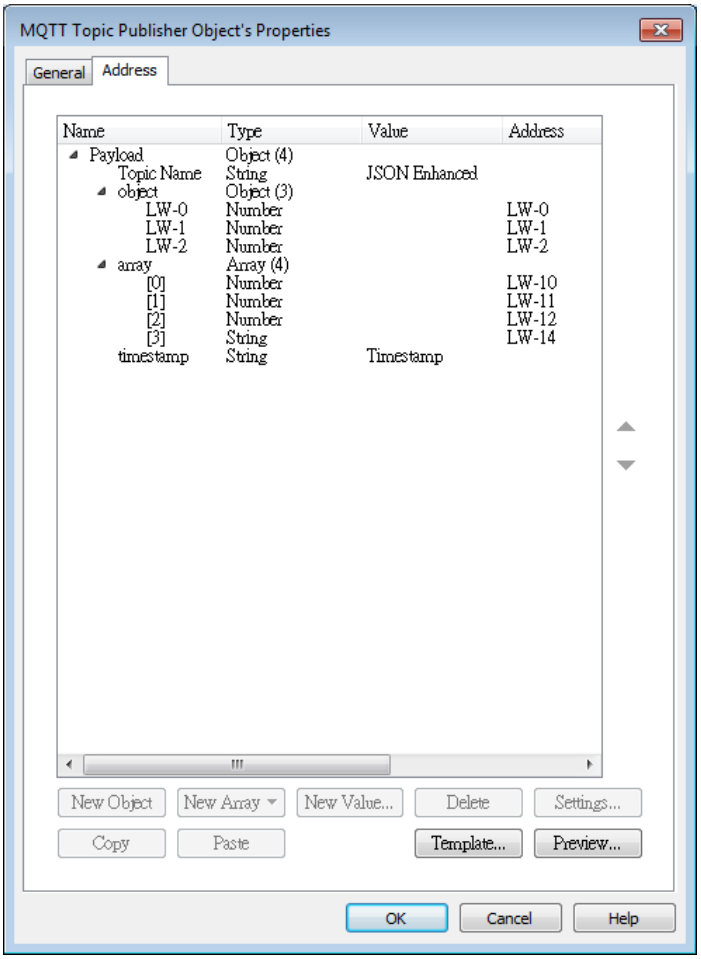
Security Tab



Messages will be published only when the state of the designated address meets the set condition. As shown above, the message will be published when LB-0 is ON.

Address Tab [JSON (Advanced)]

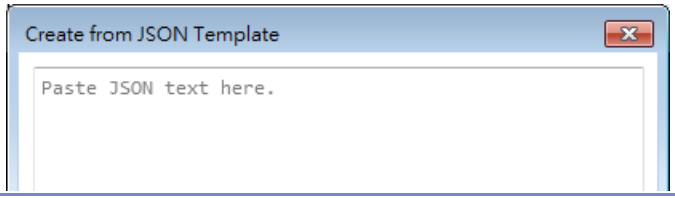
The following explains address settings for [JSON (Advanced)] content format. This is a nested format that allows using objects or arrays, and customizing timestamp and data name. Using this format provides a more flexible way of using MQTT.



When configure the settings as shown in the above screenshot, the received MQTT message by the subscriber is as below.

```
{
  "Topic Name" : "JSON Enhanced",
  "Object" : {
    "LW-0" : [ 1 ],
    "LW-1" : [ 2 ],
    "LW-2" : [ 3 ]
  },
  "Array" : [ [ 4 ], [ 5 ], [ 6 ], [ "AABBCCDD" ] ],
  "timestamp" : "2019-02-19T06:52:13.846038"
}
```

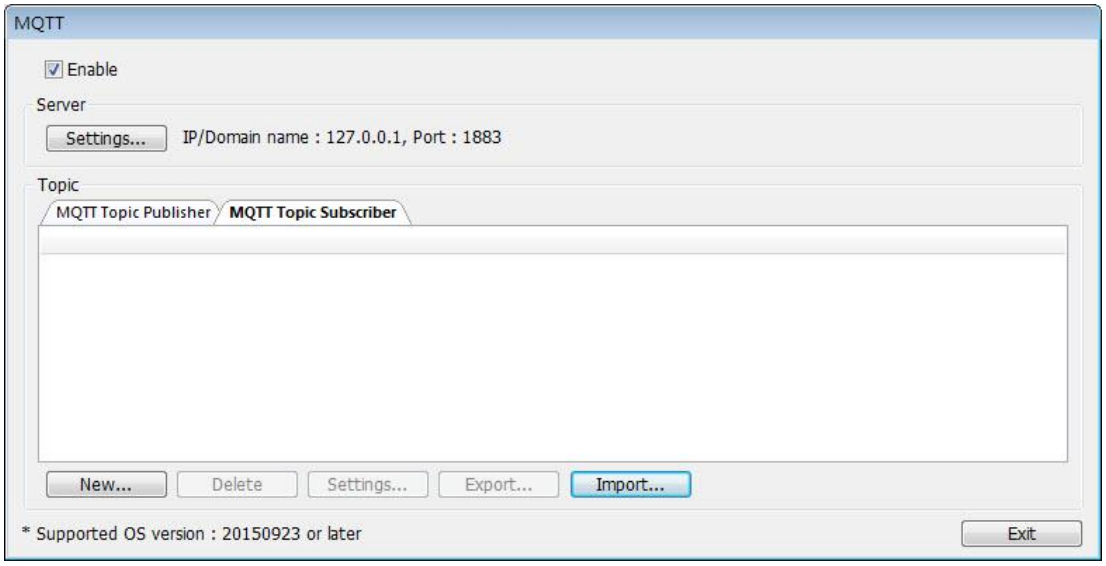
Setting	Description
New Object	Add a new object. The name, type and value of each item under the object can be configured. Items under the object are enclosed in curly brackets { }.
New Array	Add a new array. An array may contain multiple items but the name of the item is automatically generated and is unchangeable. Items under the array are enclosed in square brackets [].
New Value	Add a new number, string, or timestamp. When the

	new value is a number or a string, fixed value can be selected, or an address can be designated as the data source.
Delete	Delete the selected item.
Settings	Configure the selected item. When the selected item is an object or an array, the user may only change its name. When the selected item is contained in an object or an array, its parameters can be configured.
Copy	Copy the selected item.
Paste	Paste the copied item to the selected row.
Template	By pasting JSON string into the window, the system will automatically adjust the data structure setting according to JSON structure, saving time for users. 
Preview	Preview the JSON data in a reader-friendly format.

Note

- Maximum number of nodes for a Topic is 512 (payload included). Maximum tag length is 255 words.

42.1.2.3. MQTT Topic Subscriber

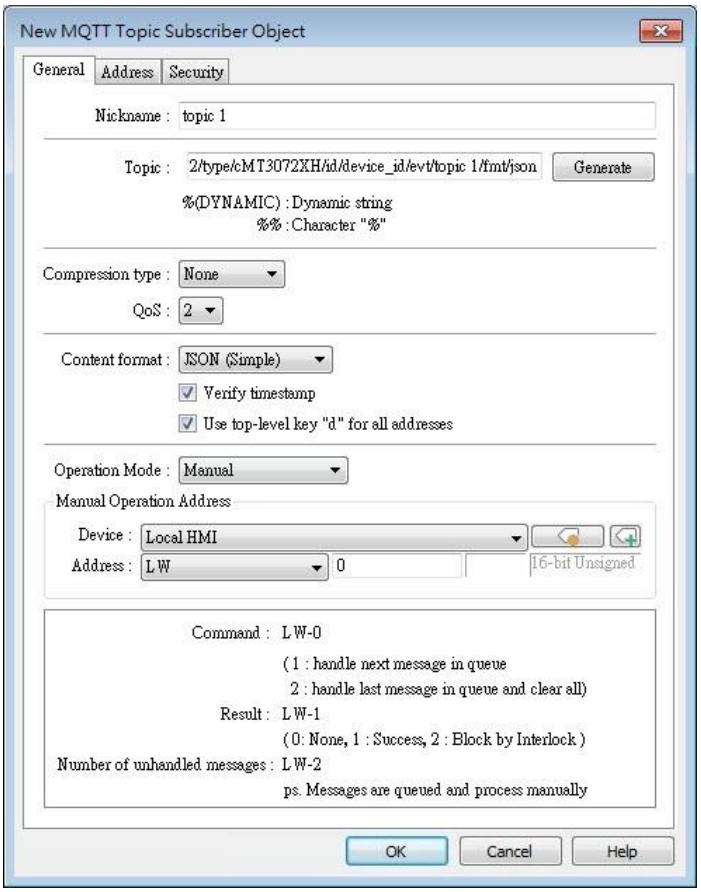


Click [New] to open General and Address settings, or click [Import] / [Export] to import or

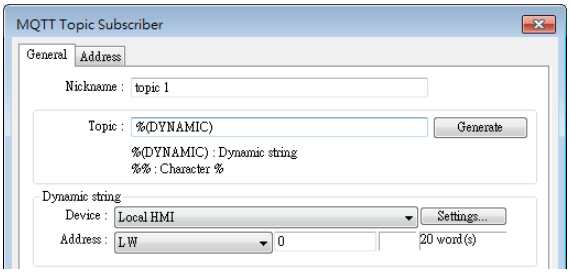
export an existing *.csv file. The maximum allowable number of topics is 255.

General Tab

The following explains the address settings for [Raw Data] and [JSON (Simple)] content formats.



Setting	Description
Nickname	Enter the nickname of the MQTT Topic for easier reference.
Topic	Subscribe to a topic in MQTT Server. The topic name can be dynamic. Entering %(DYNAMIC) in the Topic field opens Dynamic String group box for designating a word address. %(DYNAMIC) can include multiple topic levels. For example: myhome/groundfloor.



When Azure IoT Hub is used, users can only specify the last topic level, and the topic level should be the same as in MQTT Topic Publisher.

Compression type	Configure with the same setting as MQTT Topic Publisher.
Verify timestamp	When timestamp is included in the message, selecting this option will verify whether the timestamp is increasing, and update will occur when the timestamp does increase; otherwise, the message will be treated as expired message and update will not occur.

Use top-level key "d" for all addresses	When selected, the message format is as below:
	`{ "d": { "addressName1": ..., "addressName2": ... }, "ts": ... }`
	When not selected, the message format is as below:
	`{ "addressName1": ..., "addressName2": ..., "ts": ... }`
	Please use appropriate setting according to the data source.

QoS	MQTT provides three levels of reliability, which are known as qualities of service (QoS). The reliability of the message determines the persistence of the message.

	0: At most once, messages are not persistent. 1: At least once. 2: Exactly once.
Content Format	Raw Data: Unformatted raw data. JSON (Simple): Single layer JSON format. JSON (Advanced): JSON format with user-defined JSON structure.
Operation Mode	Operation mode for subscribing topics can be selected. Process immediately: Write the value to the designated address immediately after receiving subscribed data. Manual: Place the subscribed data in a queue before processing the data manually. The queue can hold 100 records. **Control address (Manual)** LW-n: Command

Value	Description
1	Write the oldest data in the buffer to the designated address. If there are 10 records in the buffer, the user can enter command 1 for ten times to write the data to the address sequentially.
2	Write the latest data in the buffer to the designated address, and then clear all data in the buffer.

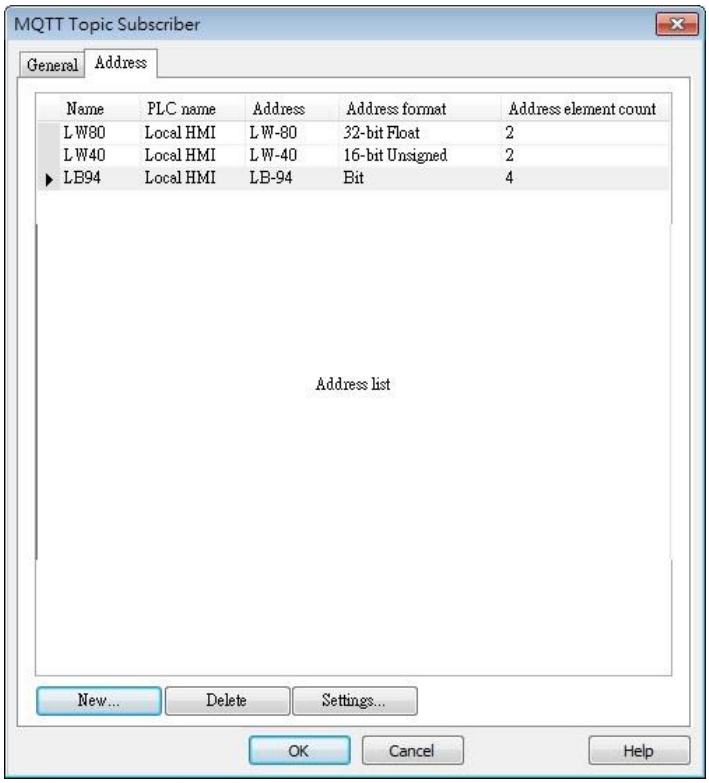
LW-n+1: Execution Result

Value	Description
0	The buffer is currently empty.
1	The command is executed successfully.
2	The topic subscription is blocked so command execution failed. (See Security tab in this chapter.)

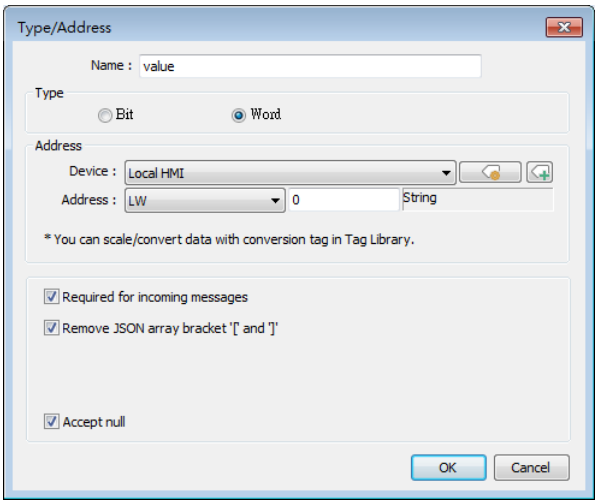
LW-n+2: Number of unhandled messages

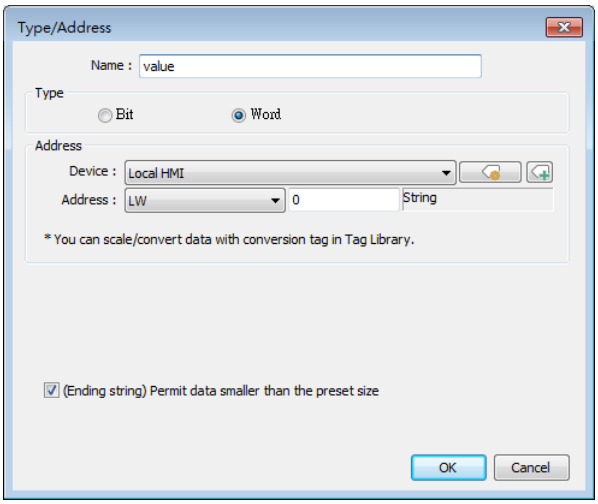
Displays the number of messages in the buffer.

Address Tab



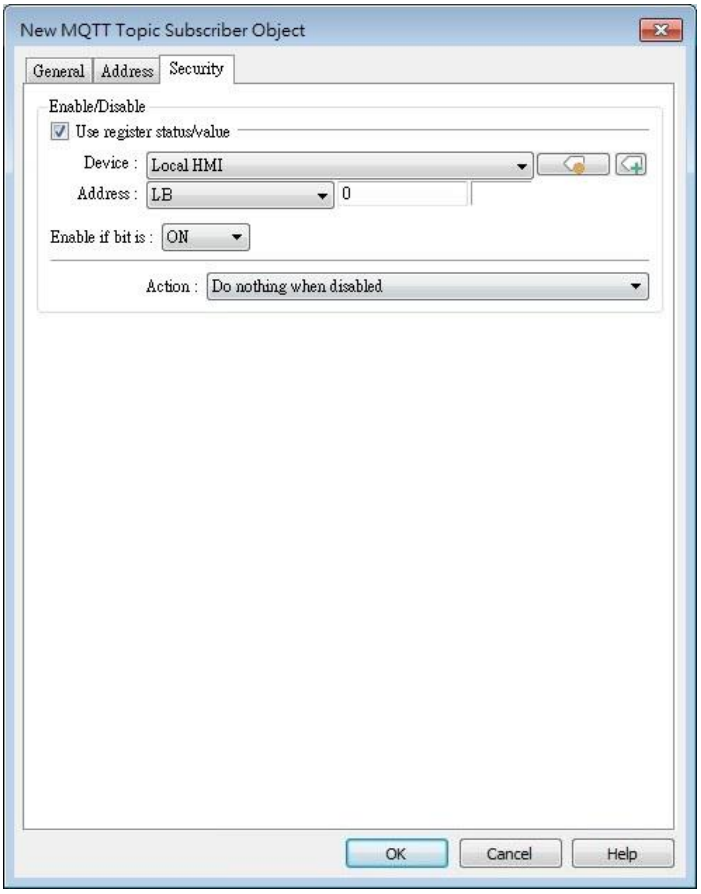
Setting	Description
New	Add the destination address of the subscribed topic. The length of each address can be specified respectively.
Delete	Delete the address.
Setting	Change the name and address.





Setting	Description
Required for incoming messages	When the value from one of the destination addresses changes, the data in this address must be included in all the messages received. This option is available when the content format is [JSON (Simple)] or [JSON (Advanced)].
Remove JSON array bracket "[" and "]"	For JSON formatted messages, selecting this option can remove bracket "[" and "]". This option is available when the content format is [JSON (Simple)].
Accept null	Null can be accepted. This option is available when the content format is [JSON (Simple)] or [JSON (Advanced)].
(Ending string) Permit data smaller than the preset size	A string that has a length shorter than the preset length can be accepted. This setting is effective only for the ending string, and it will not be effective when the string is followed by other values or bit data. This option is available when the content format is [Raw data].

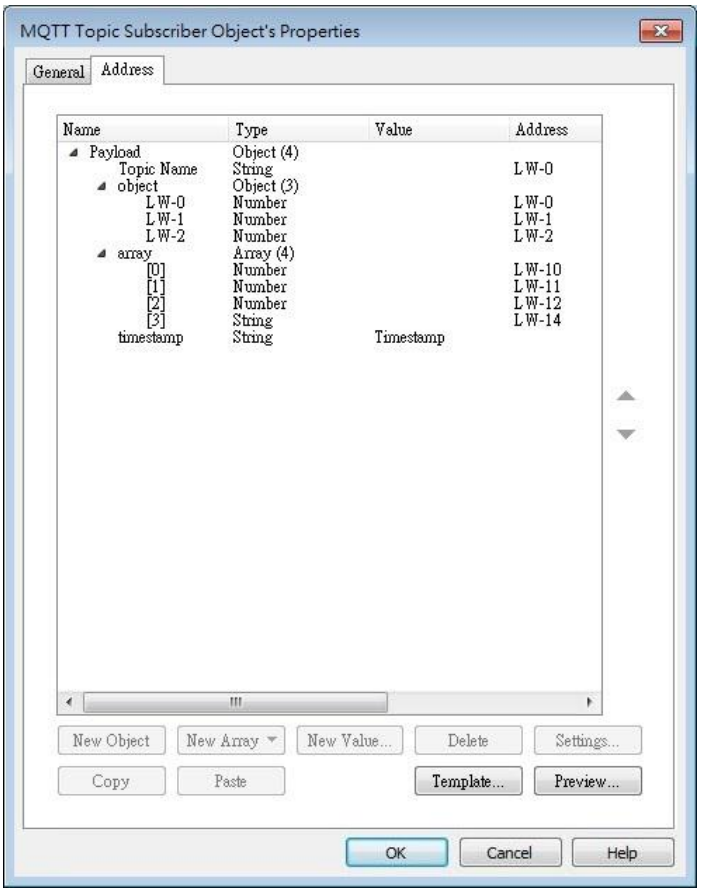
Security Tab



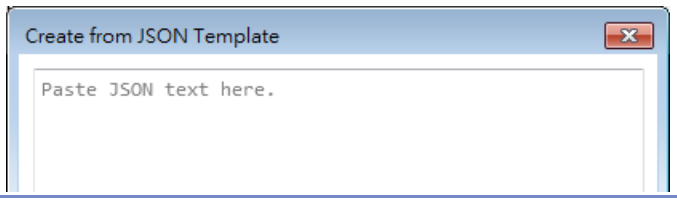
Messages will be subscribed only when the state of the designated address meets the set condition. As shown above, the message will be subscribed when LB-0 is ON.

Address Tab [JSON (Advanced)]

The following explains address settings for [JSON (Advanced)] content format. This is a nested format that allows using objects or arrays, and customizing timestamp and data name. Using this format provides a more flexible way of using MQTT.



Setting	Description
New Object	Add a new object. The name, type and value of each item under the object can be configured. Items under the object are enclosed in curly brackets { }.
New Array	Add a new array. An array may contain multiple items but the name of the item is automatically generated and is unchangeable. Items under the array are enclosed in square brackets [].
New Value	Add a new number, string, or timestamp. When the new value is a number or a string, fixed value can be selected, or an address can be designated as the data source.
Delete	Delete the selected item.
Settings	Configure the selected item. When the selected item is an object or an array, the user may only change its name. When the selected item is contained in an object or an array, its parameters can be configured.
Copy	Copy the selected item.
Paste	Paste the copied item to the selected row.

Template	By pasting JSON string into the window, the system will automatically adjust the content according to JSON structure, saving time for users. 

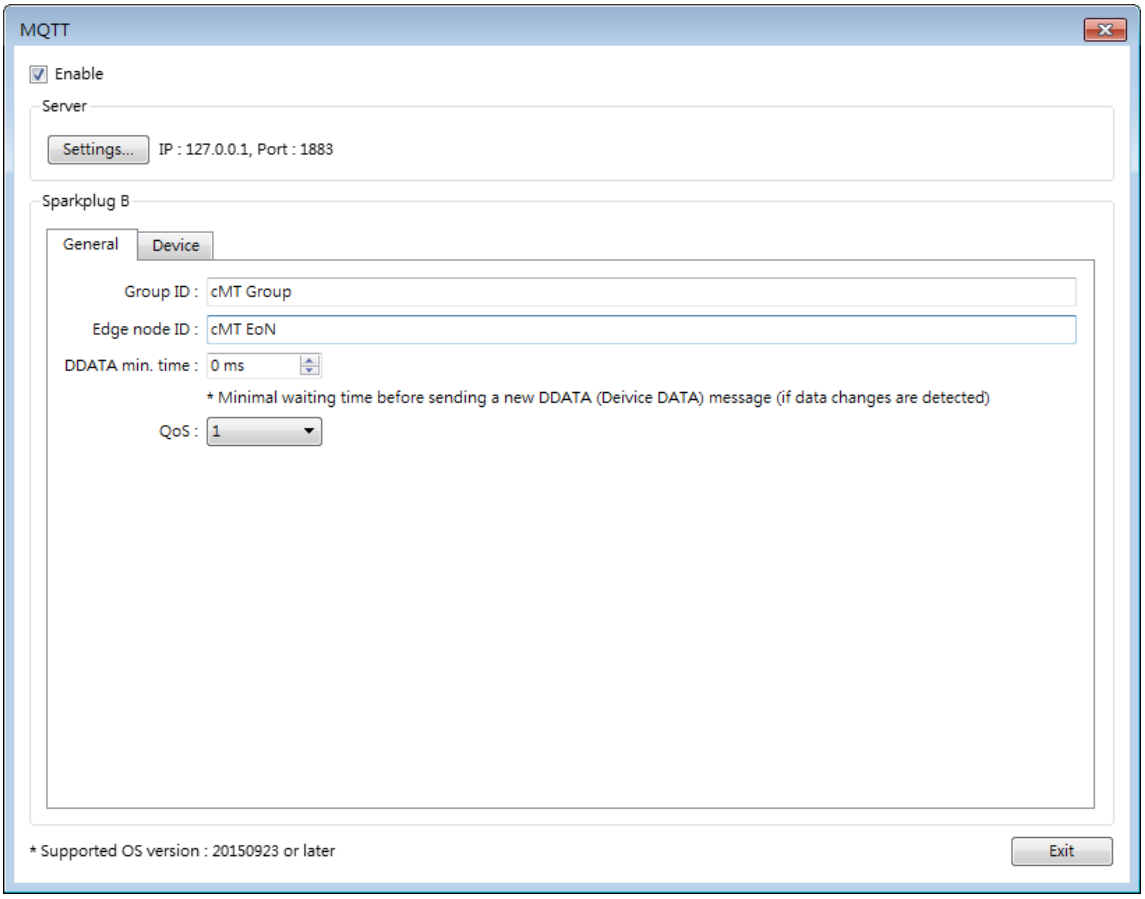
Note

- Amazon Web Service (AWS) IoT Core supports standard MQTT protocol. However, please note the following restrictions:
  1. The maximum number of layers in a topic is 8 (iot-2/type equals to 2 layers).
  2. Authentication in General tab is not supported, please use TLS/SSL.
  3. Supports only Qos 0 and Qos 1.
  4. Retaining the latest message in MQTT server is not supported.

42.1.2.4. Sparkplug B

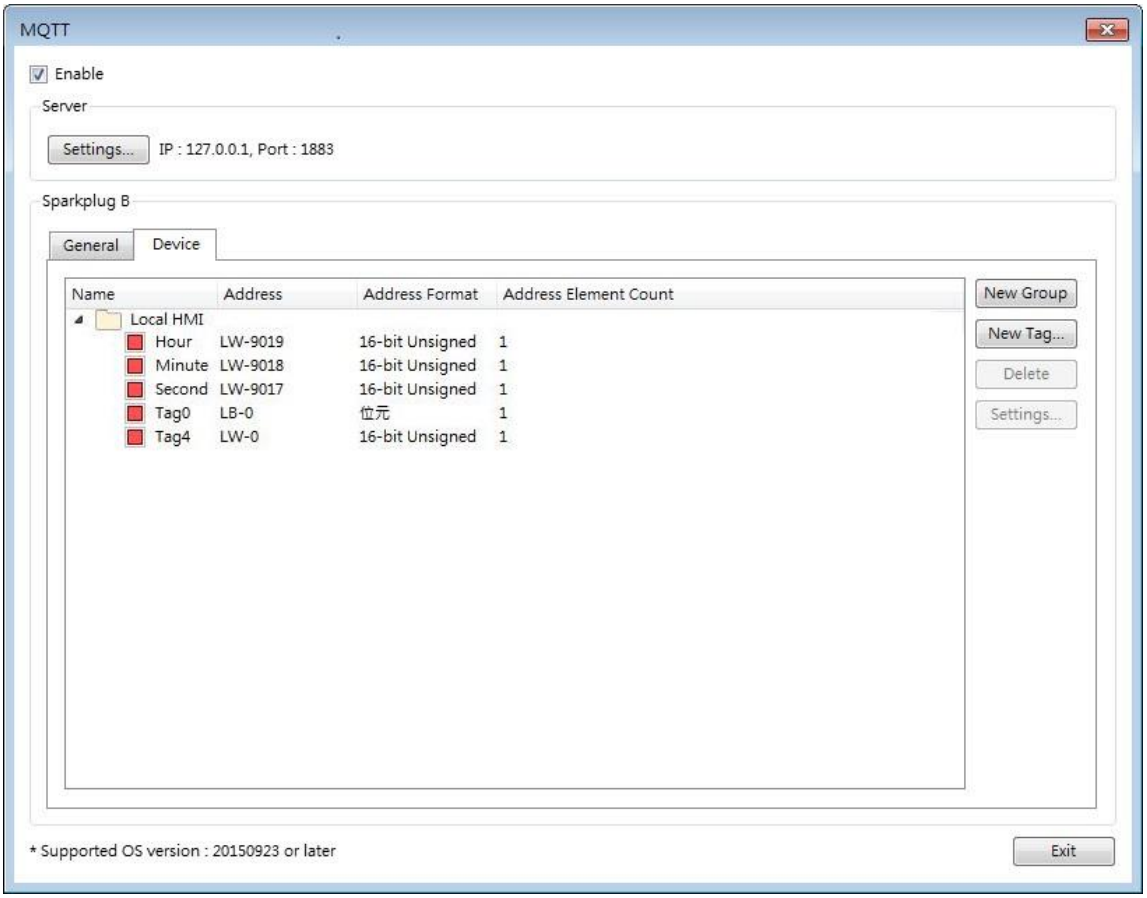
General settings and Device settings for cloud service Sparkplug B are as shown below.

General Tab



Setting	Description
Group ID	The group ID that identifies the group in which the Edge of Network Nodes belong to.
Edge ID	The ID that identifies a specific Edge of Network Node.
DDATA min. time	The minimum-wait-time duration before a new DDATA (Device DATA) message is sent when data change is detected.
QoS	MQTT provides three levels of reliability, which are known as qualities of service (QoS). The reliability of the message determines the persistence of the message. 0: At most once, messages are not persistent. 1: At least once. 2: Exactly once.

Device Tab



Setting	Description
New Group	Add a group to manage the tags.
New Tag	Add the tags of this EoN node monitored by MQTT engine. Please note that the Name field should not be blank.
Delete	Delete an existing group or tag.
Settings	Configure an existing group or tag.

Click the icon to download the demo project. Please confirm your internet connection before downloading the demo project.

42.2. OPC UA Server

42.2.1. Overview

OPC UA (Unified Architecture) is a communication technology often used in industrial automation fields. OPC UA features cross-platform interoperability, unified access, standardized communication, and security. In this architecture, cMT / cMT X Series HMI models with built-in OPC UA server play a key role as Communication Gateway, and allow OPC UA clients to access HMI or PLC data by subscribing to tags to receive real-time updates. This new architecture can help you achieve vertical integration.

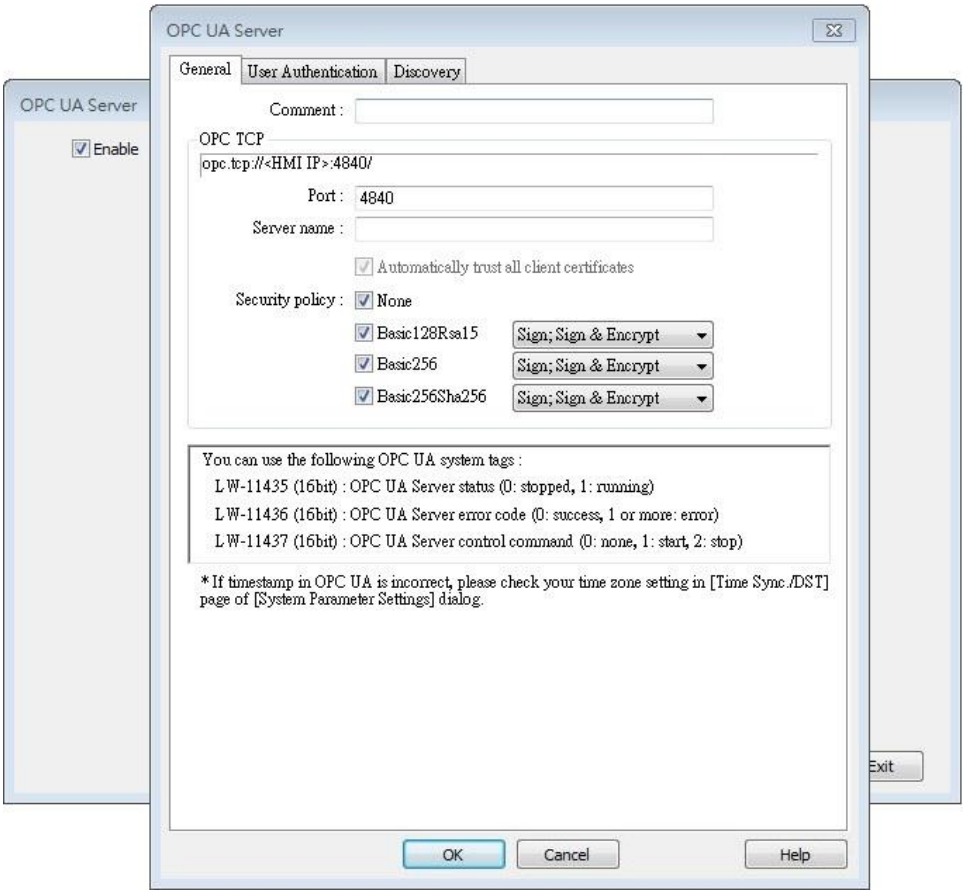
Hardware & Software requirements:

- HMI Model: cMT / cMT X Series models. *A license must be loaded for cMT-SVR / cMT-SVR-200 and cMT-HDM / cMT-FHD / cMT-FHDX.
- Software: EasyBuilder Pro V5.06.01 or later
- Recommended OPC UA Client: Unified Automation UaExpert

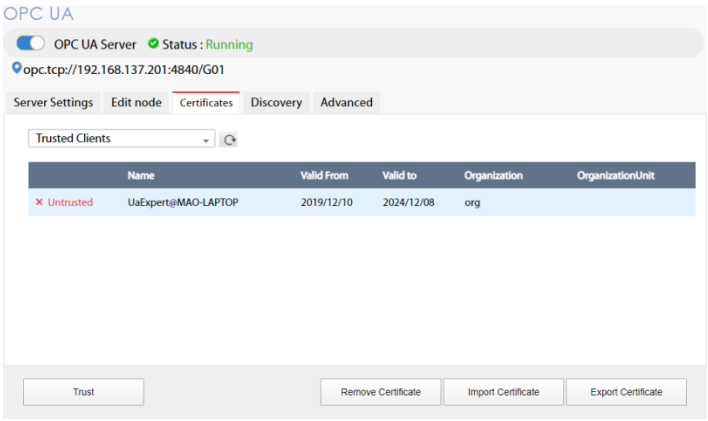
42.2.2. Configuration

Click [Object] » [IIoT] » [OPC UA Server] in the menu to open the settings dialog box.

General Tab



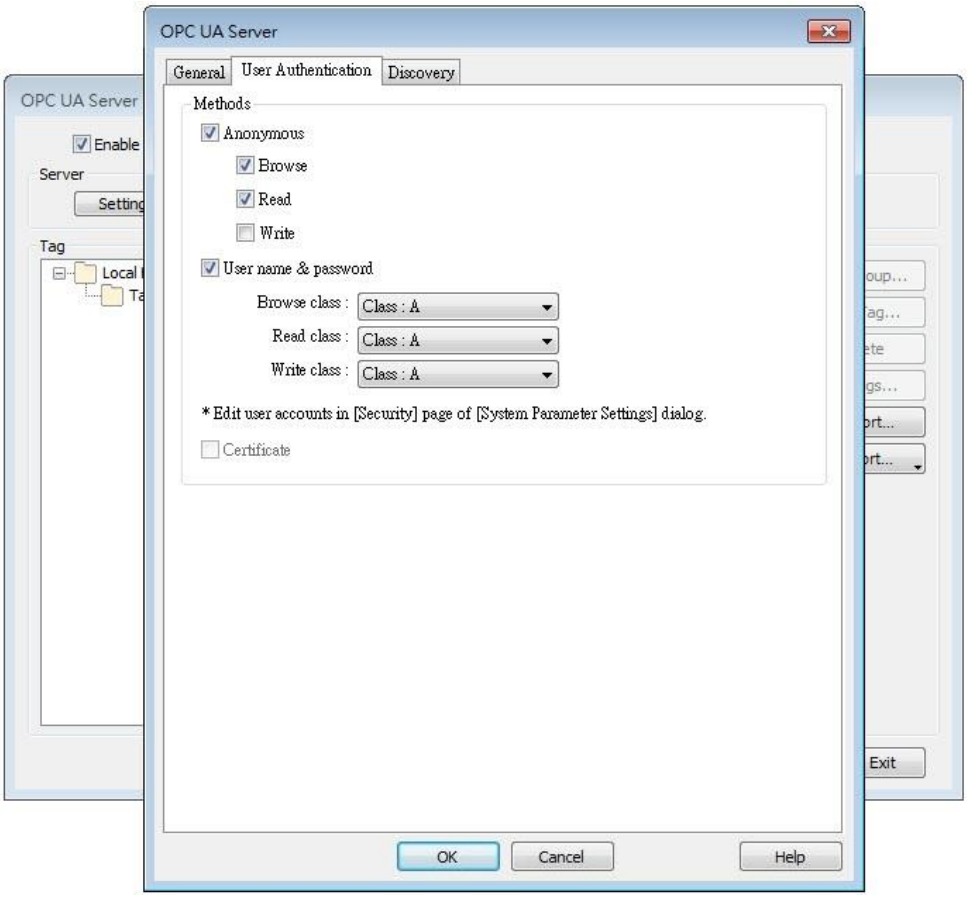
Setting	Description
Comment	The description about the OPC UA Server.
OPC TCP	The URL of the server.
Port	The port number for the clients to connect with OPC UA Server. The default port number is 4840.
Server name	The server name, this field is allowed to remain blank. **[Automatically trust all client certificates]** This option is enabled by default, but may be toggled for cMT Gateway series only. When this option is disabled, all OPC UA clients will be refused connection unless their corresponding client certificates have been trusted in the OPC UA web interface like shown below:

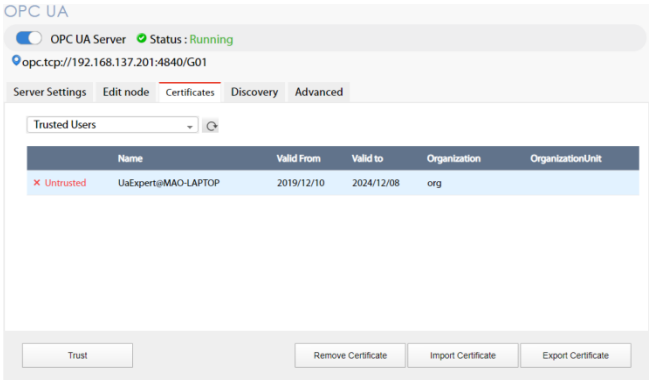


Note: According to OPC UA specification, an OPC UA client, in making a connection, will use a client certificate which will be checked by the OPC UA server for its legitimacy. The exception is if the security policy allows for the “None” option.

Security Policy	Configure the security policy and available algorithms that can be used by clients.

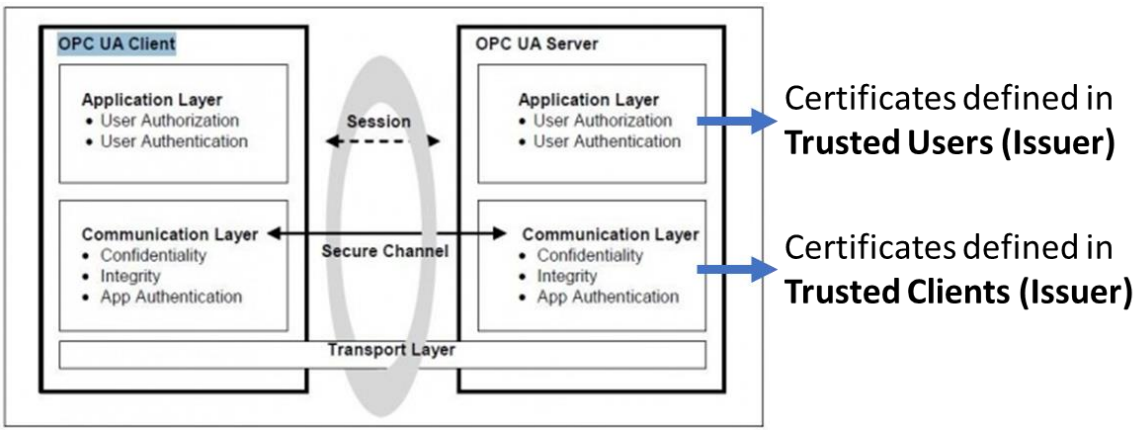
User Authentications Tab



Setting	Description
Methods	**Anonymous** Grant Browse, Read, Write permissions to anonymous login by selecting the checkboxes. **User name & password** Use the same user name and password as HMI. The permissions are granted to the security classes specified in System Parameter Settings » Security. **Certificate** This option is available only for cMT Gateway series. OPC UA client may use certificates as authentication method instead of username-and-password method to login. Use web interface to configure trusted/untrusted user certificates, as shown below: 

Note

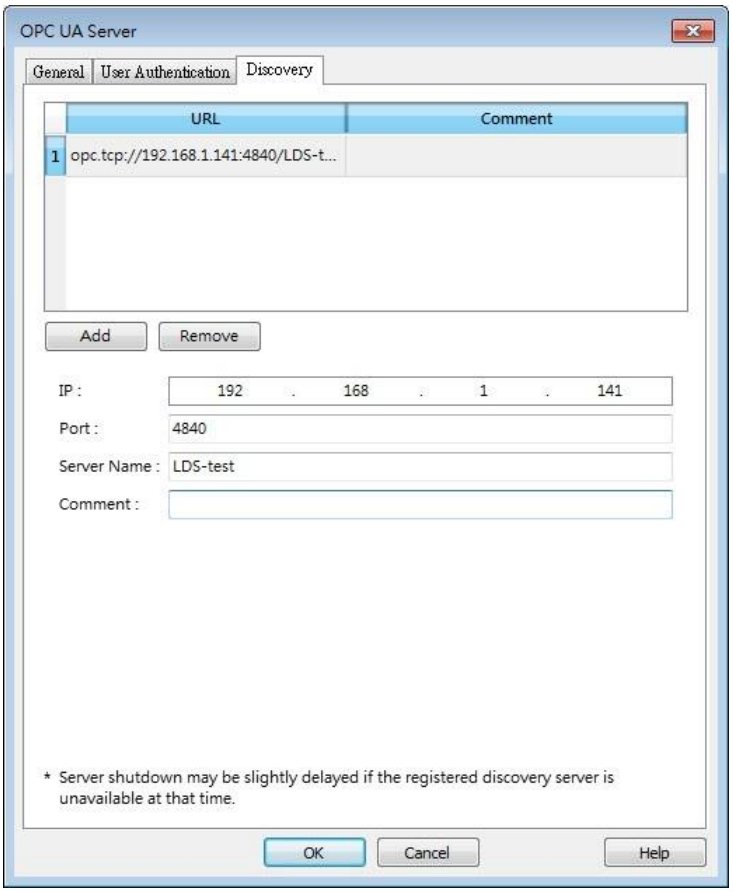
- OPC UA security layers can be split into
  (1) communication layer (e.g. SecurityPolicy)
  (2) application layer, as shown in the image below:



Security Layers (from http://wiki.opcfoundation.org/index.php/File:SecurityLayers.jpg)

- Client certificate is at communication layer and its use is required when using SecurityPolicy other than None.
- User certificate is at application layer and using it is one of the ways for authentication.

Discovery Tab



When configured, OPC UA server will register to the Local Discovery Server (LDS).

OPC UA Discovery service is used to simplify server location maintenance when there are many OPC UA servers in the network. An OPC UA client can access one LDS Server and obtain all registered OPC UA server.

Setting	Description
IP	IP address of the OPC UA client.
Port	Port number used by the OPC UA client.
Server Name	Server name of the OPC UA client.
Comment	A memo on the server and will not influence communication.

Example 1

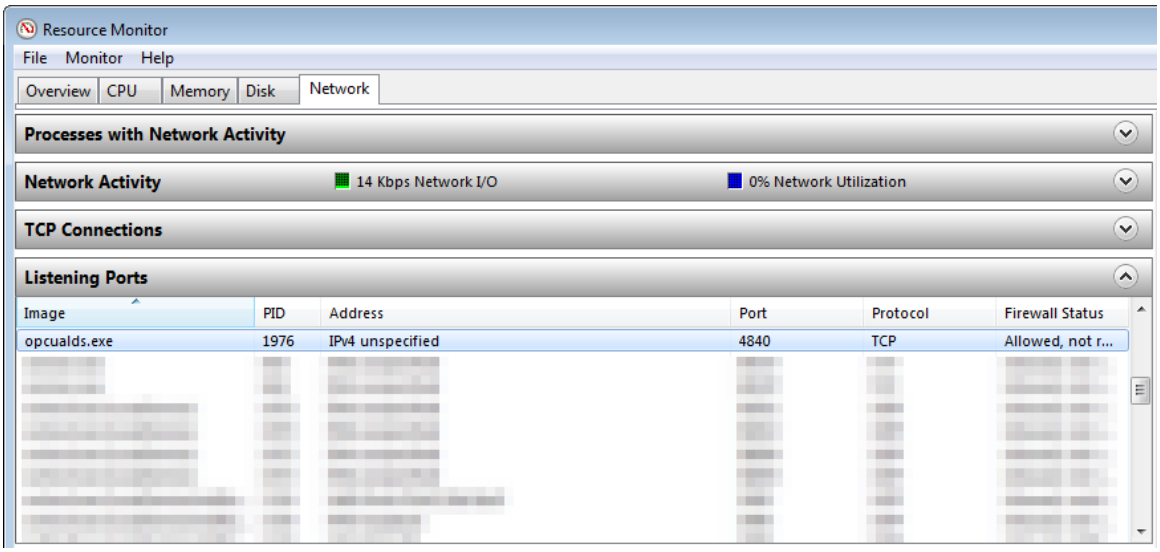
The following is an example showing how to set up Discovery service.

1. Install Local Discover Server (LDS) on a PC (for example, the PC name is DESKTOP-ABCD). Download the LDS provided by OPC Foundation from the link below: https://opcfoundation.org/developer-tools/developer-kits-unified-architecture/local-discovery-server-lds/

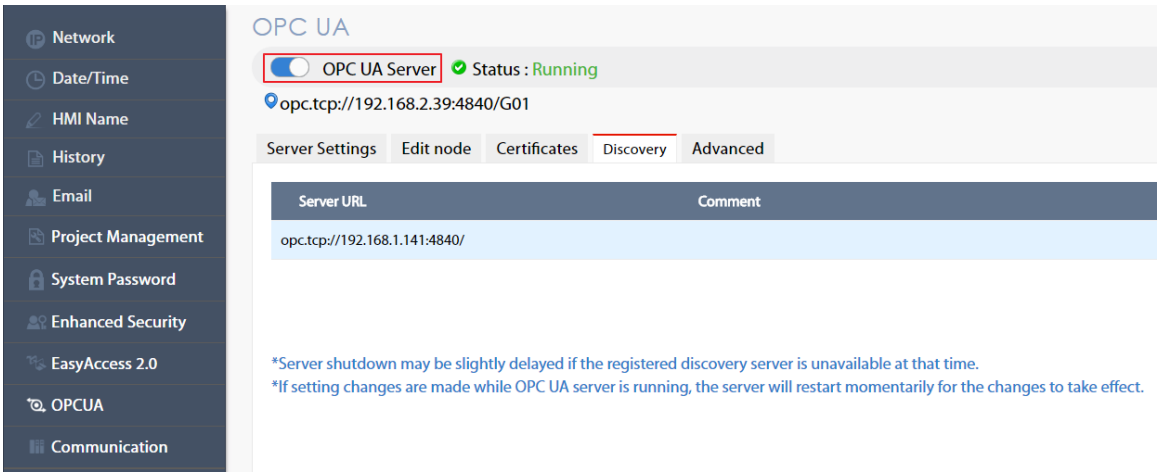
2. If the DNS service of router cannot resolve the HMI name to IP address, the HMI name should be changed to the IP address of the HMI. For example: If HMI IP address is 192.168.1.100, then the HMI name should be 192.168.1.100 or 0.0.0.0.
3. On the PC with OPC UA LDS installed, please manually copy the certificate from folder "C:\ProgramData\OPC Foundation\UA\pki\rejected\certs" (Folder for rejected certificates) to folder "C:\ProgramData\OPC Foundation\UA\pki\trusted\certs" (Folder for trusted certificates).
4. Launch the software of OPC UA Client, enter the name of the PC with OPC UA LDS installed or its IP address to obtain all the registered OPC UA servers.

When Discovery does not work properly, please:

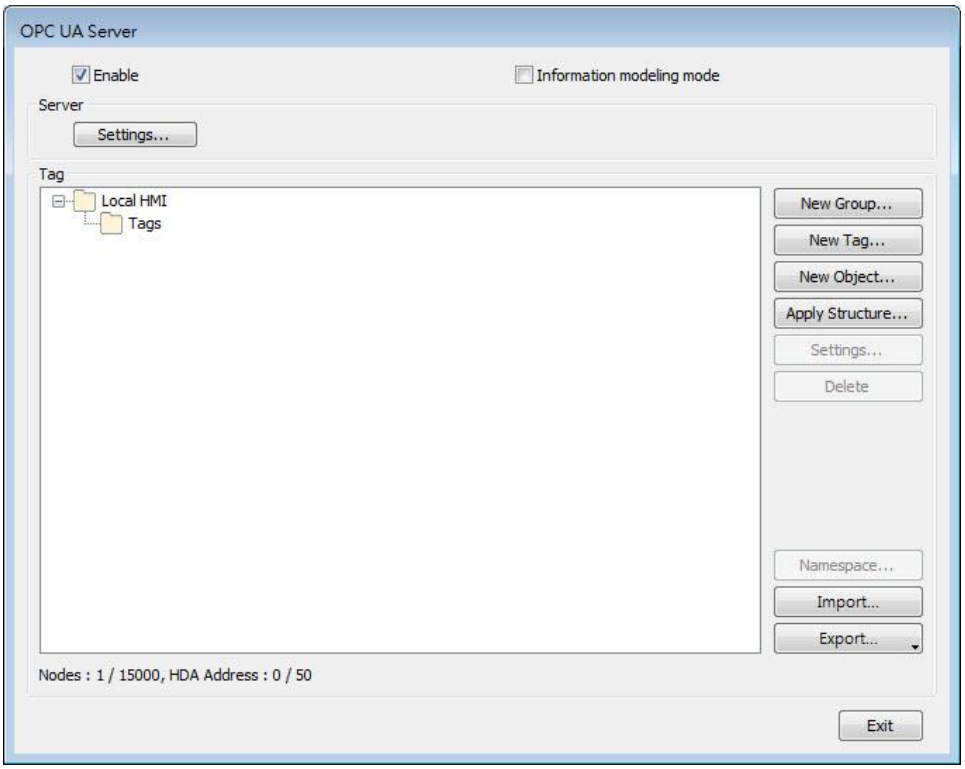
1. Open Windows Task Manager » Performance » Resource Monitor » Network » Listening Ports, and find the port number used by opcualds.exe. As shown in the following screenshot, in this example the PC's opcualds.exe uses port 4840.



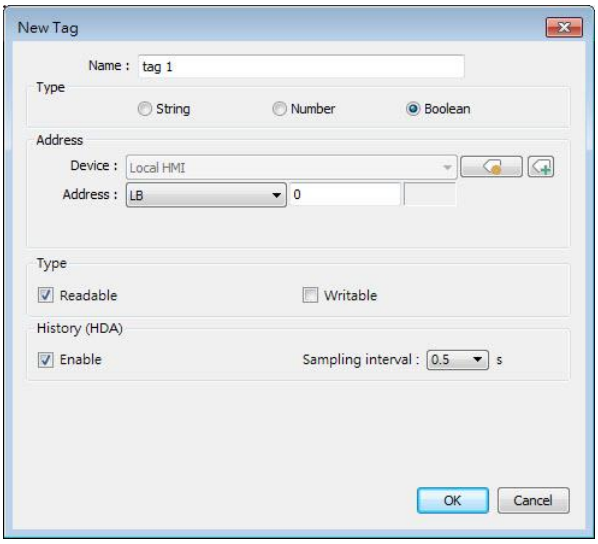
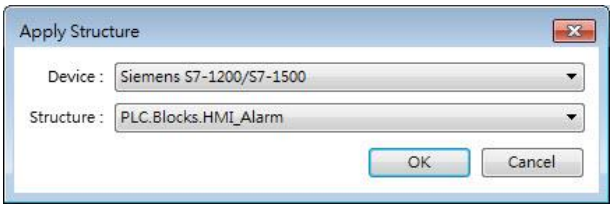
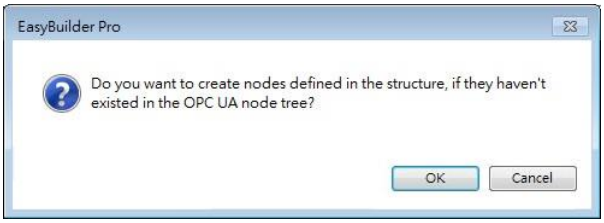
2. Enter HMI's IP address in the web browser, and enter the password to log in. Open OPC UA settings page and restart OPC UA Server. Please note that OPCUA settings tab is only supported on cMT Gateway Series models.



Tag

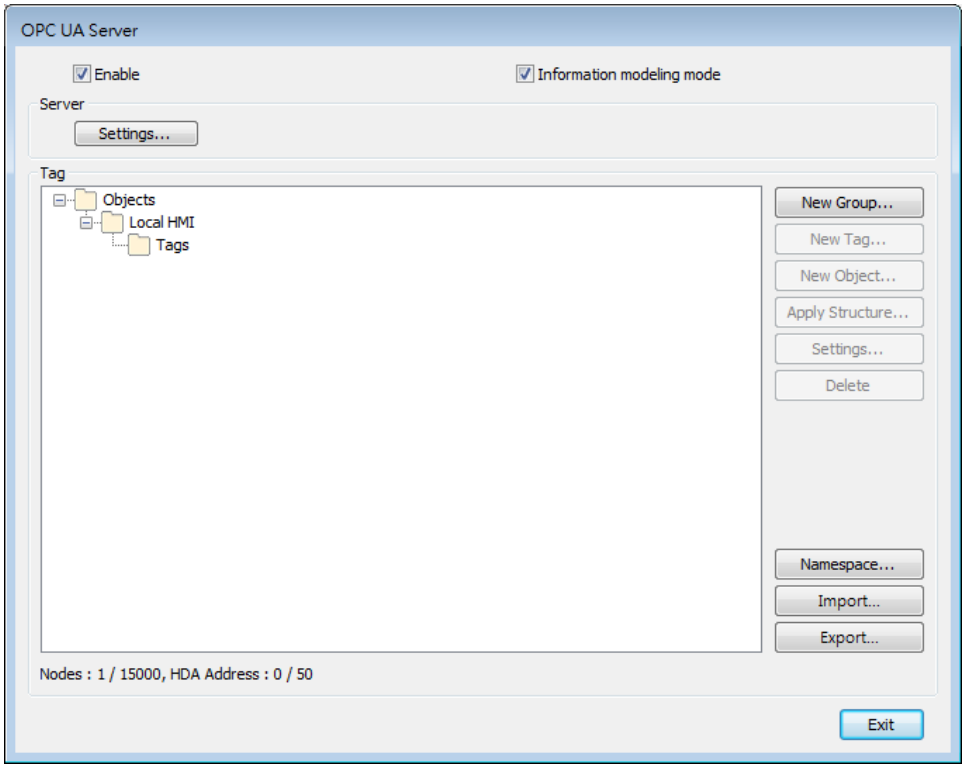


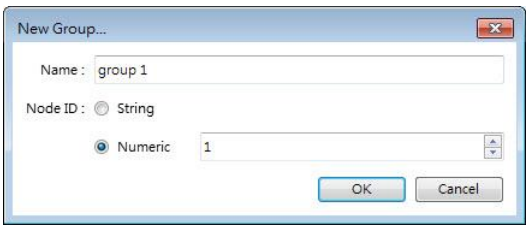
Setting	Description
New Group	 Add a new group for managing tags.

New Tag	 Add a new tag for the client to monitor or control. The name must be specified, and the address can be Readable or Writeable. **History(HDA)** Enable OPC UA HDA.
Apply Structure	 Structured node set under a device can be added, only if the device is a symbolic PLC and has structured data type defined. After clicking OK in the Apply Structure window, a prompt window shows asking whether to create nodes that do not exist in the OPC UA node tree. 
Settings	Set an existing group or tag.
Delete	Delete an existing group or tag.
Import	Import a tag file. Applicable import formats include: *.xlsx, *. xls, *.csv, *. xml
Export	Export current tags. Applicable export formats

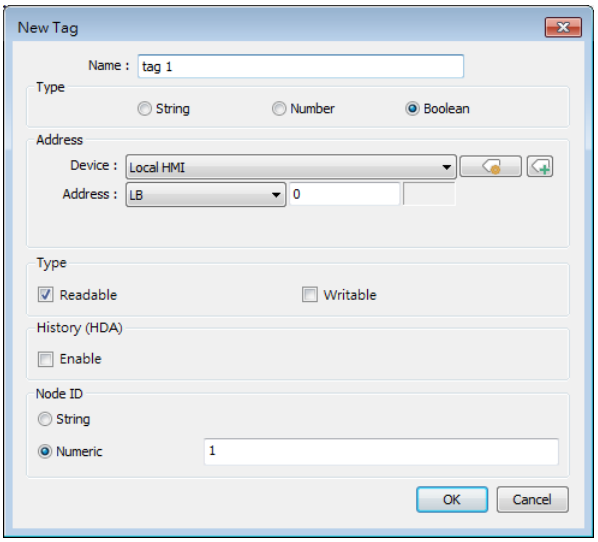
include: Excel format or XML format.

Tag – Information Modeling Mode



Setting	Description
New Group	 Add a new group for managing tags. A Node ID can be defined.

New Tag



Add a new tag for the client to monitor or control.

Two types of tags can be added: Data Variable and Property.

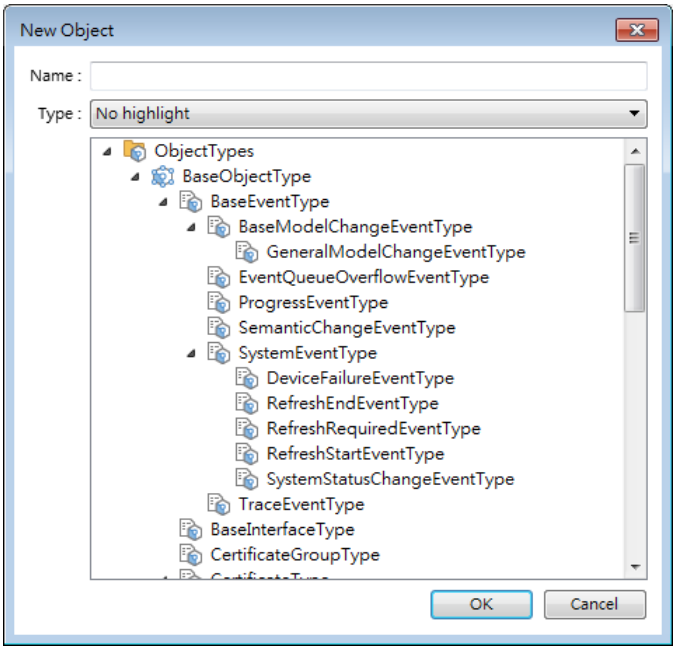
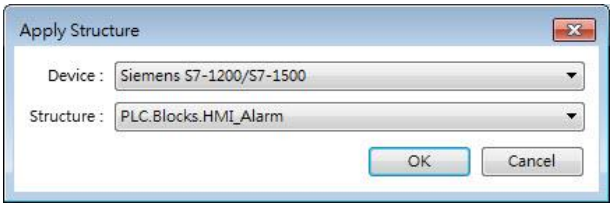
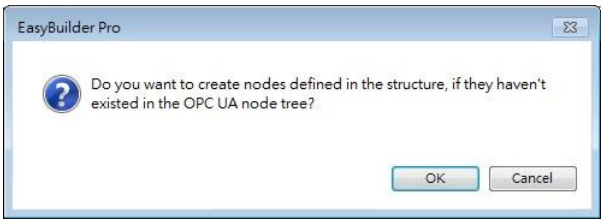
Data Variable: The data collected by the device. New tags, either data variable or property, can be added under a data variable.

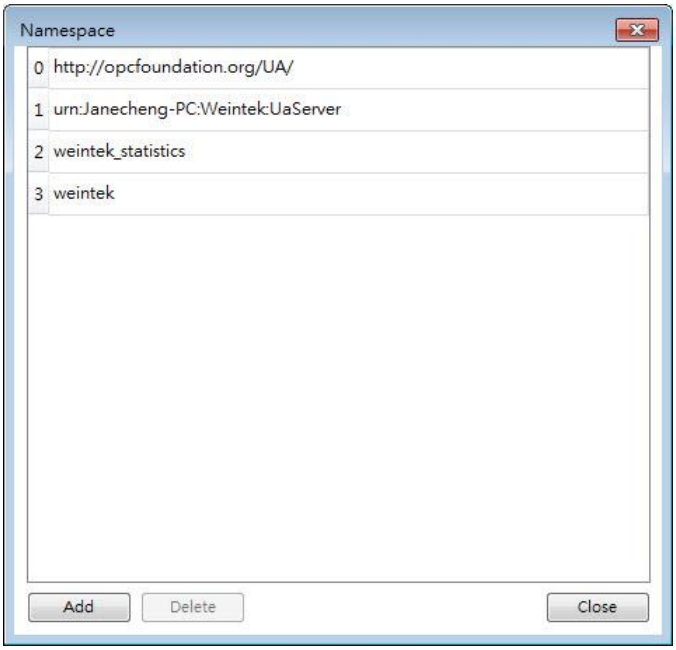
Property: The parameters of the device. No new tags can be added under a property.

The name must be specified, the address can be Readable or Writeable, and a Node ID can be defined.

History(HDA)

Enable OPC UA HDA.

New Object	 Add an object in the Object Types list. The name must be specified.
Apply Structure	 Structured node set under a device can be added, only if the device is a symbolic PLC and has structured data type defined. After clicking OK in the Apply Structure window, a prompt window shows asking whether to create nodes that do not exist in the OPC UA node tree. 
Settings	Set an existing group or tag.
Delete	Delete an existing group or tag.

Namespace	 Object types of a device can be added to or deleted from this list.
Import	Import a tag file. Applicable import formats include: *.xlsx, *. xls, *.csv, *. xml
Export	Export current tags. Applicable export formats include: Excel format or XML format.

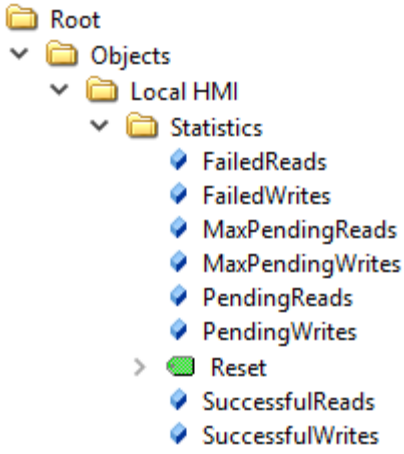
Note

- When downloading the project file to HMI, please make sure that the HMI time and time-zone settings are correct. Otherwise, the client program may not be able to authenticate, and the communication may fail due to authentication error caused by incorrect certificate valid time.
- Changing from Information Modeling Mode back to general mode is possible but please note that the node definition will be lost by doing so.

Click the icon to watch the demonstration film. Please confirm your internet connection before playing the film.

42.2.3. Device Statistics

Device-specific statistical data can be found in “Statistics” node, as shown below:



Meaning of each node:

Node Name	Description
FailedReads	No. of failed read commands. If it is not zero, there may be communication errors.
FailedWrites	No. of failed write commands. If it is not zero, there may be communication errors.
MaxPendingReads	Max. no. of pending read commands.
MaxPendingWrties	Max. no. of pending write commands.
PendingReads	No. of pending read commands in the queue. If the number stays high for a long time, it means the communication module is not able to process all commands in time. OPC UA nodes may update slower. Under extreme circumstances (e.g. >30), OPC UA node may not update in a long time.
PendingWrites	No. of pending write commands. Write commands have higher priority than read commands. If PendingWrites stays high, it will affect read commands.
Reset	Reset all statistical data.
SuccsessfulReads	No. of successful read commands.
SuccsessfulWrites	No. of successful write commands.

42.2.4. Limitation

The limitation of OPC UA server are listed below:

Item	Description
OPC UA Profile	UA 1.02 Standard UA Server Profile, including but not limited to * Core Server Facet

	* UA-TCP UA-SC UA-Binary * SecurityPolicy – None * Enhanced DataChange Subscription Server Facet * Standard DataChange Subscription Server Facet * Embedded DataChange Subscription Server Facet * User Token – X509 Certificate Server Facet * User Token – User Name Password Server Facet * Standard DataChange Subscription Server Facet * Embedded DataChange Subscription Server Facet See Profile Reporting Visualization Tool by OPC Foundation for more details.
Security policies	None Basic128Rsa15 Basic256 Basic256Sha256
Number of nodes	15 000
Max. array size	255
Read cache	100ms (Cache will be used for 100ms from previous read)
Max. client sessions	100
Max. subscription per session	64
Min. publishing interval	100ms
OPC UA HDA	Supports up to 50 node addresses with each node address can storing up to 10000 HDA data records. What constitutes a node address? Each HDA-enabled node is considered to take up the number of node addresses that is equal to the Element Count setting. If the data type is String, it is the No. of word setting instead. When the remaining space in HMI memory is less than 10%, the system will delete the earliest data and store the latest data. The system will stop deleting data when the remaining space increases exceeding 10%.
Performance (Values may change for different hardware/EBPro version)	
Max. Read/Subscribe	Built-in registers (e.g. LW): 27000 words/second (WPS)

Throughput (Security: None)	MODBUS RTU@9600bps: 500 WPS MODBUS RTU@115200bps: 4000 WPS MODBUS TCP/IP: 10000 WPS Tested Environment EBPro version: V6.02.02.242 cMT-G02 OS version: 20180917 Test uses as many as words as possible in one node (using array) to optimize reading.

Note

- Examples showing how to count OPC UA HDA node addresses:
  If there are 50 nodes (node1, node2…node50) and each node maps to one bit only(Element Count is 1), all the nodes altogether takes up 50 node addresses.
  If a node maps to a 16-bit unsigned array of size 50 (which is when Element Count is 50), every element in the array takes up a node address, so the number of node addresses taken by this node is 50.
  If a node maps to a string where No. of word is set to 50, the number of node addresses taken by this node is 50.