Introduction of Advantech EdgeLink Studio

In an on-site application, one or several RTU devices may have been installed. If there is a tool which manages to carry out the configuration and management of these RTU devices as well as the whole project, the customers will definitely benefit a lot from it. Therefore, we have developed EdgeLink Studio to configure and manage the devices and the project which may have multiple devices under it.

Advantech EdgeLink Studio can run stably on Windows XP/ Windows 7/ Windows 10.

Double-click the installer icon and follow the instructions to install the studio. After the installation, the icon of Advantech EdgeLink Studio will appear on the desktop. Double-click it to start the configuration and management.

The main functions of Advantech EdgeLink Studio include:

1. Configure the project and the devices offline. The studio can identify different Node IDs and download them to the device batch by batch.
2. Create IO tags and local tags of engineering significance and implement the mapping between the

tags and the addresses through Modbus and DNP3 server.

3. Support the configuration of the input/output range of each channel for both onboard IO and extended IO, as well as AI calibration.
4. For network communication, Ethernet, Wifi, Cellular are all supported.
5. Since protocol services are crucial to communication devices, EdgeLink offers Modbus RTU, Modbus TCP and BACnet servers for users to select according to their specific requirements.
6. Moreover, monitoring the communication status of both remote serial ports and network ports is supported. The acquisition path for EdgeLink Studio installation package is as follows: http://www.advantech.com.cn

Advantech EdgeLink Studio implements project configuration

Project management

The Device in the EdgeLink usage scenario is uniformly managed by the project, and EdgeLink Studio implements a series of activities such as project creation, device creation, and meter addition

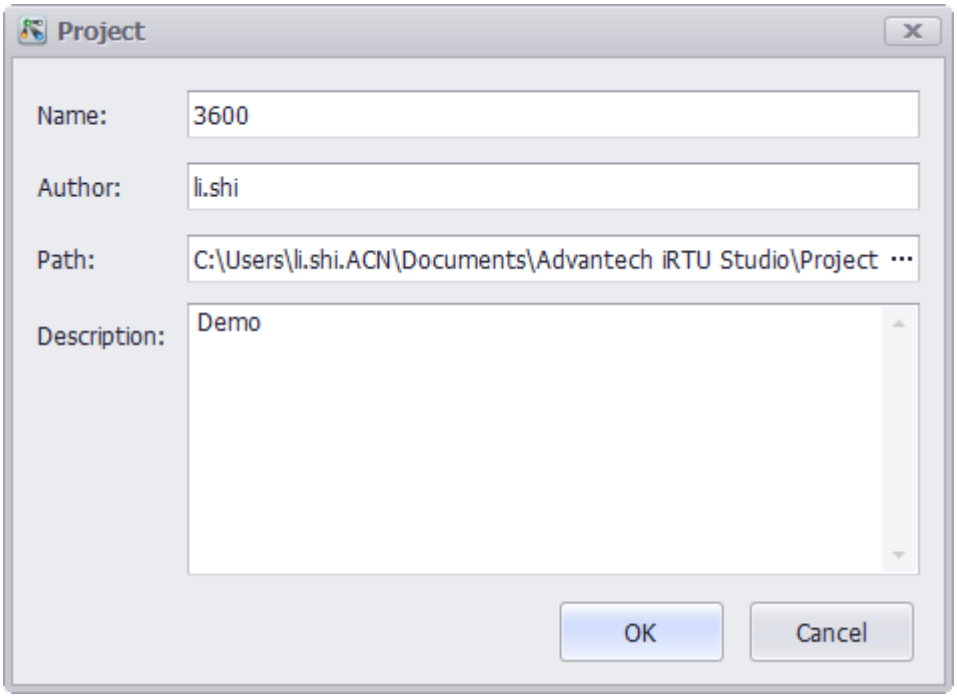
Project Configuration by Advantech EdgeLink Studio

Project Management

When EdgeLink Studio is opened for the first time, users can follow the procedures of “Create Project” -> “Add Device” -> “Copy” (if multiple devices are required) -> “Save” to initialize the project.

Create Project

Click “Create Project” under “Project” tab to pop up the below window. Then enter a name, path and description, and click “OK” button.



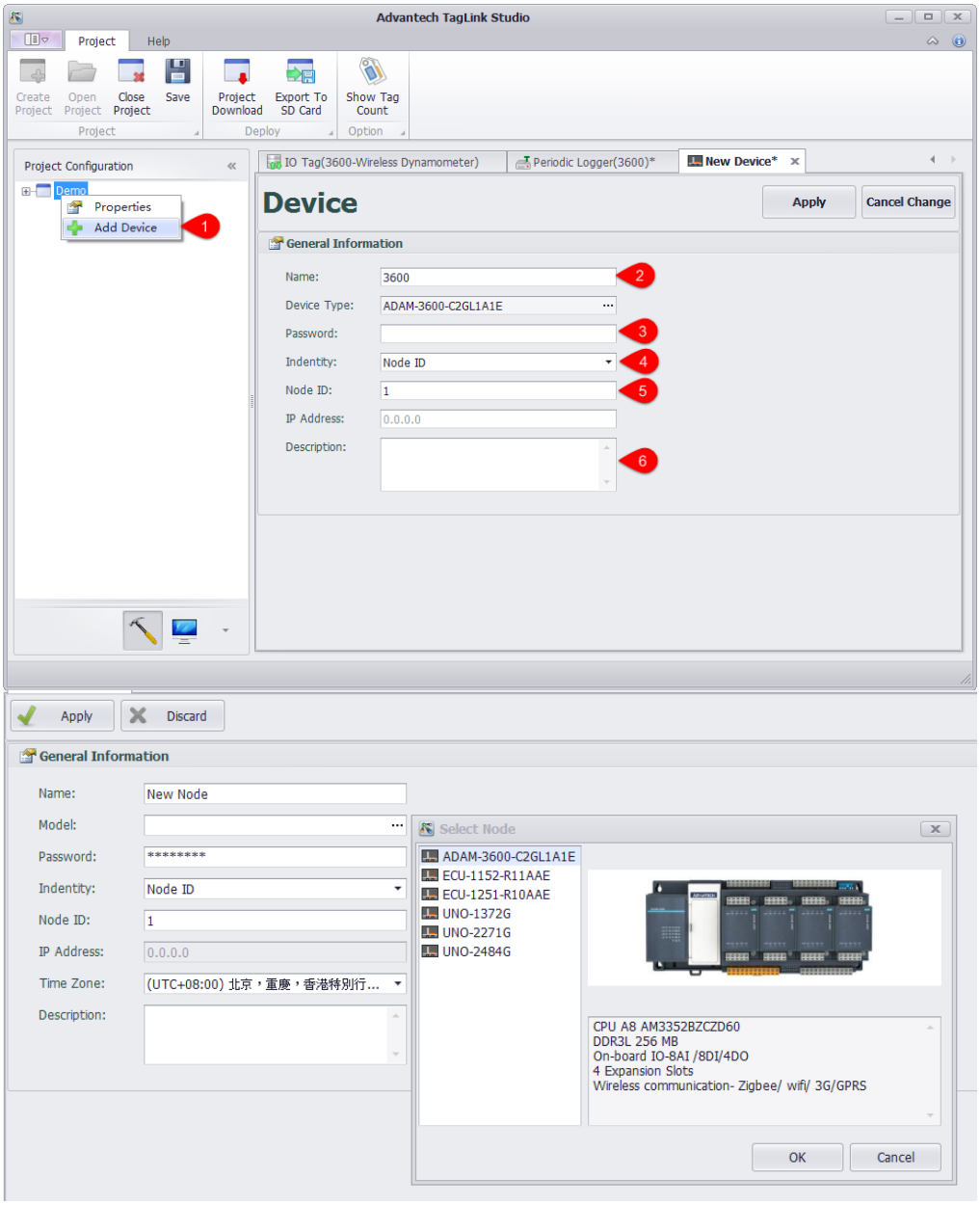
Add Device

There are two ways to add device to a created project

- Add blank device: After adding, all configurations are empty, and the user can manually configure it, please refer to Section 2.1.2.1 for specific steps
- Copy from existing device: When adding, you can copy and add the device that has been configured in the project, and you can copy each other regardless of the device model, but because the number of hardware interfaces between different models of device is different, the actual copy content is determined by the final device type, and the specific steps can refer to Section 2.1.2.2

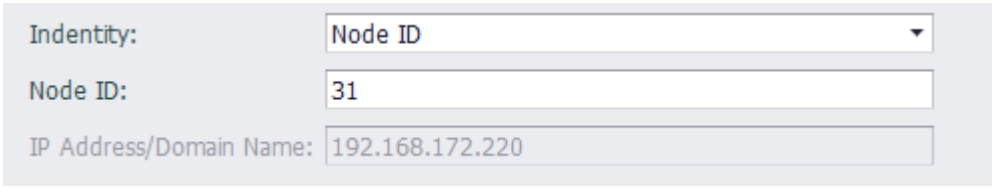
Add Device and Edit Information

1. Right-click on the project name to add a device.
2. Enter a device name.
3. Enter a password. This default password is 00000000. Users can change the password referring to 3.1.4 “Password Setting”. After the password is changed, users need to enter the new one to download the project.
4. Here allows users to identify the device by Node ID or IP Address.
5. Enter the corresponding Node ID or IP Address.
6. Select the time zone in which the device is located.
7. Fill in the device description (optional).



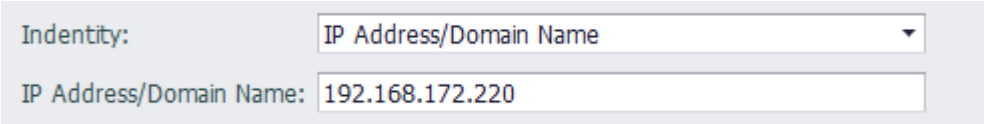
Identify Types

- Node ID：



When downloading, search the network for the device IP with node ID as the configuration value, and download the project to this device.

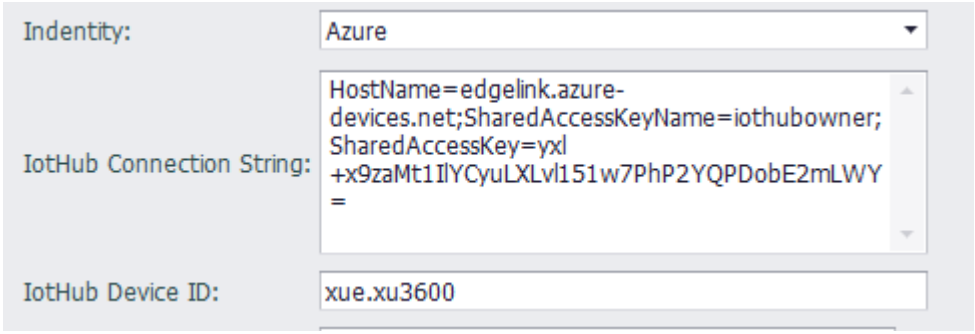
- IP Address/Domain Name：



You can download the project to the configured device with the device IP or domain name. When using remote.it or devices in the gateway with port forwarding service to download the project, the port number can be configured, such as:

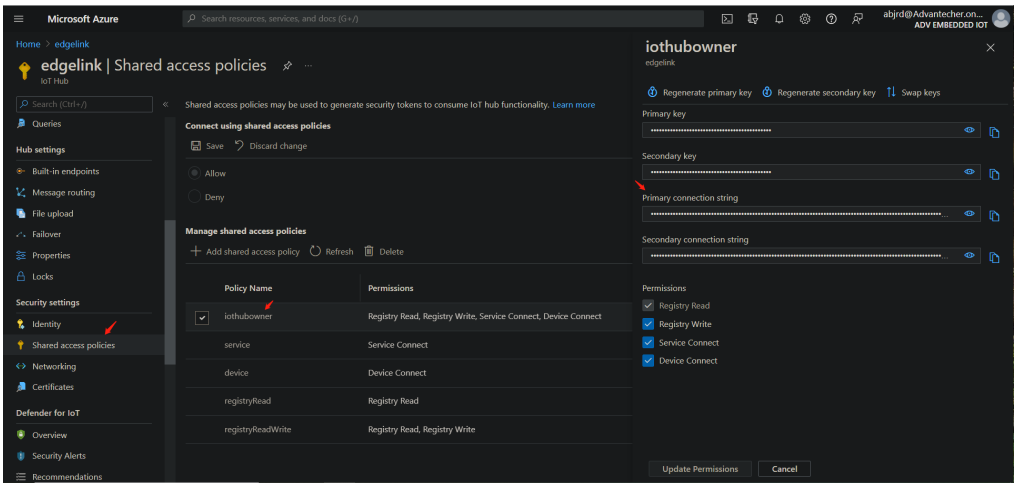
`adam3600-generic-tcp.at.remote.it:30000`

- Azure

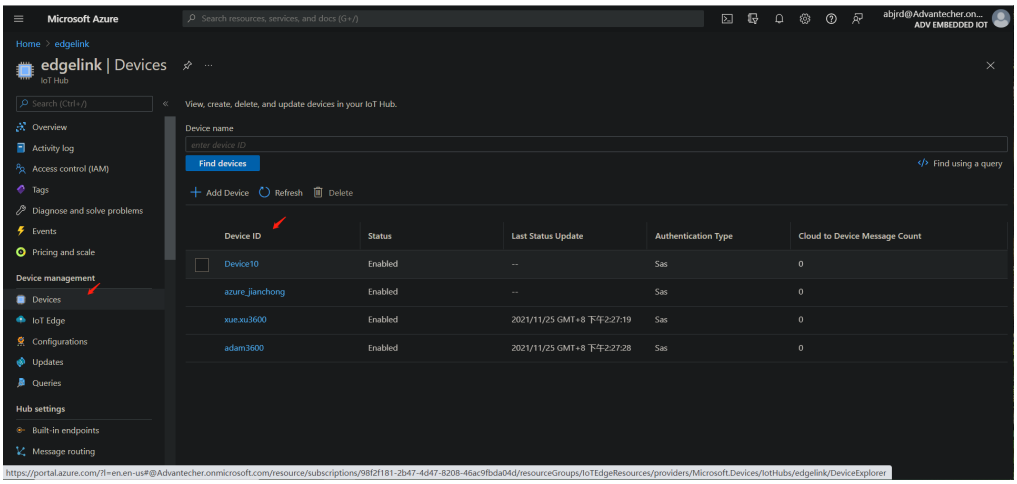


You can download the project to the device through azure cloud service. You need to configure the primary connection string in iothub and the device ID in iothub.

IotHub Connect String：

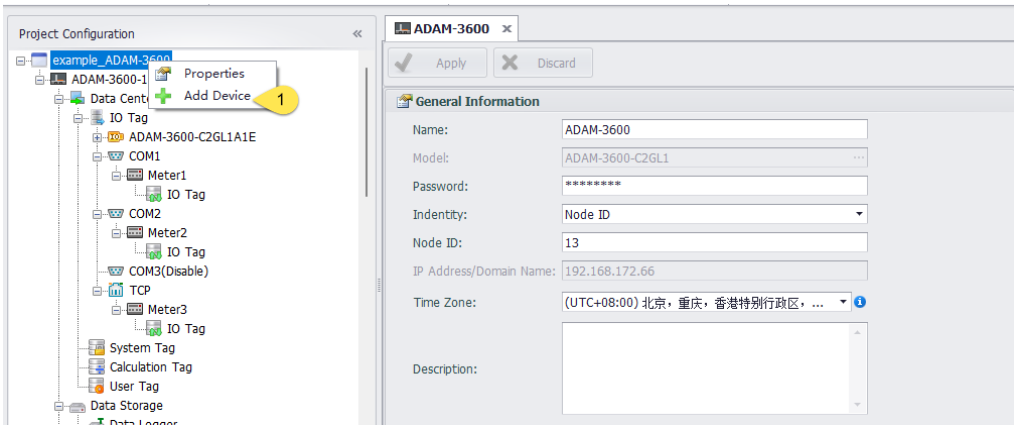


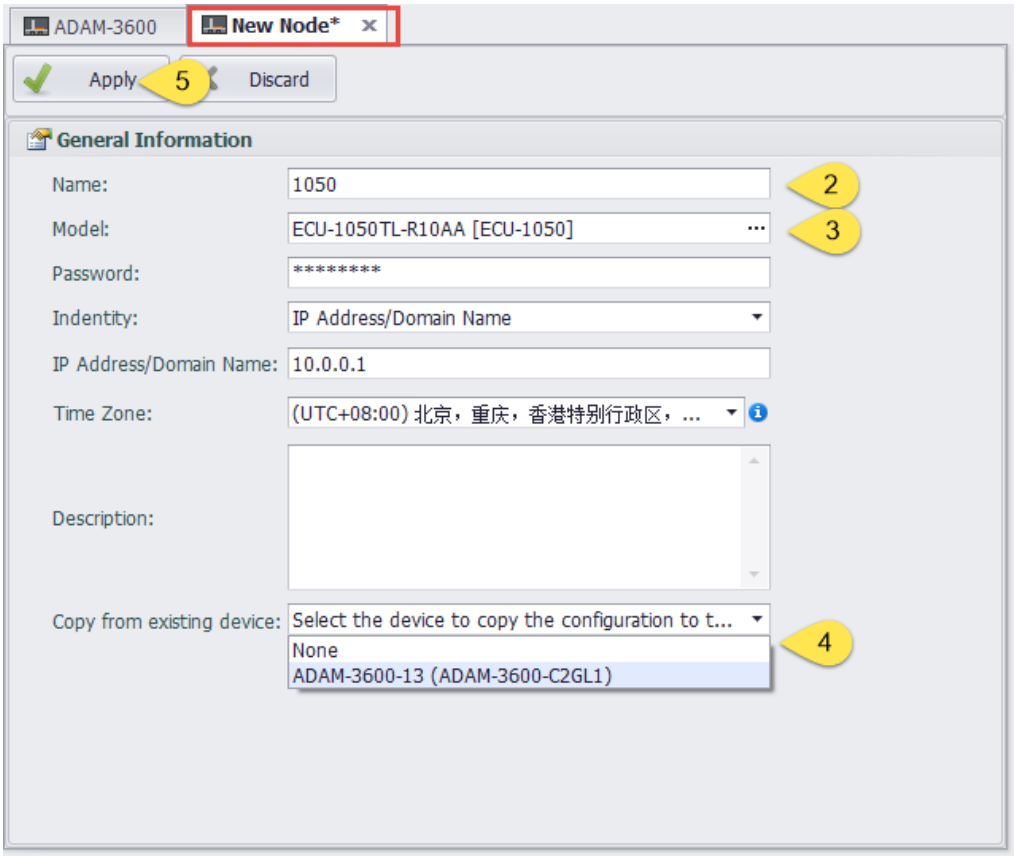
IotHub Device ID：



copy from existing device

1. At this time, there is already a device in the project file: ADAM-3600-13, right-click the project name to add a new device.



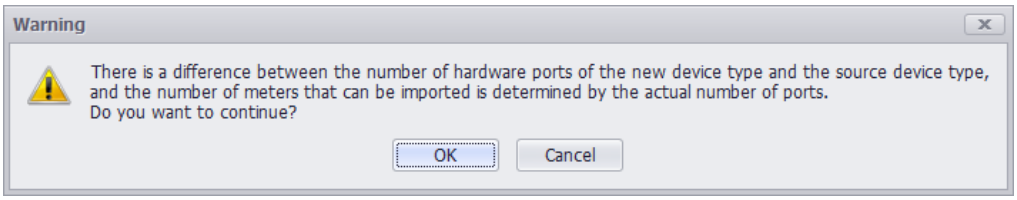


2. Enter the device name.

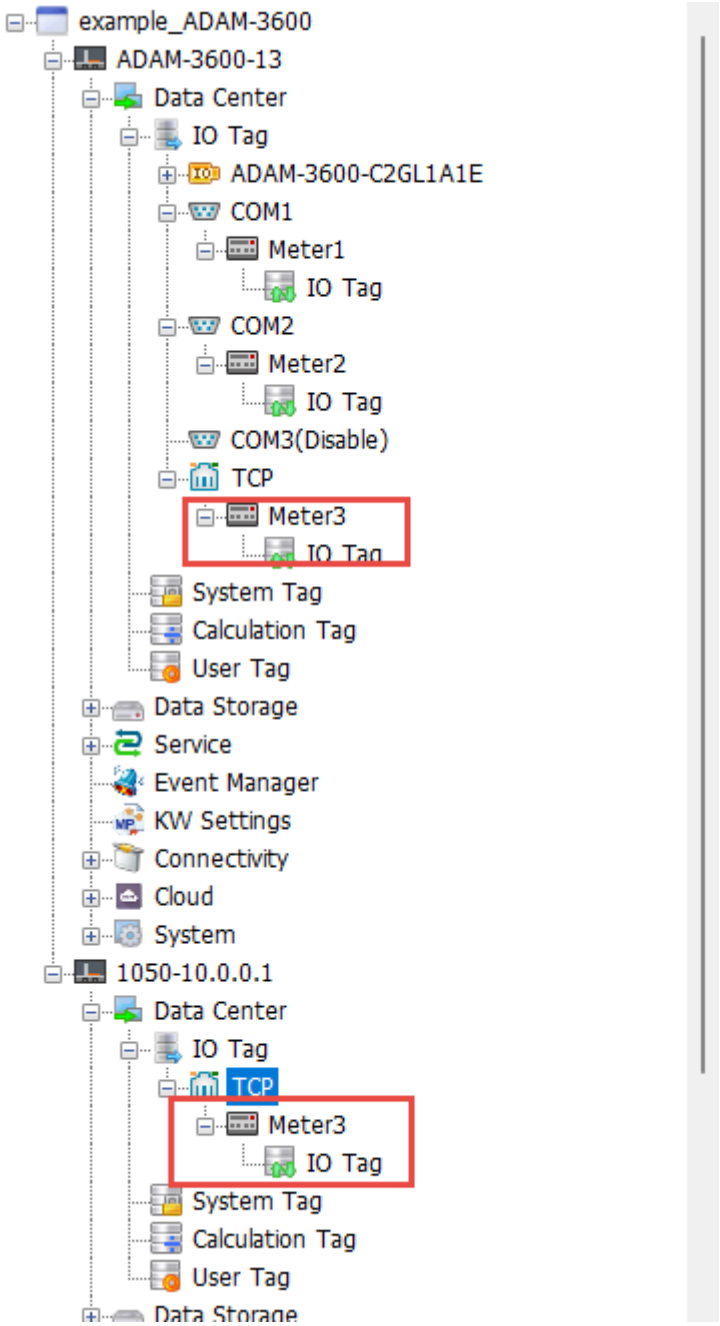
3. Select the type of device you want to add.

4. Copy the file from an existing device
5. Apply

When the device type is inconsistent, the following picture will be displayed. If you confirm the creation, click OK



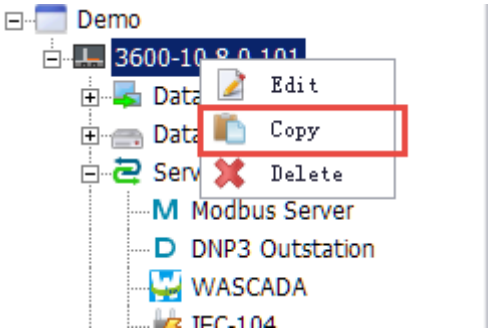
At this time, a new device is added to the project. The model is the model selected during the addition, and the configuration information is copied from ADAM-3600-13 (the number of ports is determined by the model selected during the addition).


example_ADAM-3600
ADAM-3600-13
Data Center
IO Tag
ADAM-3600-C2GL1A1E
COM1
Meter1
IO Tag
COM2
Meter2
IO Tag
COM3(Disable)
TCP
Meter3
IO Tag
System Tag
Calculation Tag
User Tag
Data Storage
Service
Event Manager
KW Settings
Connectivity
Cloud
System
1050-10.0.0.1
Data Center
IO Tag
TCP
Meter3
IO Tag
System Tag
Calculation Tag
User Tag
Data Storage

Copy

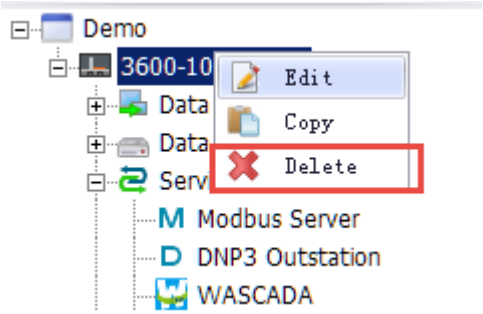
This feature is suitable for copying between identical devices.

For the project which has multiple devices to be configured, it will be relatively complicated to repeatedly add a new device. EdgeLink Studio supports to completely copy the existing device information. Users only need to right-click on the device name and select “Copy” to add another device. Then users can edit the device information (name, Node ID and description. etc) via two ways: double-click the device name or right-click on the device name and select “Edit”.



Delete

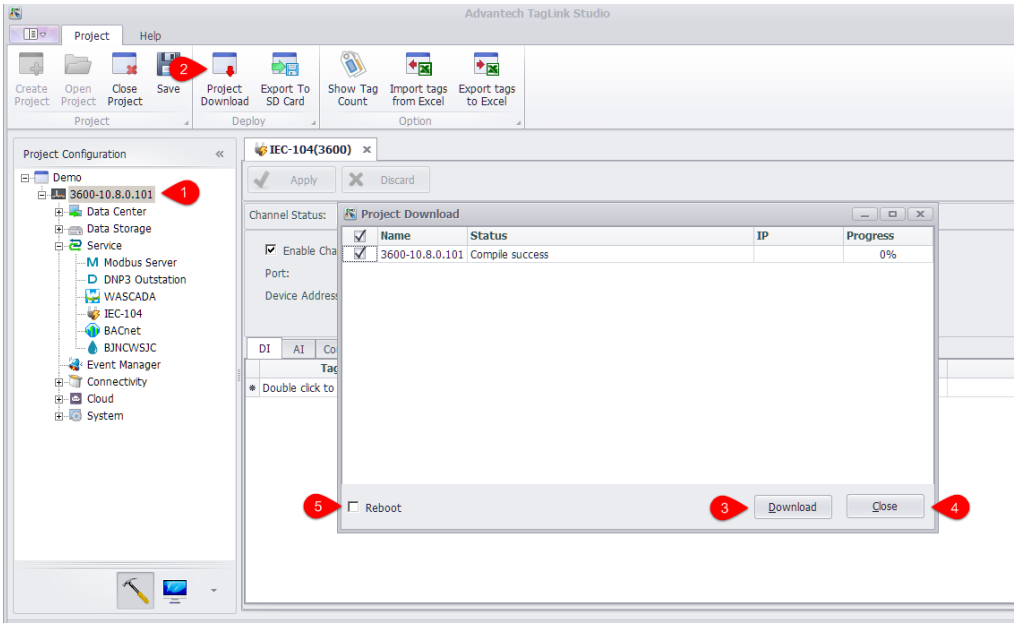
If users need to completely delete a device from the project, please right-click on the device name and select “Delete” to remove it.



Project Download

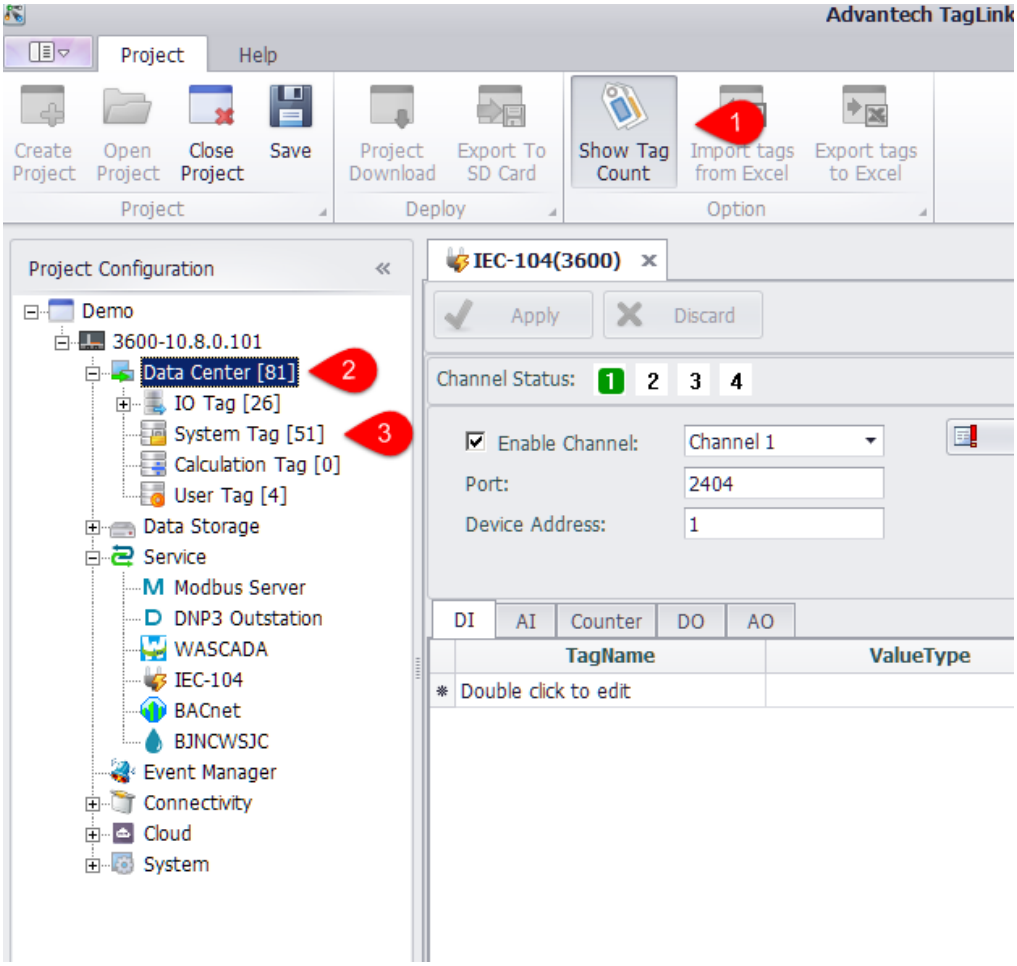
After the device has been identified, users can download the device information to the relevant device. Batch download function is supported. If users select a project on the left tree menu and then click “Project Download”, a dialog will pop up listing all RTU devices for batch download; if users select a certain device and then click “Project Download”, a dialog will pop up with only one RTU device to be downloaded.

1. Select a device.
2. Click “Project Download”.
3. Click “Download” button to start downloading.
4. In “Project Download” dialog, “Progress” shows the current download progress. When complete, click “Close” button.
5. In “Project Download” dialog, “Reboot” allows users to set whether to reboot the device after the downloading is complete.


Advantech TagLink Studio
Project
Help
Create Project
Open Project
Close Project
Save
Project Download
Export To SD Card
Show Tag Count
Import tags from Excel
Export tags to Excel
Project
Deploy
Option
Project Configuration
Demo
3600-10.8.0.101
Data Center
Data Storage
Service
Modbus Server
DNP3 Outstation
WASCADA
IEC-104
BACnet
BJNCWSJC
Event Manager
Connectivity
Cloud
System
IEC-104(3600)
Apply
Discard
Channel Status:
Enable Cha
Port:
Device Addres
DI
AI
Double click to
Project Download
Name
Status
IP
Progress
3600-10.8.0.101
Compile success
0%
Reboot
Download
Close
1
2
3
4
5

Show Tag Count

Click “Show Tag Count” to show the number of the configured tags of each device under a project.



1. Click this button to show/hide the tag number on the left tree menu.
2. The number within the brackets after “Data Center” indicates the total count of tags that have been configured in the selected device.
3. The number within the brackets under “Data Center” indicates the count of tags that have been configured under a certain node.

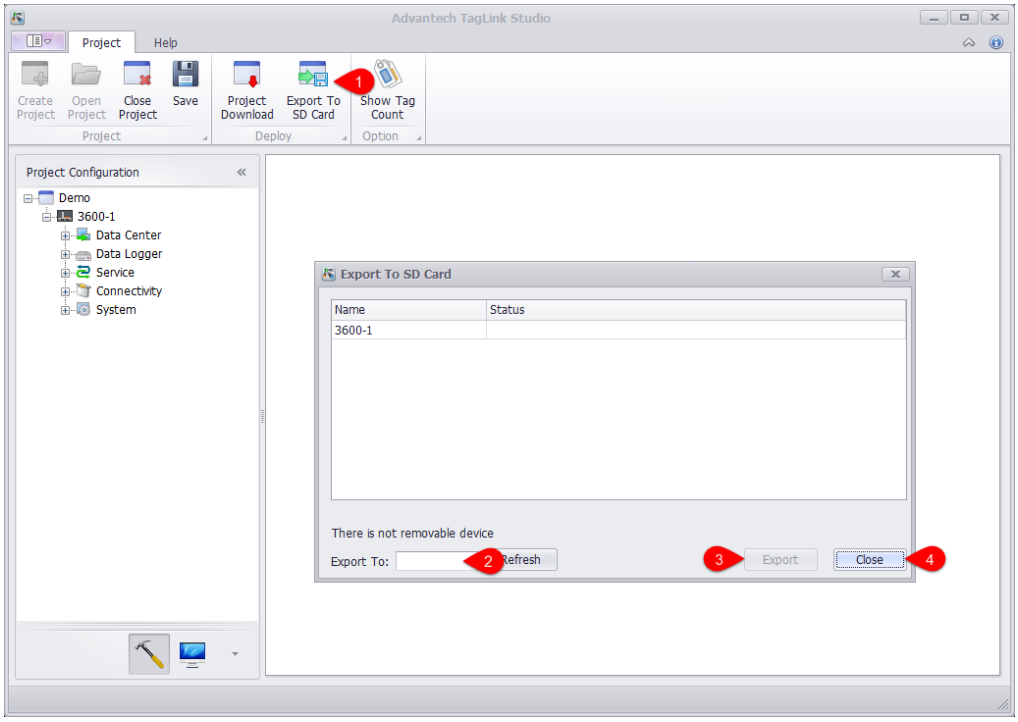
Export to SD Card

This function exports the configured project to the SD card. In the absence of a network connection, the SD card can be plugged into the device to update EdgeLink.

1. No matter the project is selected or not, click “Export to SD Card” will pop up the window listing all devices in the project.
2. Select a target path to export to.
3. Click “Export” button. When the progress bar is complete, export action is successfully completed.
4. Click “Close” button.

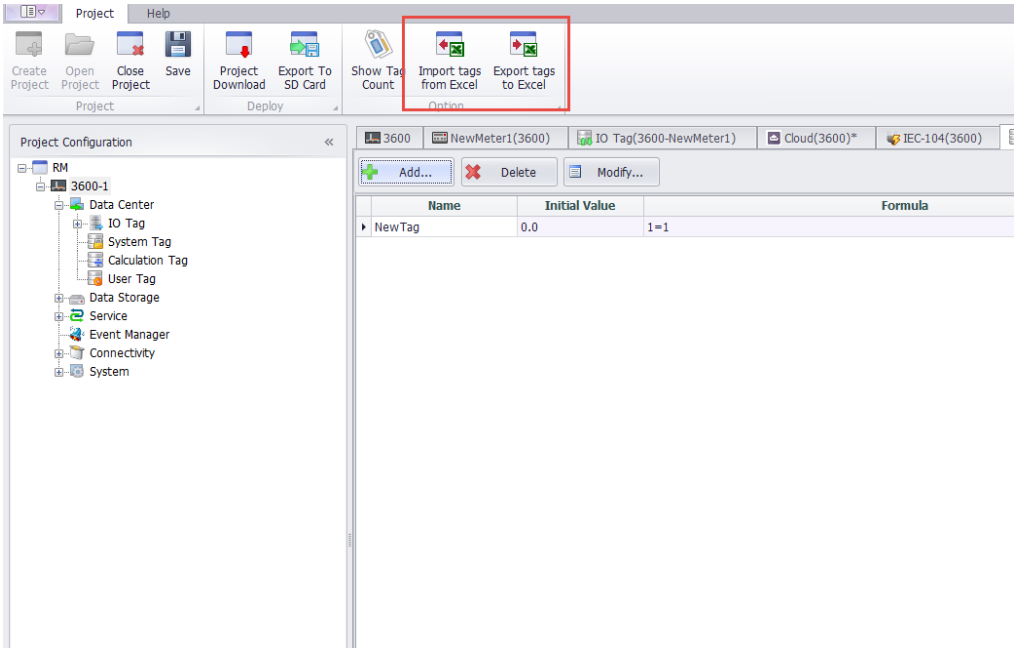
Then insert SD card into EdgeLink and power on it to update the project.

> **Note!**: The device with identification method of Node ID can use this feature to update EdgeLink.


Advantech TagLink Studio
Project
Help
Create Project
Open Project
Close Project
Save
Project
Project Download
Export To SD Card
Deploy
Show Tag Count
Option
1
Project Configuration
Demo
3600-1
Data Center
Data Logger
Service
Connectivity
System
Export To SD Card
Name
Status
3600-1
There is not removable device
Export To:
2
Refresh
3
Export
Close
4

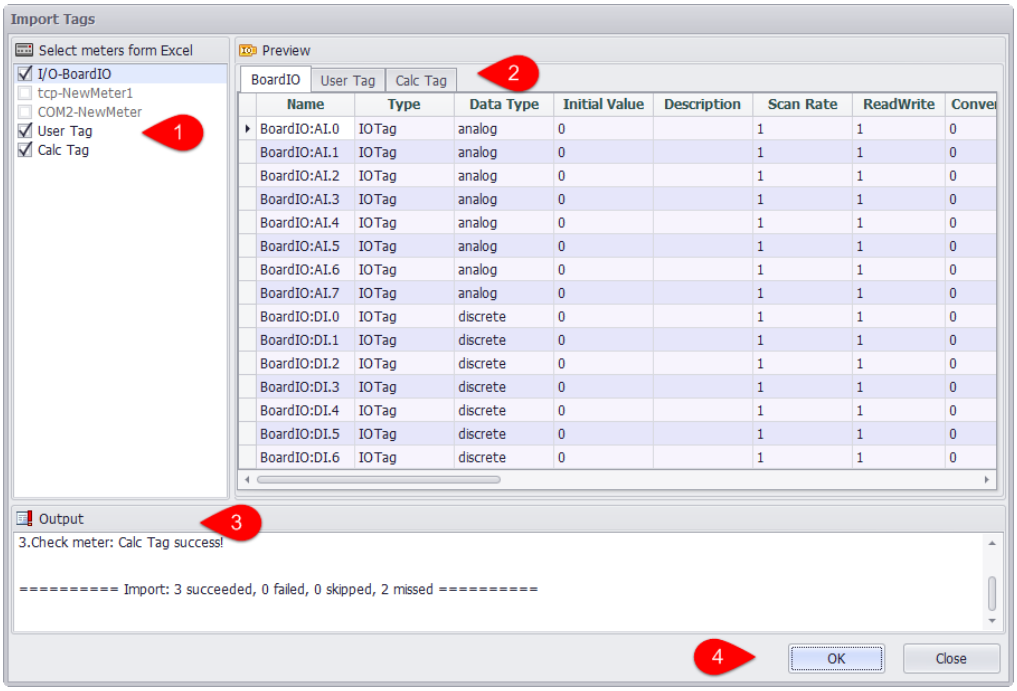
Device Tag Import and Export

EdgeLink Studio supports bulk importing and exporting the IO tags, calculation tags and user tags of a device in Excel format.



Import from Excel

The IO tags, calculation tags, and user tags in the Excel table should be saved in the format defined by the project definition, including the sheet name, header name, table data format, and so on. Users select the device to import the tag, click the “import from Excel” button, and select the Excel file to import in the pop-up window.



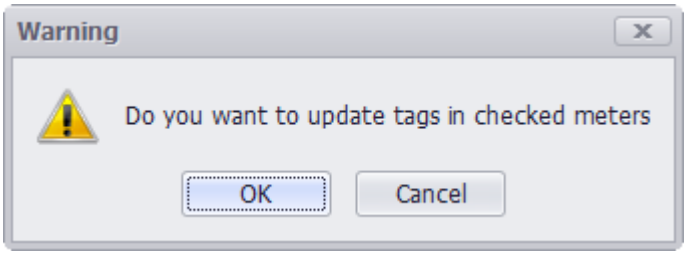
1.Select the Excel table that you want to import in the left checkbox.

2.In the “Excel Preview” pane, click the tab to preview the data in the table.

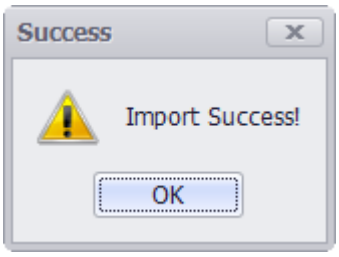
3.The system automatically checks whether the selected Excel table file format meets the import requirements and, if not, displays the error content in the export window.

4.If the Excel file format is checked correctly, click the OK button to start importing.

After you start importing, the system will ask whether to update the Tag of the selected device. Click “OK” button to confirm the import.

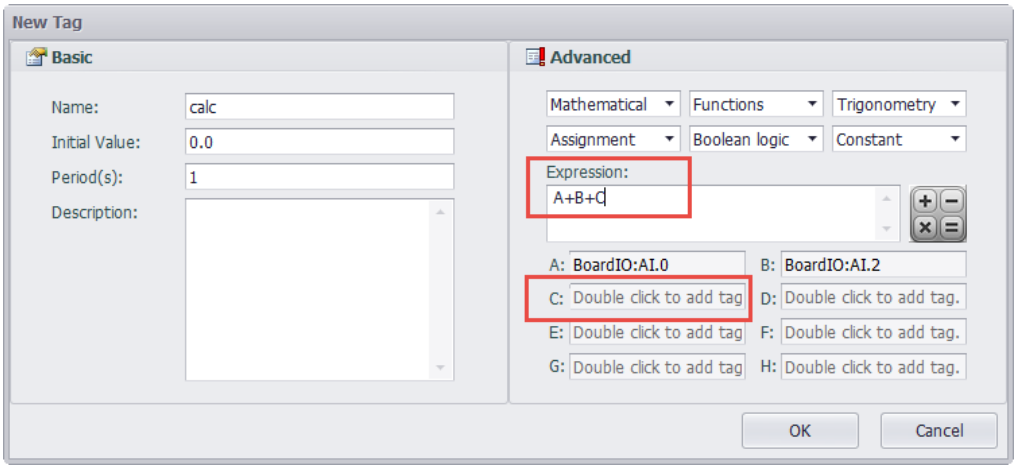


When the import is successful,the system will pop up a successful prompt.



When you import a device calculation tag, the system will check the calculation tag formula and the variable definition in the Excel table. If the formula is incorrect or the variable in the formula is not defined as the tag in the system, a prompt will be given in the export window so that the user can check the formula and variable definitions.

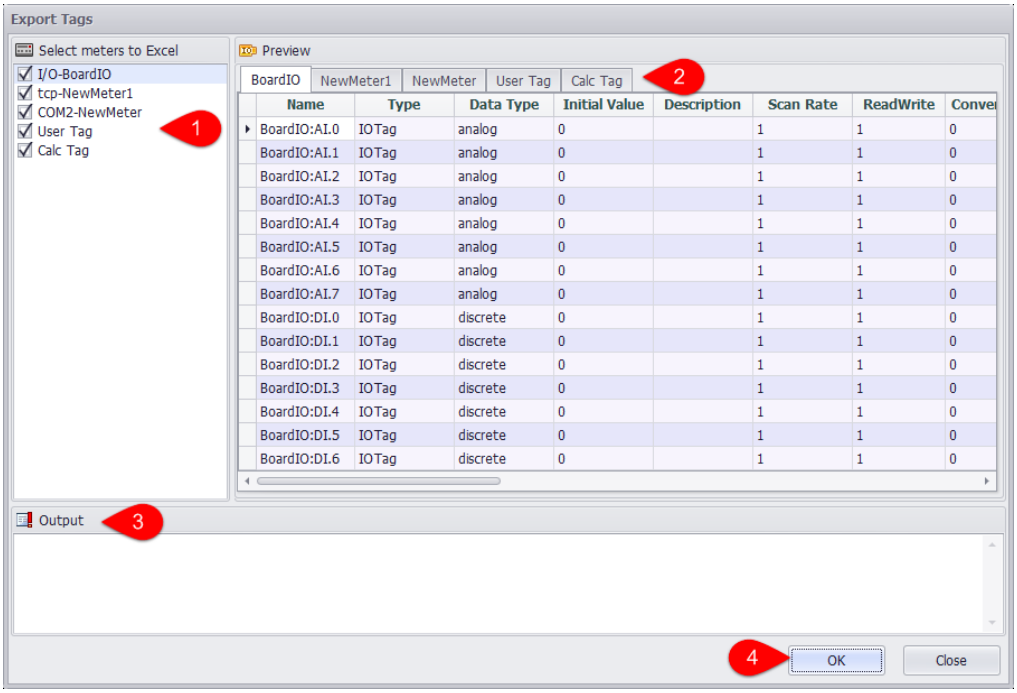
At this point, the contents of the first line in the Calc Tag table are:



You can see that the formula in the Excel table is “A+B+C”, and the variable ParametersC is empty, that is, the Tag corresponding to the variable “C” is not correctly defined in the formula.

Export to Excel

Select the device to export tags in the project, click the “export to Excel” button, in the pop-up window, you can export Tags to the Excel file.



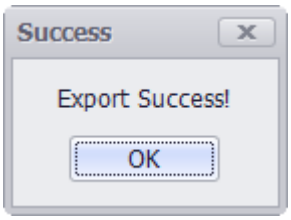
1.Select the tag you want to export in the left checkbox.

2.In the “EXcel preview” pane,click the tab to preview the device tag data.

3.The export content is displayed in the export window.

4.Click the OK button to start the export operation.

5.When the export is successful,the system will pop up a successful prompt.



Data Acquisition Configuration

Data acquisition is an important function for RTU devices. EdgeLink supports the acquisition of onboard IO, extended IO, IO of serial devices, Ethernet devices to satisfy the diversified acquisition needs. Therefore in EdgeLink Studio, users need to add and configure those tags based on the specific acquisition requirements.

These IO tags added into the project are real tags; while in actual project deployment, local tags of engineering significance are also needed. Users are required to add and configure them in EdgeLink Studio.

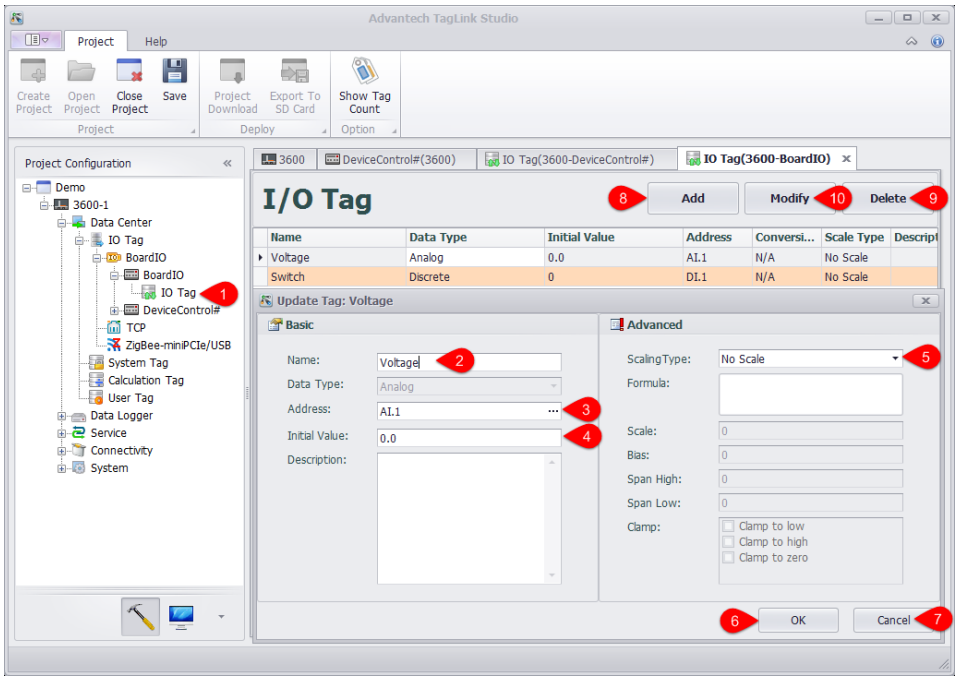
Configure Onboard IO

In project configuration, users can add and configure IO tags based on the real input. The detailed operation procedures are as follows:

1. Double-click “IO Tag” in the left tree menu or right-click on it and select “Edit”.
2. Fill in a tag name.
3. Select a tag address.
4. Set its initial value.
5. Select its scaling type.
6. Click “OK” button to successfully add the tag. Then this new tag will appear in I/O Tag list.
7. Click this button to cancel the changes.
8. Add another new tag.
9. Choose one or several tags to delete.
10. Choose one or several tags to modify.

- ADAM-3600 supports 8-ch AI, 8-ch DI and 4-ch DO.

- UNO-1372G supports 4-ch DI, 4-ch DO.



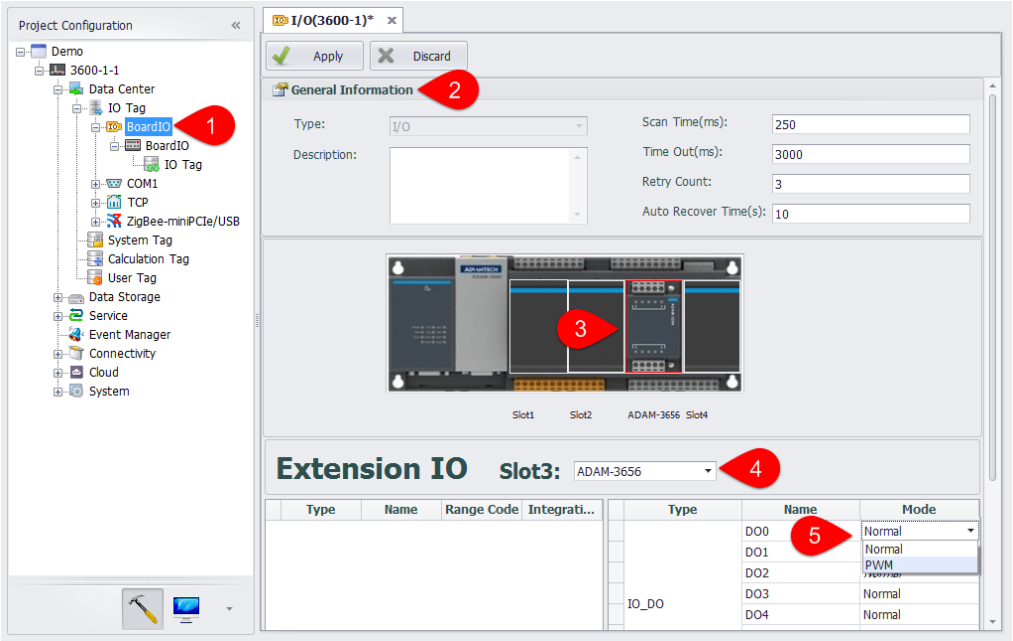
Expansion Module Configuration

ADAM-3600 supports a variety of extension modules, including DO, DI, AI, AO, and other types. The currently supported modules are as follows:

1. ADAM-3617 AI module supports the 4channel AI
2. ADAM-3618 AI module supports the 4channel AI
3. ADAM-3624 AO module supports the 4channel AO
4. ADAM-3651 DI module supports the 8channel DI
5. ADAM-3656 DO module supports the 8channel DO
   UNO devices support iDoor extension modules:
6. PCM-24R1TP and PCM-24R2GL LAN card
7. PCM-24D2R4, PCM-24D2R2, PCM-24D4R2, PCM-24D4R4 serial cards
8. PCM-24S2WF Wifi module
9. PCM-2300MR-AE FRAM module
10. PCM-24S33G 3G module

Add Extension Module

EdgeLink supports various extension modules, including DO, DI, AI and AO, etc. Please follow the below procedures to add an extension module.

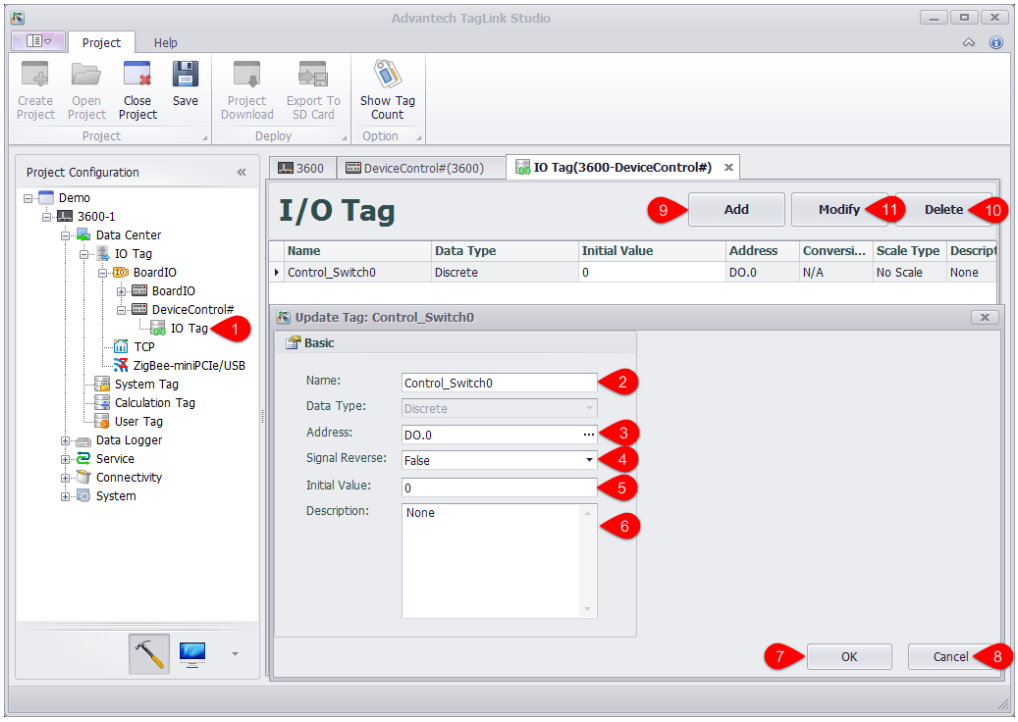


1. Double click to open the BoardIO node.
2. Modify the basic properties of the BoardIO port.
3. Users can select a Board or Slot picture on the EdgeLink schematic, and edit the IO tag property and the slot type.
4. After clicking on the Slot picture, users can select the module type of the ExtensionIO.
5. AI tag supports four range options for +/-10V, +/-2.5V, 0-20mA, and 4-20mA. DI tag supports Normal, Counter two working modes. DO tag supports Normal, PWM two working modes.

Configure Extended IO

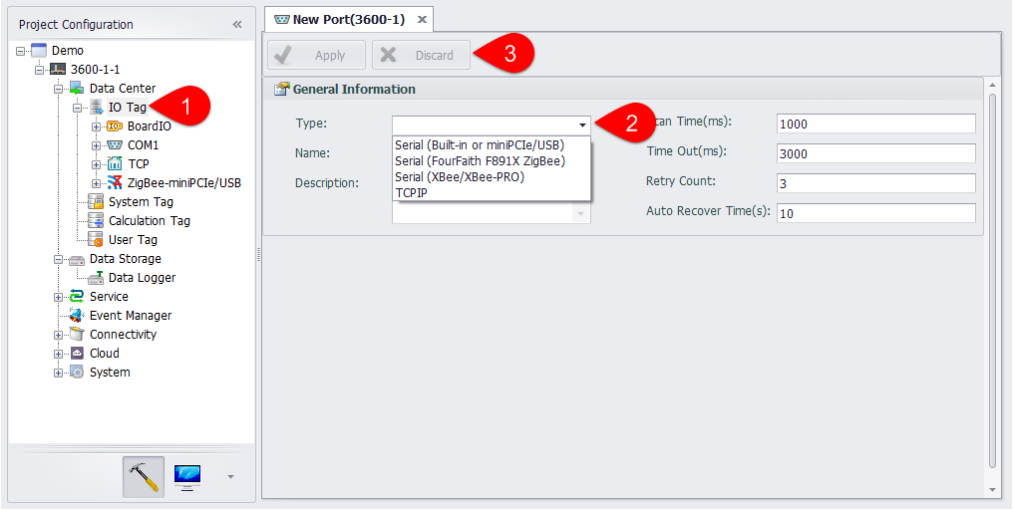
Please follow the below procedures to configure IO tag of the extension module.

1. Double-click “IO Tag” in the left tree menu or right-click on it and select “Edit”.
2. Fill in a tag name.
3. Select a tag address.
4. Select whether to reverse the signal, which is only available for DO module.
5. Set its initial value.
6. Give a description of the IO tag, which is optional.
7. Click “OK” button to successfully add the tag. Then this new tag will appear in I/O Tag list.
8. Click this button to cancel the changes.
9. Add another new tag.
10. Choose one or several tags to delete.
11. Choose one or several tags to modify.


Advantech TagLink Studio
Project
Help
Create Project
Open Project
Close Project
Save
Project
Project Download
Export To SD Card
Deploy
Show Tag Count
Option
Project Configuration
Demo
3600-1
Data Center
IO Tag
BoardIO
BoardIO
DeviceControl#
IO Tag
TCP
ZigBee-miniPCIe/USB
System Tag
Calculation Tag
User Tag
Data Logger
Service
Connectivity
System
3600
DeviceControl#(3600)
IO Tag(3600-DeviceControl#)
I/O Tag
Add
Modify
Delete
Name
Data Type
Initial Value
Address
Conversi...
Scale Type
Descript
Control_Switch0
Discrete
0
DO.0
N/A
No Scale
None
Update Tag: Control_Switch0
Basic
Name:
Control_Switch0
Data Type:
Discrete
Address:
DO.0
Signal Reverse:
False
Initial Value:
0
Description:
None
OK
Cancel
1
2
3
4
5
6
7
8
9
10
11

Configure IO of Serial Devices

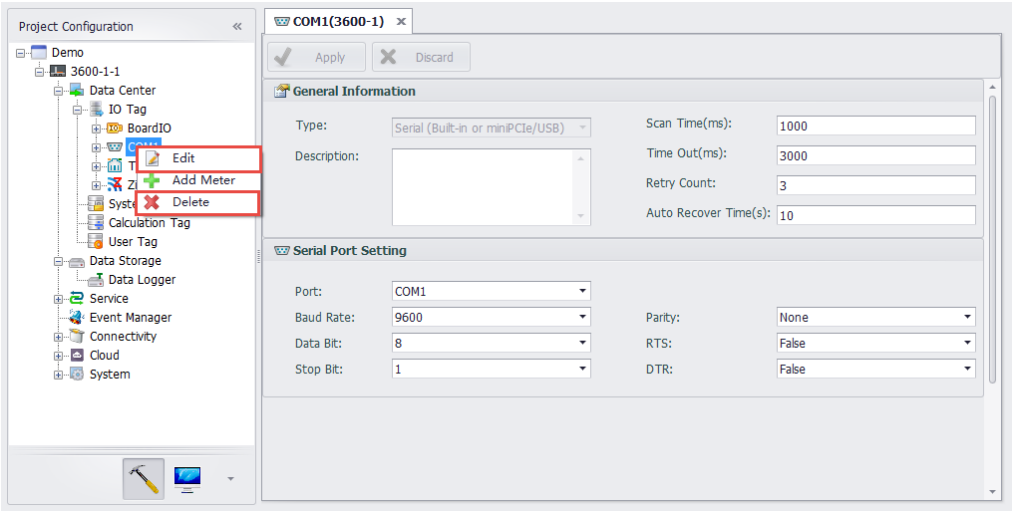
When creating the device, all serial ports on devices will be created at the same time. Users need to add new ports into EdgeLink Studio following the below procedures.



1. Right-click on “IO Tag” and choose “Add Port”.
2. Select the port type from the drop-down list. Then “Serial Port Setting” will appear and allow users to set the related parameters according to their requirements.
3. After the setup, click “Apply” button to save the changes.If users do not want to save the changes, click “Discard” button.

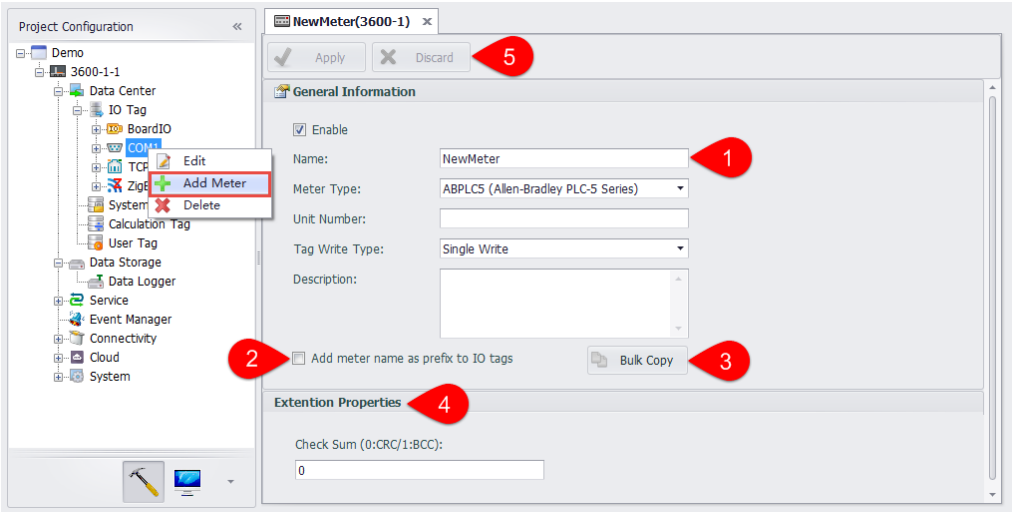
After the port has been added successfully, users can edit/delete it and add device.

A. Right-click on the port name and select “Edit” to change the serial port settings which are shown in below.



B. Right-click on the port name and select “Delete” to remove this port.

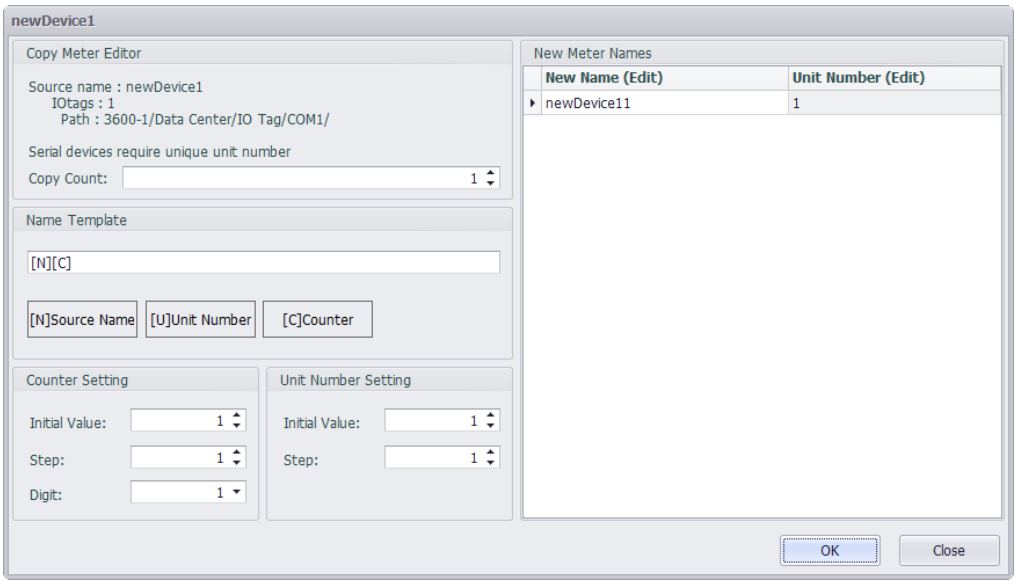
C. Right-click on the port name and select “Add Device” to configure the serial device, whose detailed settings are shown in the below figure.



1.Fill in the device name information, select the device type, set the device unit number, IO tag write mode, fill in the description information (optional).

2.Select whether to add a name prefix to the IO tag. If you select “Yes”, the Tag name is composed of “Device name: Tag name” when you add a Tag under this device.

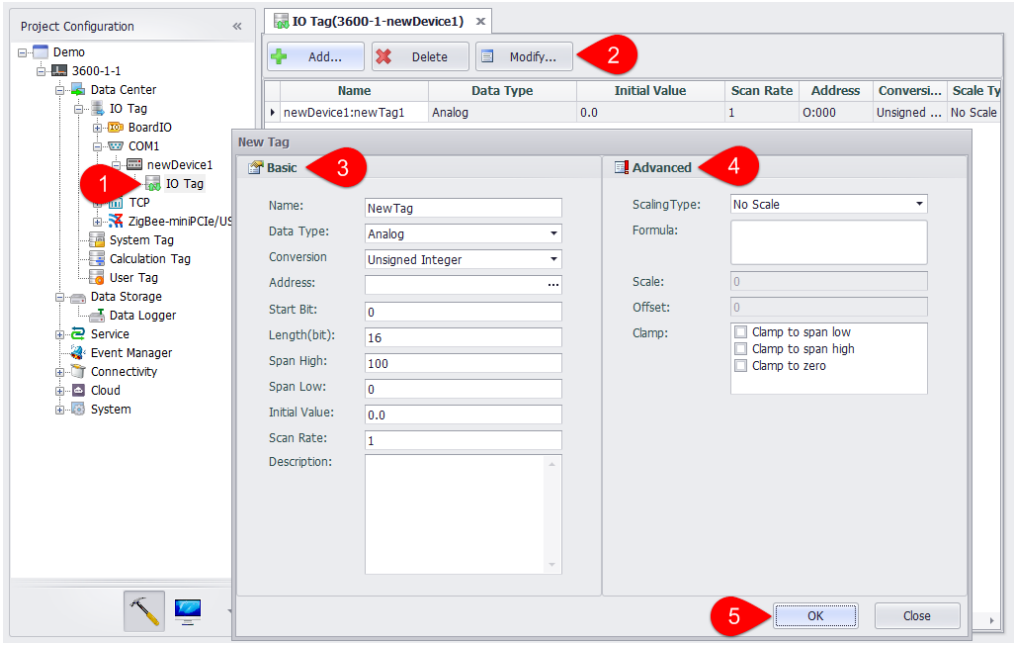
3.Whether to batch copy the Tags under this device. The button is only available if you have chosen to add a name prefix to the IO tag.



4.In “Extension Properties”, users can know the different protocols and their corresponding configurations.

5.Then, click “Apply” button save the settings.If users do not want to save the changes, click “Discard” button.

D.After a new device has been successfully added, users need to configure IO tag, the procedures of which are similar as for “Configure Onboard IO” (see below).。

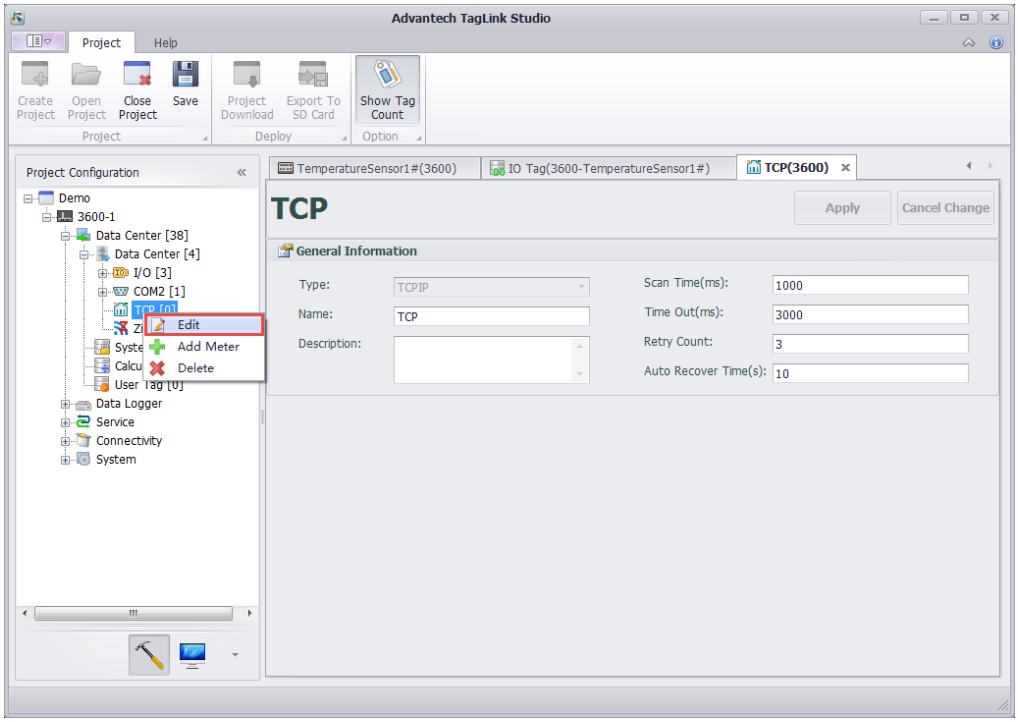


E.If users want to delete the newly added device, right-click on the device name and select “Delete” to remove it.

Configure IO of Ethernet Devices

EdgeLink Studio supports to edit/delete the port via Ethernet and add device to it.

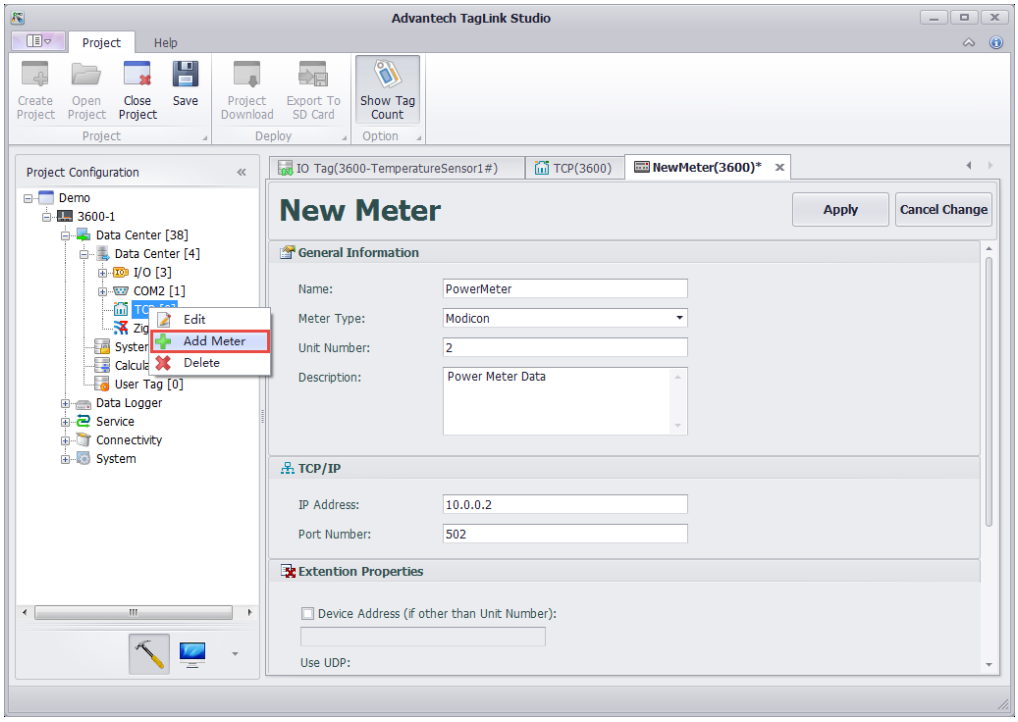
1. Right-click on the port name and select “Edit” to change the Ethernet port settings which are shown in below.



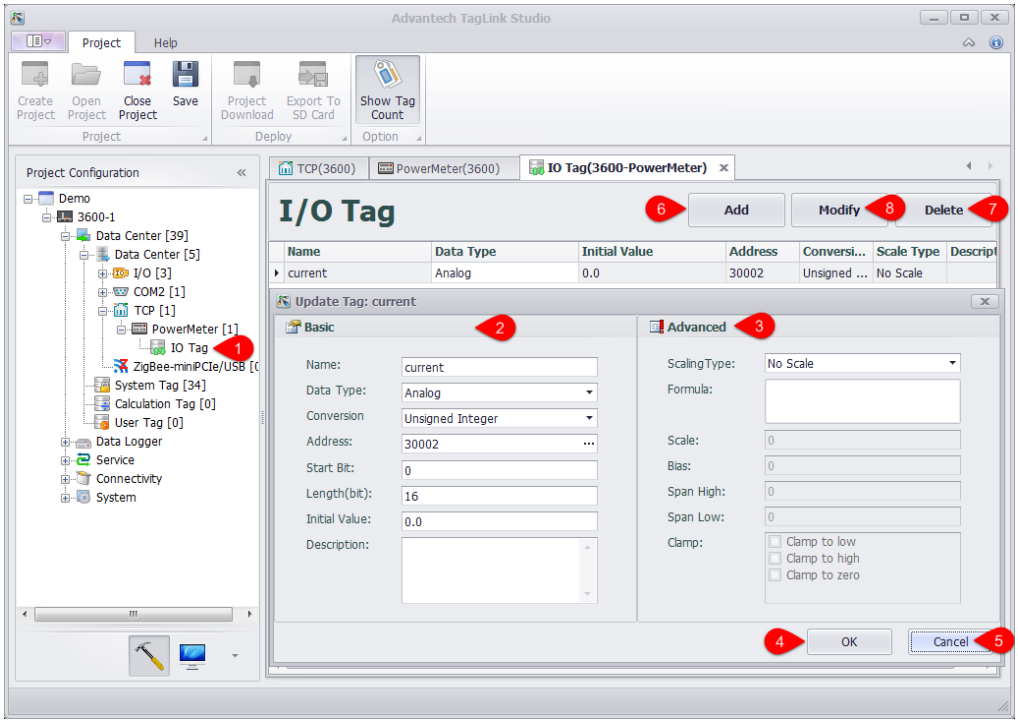
Note! This TCP port is a software port, so the quantity of its entity ports is not restricted to 2 . Users can freely add a new port as required.

2. Right-click on the port name and select “Delete” to remove this port.
3. Right-click on the port name and select “Add Device” to configure the Ethernet device, whose detailed

settings are shown in the below figure.



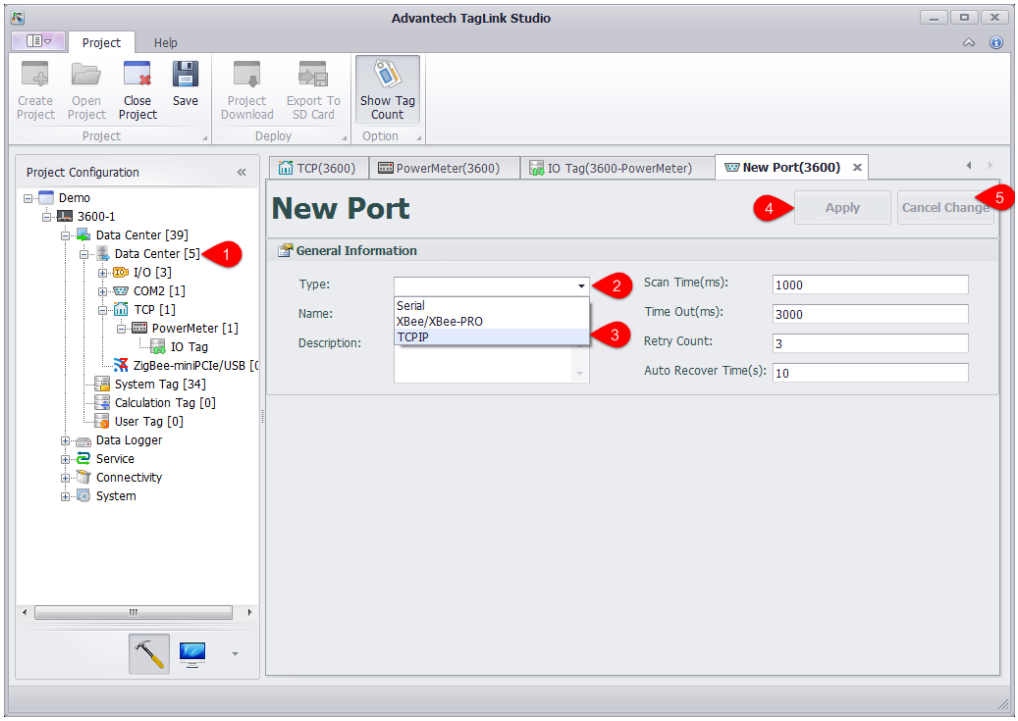
4. After a new device has been successfully added, users need to configure IO tag, the procedures of which are similar as for “Configure Onboard IO” (see below).



If users want to delete the newly added device, right-click on the device name and select “Delete” to remove it.

It should be noted that EdgeLink Studio supports one Ethernet port by default. If two or more Ethernet ports are required, users need to add new ports referring to the following procedures.

1. Right-click on “Data Center” and select “Add Port”.
2. Select the port type and fill in the port name.
3. Give a description of the port, which is optional.
4. Then, click “Apply” button save the settings.
5. If users do not want to save the changes, click “Discard” button.

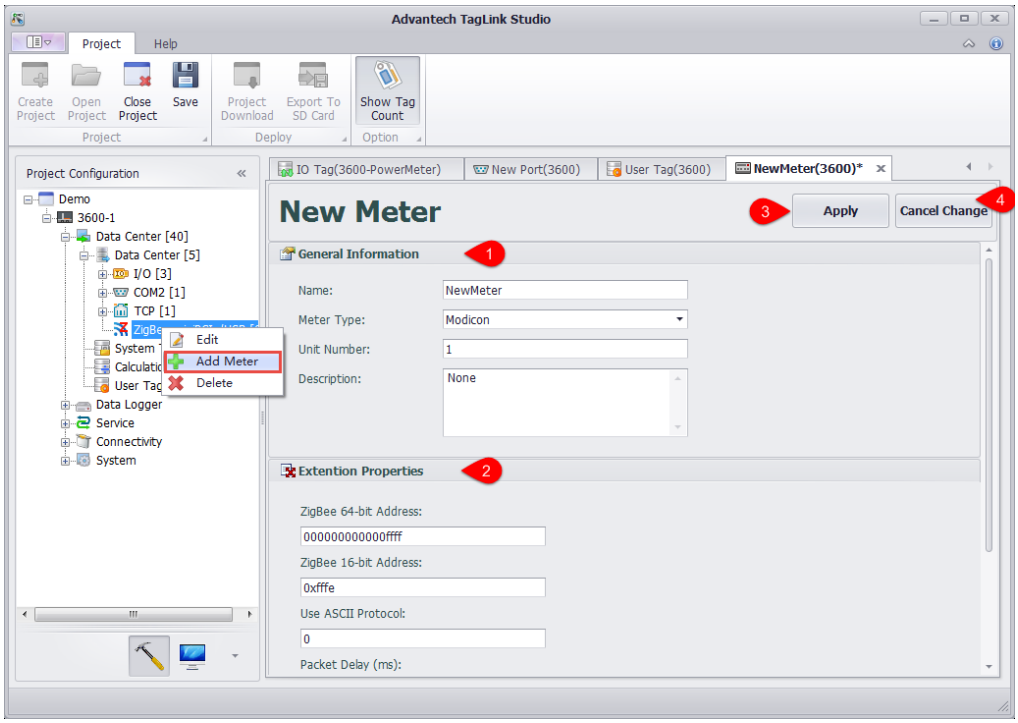


Configure IO of Wireless Zigbee Devices

For acquisition requirements of wireless Zigbee devices, users can right-click on the port name to edit/delete it and add device to it.

a. The port settings are preset when Zigbee port was firstly added. If there is any information needed to be changed, right-click on the port name and select “Edit” to modify, then click “Apply” button to save the changes.

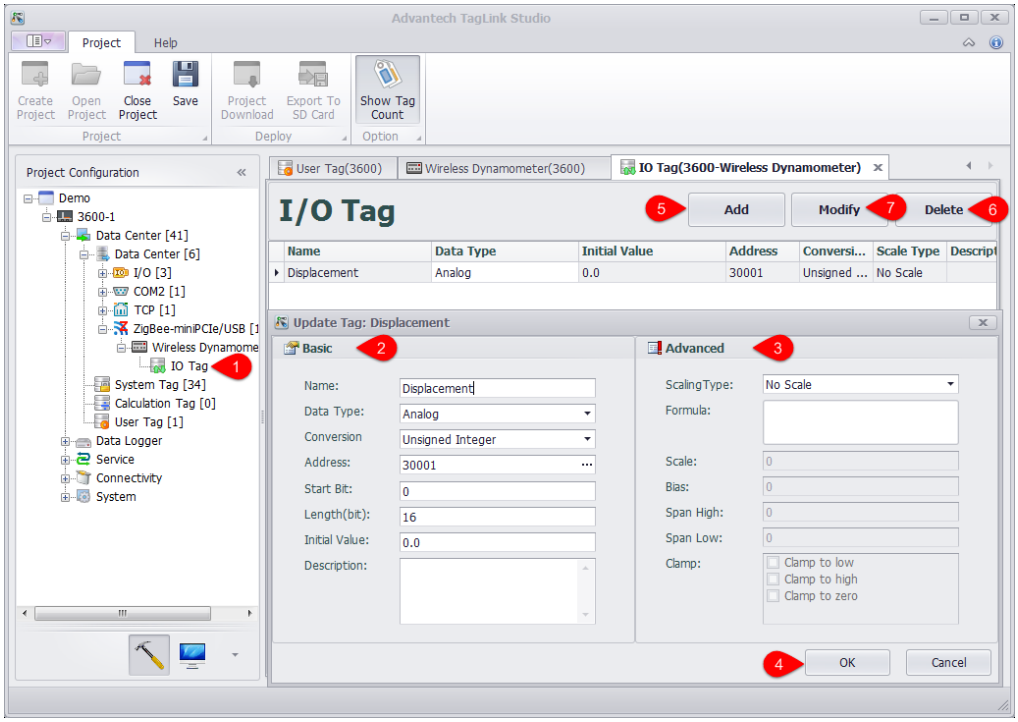
B. Right-click on the port name and select “Add Device” to add a new Zigbee device.



C. Add IO tag of wireless Zigbee device, the procedures of which are similar as for “Configure Onboard IO” (see

below).

1. Double-click or right-click IO tag to edit it.
2. Fill in the basic information of the tag.
3. Set the scaling type of the tag.
4. Click “OK” button to add this new tag.
5. Click “Add” button to add another tag.
6. Select one or several tags and click “Delete” button to remove it/them.
7. Select one or several tags and click “Modify” button to modify it/them.



The Zigbee wireless device supports configuring tags in the device template mode. For details, see 2.2.12 Device Template.

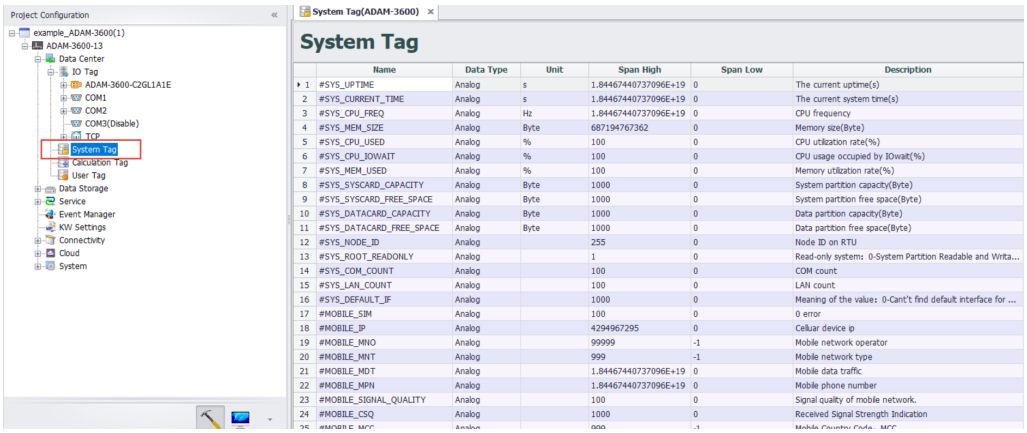
System Tag

There are two types of system tags：**General system tag**和**Special system tag**

General system tag：It is generally read-only. System-related information, module (4G, Wifi, GPS) information, serial port, network port information, etc

Special system tag：Some can be read and written

1. When a meter is added to DataCenter, three system tags are generated, representing information about the meter.
2. DatLogger Status



	Name	Data Type	Unit	Span High	Span Low	Description
1	#SYS_UPTIME	Analog	s	1.84467440737096E+19	0	The current uptime(s)
2	#SYS_CURRENT_TIME	Analog	s	1.84467440737096E+19	0	The current system time(s)
3	#SYS_CPU_FREQ	Analog	Hz	1.84467440737096E+19	0	CPU frequency
4	#SYS_MEM_SIZE	Analog	Byte	687194767362	0	Memory size(Byte)
5	#SYS_CPU_USED	Analog	%	100	0	CPU utilization rate(%)
6	#SYS_CPU_IOWAIT	Analog	%	100	0	CPU usage occupied by IOwait(%)
7	#SYS_MEM_USED	Analog	%	100	0	Memory utilization rate(%)
8	#SYS_SYSCARD_CAPACITY	Analog	Byte	1000	0	System partition capacity(Byte)
9	#SYS_SYSCARD_FREE_SPACE	Analog	Byte	1000	0	System partition free space(Byte)
10	#SYS_DATACARD_CAPACITY	Analog	Byte	1000	0	Data partition capacity(Byte)
11	#SYS_DATACARD_FREE_SPACE	Analog	Byte	1000	0	Data partition free space(Byte)
12	#SYS_NODE_ID	Analog		255	0	Node ID on RTU
13	#SYS_ROOT_READONLY	Analog		1	0	Read-only system: 0-System Partition Readable and Writa...
14	#SYS_COM_COUNT	Analog		100	0	COM count
15	#SYS_LAN_COUNT	Analog		100	0	LAN count
16	#SYS_DEFAULT_IF	Analog		1000	0	Meaning of the value: 0-Can't find default interface for ...
17	#MOBILE_SIM	Analog		100	0	0 error
18	#MOBILE_IP	Analog		4294967295	0	Cellular device ip
19	#MOBILE_MNO	Analog		99999	-1	Mobile network operator
20	#MOBILE_MNT	Analog		999	-1	Mobile network type
21	#MOBILE_MDT	Analog		1.84467440737096E+19	0	Mobile data traffic
22	#MOBILE_MPN	Analog		1.84467440737096E+19	0	Mobile phone number
23	#MOBILE_SIGNAL_QUALITY	Analog		100	0	Signal quality of mobile network.
24	#MOBILE_CSQ	Analog		1000	0	Received Signal Strength Indication

General system tag description(Read Only)

Name	Description
#SYS_UPTIME	The current uptime(s)
#SYS_CURRENT_TIME	The current system time(s)
#SYS_CPU_FREQ	CPU frequency
#SYS_MEM_SIZE	Memory size(Byte)

Name	Description
#SYS_CPU_USED	CPU utilization rate(%)
#SYS_CPU_IOWAIT	CPU usage occupied by IOwait(%)
#SYS_MEM_USED	Memory utilization rate(%)
#SYS_SYSCARD_CAPACITY	System partition capacity(Byte)
#SYS_SYSCARD_FREE_SPACE	System partition free space(Byte)
#SYS_DATACARD_CAPACITY	Data partition capacity(Byte)
#SYS_DATACARD_FREE_SPACE	Data partition free space(Byte)
#SYS_NODE_ID	Node ID on RTU
#SYS_ROOT_READONLY	Read-only system：0-System Partition Readable and Writable, 1-System Partition Read-Only
#SYS_COM_COUNT	COM count
#SYS_LAN_COUNT	LAN count
#SYS_DEFAULT_IF	Meaning of the value：0-Cant’t find default interface for route, 1-LAN1, 2-LAN2, 3-LAN3, 4-LAN4, 101-WiFi, 201-Cellular

#MOBILE_SIM	**Name**	**Description**
		0 error 1 READY: MT is not pending for any password 2 SIM PIN: MT is waiting SIM PIN to be given 3 SIM PUK: MT is waiting SIM PUK to be given 4 SIM PIN2: MT is waiting SIM PIN2 to be given 5 SIM PUK2: MT is waiting SIM PUK2 to be given 6 PH-NET PIN: MT is waiting network personalization password to be given 7 PH-NETSUB PIN: MT is waiting network subset personalization password to be given 8 PH-SP PIN: MT is waiting service provider personalization password to be given 9 PH-CORP PIN: MT is waiting corporate personalization password to be given 10 PH-SIM PIN:

Name	Description
	MT is waiting phone to SIM/UICC card password to be given 99 not known
#MOBILE_IP	Celluar device ip
#MOBILE_MNO	Mobile network operator
#MOBILE_MNT	Mobile network type
#MOBILE_MDT	Mobile data traffic
#MOBILE_MPN	Mobile phone number
#MOBILE_SIGNAL_QUALITY	Signal quality of mobile network
#MOBILE_CSQ	Received Signal Strength Indication
#MOBILE_MCC	Mobile Country Code，MCC
#MOBILE_MNC	Mobile Network Code，MNC
#MOBILE_LAC	Location Area Code, LAC
#MOBILE_CID	Cell Tower ID, Cid
#MOBILE_IMSI	IMSI, International Mobile Subscriber Identity
#MOBILE_IMEI	IMEI, International Mobile Equipment Identity

Name	Description
#MOBILE_IMEI_RAW	IMEI raw data
#MOBILE_USBID	mobile modem, usb vendor id, product id
#MOBILE_DATA_DAY	Cellular data, current day used traffic
#MOBILE_DATA_MONTH	Cellular data, current month used traffic
#MOBILE_DATA_YEAR	Cellular data, current year used traffic
#WLAN0_SIGNAL_QUALITY	Signal quality of wlan0
#WLAN0_SIGNAL_LEVEL	Signal level of wlan0
#WLAN0_SIGNAL_NOISE	Signal noise of WLAN0
#WLAN0_SIGNAL_BITRATE	Bit rate of WLAN0
#WLAN0_AP_MAC	MAC or BSSID in Wifi AP mode
#ICDM_COM1_SCORE	COM 1 score
#ICDM_COM2_SCORE	COM 2 score
#ICDM_COM3_SCORE	COM 3 score
#ICDM_LAN1_SCORE	LAN 1 score
#ICDM_LAN1_LINK	LAN 1 link state
#ICDM_LAN2_SCORE	LAN 2 score

Name	Description
#ICDM_LAN2_LINK	LAN 2 link state
#GPS_LATITUDE	Latitude for the GPS module
#GPS_LONGITUDE	Longitude for the GPS module
#GPS_ALTITUDE	Altitude for the GPS module
#GPS_SPEED	Speed for the GPS module
#GPS_COURSE	Course for the GPS module
#GPS_SATELLITE	Status of the GPS module: 0-error state, 1-use GPS module working, 2-use a preset location information
#SYS_BATTERY_LOW	Battery power: 1 indicates that the battery is low, 0 indicates that the battery is normal
#SYS_TIME_SECOND	(0~59, when leap seconds: 60)
#SYS_TIME_MINUTE	Minutes（0~59）
#SYS_TIME_HOUR	Hours (0~23)
#SYS_TIME_DAY	Day (1~31)
#SYS_TIME_MONTH	Month (1~12)
#SYS_TIME_YEAR	Year (for example,2016)

Name	Description
#SYS_TIME_WDAY	Week (0~6, Sunday: 0, Monday to Saturday: 1~6)
#SYS_TIME_YDAY	Number of days from the beginning of the annual January 1st (0~365,January 1st: 0, January 2nd: 1, and so on)
#SYS_TIME_ISDST	Daylight saving time identifier, implementing daylight saving time, the value is positive. Do not implement the time in the summer, the value is 0. Cannot be determined when the value is negative
#SYS_TIME_GMT_OFFSET	The deviation of GMT seconds and local time, the eastern time zone is positive and negative for West Zone, such as China, should be 28800
#DATALOG_ENABLE	Enable Datalogger storage when the value is 1, and stop storage when the value is 0

Name	Description
#DATALOG_ERROR	When the value of DATALOG_ERROR is 0, it means that there is no error in the program. Check the manual for other error code information
#SYS_MAC_LAN1	MAC address of lan1
#SYS_MAC_LAN2	MAC address of lan2
#SYS_TFCARD_CAPACITY	TF card capacity(Byte)
#SYS_TFCARD_FREE_SPACE	TF card root partition free space(Byte)
#SYS_SDCARD_CAPACITY	SD card capacity(Byte),the value is 0 if there is no SD card
#SYS_SDCARD_FREE_SPACE	SD card free space(Byte),the value is 0 if there is no SD card
#SYS_DNP3_AI_POLLED_COUNTER	The number of times AI data was polled in DNP3 Outstation

Name	Description
#MQTTStatus_WISE-Edge365_0	0- Not connected; 1- Connecting; 2- Connected, subscribing to topics; 3- Connected，the topics is subscribed

Special system tag description

- **#DATALOG_ENABLE** ： Read-write, enabling DataLogger storage when the value is 1 and stopping the DataLogger storage when the value is 0
- **#DATALOG_ERROR** ： Read-only, 0—The program runs normally, other error codes need to be found in the DataLogger manual section
- **#DISABLE_DEVICE_MeterName** ： Read-write, each meter in the DataCenter has its own tag, distinguished by the name of the meter. 0—meter available, 1—meter not available. For example, if the meter name is Test Device 1, there will be a corresponding system tag #DISABLE_DEVICE_ Test Device 1, through which the meter can be disabled or started
- **#BATCH_WRITE_MeterName** ： Read-write, each meter in the DataCenter has its own tag, distinguished by the name of the meter. 0—meter single point write, 1—meter batch write. For example, if the name of the meter is testdevice1, there will be a corresponding system point #BATCH_WRITE_ testdevice1, through which the writing method of the meter can be set

- **#DEVICE_ERROR_MeterName** ： Read-only, each meter in the DataCenter has its own tag, distinguished by the name of the meter. The error code when the current meter is collecting errors. For example, if the instrument name is TestDevice1, there will be a corresponding system tag #DEVICE_ERROR_TestDevice1, through which the current meter collection status can be viewed
- **#DISABLE_PORT_PortName** ： Read-write, each port has its own tag, 0—port available, 1-disable port. For example, the COM1 port will have a corresponding system tag #DISABLE_PORT_COM1, through which the port can be turned on or disabled

Configure Calculation Tag

Calculation tag is a kind of special tags, the value of which indicates the calculation result of an formula. The parameter of this formula can be a tag or a constant. Also, the expression can utilize some common calculation methods, including arithmetic & logic operation and trigonometric function, etc..

Calculation tag can perform some relatively complex operations, such as converting the acquired sensor value to the real physical quantity (liquid level, wind speed, etc.), so as to make the computation less intensive for the upper computer as well as the device more intelligent.

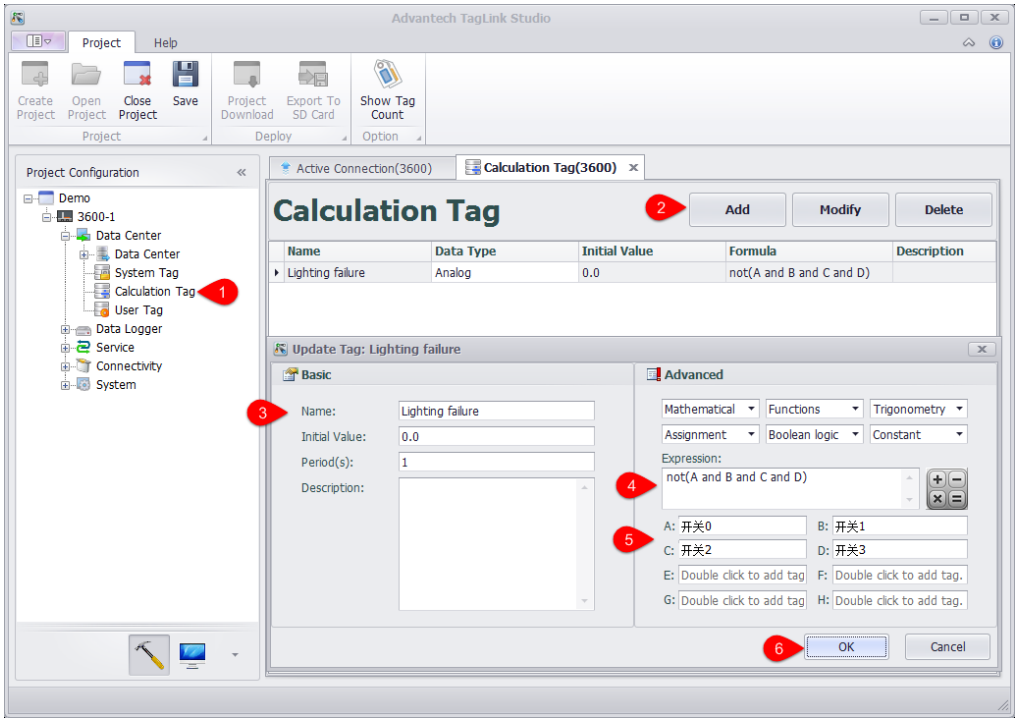
Each calculation tag corresponds to one expression which may support at most 8 tags as its input variables. For users' convenience, 8 tags are represented by A, B, C, D, E, F, G and H (case insensitive) in the expression.

Add Calculation Tag

Please follow the procedures to add a calculation tag:

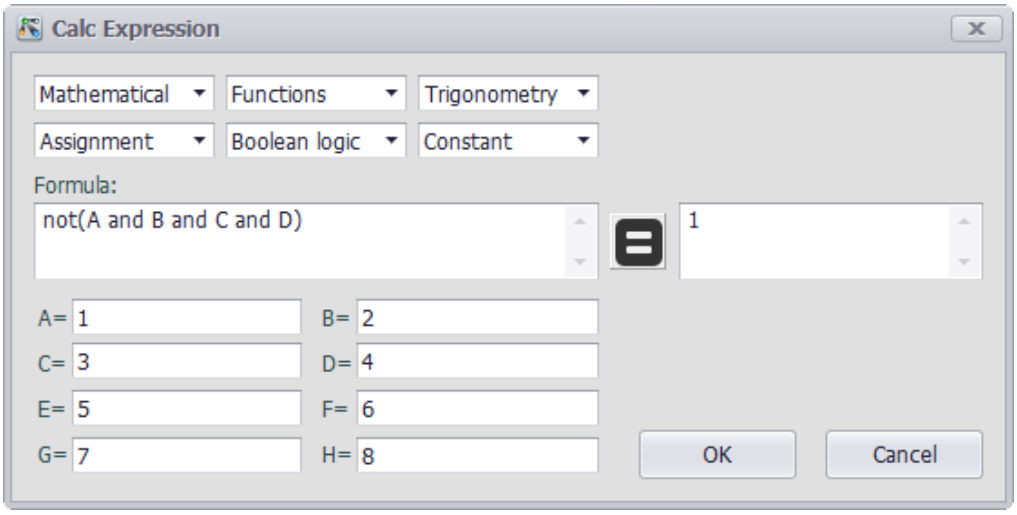
1. Double-click on "Calculation Tag" in the left tree menu.
2. Click "Add" button to add a new calculation tag.
3. Fill in the basic information. "Periods (s)" specifies how often the tags are calculated, and its unit is second.

4. Enter an expression. Uses can select default function or operator from the pull-down lists or type them manually. The example figure shows the calculation expression of “Lighting Failure”, the expression logic of which is that the lighting is failed when the value of any tag in four switches is 0.
5. Double-click the variable box to add a tag.
6. Click “OK” button to save the changes.



Expression Check

On the right of “Expression” box there is a calculator button . Click it to open “Calc Expression” window shown as below. This interface is roughly the same as “Advanced” setting interface in the above, but with a “=” button and a box displaying the operation result. Besides, the variable boxes here require users to input the variable values rather than tag names.



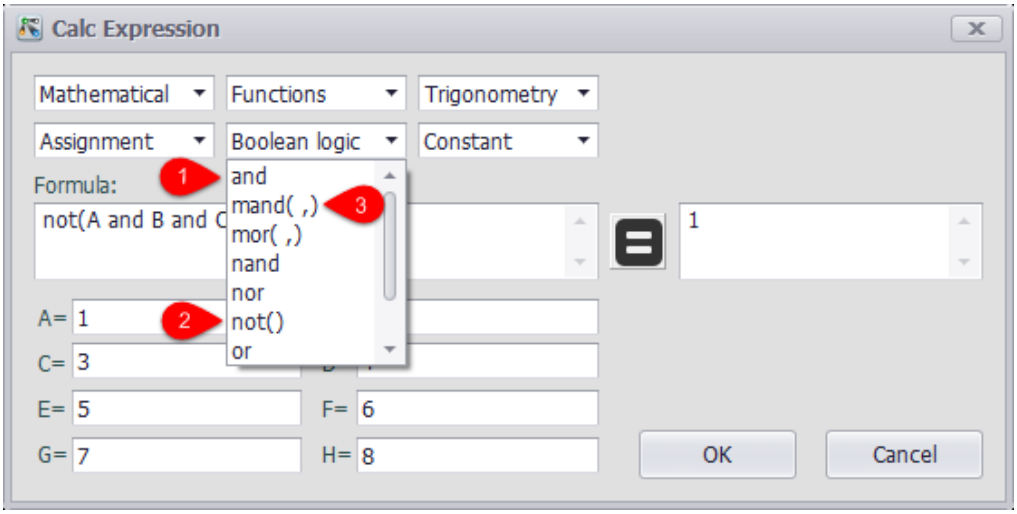
To verify the expression is correct or not, users can click this button to get the result, then review it to see its correctness. After the expression has been verified, click “OK” button to update the value; if users do not want to update it, click “Cancel” button.

Function and Operator Description

Through the drop-down boxes, users can set the functions and operators calculation tag supports, which is divided into five categories: “Mathematical”, “Functions”, “Trigonometry”, “Assignment” and “Boolean logic”. Moreover, “Constant” box is also provided,

allowing users to select from three constants: pi (the ratio of the circumference to the diameter of a circle), epsilon (the smallest positive double value that is greater than zero) and inf (infinity).

As shown in the figure below, the functions or operators listed in the box can be classified into three types: 1. With no brackets, this indicates binary operations (labeled with 1); 2. With brackets but no comma, this means this function only has one parameter (labeled with 2); 3. With brackets and comma, this means the function supports more than one parameter (labeled with 3).



All functions and operators are described as follows:

0. Arithmetic & Assignment Operators

OPERATOR	DEFINITION
+	Addition between x and y. (eg: x + y)
-	Subtraction between x and y. (eg: x - y)

OPERATOR	DEFINITION
*	Multiplication between x and y. (eg: x * y)
/	Division between x and y. (eg: x / y)
%	Modulus of x with respect to y. (eg: x % y)
^	x to the power of y. (eg: x ^ y)
:=	Assign the value of x to y. Where y is either a variable or vector type. (eg: y := x)
+=	Increment x by the value of the expression on the right hand side. Where x is either a variable or vector type. (eg: x += abs(y - z))
-=	Decrement x by the value of the expression on the right hand side. Where x is either a variable or vector type. (eg: x[i] -= abs(y + z))

OPERATOR	DEFINITION
*=	Assign the multiplication of x by the value of the expression on the righthand side to x. Where x is either a variable or vector type. (eg: x *= abs(y / z))
/=	Assign the division of x by the value of the expression on the right-hand side to x. Where x is either a variable or vector type. (eg: x[i + j] /= abs(y * z))
%=	Assign x modulo the value of the expression on the right hand side to x. Where x is either a variable or vector type. (eg: x[2] %= y ^ 2)

1. Equalities & Inequalities

OPERATOR	DEFINITION
== or =	True only if x is strictly equal to y. (eg: x == y)

OPERATOR	DEFINITION
<> or !=	True only if x does not equal y. (eg: x <> y or x != y)
<	True only if x is less than y. (eg: x < y)
<=	True only if x is less than or equal to y. (eg: x <= y)
>	True only if x is greater than y. (eg: x > y)
>=	True only if x greater than or equal to y. (eg: x >= y)

2. Boolean Operations

OPERATOR	DEFINITION
true	True state or any value other than zero (typically 1).
false	False state, value of exactly zero.
and	Logical AND, True only if x and y are both true. (eg: x and y)
mand	Multi-input logical AND, True only if all inputs are true. Left to right short-circuiting of expressions. (eg: mand(x > y, z < w, u or v, w and x))

OPERATOR	DEFINITION
mor	Multi-input logical OR, True if at least one of the
nand	Logical NAND, True only if either x or y is false. (eg: x nand y)
nor	Logical NOR, True only if the result of x or y is false (eg: x nor y)
not	Logical NOT, Negate the logical sense of the input. (eg: not(x and y) == x nand y)
or	Logical OR, True if either x or y is true. (eg: x or y)
xor	Logical XOR, True only if the logical states of x and y differ. (eg: x xor y)
xnor	Logical XNOR, True iff the biconditional of x and y is satisfied. (eg: x xnor y)

OPERATOR	DEFINITION
&	Similar to AND but with left to right expression short circuiting optimisation. (eg: (x & y) == (y and x))

3. General Purpose Functions

FUNCTION	DEFINITION
abs	Absolute value of x. (eg: abs(x))
avg	Average of all the inputs. (eg: avg(x,y,z,w,u,v) == (x + y + z + w + u + v) / 6)
ceil	Smallest integer that is greater than or equal to x.
clamp	Clamp x in range between r0 and r1, where r0 < r1. (eg: clamp(r0,x,r1))
equal	Equality test between x and y using normalised epsilon
erf	Error function of x. (eg: erf(x))

FUNCTION	DEFINITION
erfc	Complimentary error function of x. (eg: erfc(x))
exp	e to the power of x. (eg: exp(x))
expm1	e to the power of x minus 1, where x is very small. (eg: expm1(x))
floor	Largest integer that is less than or equal to x. (eg: floor(x))
frac	Fractional portion of x. (eg: frac(x))
hypot	Hypotenuse of x and y (eg: hypot(x,y) = sqrt(x*x* + *yy*))
iclamp	Inverse-clamp x outside of the range r0 and r1. Where r0 < r1. If x is within the range it will snap to the closest bound. (eg: iclamp(r0,x,r1)
inrange	In-range returns ‘true’ when x is within the range r0 and r1. Where r0 < r1. (eg: inrange(r0,x,r1)
log	Natural logarithm of x. (eg: log(x))

FUNCTION	DEFINITION
log10	Base 10 logarithm of x. (eg: log10(x))
log1p	Natural logarithm of 1 + x, where x is very small. (eg: log1p(x))
log2	Base 2 logarithm of x. (eg: log2(x))
logn	Base N logarithm of x. where n is a positive integer. (eg: logn(x,8))
max	Largest value of all the inputs. (eg: max(x,y,z,w,u,v))
min	Smallest value of all the inputs. (eg: min(x,y,z,w,u))
mul	Product of all the inputs. (eg: mul(x,y,z,w,u,v,t) == (x * y * z * w * u * v * t))
ncdf	Normal cumulative distribution function. (eg: ncdf(x))
nequal	Not-equal test between x and y using normalised epsilon
pow	x to the power of y. (eg: pow(x,y) == x ^ y)

FUNCTION	DEFINITION
root	Nth-Root of x. where n is a positive integer. (eg: root(x,3) == x^(1/3))
round	Round x to the nearest integer. (eg: round(x))
roundn	Round x to n decimal places (eg: roundn(x,3)) where n > 0 and is an integer. (eg: roundn(1.2345678,4) == 1.2346)
sgn	Sign of x, -1 where x < 0, +1 where x > 0, else zero. (eg: sgn(x))
sqrt	Square root of x, where x >= 0. (eg: sqrt(x))
sum	Sum of all the inputs. (eg: sum(x,y,z,w,u,v,t) == (x + y + z + w + u + v + t))
swap	Swap the values of the variables x and y and return the
<=>	current value of y. (eg: swap(x,y) or x <=> y)
trunc	Integer portion of x. (eg: trunc(x))

4. Trigonometry Functions

FUNCTION	DEFINITION
acos	Arc cosine of x expressed in radians. Interval [-1,+1] (eg: acos(x))
acosh	Inverse hyperbolic cosine of x expressed in radians. (eg: acosh(x))
asin	Arc sine of x expressed in radians. Interval [-1,+1] (eg: asin(x))
asinh	Inverse hyperbolic sine of x expressed in radians. (eg: asinh(x))
atan	Arc tangent of x expressed in radians. Interval [-1,+1] (eg: atan(x))
atan2	Arc tangent of (x / y) expressed in radians. [-pi,+pi] eg: atan2(x,y)
atanh	Inverse hyperbolic tangent of x expressed in radians. (eg: atanh(x))
cos	Cosine of x. (eg: cos(x))

FUNCTION	DEFINITION
cosh	Hyperbolic cosine of x. (eg: cosh(x))
cot	Cotangent of x. (eg: cot(x))
csc	Cosecant of x. (eg: csc(x))
sec	Secant of x. (eg: sec(x))
sin	Sine of x. (eg: sin(x))
sinc	Sine cardinal of x. (eg: sinc(x))
sinh	Hyperbolic sine of x. (eg: sinh(x))
tan	Tangent of x. (eg: tan(x))
tanh	Hyperbolic tangent of x. (eg: tanh(x))
deg2rad	Convert x from degrees to radians. (eg: deg2rad(x))
deg2grad	Convert x from degrees to gradians. (eg: deg2grad(x))
rad2deg	Convert x from radians to degrees. (eg: rad2deg(x))
grad2deg	Convert x from gradians to degrees. (eg: grad2deg(x))

5. String Processing

FUNCTION	DEFINITION
= , ==	All common equality/inequality operators are applicable
!=, <>	to strings and are applied in a case sensitive manner.
<=, >=	In the following example x, y and z are of type string.
< , >	(eg: not((x <= ‘AbC’) and (‘1x2y3z’ <> y)) or (z == x)
in	True only if x is a substring of y. (eg: x in y or ‘abc’ in ‘abcdefgh’)
like	True only if the string x matches the pattern y. Available wildcard characters are ‘‘ *and ‘?’ denoting* *zero or more and zero or one matches respectively.* *(eg: x like y or ‘abcdefgh’ like ‘a?d*h’)

FUNCTION	DEFINITION
ilike	True only if the string x matches the pattern y in a case insensitive manner. Available wildcard characters are ‘‘ *and ‘?’ denoting zero or more and zero or one matches respectively. (eg: x ilike y or ‘a1B2c3D4e5F6g7H’ ilike ‘a?d*h’)

FUNCTION	DEFINITION
[r0:r1]	The closed interval [r0,r1] of the specified string. eg: Given a string x with a value of ‘abcdefgh’ then: 1. x[1:4] == ‘bcde’ 2. x[:5] == x[:10 / 2] == ‘abcdef’ 3. x[2 + 1:] == x[3:] ==‘defgh’ 4. x[:] == x[:] == ‘abcdefgh’ 5. x[4/2:3+2] == x[2:5] == ‘cdef’ Note: Both r0 and r1 are assumed to be integers, where r0 <= r1. They may also be the result of an expression, in the event they have fractional components truncation will be performed. (eg: 1.67 —> 1)

FUNCTION	DEFINITION
:=	Assign the value of x to y. Where y is a mutable string or string range and x is either a string or a string range. eg: 1. y := x 2. y := ‘abc’ 3. y := x[:i + j] 4. y := ‘0123456789’[2:7] 5. y := ‘0123456789’[2i + 1:7] 6. y := (x := ‘0123456789’[2:7]) 7. y[i:j] := x 8. y[i:j] := (x + ‘abcdefg’[8 / 4:5])[m:n] Note: For options 7 and 8 the shorter of the two ranges will denote the number characters that are to be copied.

FUNCTION	DEFINITION
+	Concatenation of x and y. Where x and y are strings or string ranges. eg 1. x + y 2. x + ‘abc’ 3. x + y[:i + j] 4. x[i:j] + y[2:3] + ‘0123456789’[2:7] 5. ‘abc’ + x + y 6. ‘abc’ + ‘1234567’ 7. (x + ‘a1B2c3D4’ + y)[i:2j]
+=	Append to x the value of y. Where x is a mutable string and y is either a string or a string range. eg: 1. x += y 2. x += ‘abc’ 3. x += y[:i + j] + ‘abc’ 4. x += ‘0123456789’[2:7]
<=>	Swap the values of x and y. Where x and y are mutable strings. (eg: x <=> y)

FUNCTION	DEFINITION
[]	The string size operator returns the size of the string being actioned. eg: 1. ‘abc’[] == 3 2. var max_str_length := max(s0[],s1[],s2[],s3[]) 3. (‘abc’ + ‘xyz’)[] == 6 4. ((‘abc’ + ‘xyz’)[1:4])[] == 4

6. Control Structures

STRUCTURE	DEFINITION
if	If x is true then return y else return z. eg: 1. if (x, y, z) 2. if ((x + 1) > 2y, z + 1, w / v) 3. if (x > y) z; 4. if (x <= 2*y) { z + w };

STRUCTURE	DEFINITION

if-else	The if-else/else-if statement. Subject to the condition branch the statement will return either the value of the consequent or the alternative branch.
	eg:
	1. if (x > y) z; else w;
	2. if (x > y) z; else if (w != u) v;
	3. if (x < y) { z; w + 1; } else u;
	4. if ((x != y) and (z > w))
	{
	y := sin(x) / u;
	z := w + 1;
	}
	else if (x > (z + 1))
	{
	w := abs (x - y) + z;
	u := (x + 1) > 2y ? 2u : 3u;
	}

STRUCTURE	DEFINITION

switch	The first true case condition that is encountered will determine the result of the switch. If none of the case conditions hold true, the default action is assumed as
	the final return value. This is sometimes also known as
	a multi-way branch mechanism.
	eg:
	switch
	{
	  case x > (y + z) : 2 * x / abs(y - z);
	  case x < 3 : sin(x + y);
	  default : 1 + x;
	}

STRUCTURE	DEFINITION

while	The structure will repeatedly evaluate the internal statement(s) ‘while’ the condition is true. The final statement in the final iteration will be used as the return value of the loop.
	eg:
	while ((x -= 1) > 0)
	{
	  y := x + z;
	  w := u + y;
	}

repeat/	The structure will repeatedly evaluate the internal

until	statement(s) ‘until’ the condition is true. The final statement in the final iteration will be used as the return value of the loop.
	eg:
	repeat
	  y := x + z;
	  w := u + y;
	until ((x += 1) > 100)

STRUCTURE	DEFINITION

for	The structure will repeatedly evaluate the internal statement(s) while the condition is true. On each loop iteration, an ‘incrementing’ expression is evaluated.
	The conditional is mandatory whereas the initialiser and incrementing expressions are optional.
	eg:
	for (var x := 0; (x < n) and (x != y); x += 1)
	{
	  y := y + x / 2 - z;
	  w := u + y;
	}

break	Break terminates the execution of the nearest enclosed

STRUCTURE	DEFINITION

break[]	loop, allowing for the execution to continue on external
	to the loop. The default break statement will set the return value of the loop to NaN, where as the return
	based form will set the value to that of the break expression.
	eg:
	while ((i += 1) < 10)
	{
	  if (i < 5)
	  j -= i + 2;
	  else if (i % 2 == 0)
	  break;
	  else
	  break[2i + 3];
	}

continue	Continue results in the remaining portion of the nearest enclosing loop body to be skipped.
	eg:
	for (var i := 0; i < 10; i += 1)
	{
	  if (i < 5)
	  continue;
	  j -= i + 2;
	}

STRUCTURE	DEFINITION
return	Return immediately from within the current expression. With the option of passing back a variable number of values (scalar, vector or string). eg: 1. return [1]; 2. return [x, ‘abx’]; 3. return [x, x + y,‘abx’]; 4. return []; 5. if (x < y) return [x, x - y, ‘result-set1’, 123.456]; else return [y, x + y, ‘result-set2’];
?:	Ternary conditional statement, similar to that of the above denoted if-statement. eg: 1. x ? y : z 2. x + 1 > 2y ? z + 1 : (w / v) 3. min(x,y) > z ? (x < y + 1) ? x : y : (w * v)

STRUCTURE	DEFINITION
~	Evaluate each sub-expression, then return as the result the value of the last sub-expression. This is sometimes known as multiple sequence point evaluation. eg: ~(i := x + 1, j := y / z, k := sin(w/u)) == (sin(w/u))) ~{i := x + 1; j := y / z; k := sin(w/u)} == (sin(w/u)))

[*]	Evaluate any consequent for which its case statement is true. The return value will be either zero or the result of the last consequent to have been evaluated.
	eg:
	[*]
	{
	case (x + 1) > (y - 2) : x := z / 2 + sin(y / pi);
	case (x + 2) < abs(y + 3) : w / 4 + min(5y,9);
	case (x + 3) == (y * 4) : y := abs(z / 6) + 7y;
	}

STRUCTURE	DEFINITION
[]	The vector size operator returns the size of the vector being actioned. eg: 1. v[] 2. max_size := max(v0[],v1[],v2[],v3[])

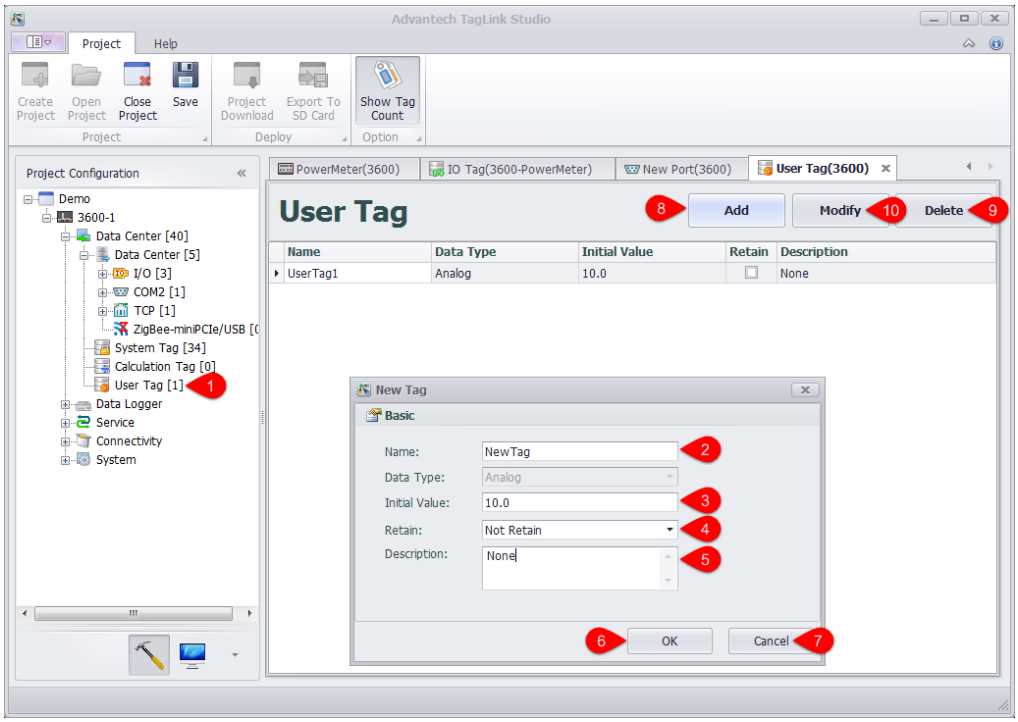
Configure User Tag

IO tags described in the previous sections are all real ones, while some unreal IO tags are also need in the process of project deployment. This kind of tags is optional and called User Tag which can be used for C and KW language programming, as a control signal or a manifestation of an operation result.

User tag configuration is supported by EdgeLink Studio. Users can configure them one by one based on real needs for future programming. Please follow the below procedures to configure a user tag:

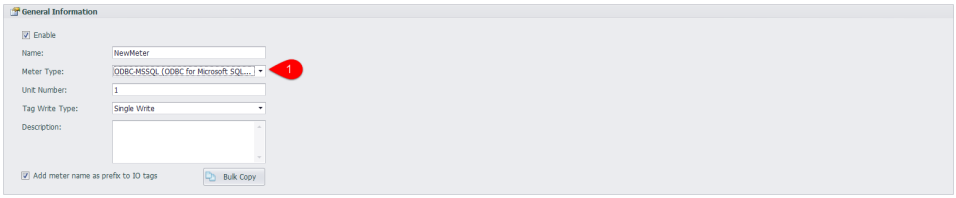
1. Double-click or right-click “User Tag” in the left menu tree to select “Edit”.
2. Fill in the tag name.
3. Select the data type.
4. Set the initial value.
5. Give a description of the user tag, which is optional.
6. Click “OK” button to save the changes.
7. If users do not want to save the changes, click “Cancel Change” button.
8. Add another new tag.
9. Users can select one or more tags and click “Delete” button.

10. Users can select one or more tags and click “Modify” button.

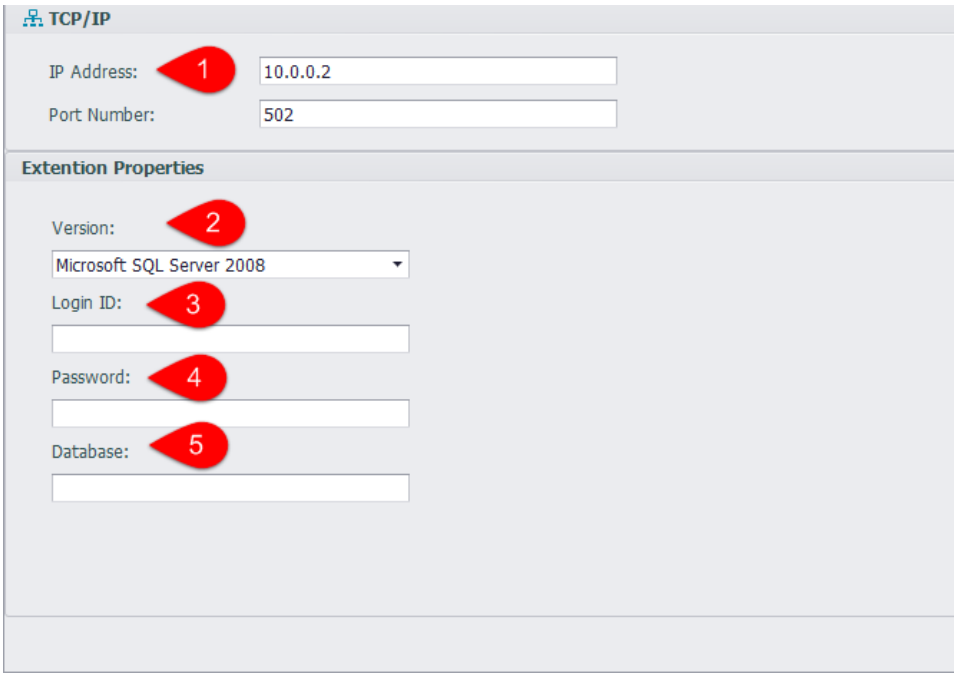


ODBC Device

1. Select the device type ODBC-MSSQL in the device interface, and can be configured to collect data via an online ODBC server



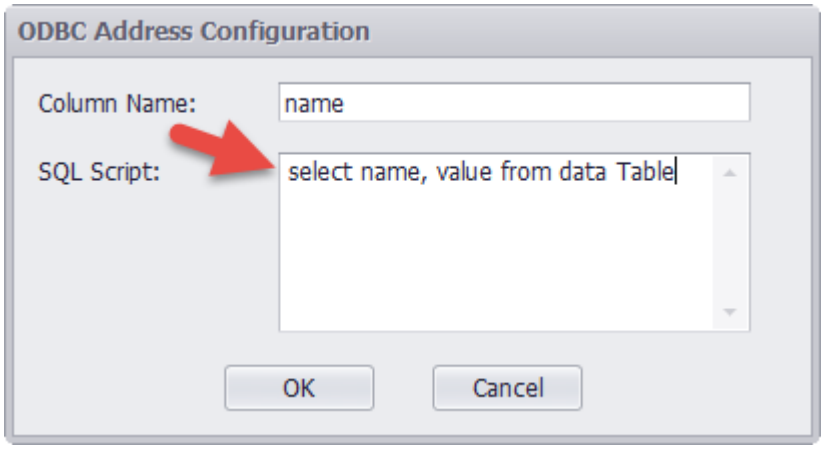
2. In the device interface, enter the ODBC service configuration.



   1. Server IP address.
   2. SQL Server version, you can choose SQL Server2008, SQL Server2005, SQL Server2000 and so on.
   3. The user name required for logging in SQL Server.
   4. The password required for logging in SQL Server.

5. The name of the database that you need to log in.

3. Data acquisition script

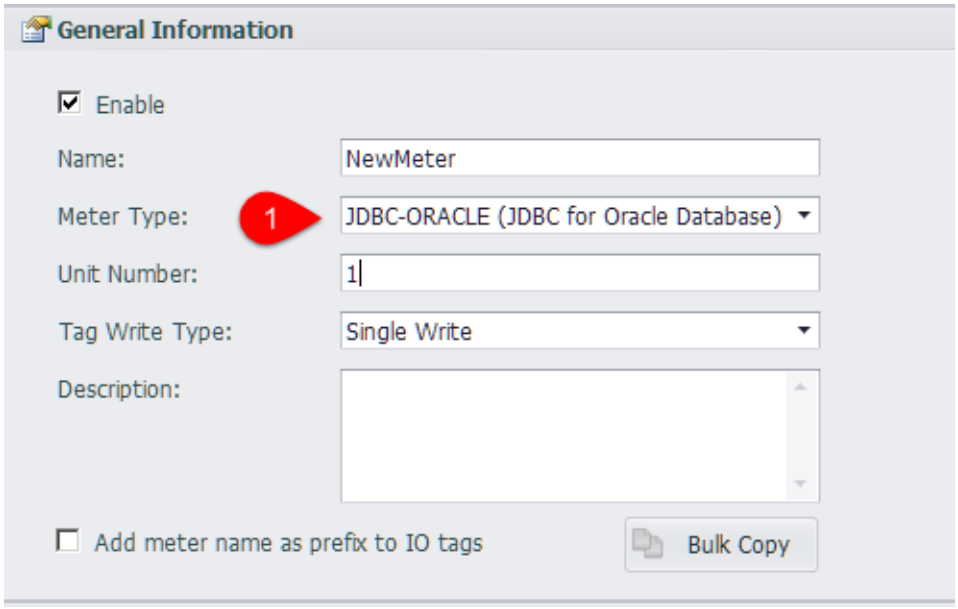


Click on the address bar of the Tag edit interface to edit the SQL scripts for data collection,

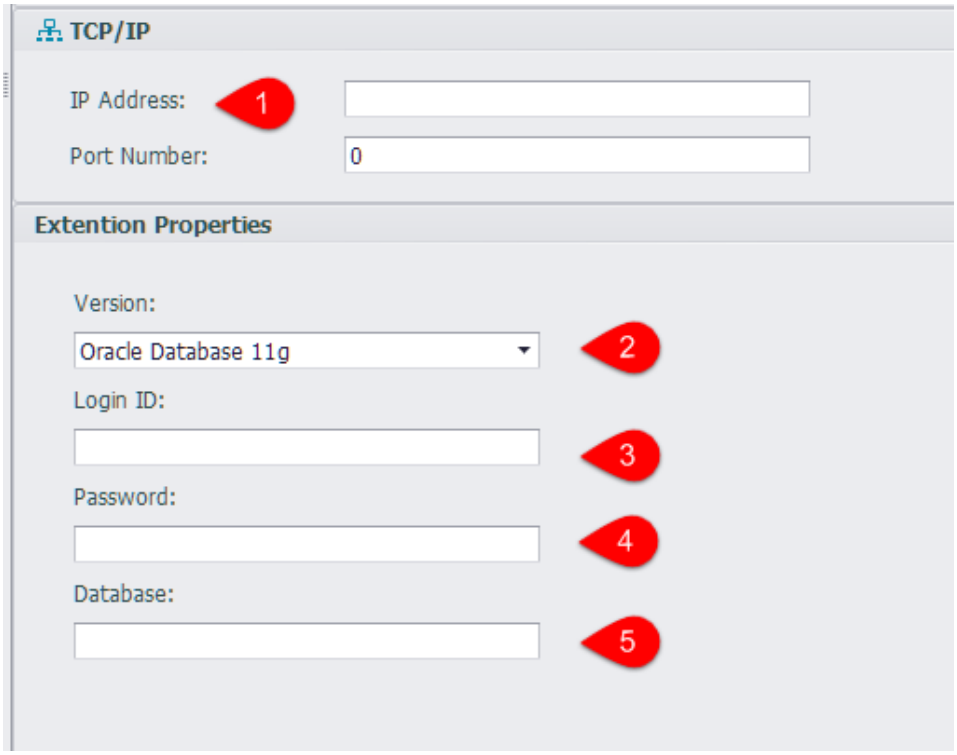
which “SQL Script” enter the SQL query script, “Column Name” enter the column name of the query result..

JDBC Device

1. Select the device type JDBC-ORACLE in the device interface, and can be configured to collect data via an online JDBC server

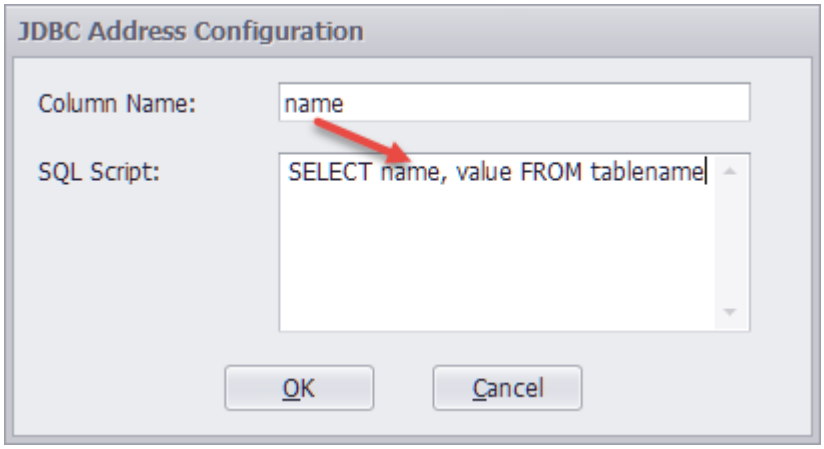


2. In the device interface, enter the JDBC service configuration.



1. Server IP address.
2. Oracle version, you can choose Oracle Database 10g、Oracle Database 11g、Oracle Database 12c and so on.
3. The user name required for logging in Oracle.
4. The password required for logging in Oracle.
5. The name of the database that you need to log in.

3. Data acquisition script



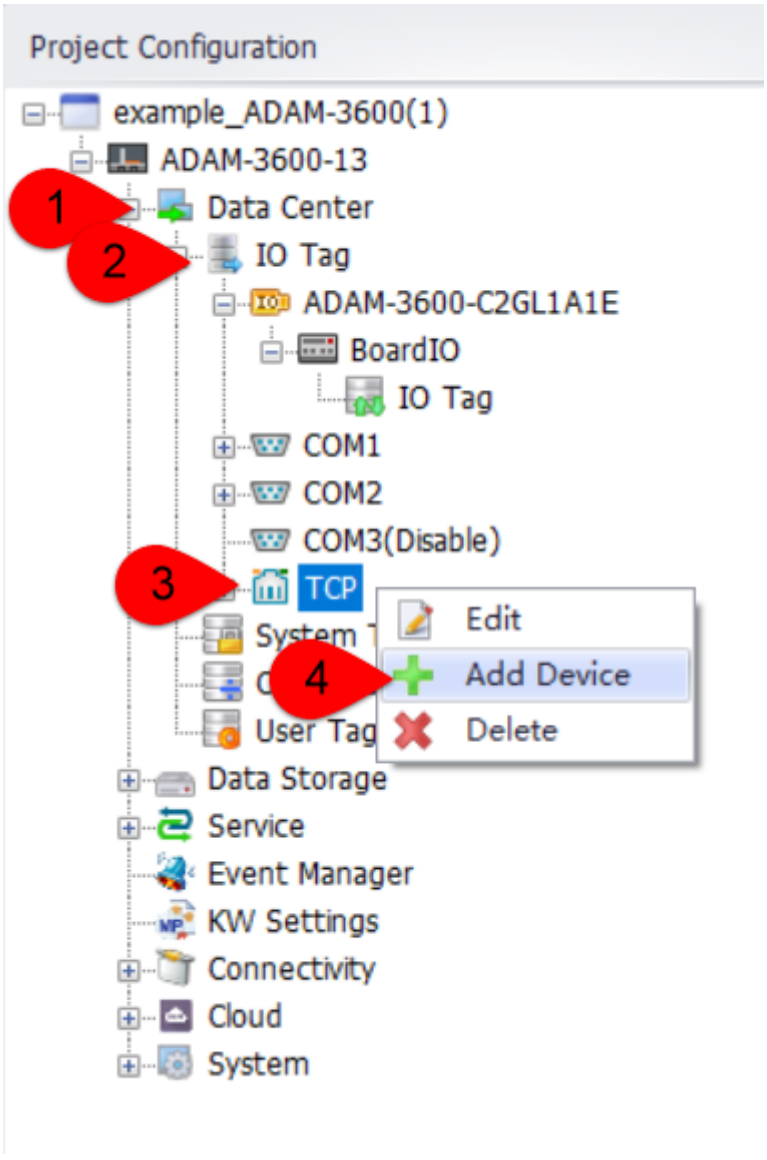
Click on the address bar of the Tag edit interface to edit the SQL scripts for data collection,

which “SQL Script” enter the SQL query script, “Column Name” enter the column name of the query result..

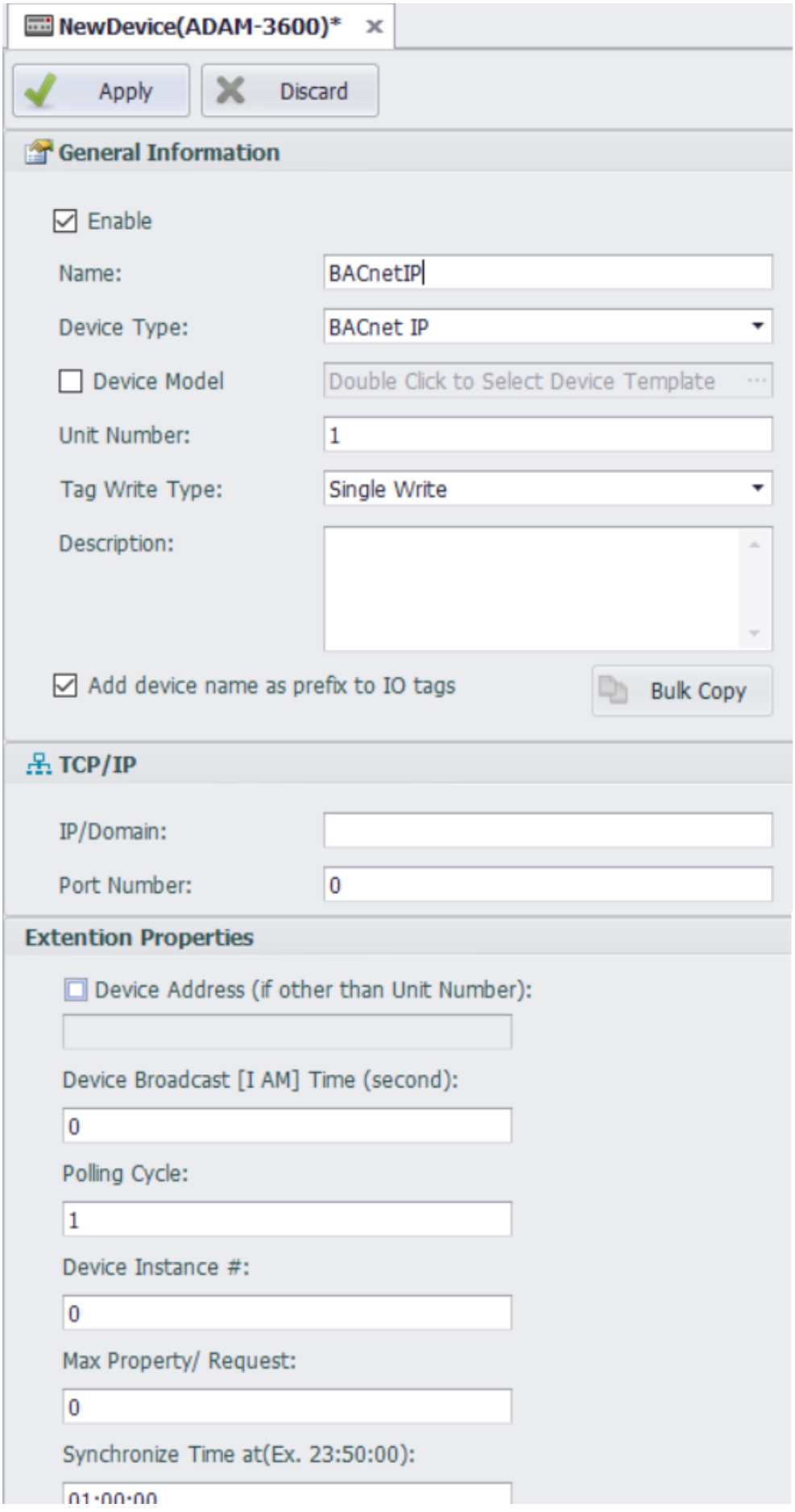
BACnet IP(TCP/IP)

1.Driver support start version number:

2.Add Meter

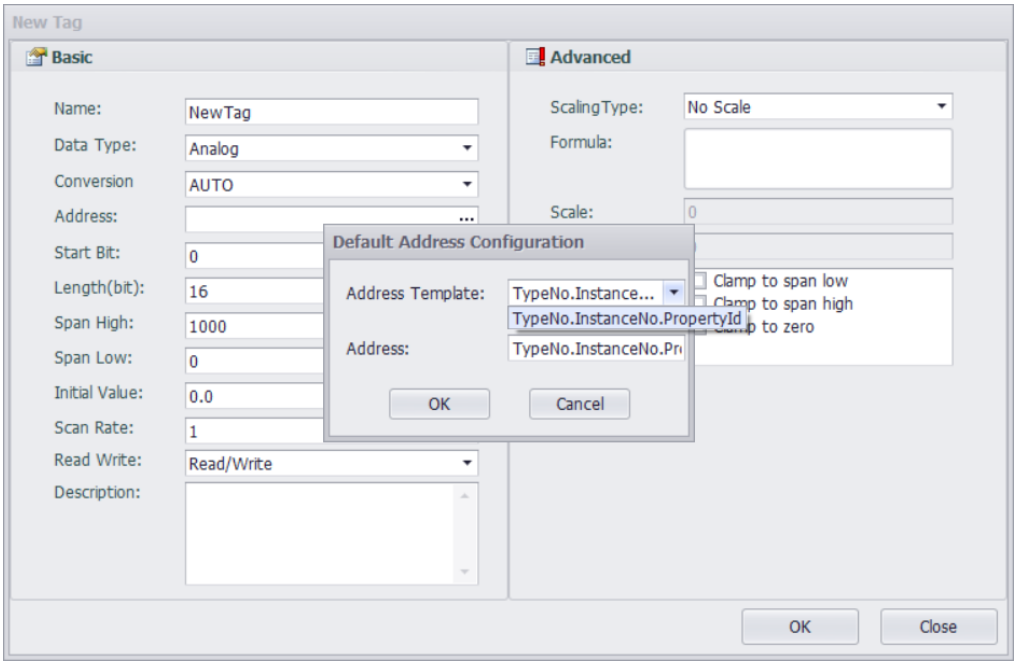


- DataCenter–>I/O点–>TCP–>Right Click：Add Device


NewDevice(ADAM-3600)*
Apply
Discard
General Information
Enable
Name:
BACnetIP
Device Type:
BACnet IP
Device Model
Double Click to Select Device Template
Unit Number:
1
Tag Write Type:
Single Write
Description:
Add device name as prefix to IO tags
Bulk Copy
TCP/IP
IP/Domain:
Port Number:
0
Extention Properties
Device Address (if other than Unit Number):
Device Broadcast [I AM] Time (second):
0
Polling Cycle:
1
Device Instance #:
0
Max Property/ Request:
0
Synchronize Time at(Ex. 23:50:00):
01:00:00

- Name: Fill in as you please。
- Device Type: Select BACnet IP。
- IP/Domain Name: The IP address of the BACnet server。
- Port Number: The port number of the BACnet server。
- Device Broadcast[I AM] Time (second)：Frequency of EdgeLink sending “I AM” messages。
- Polling Cycle：Data Collection Period
- Device Instance #：Device Instance ID of the BACnet server。
- Max Property/Request： 0 means polling 70 points in one round, and other values mean the number of points configured for one round of polling。
- Synchronize Time at (Ex. 23:50:00) ：Sync time with server at a certain time 。
- After configuring the above parameters, click “Apply” to add it. Click “Cancel” to cancel the operation。

3.Add tag



1).Fill in or select the parameters on the above interface according to the requirements, and click “OK” to save the changes。

2).Tag point address format：
TypeNo.InstanceNo.PropertyId

- TypeNo：Representing the type number。The driver protocol supports six types: Analog Input, Analog Output, Analog Value, Binary Input, Binary Output, and Binary Value：

Type	TypeNum
Analog Input	0
Analog Output	1
Analog Value	2
Binary Input	3
Binary Output	4

Type	TypeNum
Binary Value	5

- InstanceNo：Tag point sequence number in the server。
- PropertyId：Please refer to the Bacnet protocol。

example：The Property ID for “Present Value” in BACNet is 85 。 The address example for reading “Present Value” is as follows:

Type and index	Address
AI_2	0.2.85
AO_2	1.2.85
AV_2	2.2.85
BI_2	3.2.85
BO_2	4.2.85
BV_2	5.2.85

4.FAQ

4.1.ErrorCode

ErrorCode	Description
GOOD	No error
C010	Device Idle, I-AM timeout
C002	Data type mismatch
A00X	iscrete value over max state

ErrorCode	Description
QCode bit coded	0001 in alarm, 0002 Fault, 0004 Overridden, 0008 Out of service
b014	No space to write property
b01b	Read access denied
b01f	Unknown object
b020	Unknown property
b025	Value out of range
b028	Write access denied
b02a	Invalid array index
b02f	Datatype not supported
b030	Duplicate name
b031	Duplicate object id
b032	Property is not an array
b033	Abort buffer overflow
b034	Abort invalid apdu in this state
b035	Abort preempted by higher priority task
b036	Abort segmentation not supported
b037	Abort proprietary
b038	Abort other
b03b	Reject buffer overflow
b03c	Reject inconsistent parameters
b03d	Reject invalid parameter data type

ErrorCode	Description
b03e	Reject invalid tag
b03f	Reject missing required parameter
b040	Reject parameter out of range
b041	Reject too many arguments
b042	Reject undefined enumeration
b043	Reject unrecognized service
b044	Reject proprietary
b045	Reject other
b050	Parameter out of range
b07b	Abort apdu too long
b07c	Abort application exceeded reply time
b07d	Abort out of resources
b07e	Abort tsm timeout
b07f	Abort window size out of range
b0100	Loss of port connection
b0101	Header timeout error
b0102	Data timeout error
b0103	NPDU Timeout error
b0104	Header CRC error
b0105	Data CRC error
b0106	Non-NPDU message error
b0107	Timeout error

ErrorCode	Description
b0108	Serial port error
b0109	Invalid Write Properity Error
b010a	Invalid Read Properity Error
b010b	No valid read data
b010c	Unsupported Frame Type
b010d	Error in the MS/TP Network
b010e	Unknown Data Type to write
b010f	Invalid Destination MAC Address
b0110	Invalid Source MAC Address
b0111	Invalid Header Information
b0112	Unable to get a valid Invoke ID

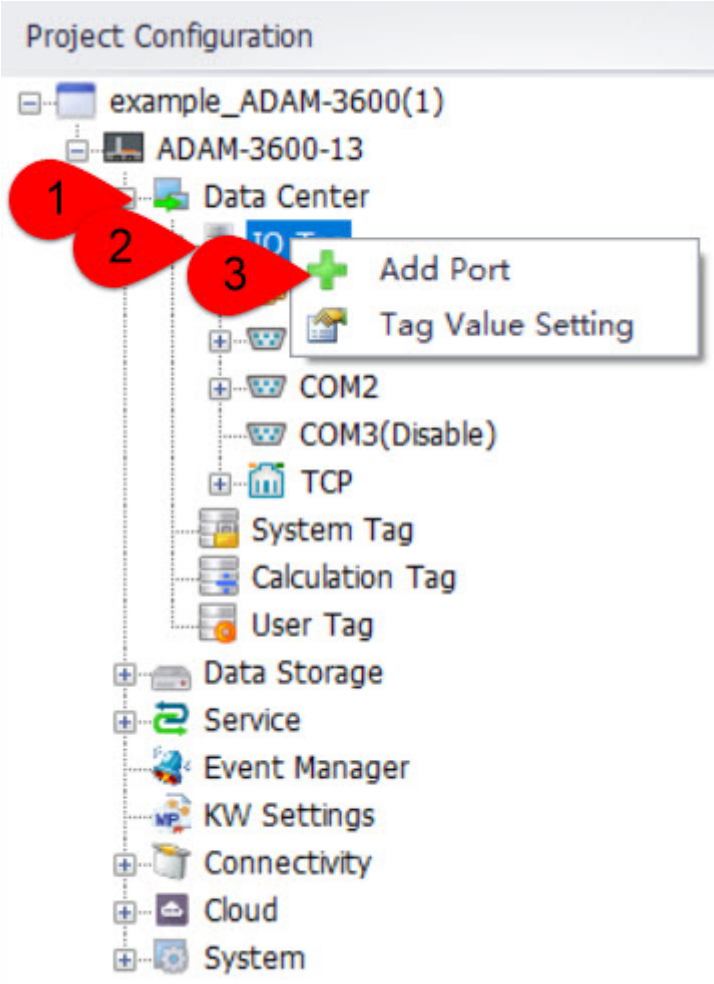
BACnet MS/TP

一、Driver support start version number：v2.8.0

二、Quic start

1.Add Port

- DataCenter–>I/O点–>Add Port



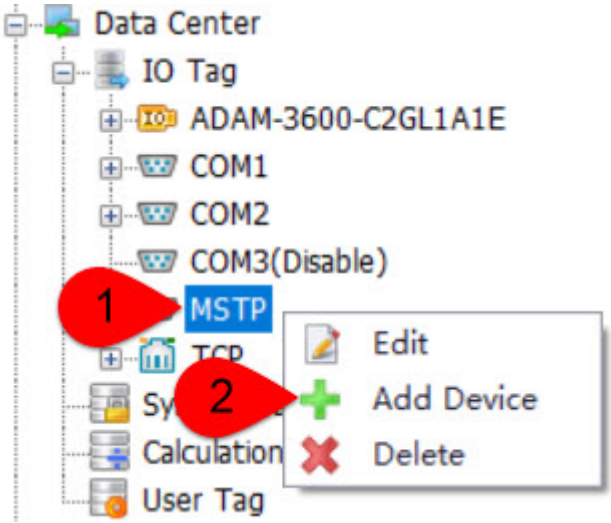
- Port Type：Select “Serial(BACnet MS/TP)”–>Name: Fill in as desired (The name used in this document is “MSTP”)

2.Configure the port

- Serial Number：Gateway serial port number
- Other parameters：Configure according to device characteristics
- After configuring, click “Apply”

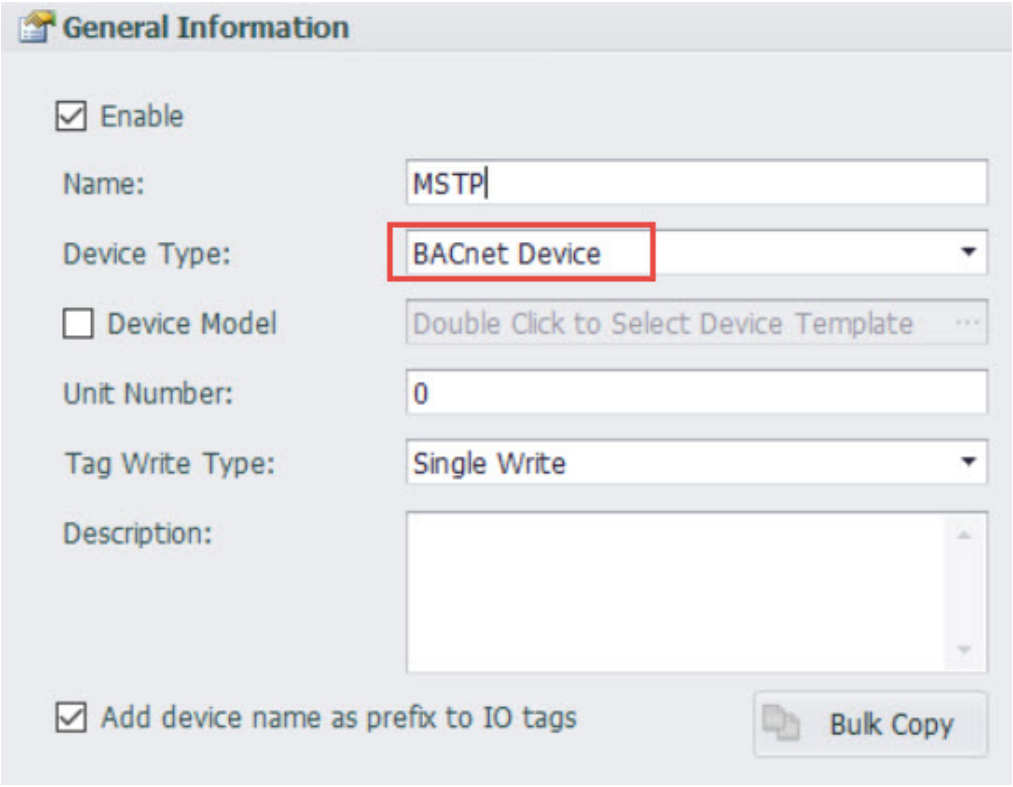
3.Add Device

- DataCenter–>I/O Tag–>MSTP–>Add Device



4.Configure Device

- Device Type：Select “BACnet Device”–>Name: Fill in as desired (The name used in this document is “MSTP”)–>click “Apply”

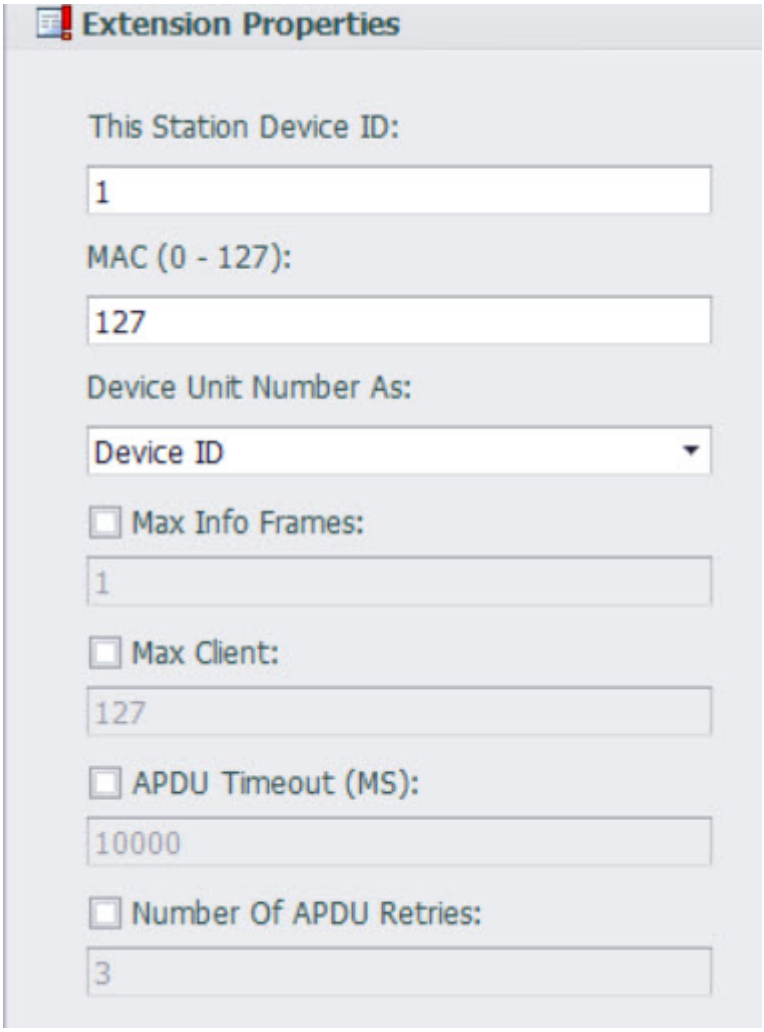


5.Add tag point

6.Download project，You have successfully completed the configuration of BACnet MS/TP.

三、Detailed configuration instructions

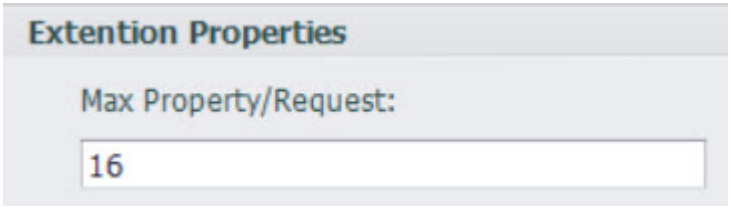
1.Detailed explanation of the extended attributes in the port configuration interface



- This Station Device ID：Device ID.
- MAC(0~127)：The MAC address of the device, default is 127.
- Device Unit Number As：The Unit Number value in the device configuration is the device ID, not the MAC address of the device.
- Max Info Frames：The maximum number of information frames that a designated node can send before the token must be transfer.
- Max Master：The highest address allowed by the master node in the network, default is 127.

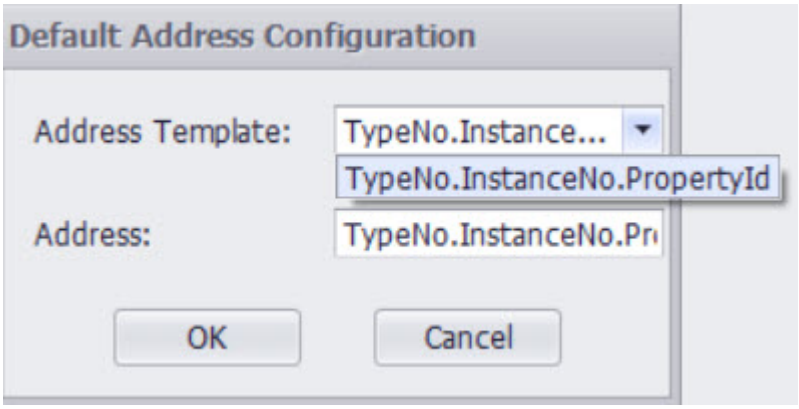
- APDU Timeout(MS)：The amount of time (milliseconds) between unconfirmed attempts to resend an APDU when confirmation is required. For devices that allow modification of this parameter, the recommended value for this property is 10000 milliseconds. Otherwise, the default value should be 60000 milliseconds.
- Number of APDU Retries：The maximum number of times an APDU should be retransmitted. The recommended value for this property is: if this device does not perform retries, this property should be set to zero. If the value of this property is greater than zero, a non-zero value should be placed in the APDU_Timeout property of the device object.

2.Detailed explanation of the extended attributes in the device configuration interface



- Max Property/ Request：The maximum number of tags included in each request packet.

3.Detailed description of tag point address



Tag point address format：

TypeNo.InstanceNo.PropertyId

The specific address instructions can be found in the BACnet IP documentation.

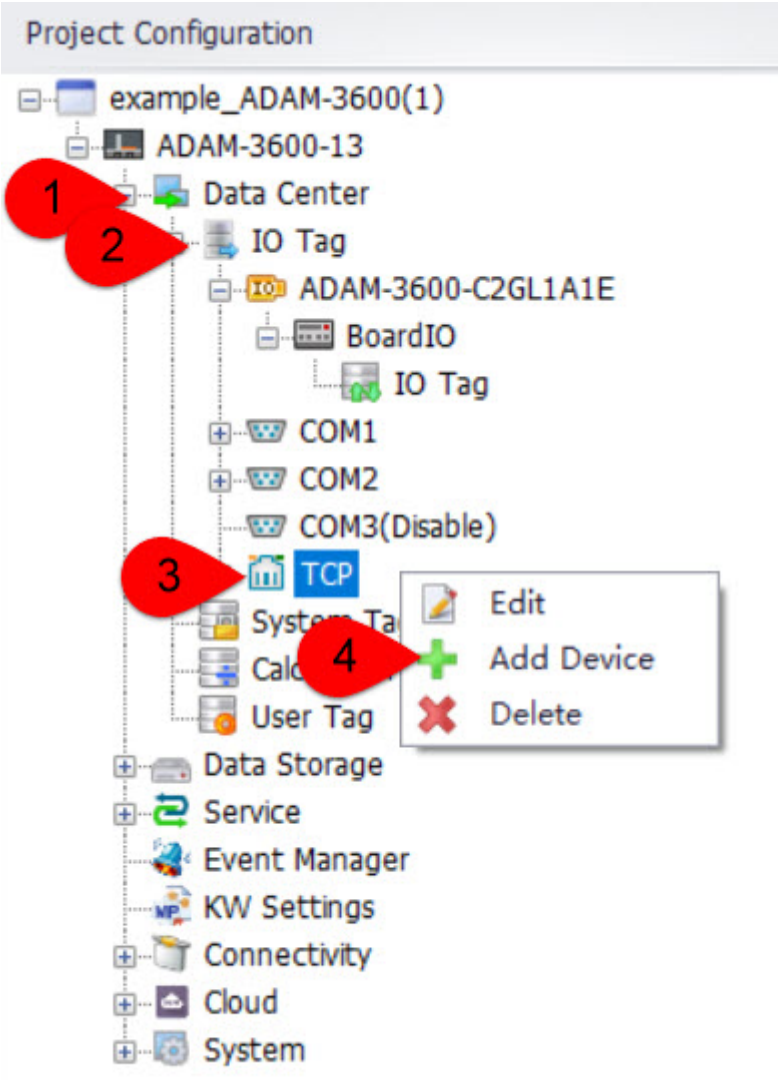
DNP3(TCP)

一、Driver support start version number：

二、Quick Connection

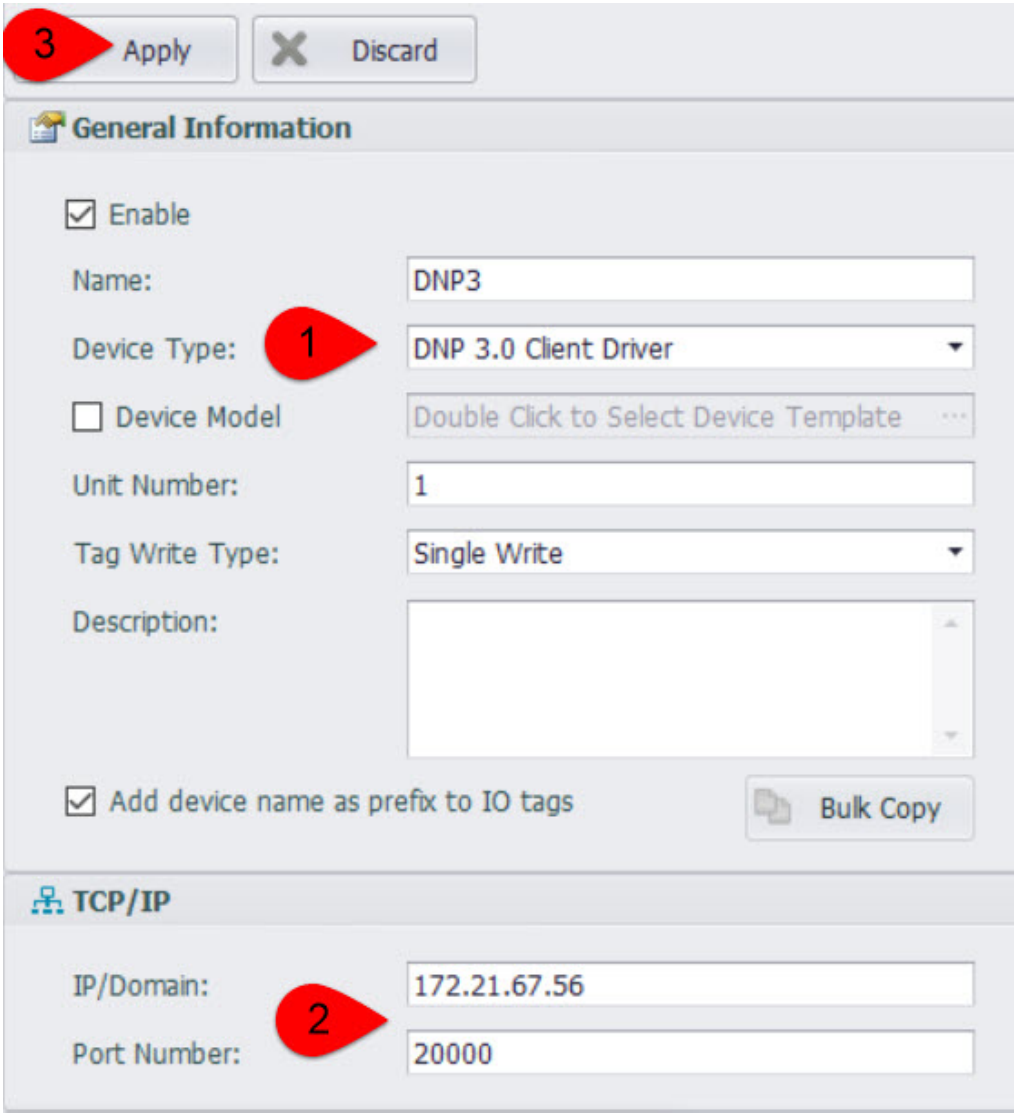
1.Add Device

- DataCenter–>I/O Tag–>TCP–>Rigth click：Add Device



2.Configure the device

- Select Device Type：DNP3.0 Master Driver–>Fill in the DNP3 server IP and port number: such as 172.21.67.56 and 20000–>click “Apply”

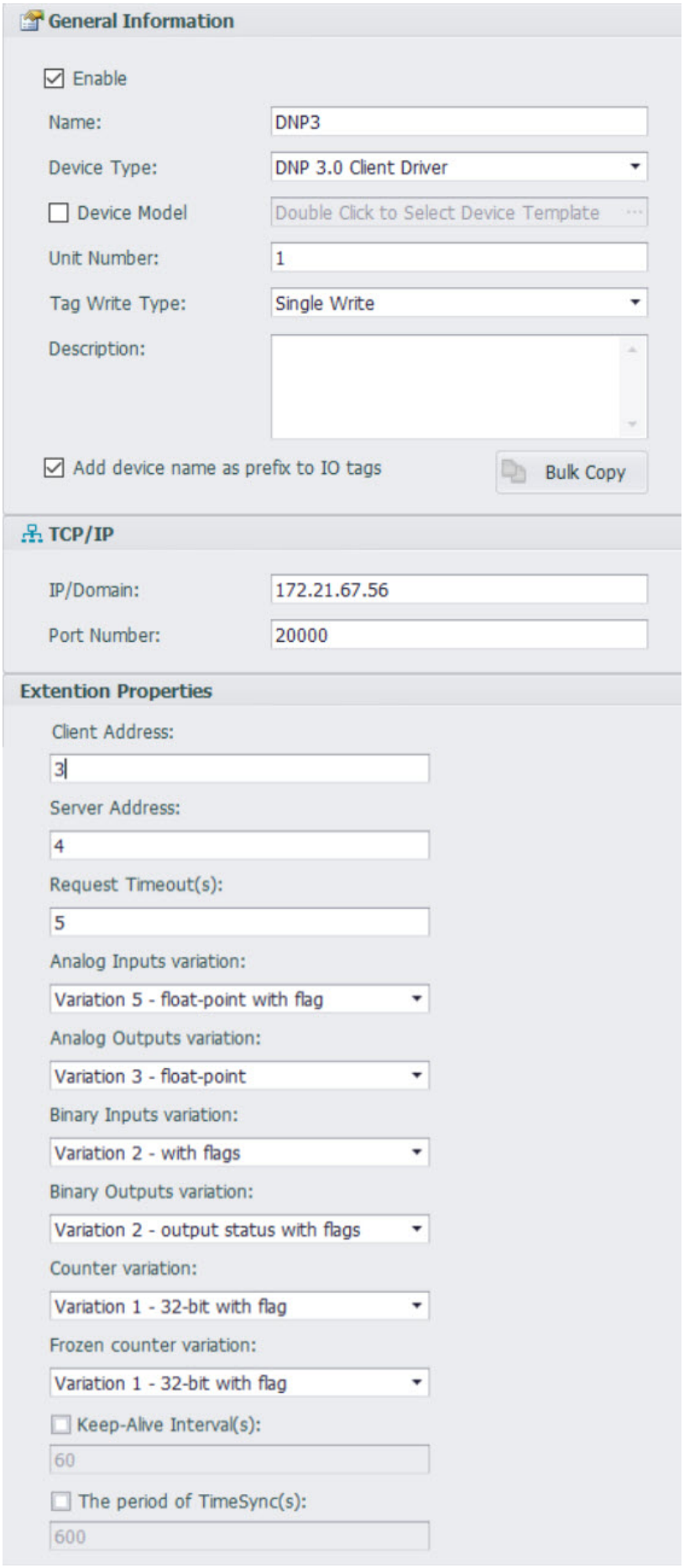


3.Add tags

4.Download project，completed the quick configuration of DNP3.

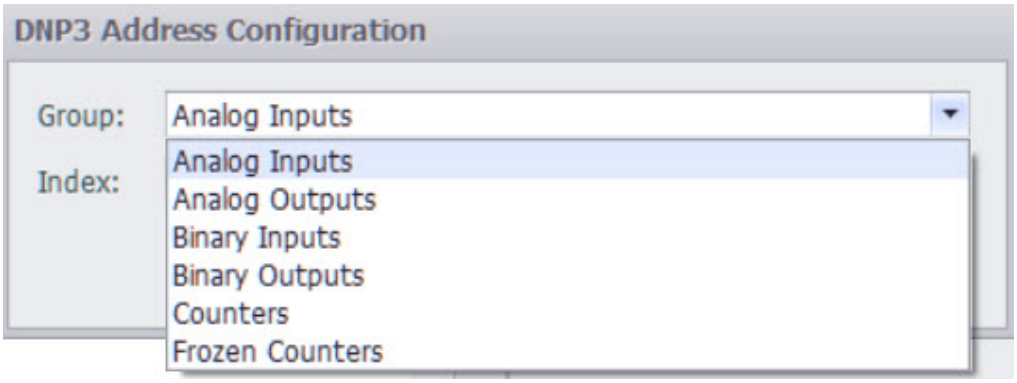
三、Detailed configuration instructions

1.Detailed configuration interface instructions


General Information
Enable
Name:
DNP3
Device Type:
DNP 3.0 Client Driver
Device Model
Double Click to Select Device Template
Unit Number:
1
Tag Write Type:
Single Write
Description:
Add device name as prefix to IO tags
Bulk Copy
TCP/IP
IP/Domain:
172.21.67.56
Port Number:
20000
Extention Properties
Client Address:
3
Server Address:
4
Request Timeout(s):
5
Analog Inputs variation:
Variation 5 - float-point with flag
Analog Outputs variation:
Variation 3 - float-point
Binary Inputs variation:
Variation 2 - with flags
Binary Outputs variation:
Variation 2 - output status with flags
Counter variation:
Variation 1 - 32-bit with flag
Frozen counter variation:
Variation 1 - 32-bit with flag
Keep-Alive Interval(s):
60
The period of TimeSync(s):
600

- Name: Fill in as desired.
- Device Type：Select DNP3.0 Master Driver.
- IP/Domain Name: The IP address of the DNP3 server.
- Port Number: The port number of the DNP3 server.
- Master Address： Session Master address.
- Slave Address：Session Slave Address.
- Request Timeout(s)： Response timeout time for data request commands.
- Keep-Alive Interval(s)： Heartbeat period: When this option is not selected, it means that the Master endpoint does not send heartbeat packets.
- The period of TimeSync(s)：Time synchronization period: When this option is not selected, it means that time synchronization operations are not performed.
- xx variation：It is possible to configure the default variation (i.e., data format) for each different data type. Please refer to the specification document for details. If there are no special requirements, it is sufficient to keep the defaults.

2.Detailed description of tag point address



- Group：There are six types in total. Please select the appropriate type from the dropdown list based on the actual situation.
- Index：Index on slave，Under the same data type, there may be multiple tag points. The index number is the sequential number of the tag point.
- Note: Due to the inability of the Master in Linux to issue the Frozen command, the Frozen counter point is only used for data collection.

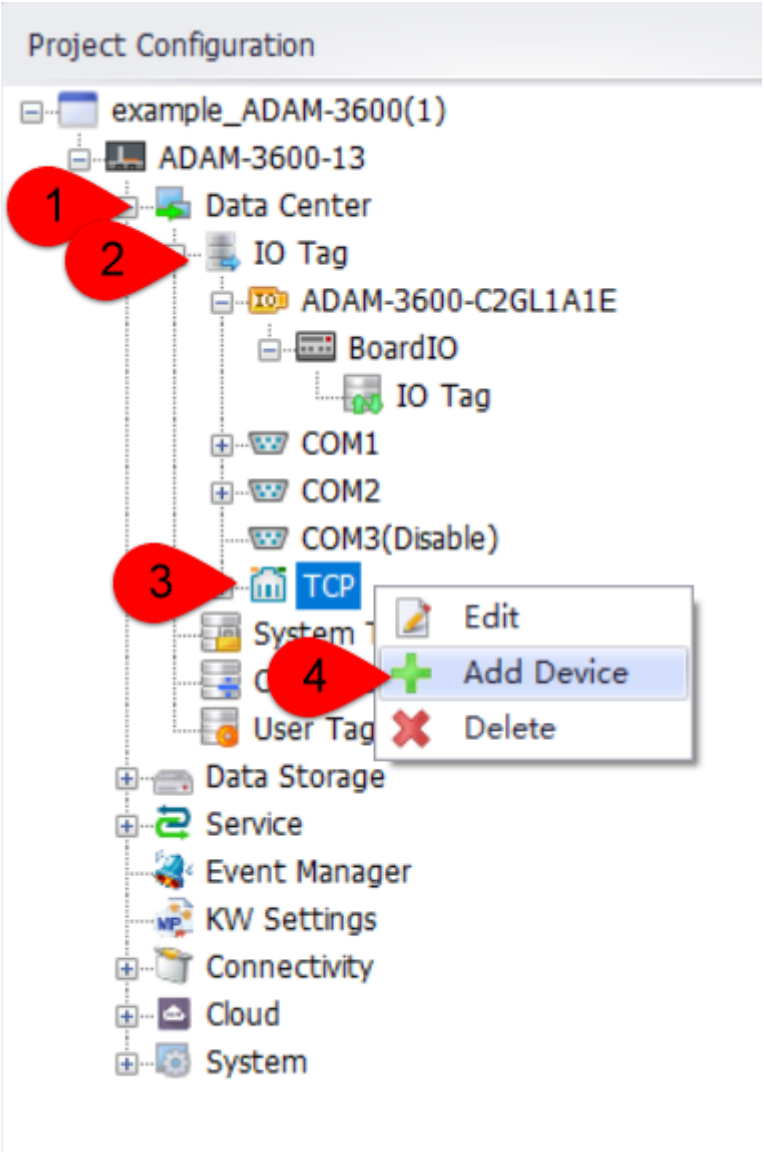
IEC104

一、Driver support start version number：

二、Quick Connection

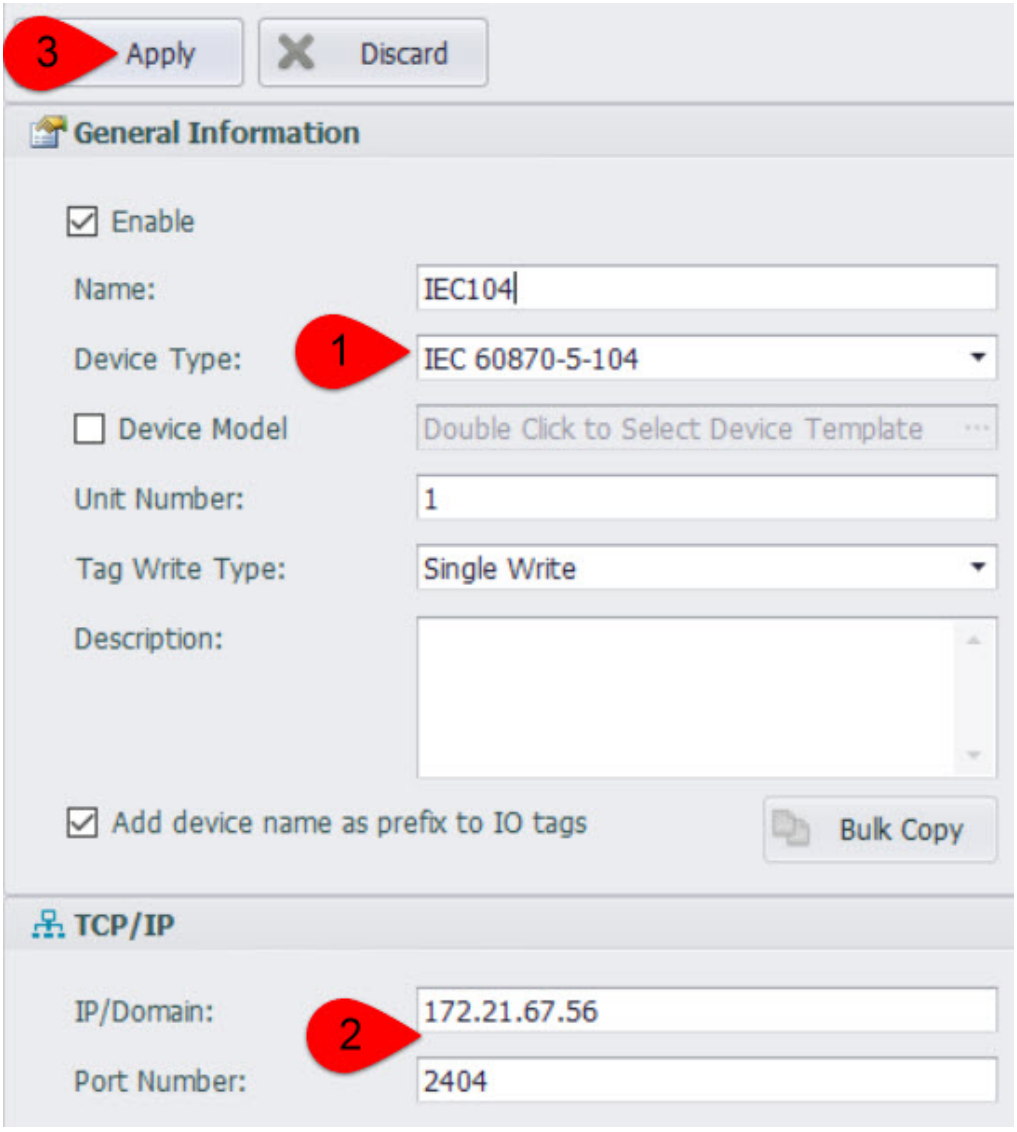
1.Add Device

- DataCenter–>I/O Tag–>TCP–>Right Click：Add Device



2.Configure the device

- Select Device Type：IEC 60870-5-104–>Fill in the IEC104 server IP and port number: such as 172.21.67.56 and 2404–>click “Apply”

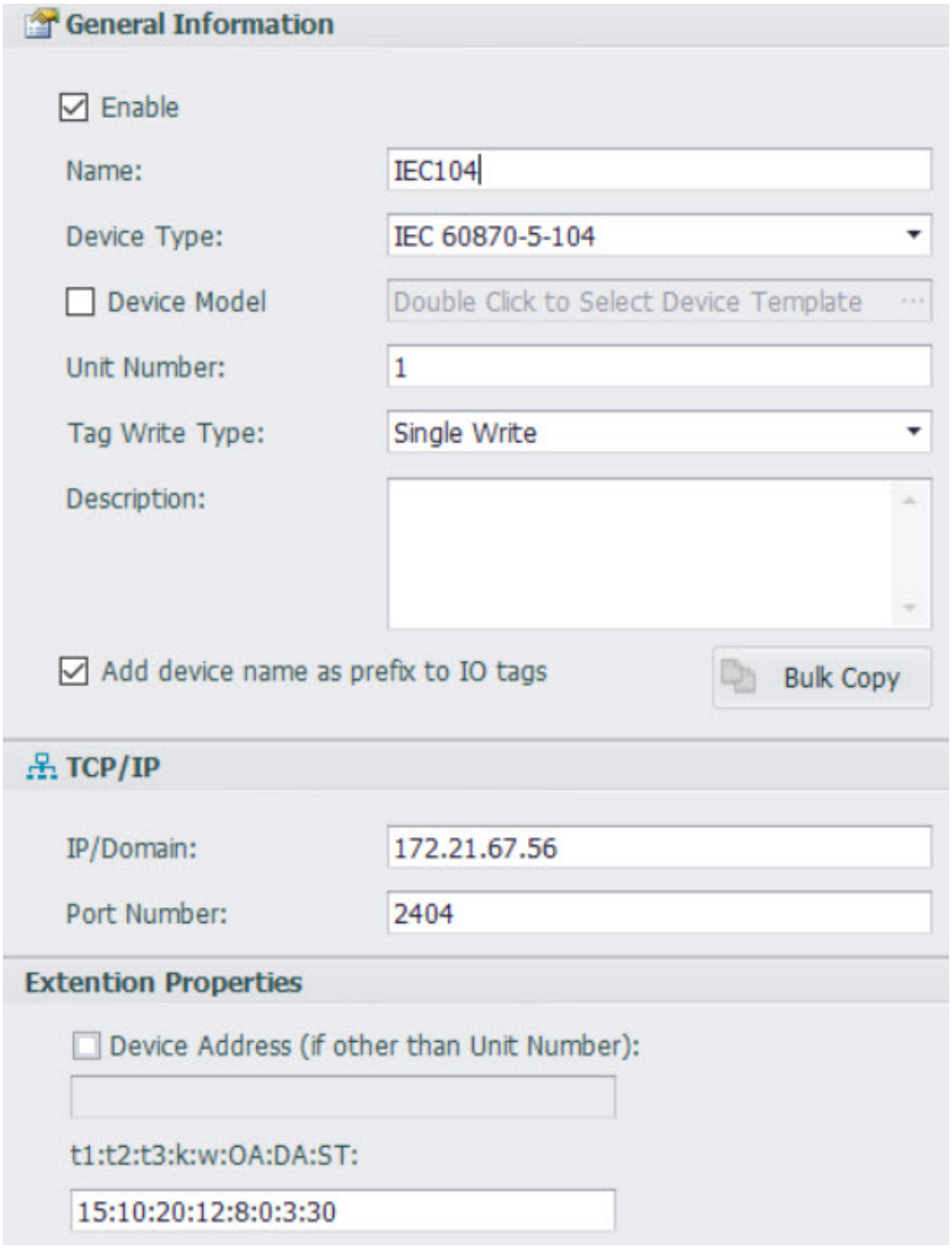


3.Add tag(s)

4.Download project，completed the quick configuration of IEC104.

三、Detailed configuration instructions

1.Detailed configuration interface instructions



- Name: Fill in as desired.
- Device Type: Select IEC 60870-5-104.
- IP/Domain Name: The IP address of the IEC104 server.
- Port Number: The port number of the IEC104 server.
- t1:t2:t3:k:w:OA:DA:ST：

- [ ] t1：1~255 seconds, Refer to the IEC104 protocol for specific requirements.
- [ ] t2：1~600 seconds, Refer to the IEC104 protocol for specific requirements.
- [ ] t3：1~600 seconds, Refer to the IEC104 protocol for specific requirements.
- [ ] k： 1~32767, Refer to the IEC104 protocol for specific requirements.
- [ ] w： 1~32767, Refer to the IEC104 protocol for specific requirements.
- [ ] OA：Master Address，Refer to the IEC104 protocol for specific requirements.
- [ ] DA：Slave public address.
- [ ] ST：Scan time. 1 ~3000 seconds.

2. Detailed description of tag point configuration

   There are three types of Tag.

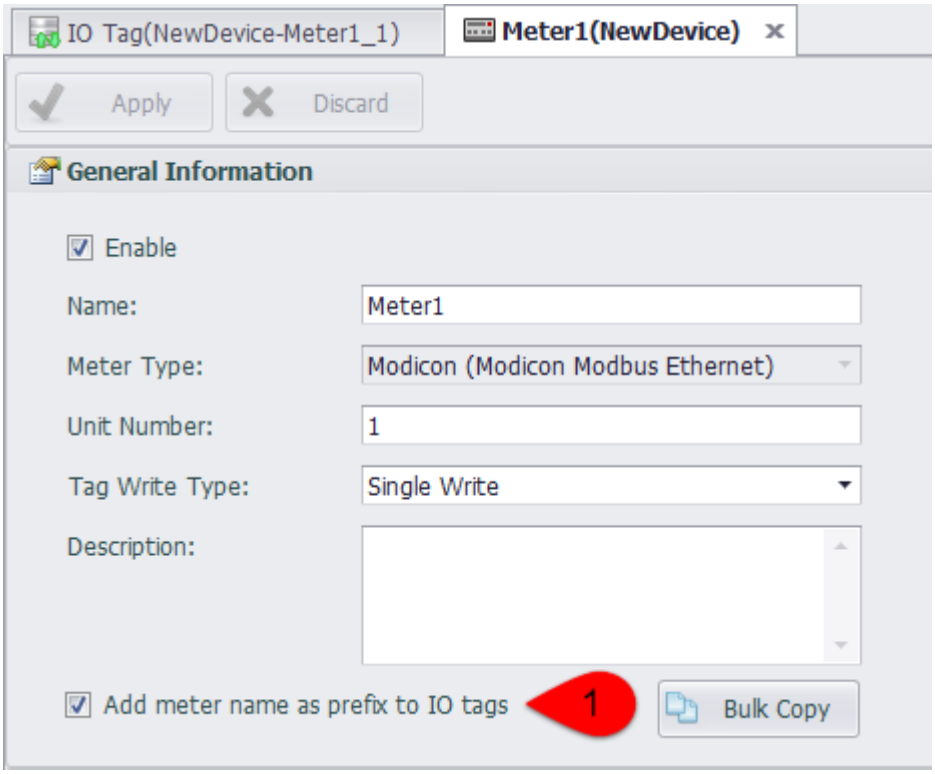
   A.
   ```
   Read Only Tag
     Format: R:Read Address / Read Data Type / Read
     Example: R:402 / M_BO_NA_1 / n
   ```

   B.
   ```
   Write Only Tag
     Format: W:Write Address / Write Command
     Example: W:2300 / C_RC_NA_1
     Note: Always show value 0 for this kind of tag
   ```

   C.
   ```
   Read And Write Tag
     Format: R:Read Address / Read Data Type / Read
     Example: R:400 / M_BO_NA_1 / n / W:2400 / n
   ```

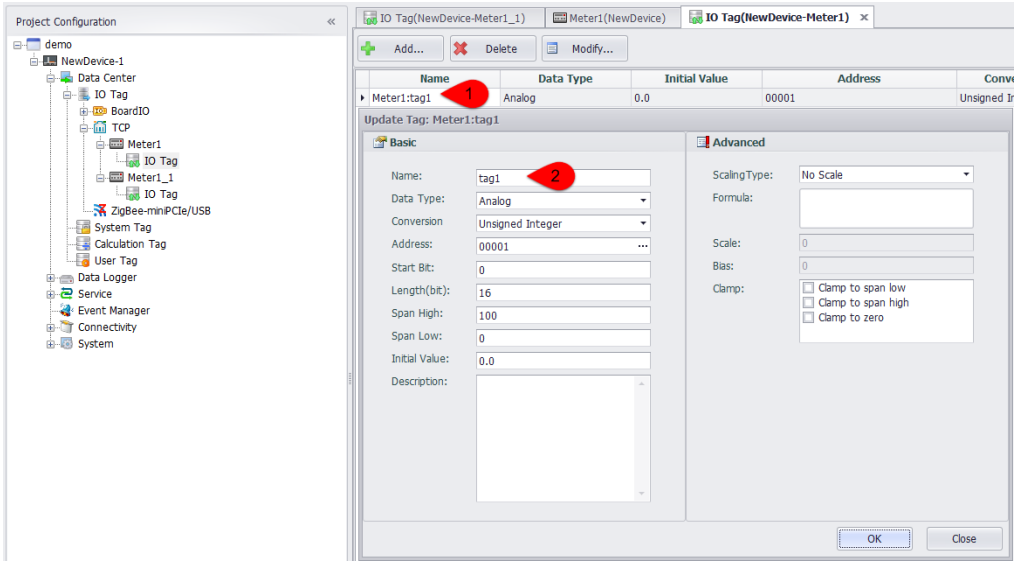
Note: Add /SE after Write Command to change “Direct Execute” to “Select and Execute” - Read And Write Tag Format: R:Read Address / Read Data Type / Read Command / W:Write Address / Write Command / SE Example: R:100 / M_SP_NA_1 / n / W:2100 / n / SE - Write Only Tag Format: W:Write Address / Write Command / SE Example: W:2100 / C_SC_NA_1 / SE

Add A Device Name Prefix for the IO tag



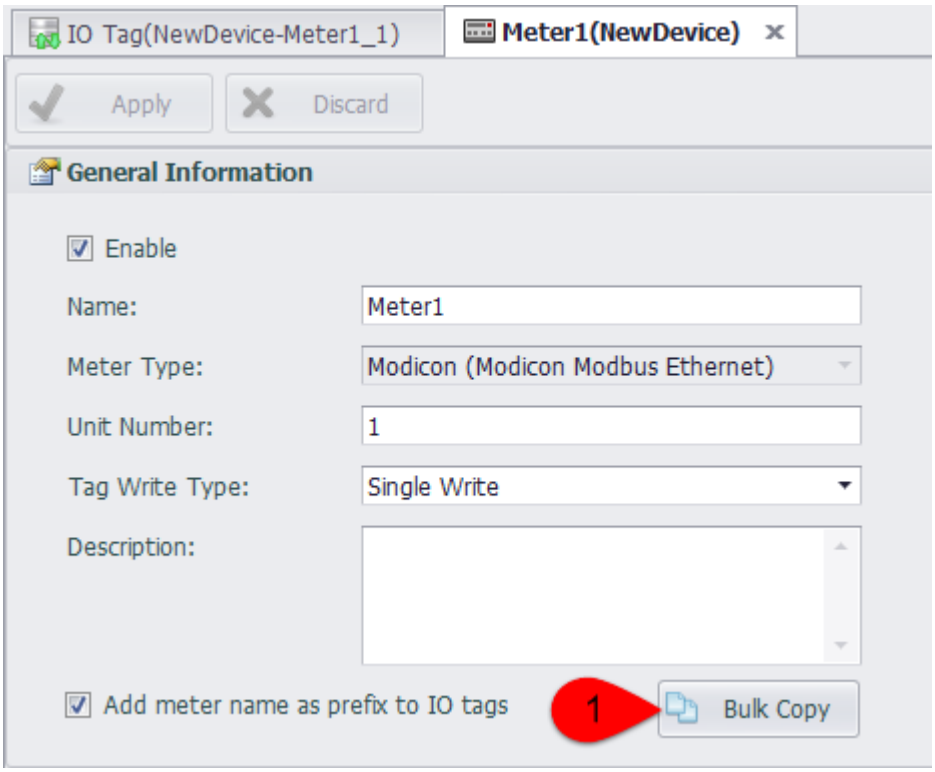
Click the option of “add device name as prefix to IO tags”,and it will add a prefix for the IO tag,format such as’meter name: IO tag name’.

The device name prefix will be removed after cancling point .If the the IO tag name is not unique after the prefix is canceled, the user will be prompted to allow the system to automatically rename the duplicate IO tag.

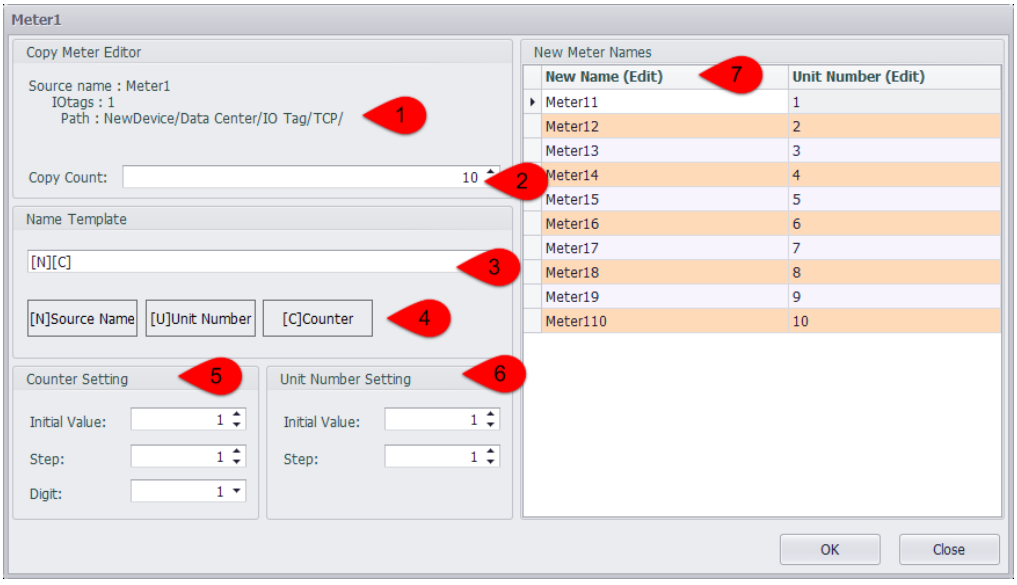


The device name prefix is displayed in the I/O tag editing interface, but cannot be edited.

Bulk Copy



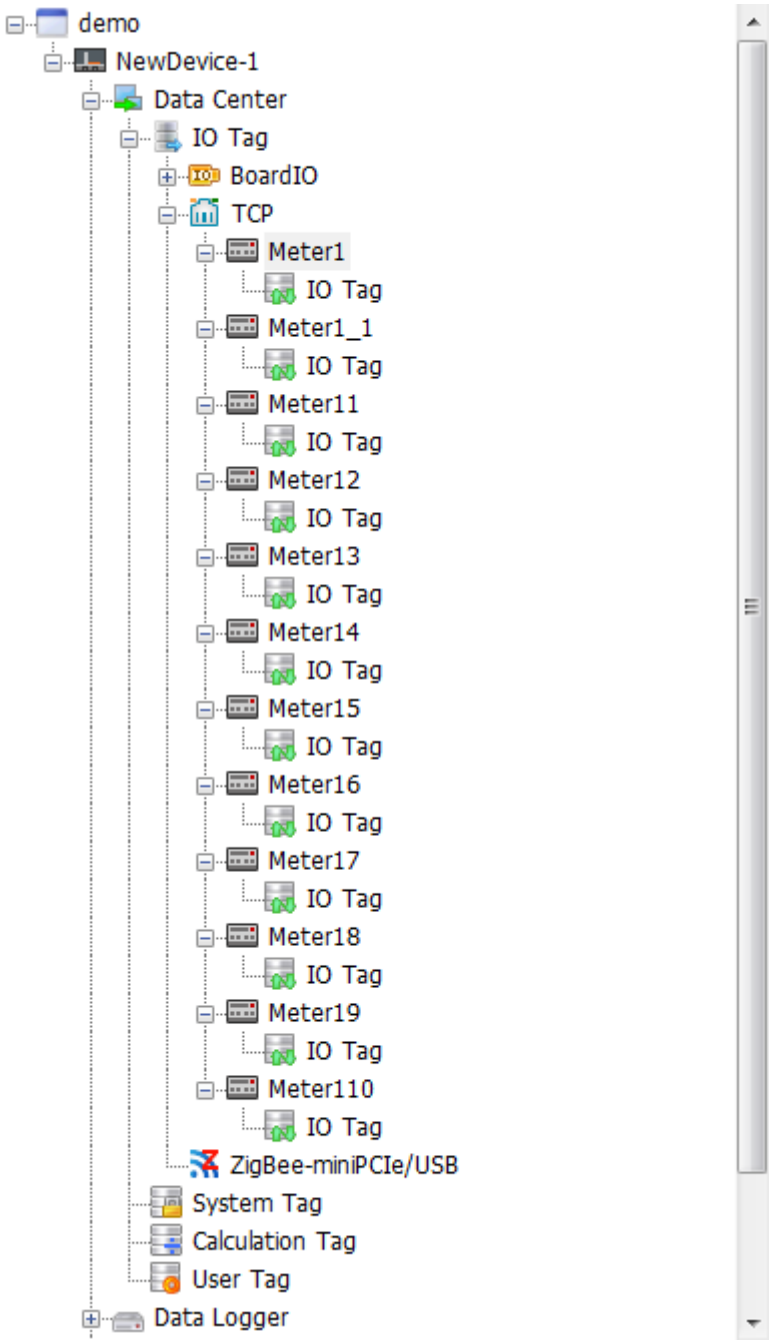
After selecting add the device name prefix, you can try to copy the current device with bulk copy function.



Click the bulk copy button to pop up the page of editing the device name, in which users can edit the number of

meters to be copied, the name of the device, and the number of units.

1. Display the basic information of the original instrument.
2. Select the number of meters to copy up to 100 once.
3. The name of the device will be generated according to the name template.
4. You can use the name of the original device and unit number and counter with the change of the number.
5. The initial value and the step size of the unit number can be set.
6. The counter can set the initial value, the step size and the number of the display.
7. The name of the generated device is showed in the right list, and the value in the device can be modified, but it will be reset after the modification to the left property.。



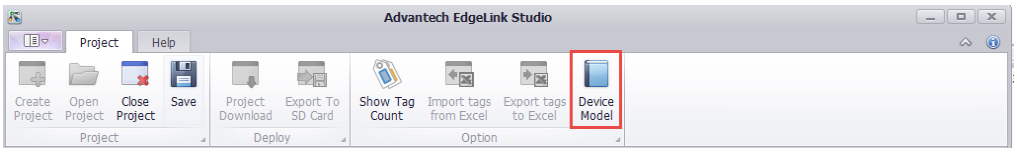
Click OK and users can see the generating bulk copied device under the port.

Device Template

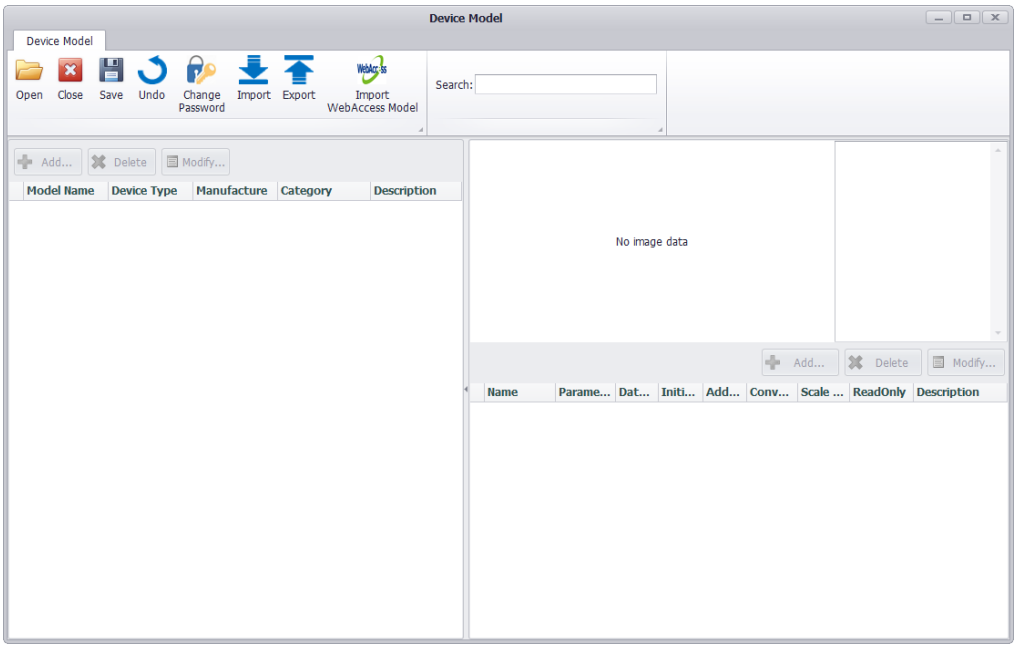
In EdgeLink Studio, a set of templates is created for each model of the device according to different device drivers and models. The template includes the basic information of the device and the tag information under the device, which is the “device template”. When adding devices in EdgeLink Studio, you can use the device template to add the tags included in the device template to the device according to certain rules, instead of adding tags one by one. The device template is a sqlite database file, which is divided into the default template and the user template. The default template is saved in the EdgeLink Studio installation directory to store the factory device templates included in the factory. The user template is saved in the template path where the project file is located. The device template can be set to an open password. The user can use the EdgeLinkStudio device template tool to open the template with the password to maintain the template. The ordinary user can only open the user template for maintenance, and the developer can open the default template for maintenance.

Device Template Tool

Click the Device Template button in the EdgeLink Studio toolbar to open the device template tool.



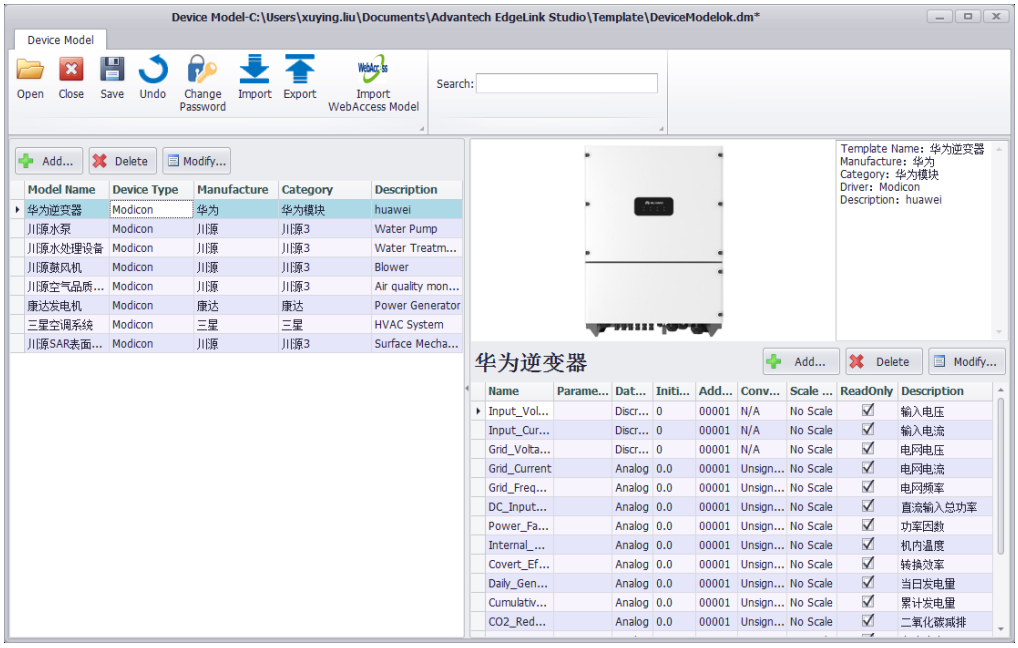
Device template tool interface：



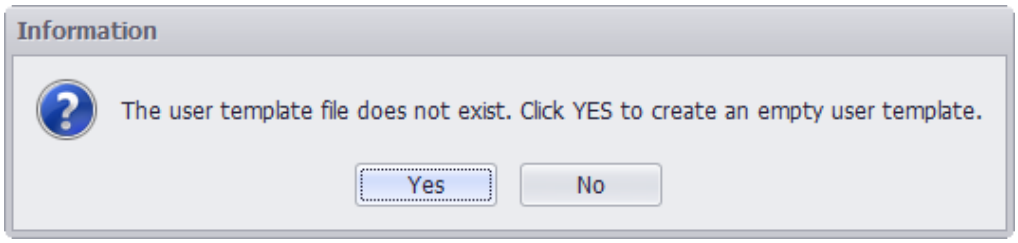
In the device template tool, the functions of opening, closing, saving, revoking, modifying password, importing and exporting, and importing Webaccess templates are supported.

1.Open the device template

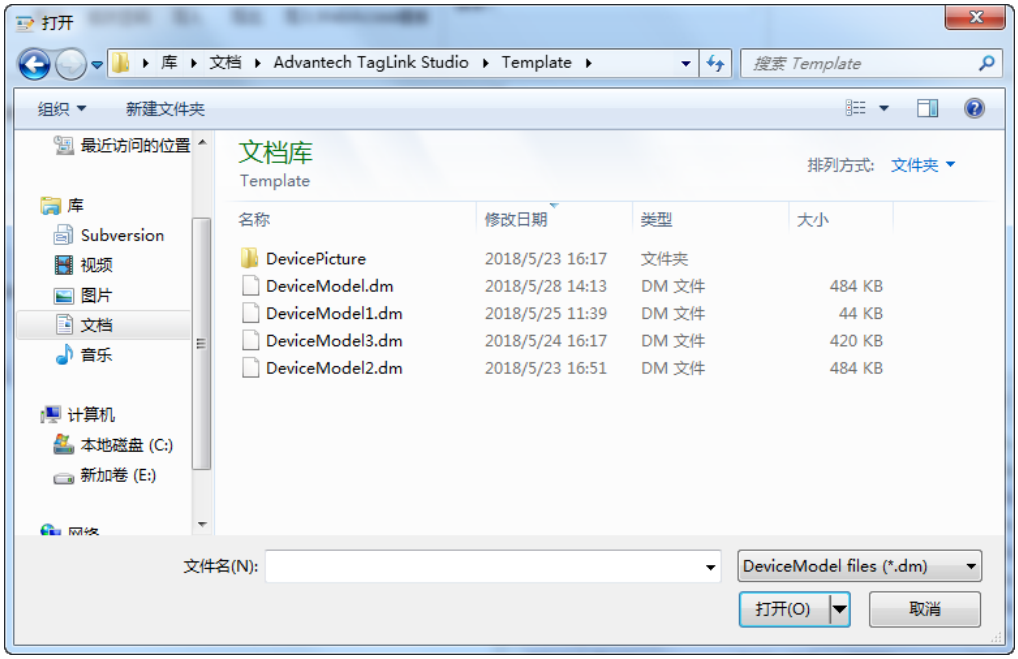
When you open the device template tool in the EdgeLink Studio page, you will open the user template by default.When you open the device template tool in the EdgeLink Studio page, the User Template will be opened by default, and users can view template information, template images, and tag information in the interface.



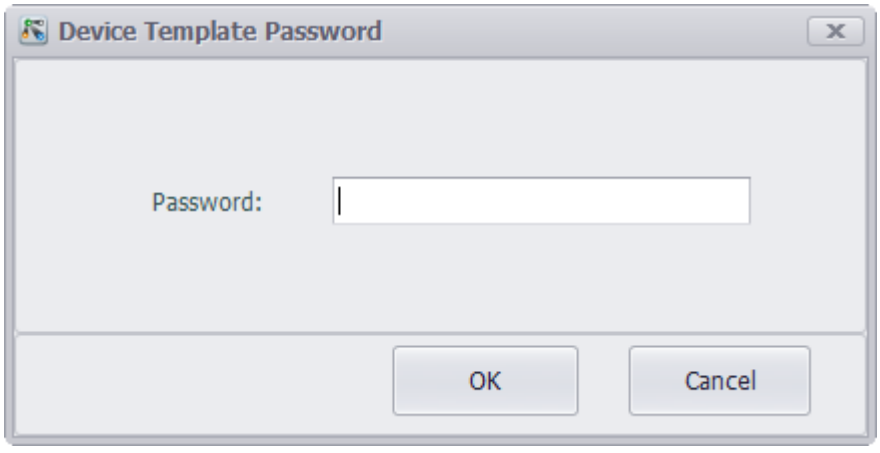
If a user template does not exist locally, a prompt box will pop up and the user can create an empty user template according to the prompt.

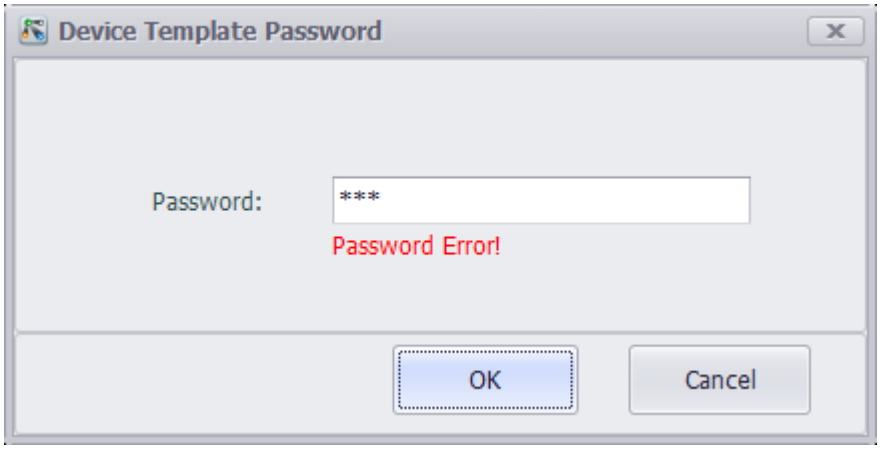


Users can click on the Open button to open any device template file.



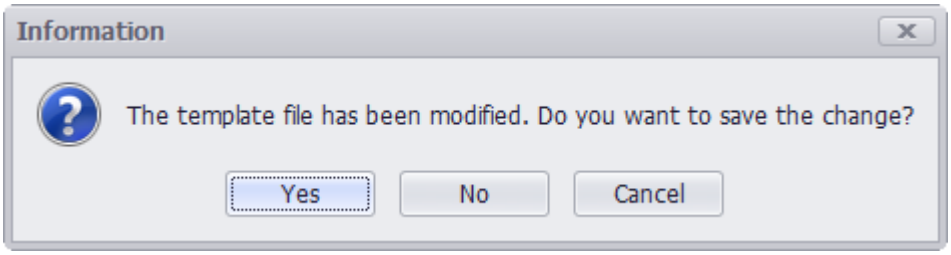
If the open device template needs to be opened with a password, you need to enter the template password. A prompt will be given when the password is wrong.





2.Close the device template

The user can click the Close button to close the current device template file. If there are unsaved changes to the template, a prompt box will pop up.



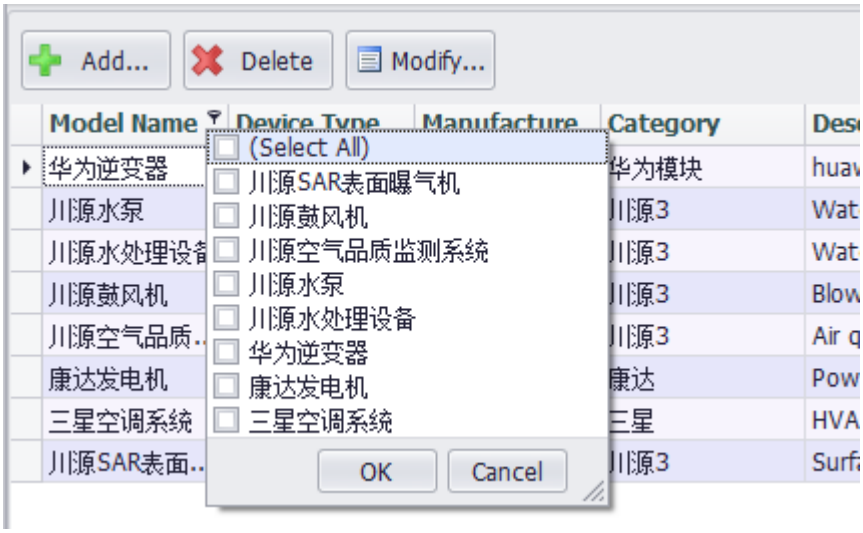
3.Modify the device template

In the device template tool, users can view, sort，search, filter, add, modify, and delete templates, and add, modify, sort，and delete tags included in the template.

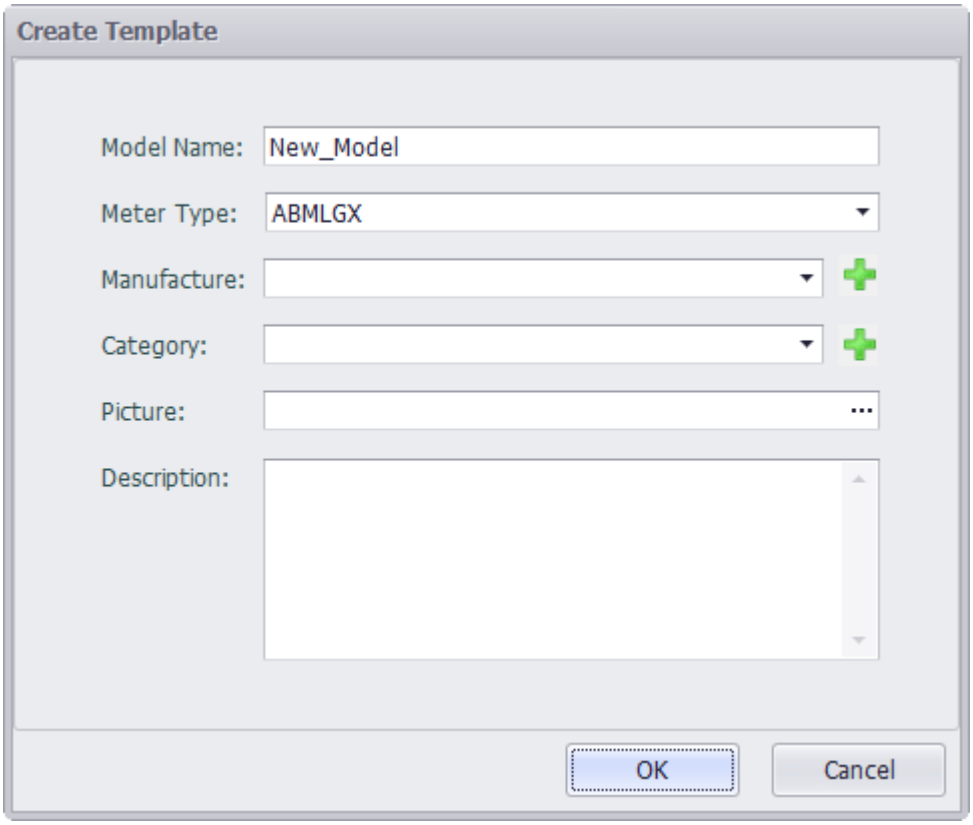
Click the device template list header to sort the template. Click the tag list header to sort the tags.

Fill in the keyword in the search box of the toolbar, and click the Enter button to search for the template information in the current template file.

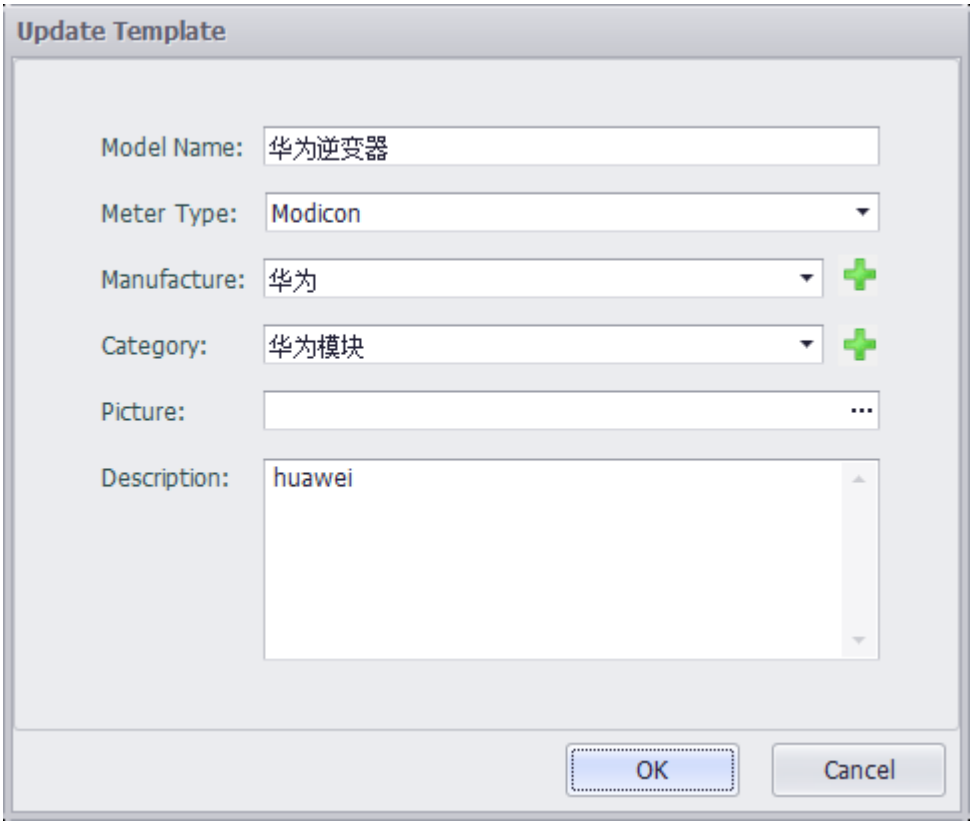
The template can be filtered by column in the header section of the template list.



Click the Add button above the template list to add a new device template. The information includes the template name, driver type, manufacturer, device category, device image, and description. The template name cannot be duplicated with other templates in the template file. The manufacturer and device categories can be added by clicking the Add button on the right side of the input box. You can also select an existing manufacturer by pull-down. Device images can upload image files of up to 200K in .PNG, .JPG, .JPGE, .BMP, and .GIF formats.

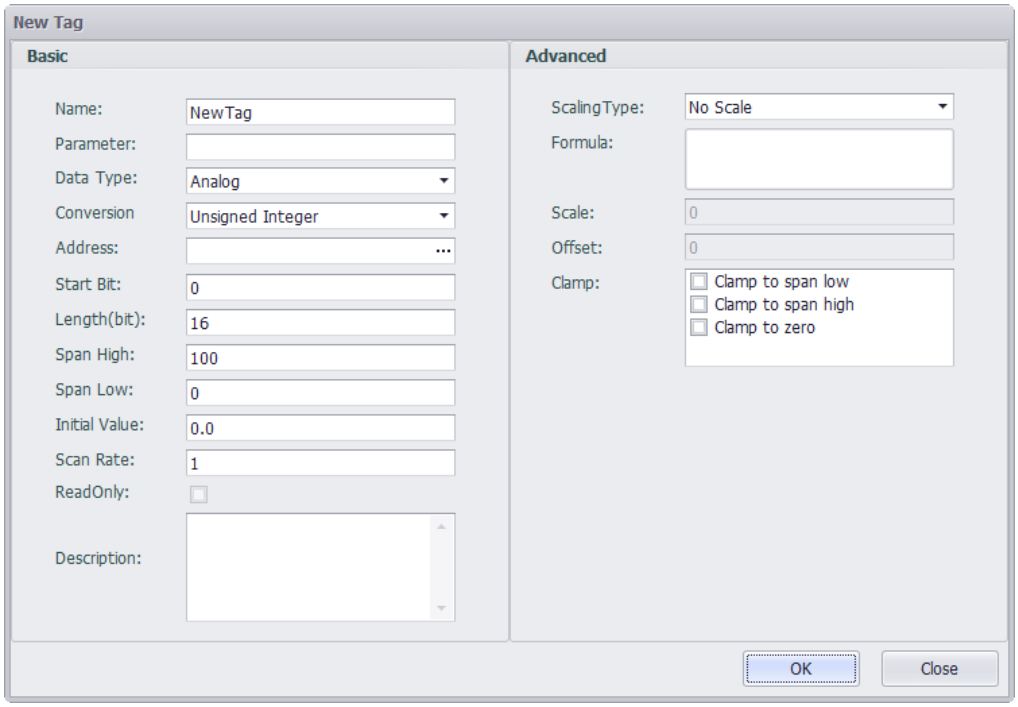


Double-click on an existing template in the list, or select a template in the list and click the Modify button above the list to modify the template.

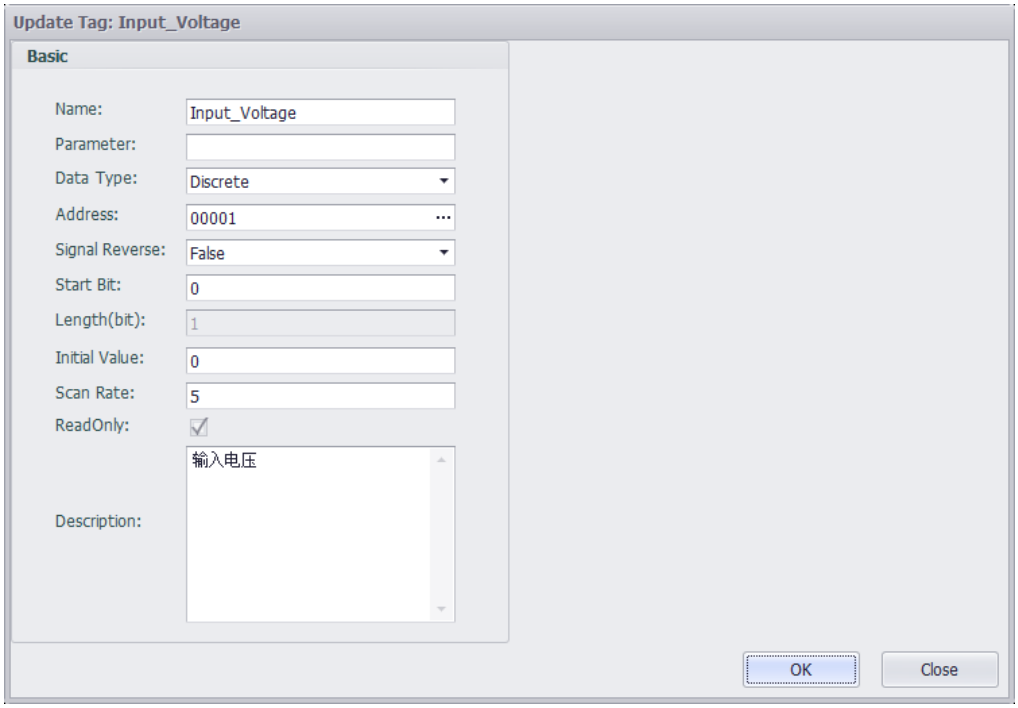


Select a template in the list and click the Delete button above the list to delete the template.

Click the Add button above the list of tags to add a new tag to the currently selected template.The tag information is similar to the IO Tag information in EdgeLink Studio. The added tag name cannot be the same as the other tags under the same template.



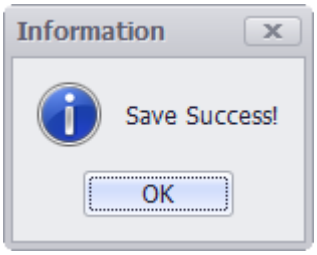
Double-click an existing tag in the list, or select a tag in the list, and click the “modify” button above the list to modify the tag.



Select a tag in the list and click the Delete button above the list to delete the tag.

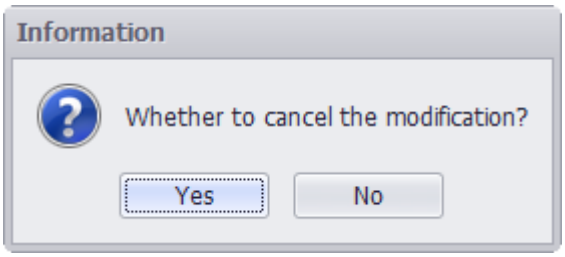
4.Save the device template modification

Adding, modifying, deleting, importing, etc. to the template file requires clicking the Save button in the page toolbar to save to the template file. After saving successfully, a prompt box will pop up.



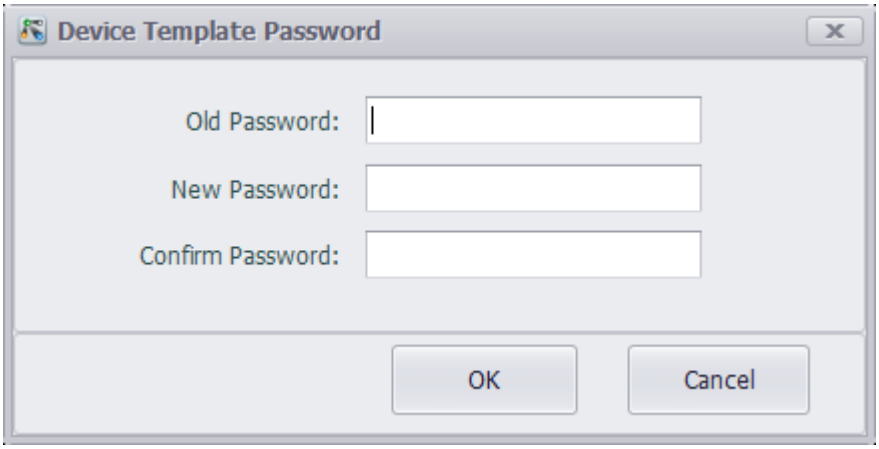
5.Undo the device template modification

Click the Undo button to undo unsaved changes, and the template will be returned to the previous save.



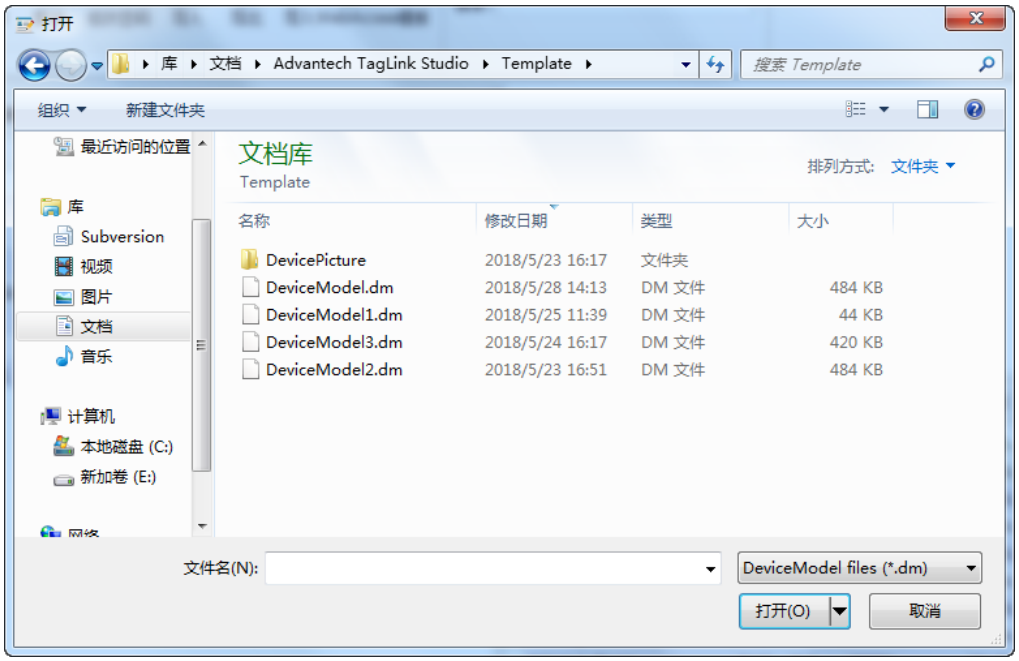
6.Modify the device template password

Click the Change Password button, and the template password can be modified in the pop-up dialog box.

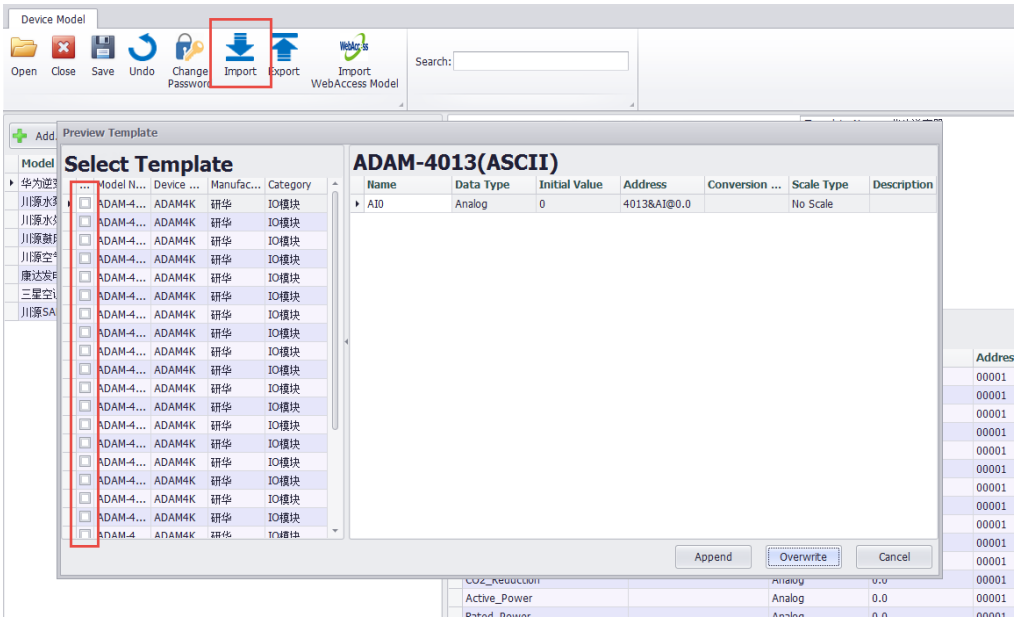


7.Import the device template

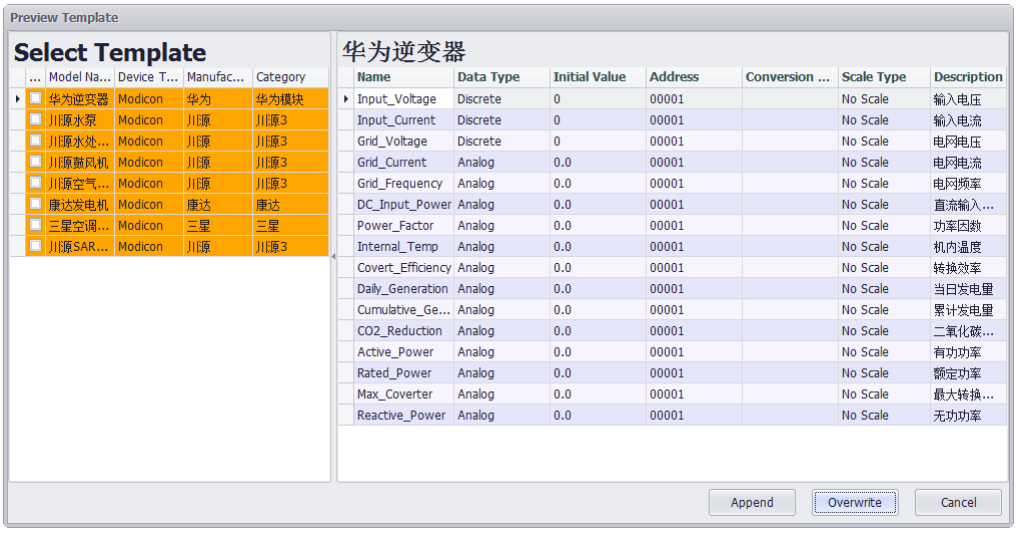
Click the Import button to import templates from other device templates files into the currently open template. To import a template that requires a password to open, a password dialog box pops up to prompt the user for a password.

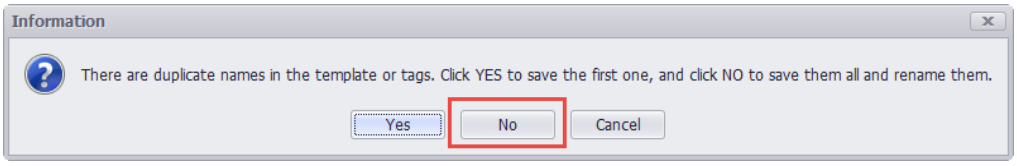


Select to open the template file to be imported, and users can view the template information in the preview panel. Check the template information to be imported. Click the Append button to import the selected template into the current template file, click the Overwrite button to clear the current template and then import the selected template to the current template.



Whether it is append or overwrite, it will judge whether there is a template duplicate name and a tag duplicate name. If there is a duplicate name, it will be highlighted in the preview panel, and you can choose to rename the duplicate template or tag.

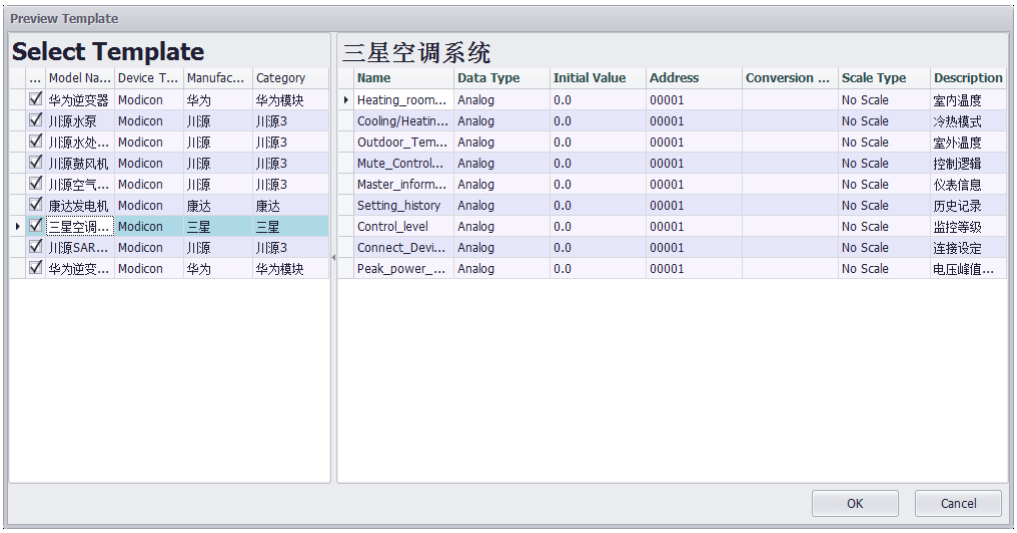


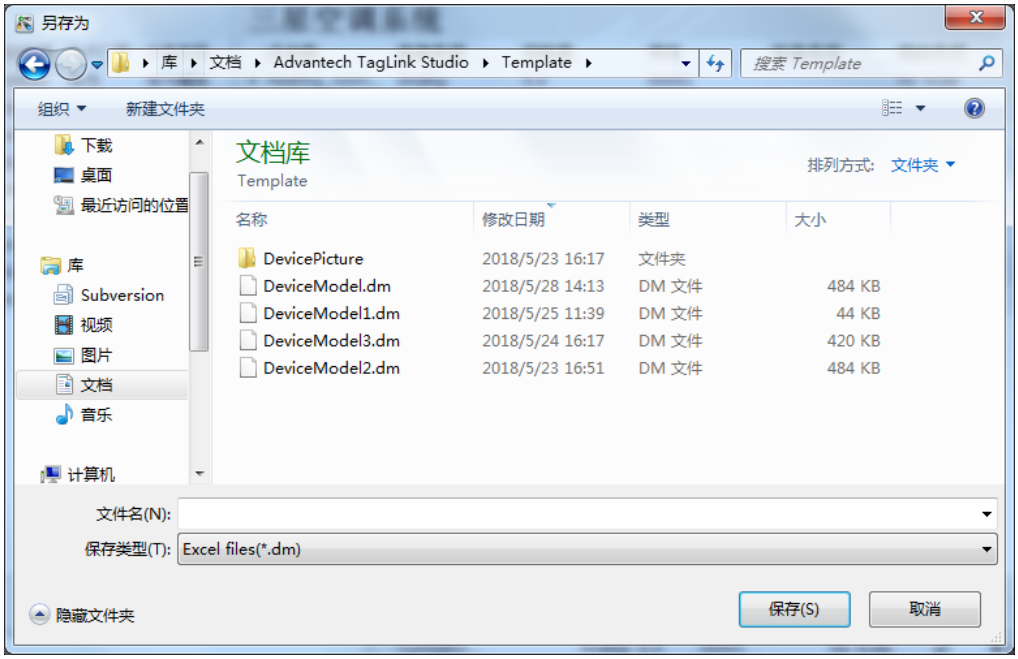


Model Name	Device Type	Manufacture	Category	Description
华为逆变器	Modicon	华为	华为模块	huawei
川源水泵	Modicon	川源	川源3	Water Pump
川源水处理设备	Modicon	川源	川源3	Water Treatm...
川源鼓风机	Modicon	川源	川源3	Blower
川源空气品质...	Modicon	川源	川源3	Air quality mon...
康达发电机	Modicon	康达	康达	Power Generator
三星空调系统	Modicon	三星	三星	HVAC System
川源SAR表面...	Modicon	川源	川源3	Surface Mecha...
华为逆变器(1)	Modicon	华为	华为模块	huawei

8.Export the device template

Click the Export button to export the currently opened template to a new template file. When exporting, you still need to check the template to be exported in the preview panel, and click the OK button to save the template file.

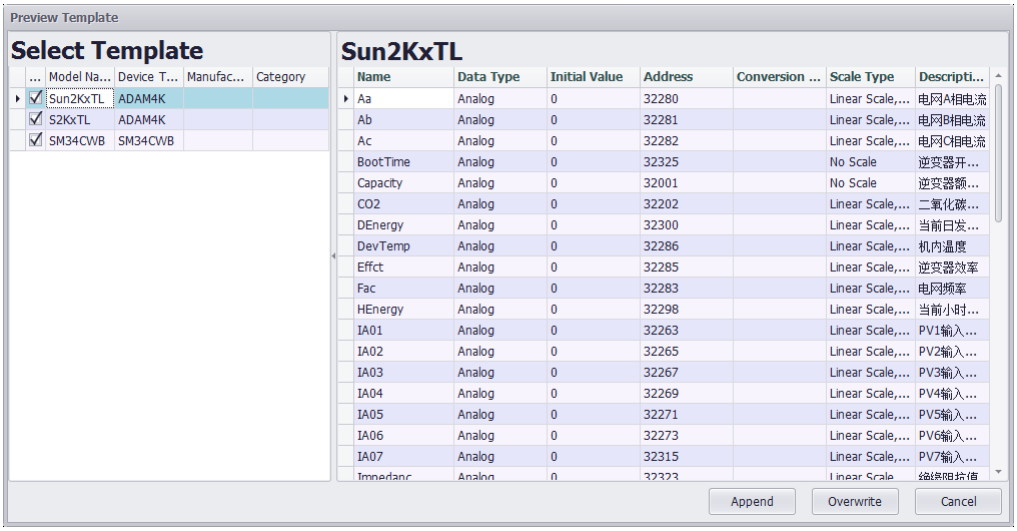




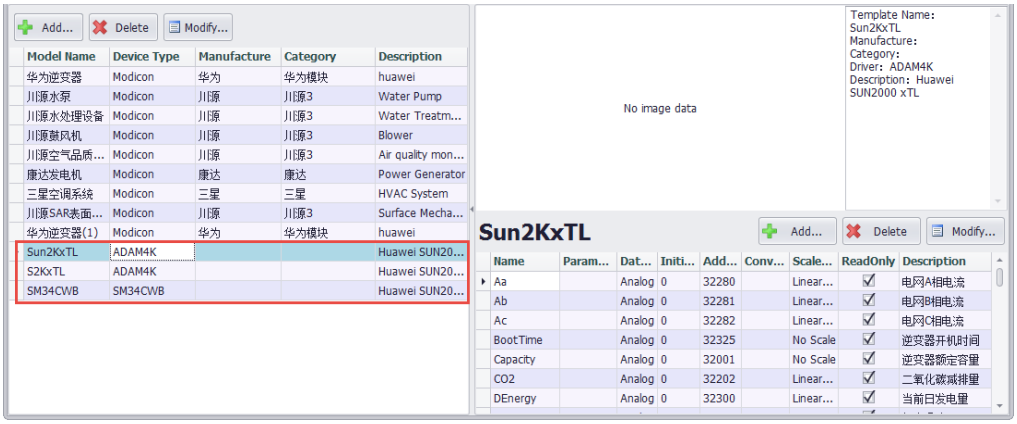
After saving successfully, the preview panel automatically closes.

9.Import Webaccess template

Webaccess template is an access database file in .mdb format. Click the Import Webaccess Template button, select the file to be imported, select the template information to be imported in the preview panel, click the Add button to import the selected template into the current template file, click the Overwrite button will clear the current template. Then import the selected template to the current template.

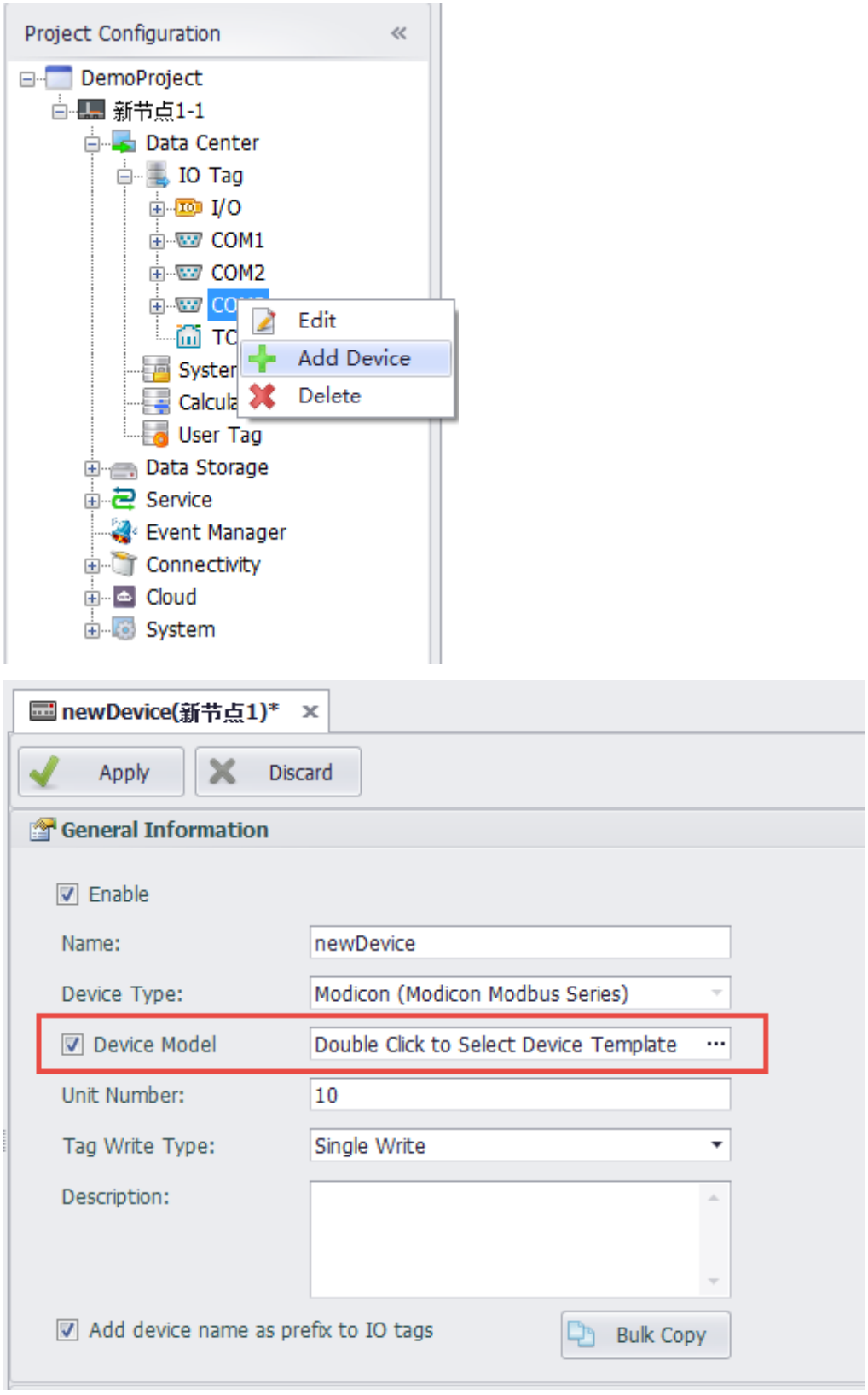


Similar to the import device template file, when importing the Webaccess template, it will also determine whether there is a template duplicate name and a tag duplicate name. If there is a duplicate name, it will be highlighted in the preview panel, and you can choose to rename the duplicate template or Tag.



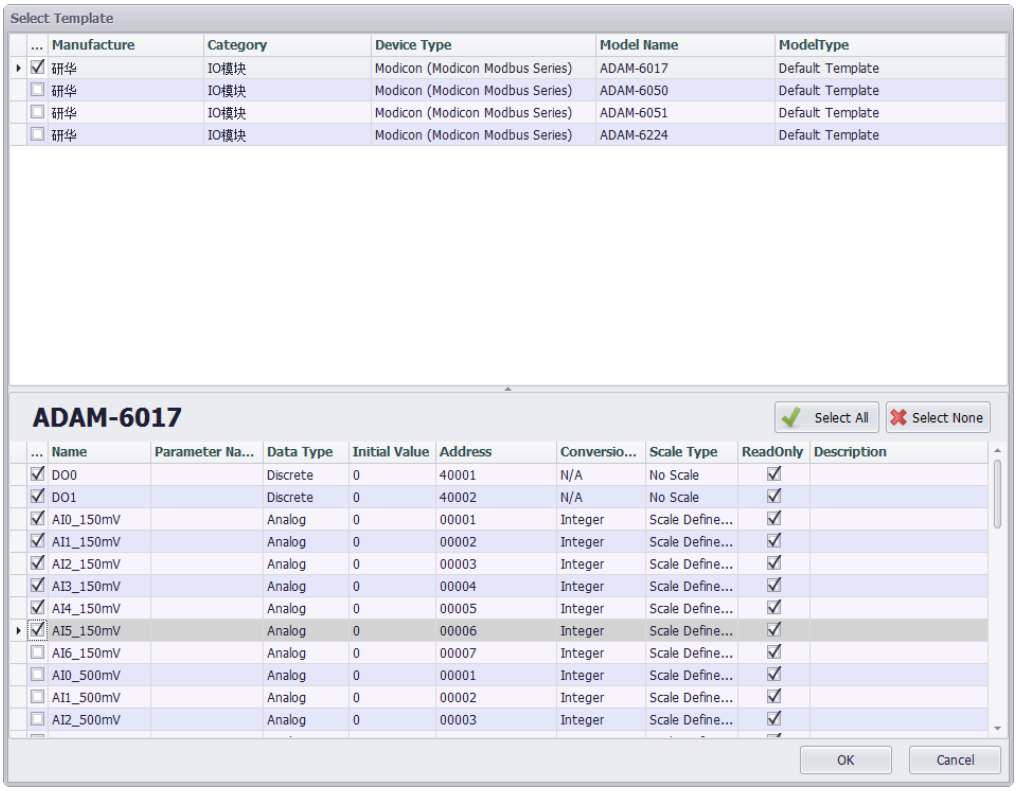
Use Device Template

1、Check the Use Device Template when adding and modifying devices.

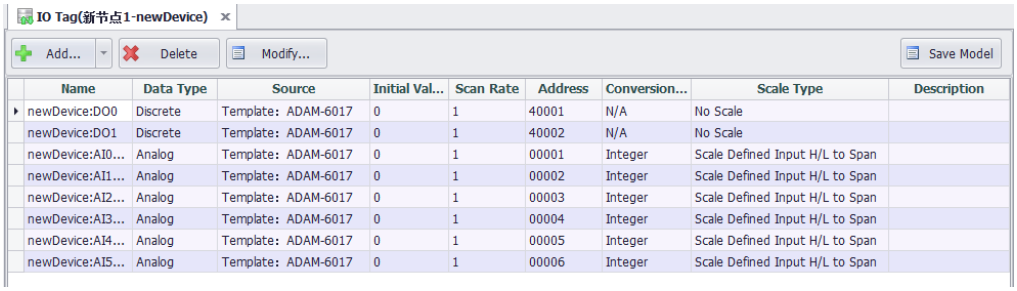


Double-click the device template selection box to bring up the panel to view and select all the device templates in the Default Template and User Template supported by

the device driver. The tags under the template can be selected all or part of them.

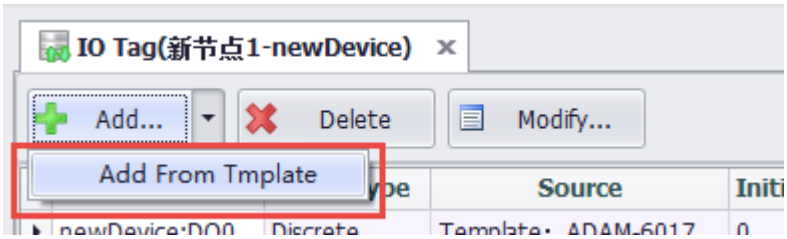


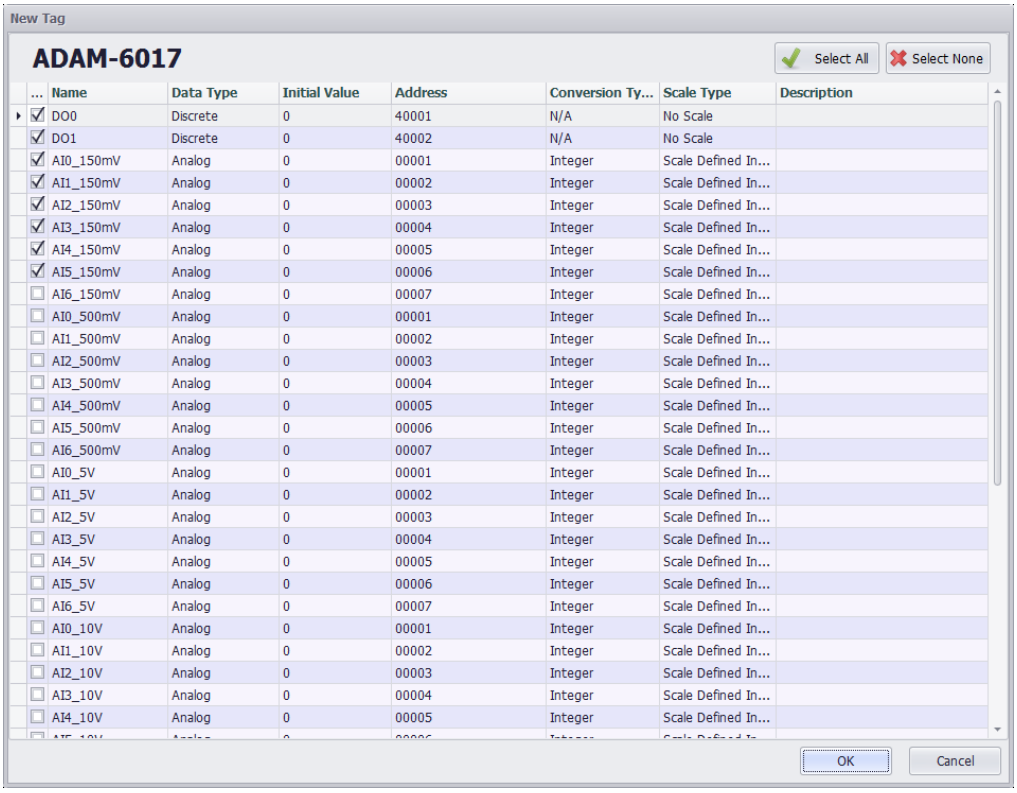
After clicking the OK button, the use template is set for the device. Click the Apply button on the device information page to add or update the device information. At the same time, the selected tag under the selected device template will be automatically added to the IO Tag list under the device.



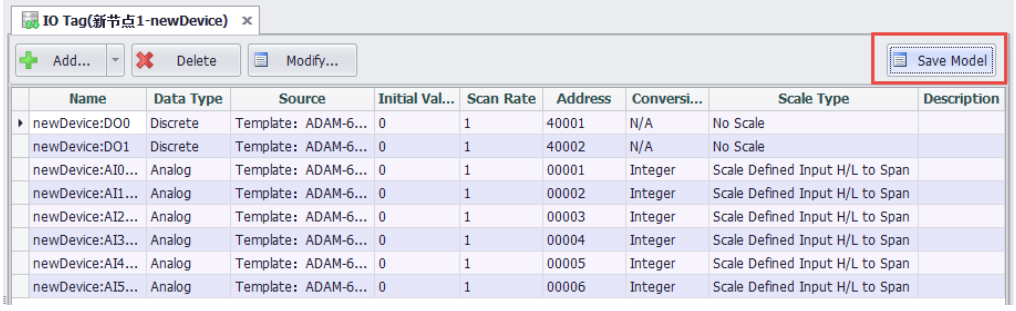
Click the Add button in the list of IO Tags to add tags customarily, and you can choose to add tags in bulk from

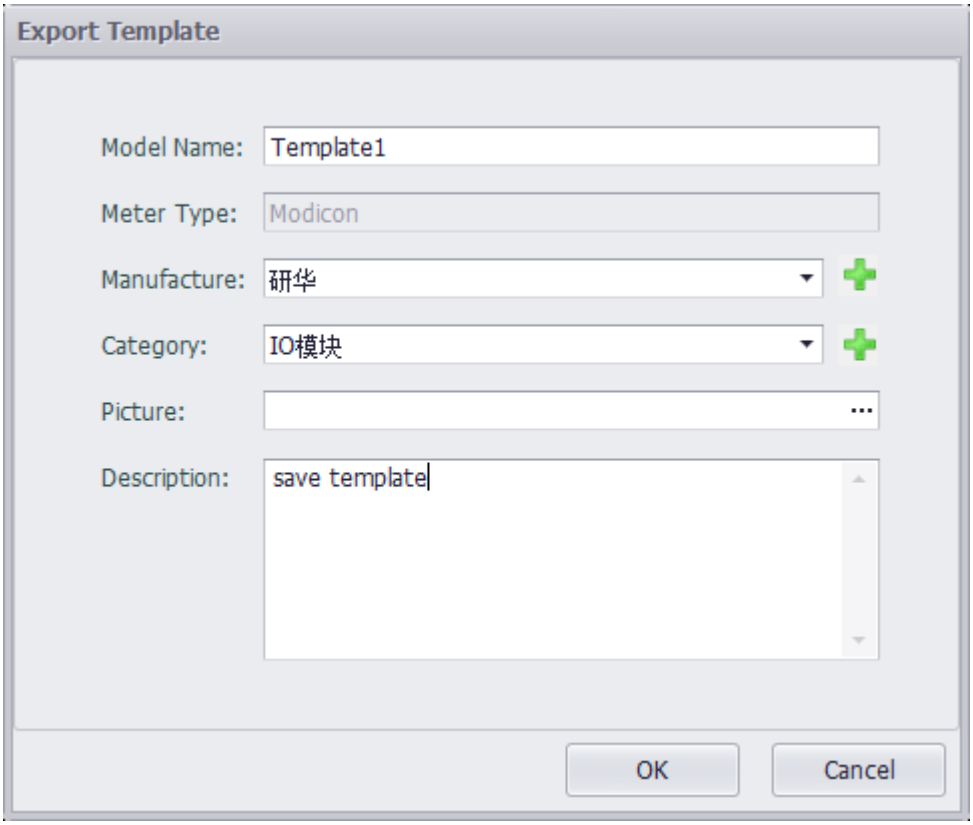
the template by clicking the Add from Template button in the Add button drop-down menu.



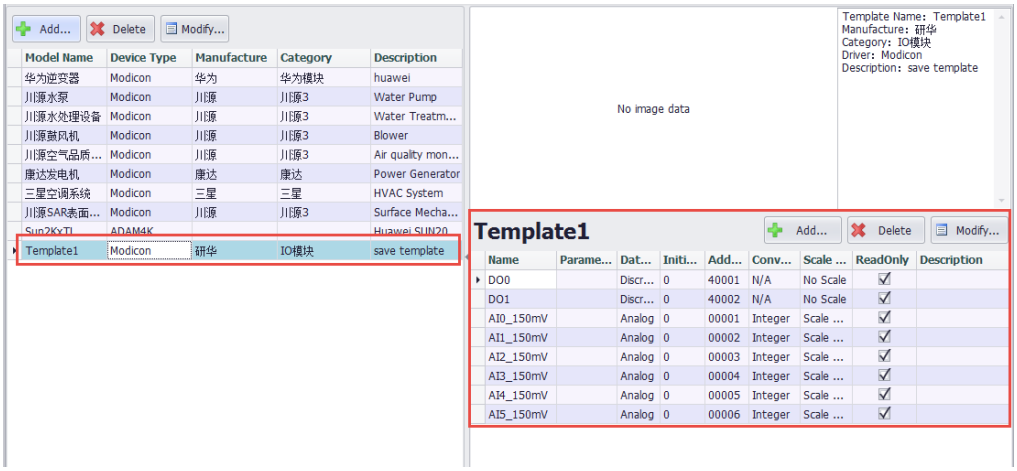


The tag information under the device can be saved as a template on the IO tag list page. Click the Save Template button to pop up the input template information panel. If the user template has an open password set, you will need to enter the open password to save the template.





After saving successfully , the newly saved device template information can be viewed in the user template .

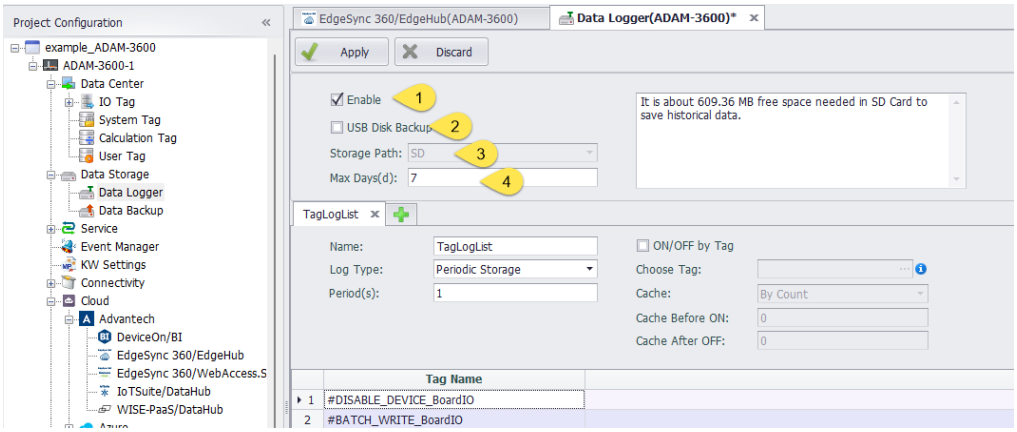


DataLogger configuration

DataLogger is the software module that implements historical data storage on EdgeLink.

The DataLogger module uses SQLite as the base storage medium, saves the data in the “Tag historical data table”, and saves the data in minutes, hours and days three historical data tables.

DataLogger Parameter Configuration：



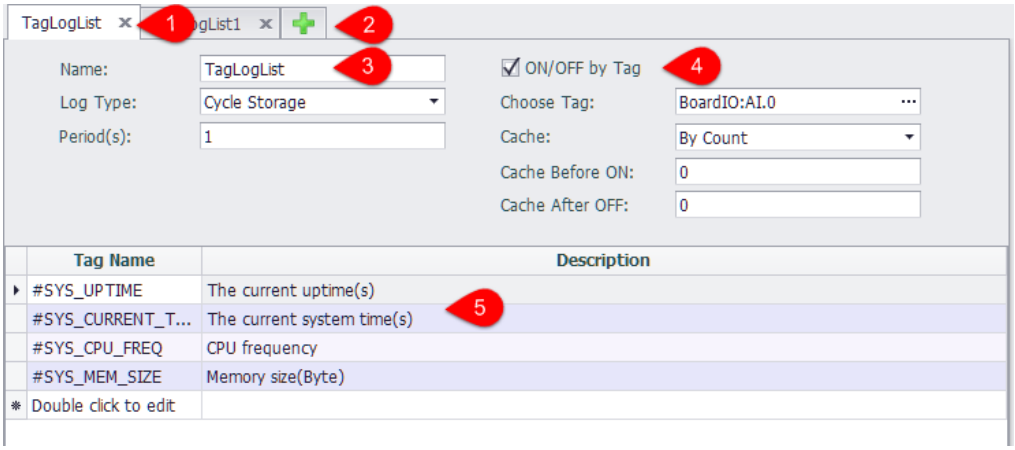
1. Enable: select this item to enable data storage;
2. USB Disk backup: select this item, the existed historical data will be copied into the USB disk from SD card only when the system detects an insertion event. The newly added historical data is still stored in the SD card.
3. Storage address enabled: the location of the data store is stored on the SD card by default. **The SD card must be installed before using DataLogger function**;

4. Save the number of days (days): the maximum number of days of historical data is 7 days by default. If the number of days saved is exceeded, the system will automatically delete the earliest stored data.

Example: - If the periodic storage period is 10S, the stored program starts to run at 13:15:17, then the time is 13:15:20 for the first stored data and 13:15:30 for the next data

Storage group parameter configuration：

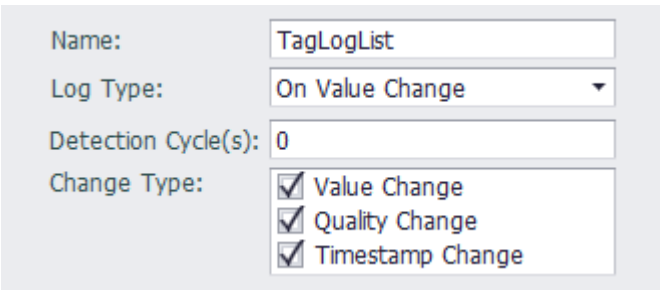
Tag values can be stored in a data table in a variety of ways depending on the configuration of the storage group



1. The storage group configures the Tab page, and the user can click “x” to close the current configuration page.
2. Users can click “+” to add storage groups
3. The basic parameters of a storage group:
    - Name: the name of the storage group, which is used only to distinguish storage groups

- Storage mode: you can select cycle storage and change storage.
- Period needs to be configured when selecting cycle storage.

4. The user can select a tag to control the current storage group ON and OFF. When the Tag value is 0, the storage group is not enabled, and the storage group is enabled when the rest of the values are present.
   - Select the control tag: select a tag in the Data Center as the control tag.
   - Cache mode: when the control tag ON and OFF, it will cache a certain amount of data. In the cache mode, you can choose to cache log information by count or time.
   - Cache before ON: some Tag data is cached before the storage group starts its storage
   - Cache after OFF： after the storage group stops storage, some Tag data is stored.
5. Edit the tags to be stored in the list，and the total number of tags stored in all storage groups is limited to 200.

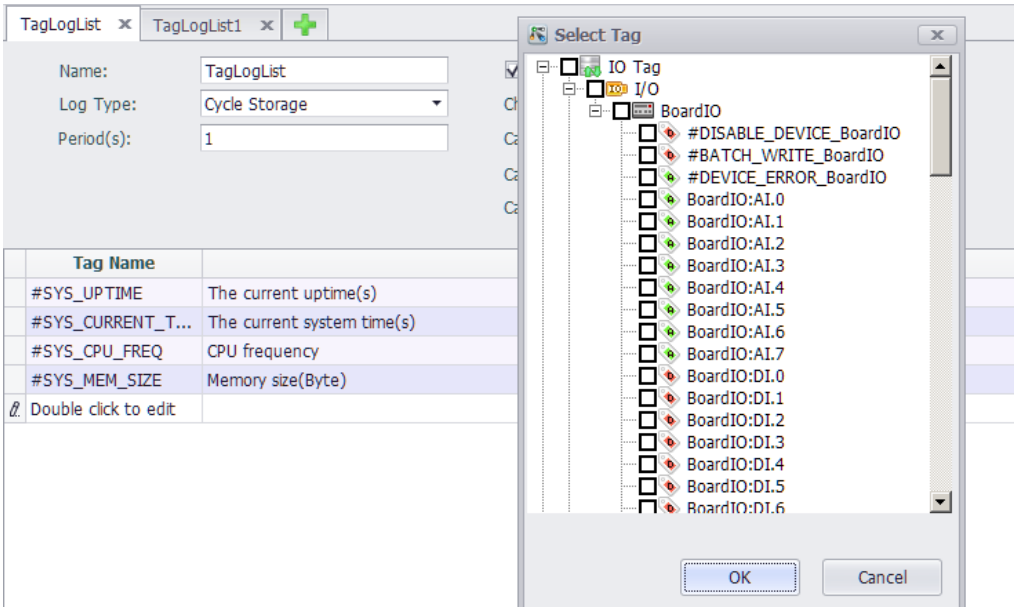


When the storage mode is selected as the change storage, it is necessary to configure ” Detection Cycle ” and ” Change Type “. The time of each ” Change Type ” after the storage group is enabled is to detect whether the tags in the storage group and the attributes selected in the ” Detection Cycle ” are consistent with the values saved after the last detection cycle. If there is a change, it will be stored in the data table.

When the value of ” Change Type ” is 0, it will be immediately stored in the data table when the change of the tag attribute is detected.

Edit the storage tag

Double-click on the last line in the tag name column to add the storage tag, and double-click the added Tag to modify. To delete the Tag, right-click on the Tag line that you want to delete, and click the delete button on the pop-up toolbar to remove the current Tag.



> **Note!** Tags are added to a storage thread and cannot be added to other storage threads

Error code information of #DATALOG_ERROR

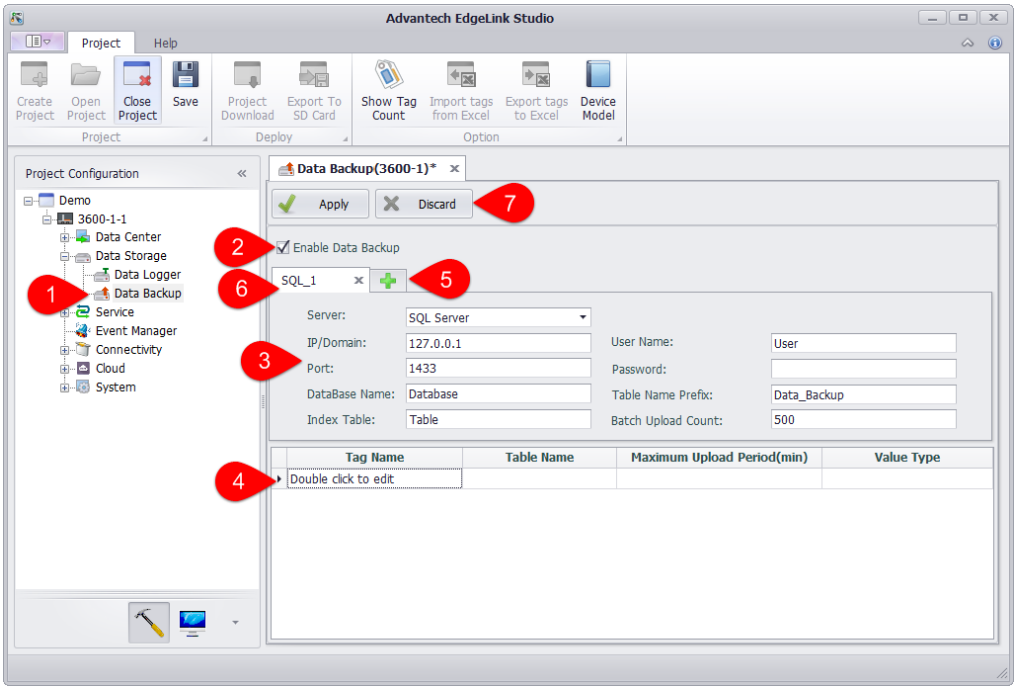
When the value of #DATALOG_ERROR is 0, it means that there is no error in the program.

Error 1 ~ 9 are critical errors

```
1: DataLogger is not enabled.
2: Storage path is invalid.
3: DataLogger SDK initialize Storage path failed.
4: DataLogger SDK initialize failed.
5: Failed to allocate memory at DataLogger startup.
6: Failed to initialize the logging thread at DataLogge
7: Open Control Tag failed.
8: Read Control Tag value failed.
9: Add Tag to data center failed.

257: Insufficient storage space. The safety space is 50
512 ~ 767: Insert value to DataLogger SDK value cache f
768 ~ 1023: DataLogger SDK write values to storage fail
1024 ~1279: DataLogger SDK reposition the write file fa
```

Data Backup

In EdgeLink Studio, users can set the historical data for the specified tag to be stored. According to the set storage method, historical data will occupy some of the SD card or U disk space.With the increase of running time, the historical data will be more and more.To improve the backup performance and security of historical data, users can backup huge amounts of data to other servers remotely.



1.Open the “Data backup” page.

2.Select Enable Data Backup.

3.Fill in data backup settings.

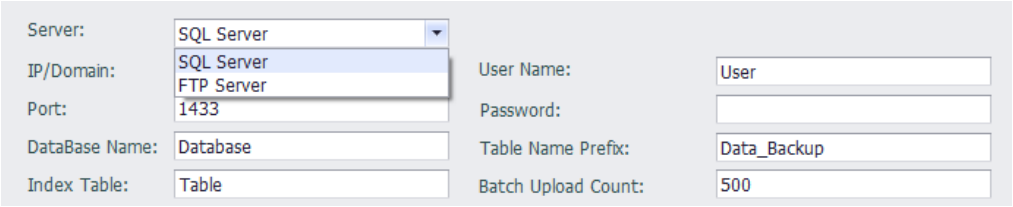
4.Select the tags to be backed up and other necessary information.

5.Click the “+” button to add a backup setting.

6.Click the “×” button to delete a backup setting.

7.Click Apply to complete the configuration.

Currently, data backup is divided into SQL Server and FTP Server according to the type of server used:



After the content to be backed up (such as a tag) has been added to the backup list under the connection, the server type cannot be modified; after all the contents in the backup list have been deleted, the server type can be modified.

SQL Server Method

In the data backup settings area, select Server Type as SQL Server to back up the selected tag data in ODBC mode. The information you need to fill out includes:

IP/Domain: The IP address or domain name of the backup server.

Port: The port number of the database.

DataBase Name: The name of the database that already exists on the connected server side.

Index Table: Custom table name. The table will be automatically generated in the SQL server, and the last time of each upload tag will be recorded in the table for the data store and forward.

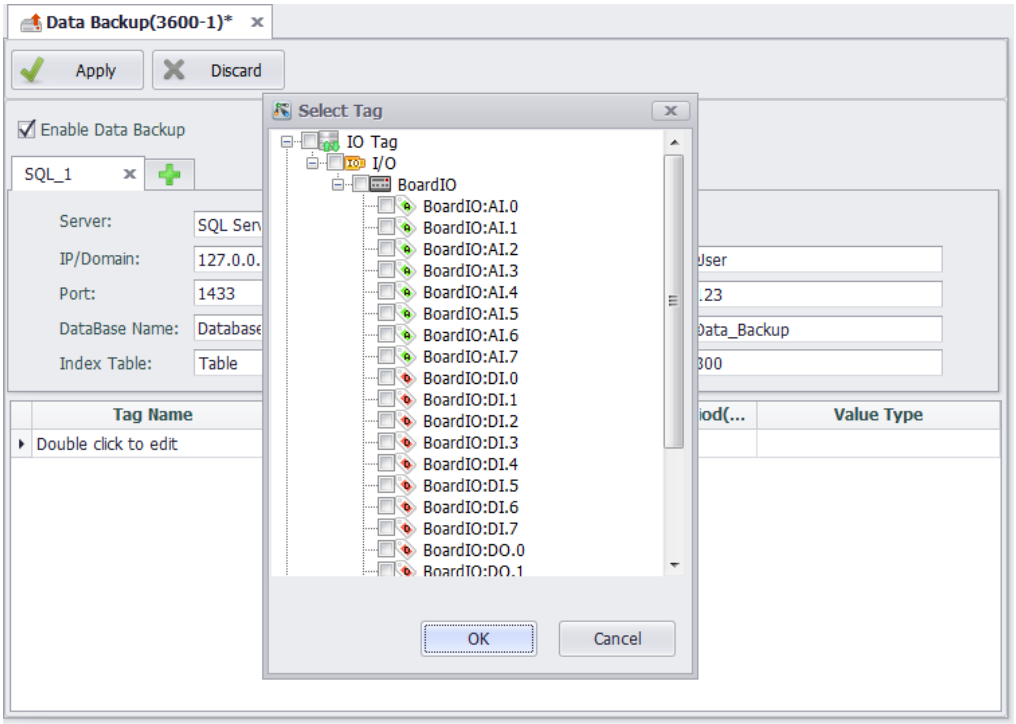
User Name: The username to log in to the remote server.

Password: The password to log in to the remote server.

Table Name Prefix: Used to automatically create a database table by table name in the connected database.

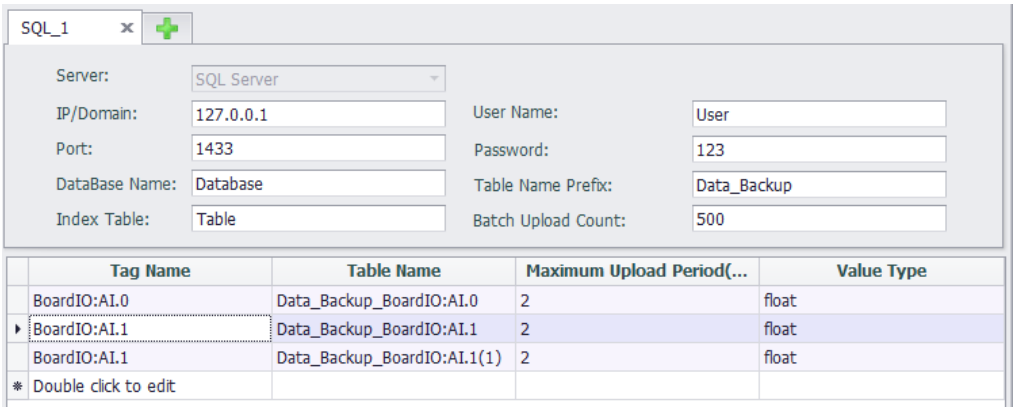
Batch Upload Count: The default limit for allowing the client to upload data each time is 500. That is, the system queries the cached 500 data and uploads them to the server in batches.

In the tag list, double-click on the blank row of the tag name column, and you can add the tags included in this backup.



A tag is saved as a database table during backup. By default, the “table name prefix _tag name” is used as the

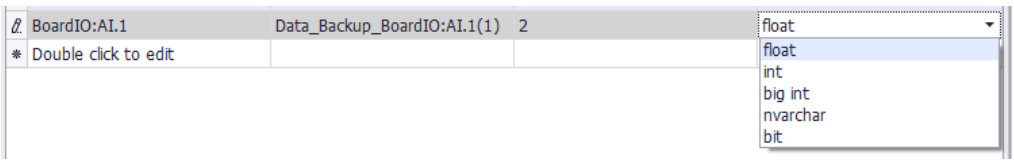
table name stored in the tag. To distinguish the storage table of the same name tag, you can specify different contents for the “table name prefix” in different connections, or modify the table name column by yourself. If the table name prefix and the tag are the same, the system will automatically rename the table name.



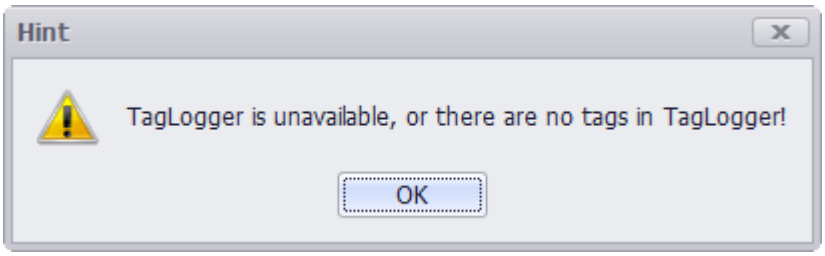
The default maximum upload period of the tag is 2 minutes. It is compatible with the “batch upload count”. New data is not queried beyond the maximum upload period, and if the single maximum upload limit is not reached, the data cached at this time will be uploaded to the server.

The tag storage value type is the format of the stored data. The default value type is float, and can be saved as float, int, big int, navarchar, bit type.

Users can modify the “table name”, “maximum upload period”, and “value type” in the tag list as needed.



If the “TagLogger” function is unavailable or the stored Tag is not specified in “TagLogger”, a dialog box will pop up and indicate that the user should set the “TagLogger” function before setting the backup tag when adding the tag to data backup. ***

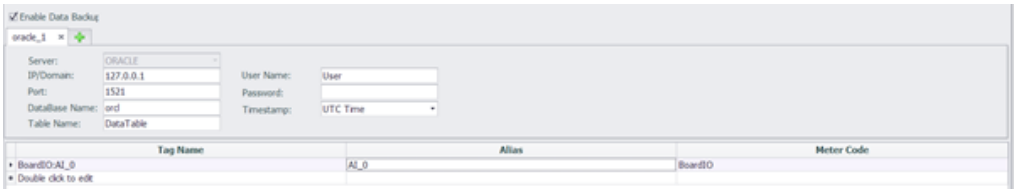


MySQL Server Method

In the data backup settings area, select Server Type as MySQL Server to back up the selected tag data in MySQL mode. The information you need to fill out is same as SQL Server.

ORACLE Method

In the data backup setting area, select Server Type as ORACLE Server to back up the selected tag data by ORACLE. The information you need to fill out includes:



1. IP/Domain：The IP address of the database, where the domain mode is not tested.
2. Port：The port that the database listens to. When the database is installed, the default is 1521. If there is

no modification when configuring the database, the default is 1521.

3. DataBaseName：The instance name of the Oracle database . The name of this instance is orcl by default during installation. If there are changes during the installation process, please use the custom instance name.

4. TableName: The table in Oracle that stores data. This version of the data upload mechanism is that all data that needs to be backed up on the device side is stored in this table on the database side. The database does not need to be created manually. When the device uploads data, the table will be created automatically if it does not exist, and must start with a letter. Table 2 is the table structure.

	COLUMN_NAME	DATA_TYPE	NULLABLE	DATA_DEFAULT	COLUMN_ID	COMMENTS
1	RECDATETIME	DATE	No	(null)	1	(null)
2	METERCODE	VARCHAR2(20 BYTE)	No	(null)	2	(null)
3	ATTRCODE	VARCHAR2(20 BYTE)	No	(null)	3	(null)
4	VALUE	FLOAT	No	(null)	4	(null)

   - RECDATETIME field：Tag timestamp，stored in Date format.
   - METERCODE field：Corresponds to the MeterCode in table 1, same as in Tagname.
   - ATTRCODE field: Corresponds to the Alias content in Table 1.
   - VALUE field：Tag value.

   The rules for defining transmission fields are as follows:

    - Tag name format：devicename:tagname . Tagname automatically corresponds to the field Alias，and devicename corresponds to the field metercode.
    - When the tag name format is tagname, Tagname automatically corresponds to the field Alias, the field metercode can be empty, and the field Alias cannot be empty
5. UserName and Password are the credentials for remote login to oracle.
6. Timestamp: The type of time stored in the RECDATETIME field in the database table. Local time and UTC time can be selected. The table storing the timestamp of the tag value cannot be customized. When the device connects to the database, the FORRECORDTIME table will be created by default to store the last uploaded timestamp of the tag, which is used for the device’s data resume function.

FTP Server Method

In the data backup setting area, select Server Type as FTP Server to back up the selected tag data by FTP. The information you need to fill out includes:

IP/Domain: The IP address or domain name of the backup server.

Port: The port number of the database.

User Name: The username to log in to the remote server.

Password: The password to log in to the remote server.

Upload Interval: The interval at which the device uploads files to the server. The default is 5 minutes.

Whether to enable active mode: whether the mode of connecting to the server is active. FTP supports two modes, one is Standard (PORT), and the other is Passive (PASV). In active mode, the FTP client sends a PORT command to the FTP server. In passive mode, the FTP client sends a PASV command to the FTP server. Active mode is not enabled by default, ie passive connections are used.

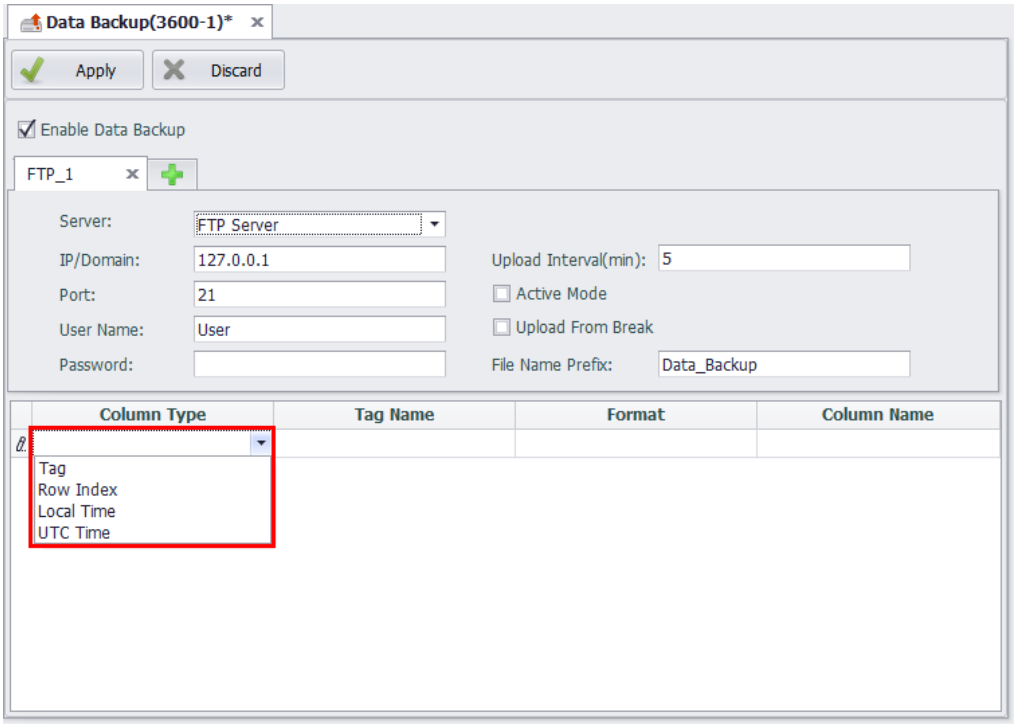
Whether to enable upload from break: For files that are incompletely transmitted due to network reasons during transmission, continue to transmit or delete incomplete files and retransmit after network recovery. Consider that some servers do not support this feature and are not enabled by default.

File name prefix: Multiple users or multiple devices transmitting to the same server at the same time will result in consistent file name conflicts, prefixing the file names for differentiation.

Column type: Click on the blank line in the “column type” in the list, you can choose to add a column of data to the backup FTP file. The optional types include “tag” and the corresponding “row index”, “local time”, and “UTC time” when the tag is stored.

Format: Only for the format of “serial number”, “local time”, “UTC time”.

Column Name: Users can rename the name of the data column that needs to be stored.

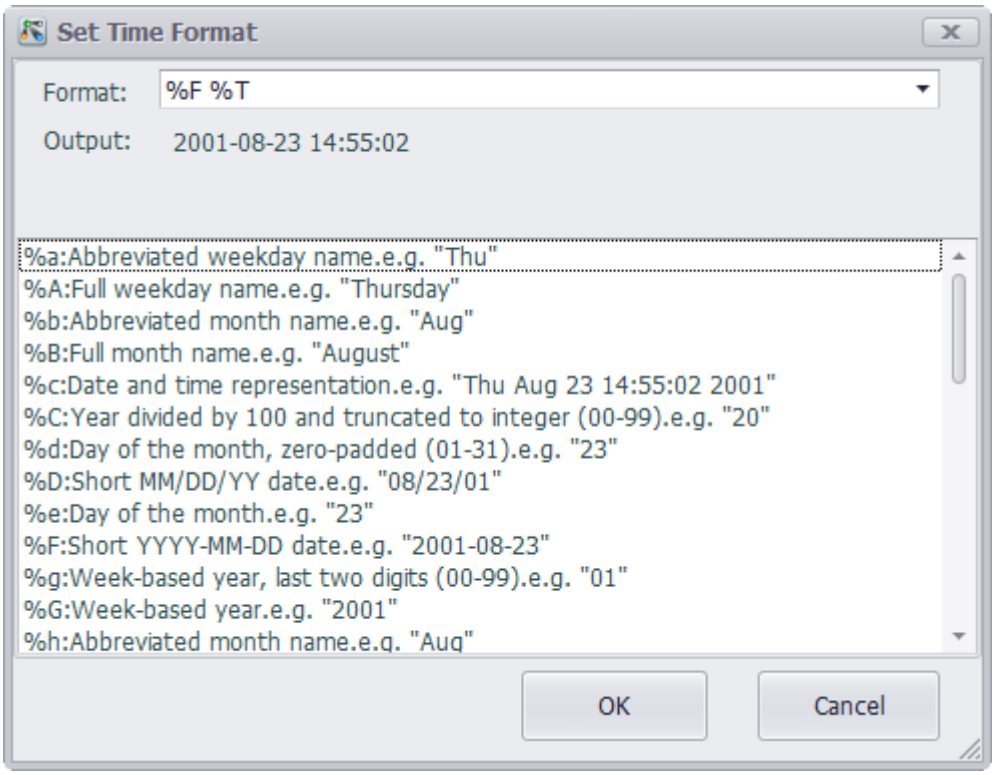


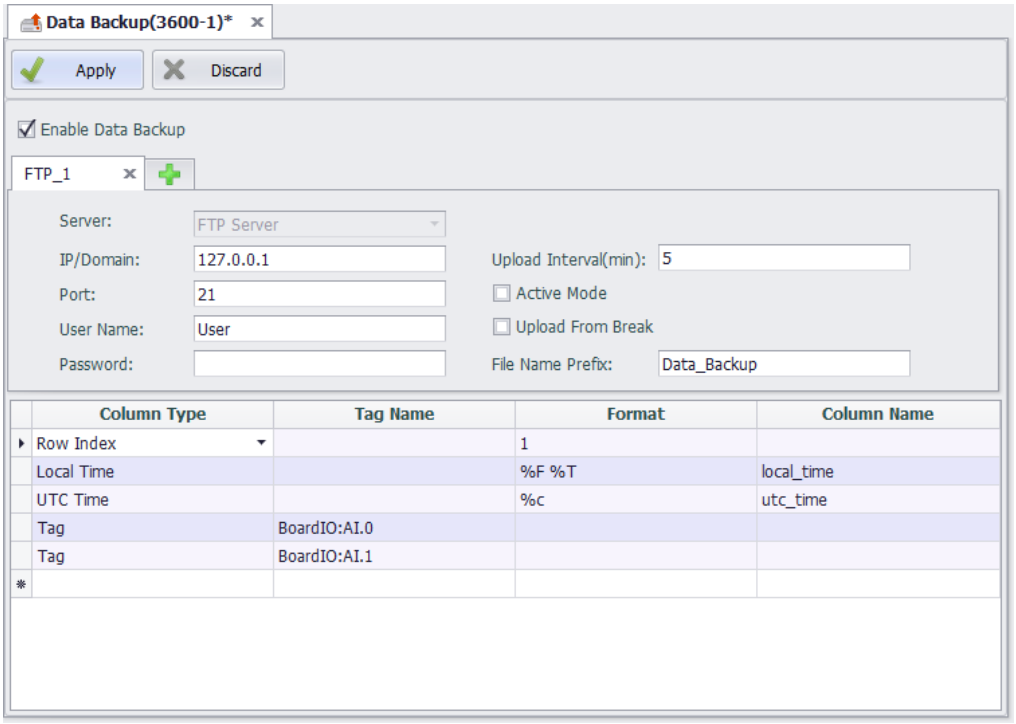
Tag: When the selected column type is “tag”, the user can select the tag to be backed up in the pop-up dialog box and modify the “column name” in the list. The contents of the data will be displayed in the FTP file according to the “column name” set by the user.

Row Index: When the selected column type is “serial number”, the user can modify the “format” and “column name” in the list. The “format” should be filled with an integer greater than 0, indicating the index value of the first row of the backup data.

Local Time or UTC Time: When the selected column type is “local time” or “UTC time”, the default saved data

format is “% F% T”. Users can set the time format of the backup in the pop-up dialog box. The code in different time formats is given in the date list at the bottom of the window, and an example of the time format is shown in “Save as”. Users can use the various formats in the date list. Specify the time format and click the OK button, and the “time format” code will appear in the list, where the user can modify the “column name” that is saved by the time column.





The file uploaded by FTP Server is a csv file. The system records the value of the same timestamp of all tags selected for backup as one piece of data in the table.

Protocol Service Configuration

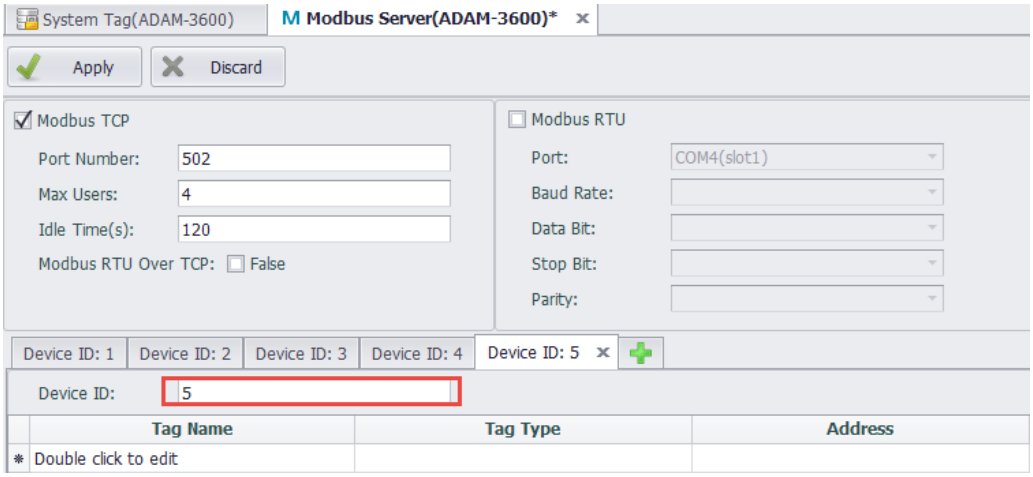
EdgeLink supports four standard protocols: Modbus service, BACnet service, WASCADA service, IEC-104 service, which can realize the communication between RTU and the lower acquisition devices as well as the upper central devices.

Modbus Server

Modbus server achieves the mapping from tag to Modbus address, allowing Modbus Client on the upper computer to read/write tags via Modbus TCP or Modbus RTU.

Device ID Setting

Set a different Device ID for ModbusServer for client access



Modbus TCP Configuration

Modbus TCP service allows the upper computer to access the device through Modbus TCP protocols of TCP/IP.

The configurations of Modbus TCP are as follows:

- Port Number: Set the number of the port Modbus TCP listens on. The default number is 502.
- Max Users: Set the maximum number of users that can be connected at the same time. The default value is 4, which means at most 4 client ends can simultaneously access the device through Modbus TCP protocol.
- Idle Time: Specify the maximum time when the client writes/reads no data to/from the server after the TCP connection has be established. The default value is 120

seconds. After that, the client will be automatically disconnected from the server. If this value is set to 0, the server will never be disconnected.

Modbus RTU Configuration

Modbus RTU service allows the upper computer to access the device through serial port connection (RS-232/485) or virtual serial port connection via Modbus RTU protocol.

The configurations of Modbus RTU are as follows:

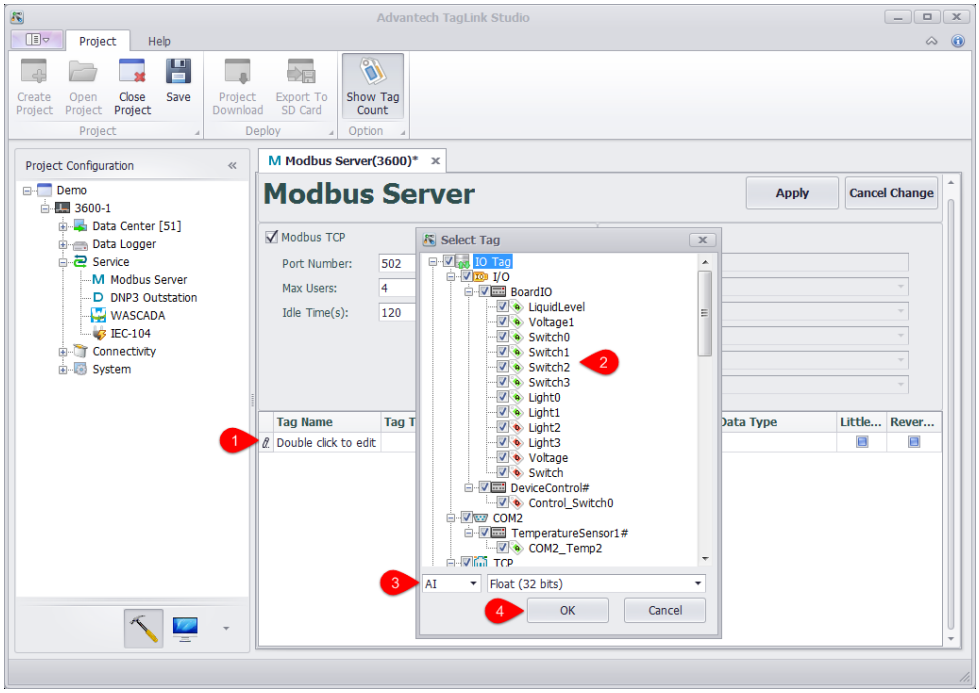
- Device ID: It is sometimes called Station Number, which is the node ID of a Modbus RTU device on serial bus.
- Port: Specify the serial port number Modbus RTU service will apply to. The drop-down list shows all available ports of the current device. If a certain port is missed, it means this port may be occupied by other services. At this time, you need to manually delete the occupied COM port in the data center to configure this port.
- Baud Rate: Set the baud rate of the serial transmission. The default value is 9600.
- Data Bit: Set the data bit of the serial transmission. The default value is 8.
- Stop Bit: Set the stop bit of the serial transmission. The default value is 1.
- Parity: Specify the parity check rules of the serial transmission. The default option is Node, which means no parity check is applied.

Modbus Address Mapping

To let Modbus client capable of accessing to the tags on the device, users should map the tags to the corresponding Modbus addresses first. The procedures are as below:

1. Add the tag to Modbus address list.

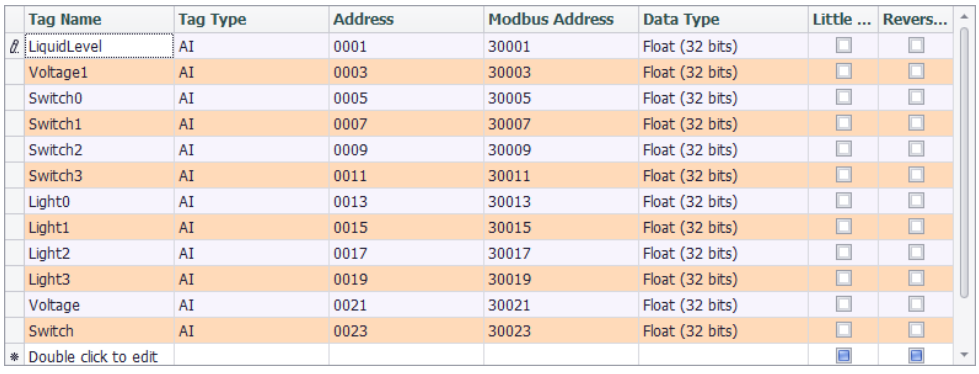
- Double-click “Double click to edit” cell.
- Tick the tag(s) to be added into Modbus address list. One or multiple tags can be selected at the same time.
- Select the data type and data converting method of the mapping, which will be applied to all the selected tags.
- Click “OK” button to finish adding tags to the address list.
- Repeat the above steps to add more tags.



2. If users want to change the mapping settings, the available options are:

- Tag Type: There are four tag types: AI, AO, DI and DO, respectively corresponding to four tag types of Modbus protocol.

- Address: Set the starting address of a tag in Modbus address space. The minimum address is 1. On the right is Modbus Address column, which is non-editable. The values within this column are made of tag type and tag address, ruled by Modicon.
- Data Type: There are 2 broad types: Integer and Float. The former one is further classified to 6 categories by sign and bit number (16, 32, 64); while the later one is classified to 2 categories (Float and Double) by its precision (single or double).
- Little Endian: The default option is big endian (Network Byte Order). If the client only can accept the data of little endian, please tick “Little Endian” box.
- Reverse Word: If “Little Endian” is ticked, then this option will reverse the byte order. Normally, this option will reverse the word (two bytes) order. It should be noted that “Little Endian” option is before “Reverse Word” option, which means if both options are ticked, the byte oder will be firstly reversed and then the word order will be reversed when the mapped tag value is read.



	Tag Name	Tag Type	Address	Modbus Address	Data Type	Little ...	Revers...
	LiquidLevel	AI	0001	30001	Float (32 bits)	☐	☐
	Voltage1	AI	0003	30003	Float (32 bits)	☐	☐
	Switch0	AI	0005	30005	Float (32 bits)	☐	☐
	Switch1	AI	0007	30007	Float (32 bits)	☐	☐
	Switch2	AI	0009	30009	Float (32 bits)	☐	☐
	Switch3	AI	0011	30011	Float (32 bits)	☐	☐
	Light0	AI	0013	30013	Float (32 bits)	☐	☐
	Light1	AI	0015	30015	Float (32 bits)	☐	☐
	Light2	AI	0017	30017	Float (32 bits)	☐	☐
	Light3	AI	0019	30019	Float (32 bits)	☐	☐
	Voltage	AI	0021	30021	Float (32 bits)	☐	☐
	Switch	AI	0023	30023	Float (32 bits)	☐	☐
*	Double click to edit					☐	☐

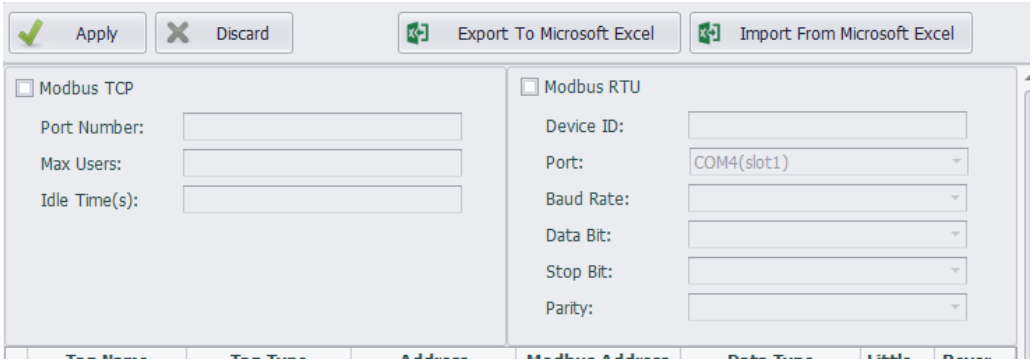
Comparison Table of Modbus Data Type Conversion

To facilitate the understanding of the data type conversion, please refer to the below examples, in which the tag values are hexadecimal and every byte is separated by space.

Name	Original Value	Little Endian	Reserve Word	Little Endian + Reverse Word
Signed/Unsigned Integer (16 bits)	12 34	34 12	12 34	34 12
Signed/Unsigned Integer / Float (32 bits)	12 34 56 78	78 56 34 12	56 78 12 34	34 12 78 56
Signed/Unsigned Integer / Double (64 bits)	12 34 56 78 90 AB CD EF	EF CD AB 90 78 56 34 12	CD EF 90 AB 56 78 12 34	34 12 78 56 AB 90 EF CD

Tag List Import & Export

The user can export the tag list into the EXCEL, and then edit it and import into the EdgeLink Studio.



Users can edit the list of tags exported to EXCEL, but note that the order of columns cannot be adjusted.

	A	B	C	D	E	F	G
1	tagName	address	modbusDataType	isLittleEndian	isReverse		
2	#DISABLE_DEVICE_BoardIC	30001	uint32	TRUE	FALSE		
3	#BATCH_WRITE_BoardIO	30003	float	TRUE	FALSE		
4	#DEVICE_ERROR_BoardIO	30005	float	TRUE	FALSE		
5	BoardIO:AI.0	30007	float	TRUE	FALSE		
6	BoardIO:AI.1	30009	float	TRUE	FALSE		
7	BoardIO:AI.2	30011	float	TRUE	FALSE		
8	BoardIO:AI.3	30013	float	TRUE	FALSE		
9	BoardIO:AI.4	30015	float	TRUE	FALSE		
10	BoardIO:AI.5	30017	float	TRUE	FALSE		
11	BoardIO:AI.6	30019	float	TRUE	FALSE		
12	BoardIO:AI.7	30021	float	TRUE	FALSE		
13	BoardIO:DI.0	30023	float	TRUE	FALSE		
14	BoardIO:DI.1	30025	float	TRUE	FALSE		
15	BoardIO:DI.2	30027	float	TRUE	FALSE		
16	BoardIO:DI.3	30029	float	TRUE	FALSE		
17	BoardIO:DI.4	30031	float	TRUE	FALSE		
18	BoardIO:DI.5	30033	float	TRUE	FALSE		
19	BoardIO:DI.6	30035	float	TRUE	FALSE		
20	BoardIO:DI.7	30037	float	TRUE	FALSE		
21	BoardIO:DO.0	30039	float	TRUE	FALSE		
22	BoardIO:DO.1	30041	float	TRUE	FALSE		
23	BoardIO:DO.2	30043	float	TRUE	FALSE		
24	BoardIO:DO.3	30045	float	TRUE	FALSE		
25							
26							

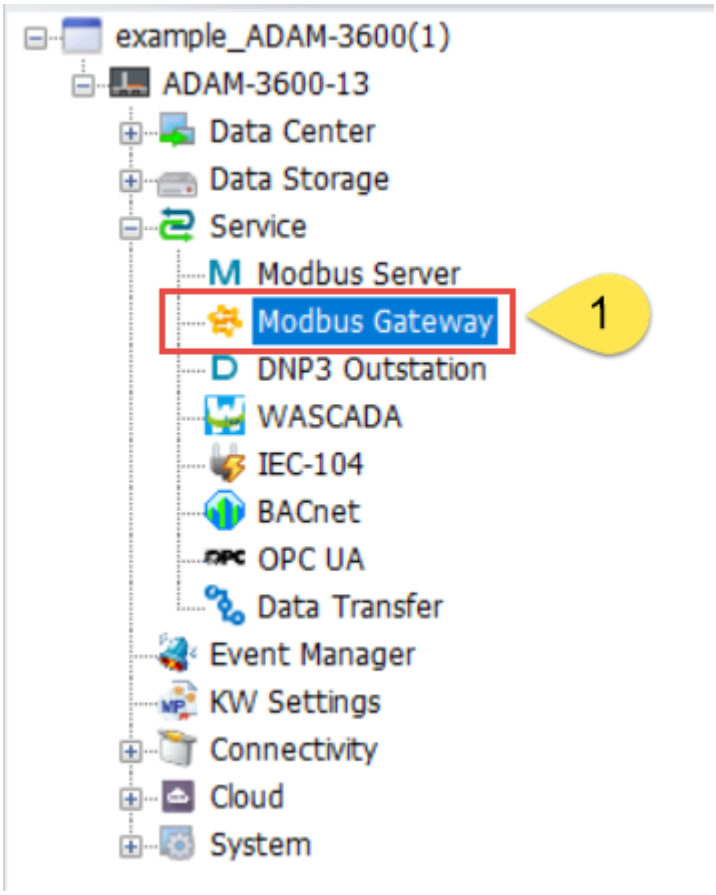
ModbusGateway

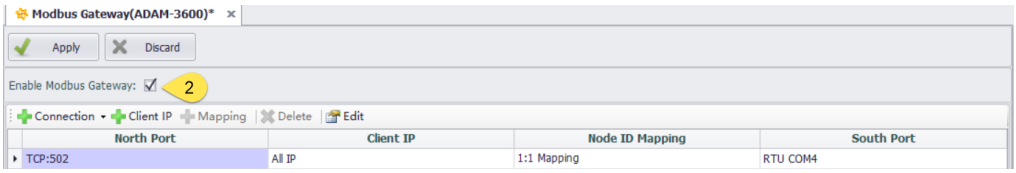
Architecture

The ModbusGateway program primarily performs the conversion between Modbus TCP and Modbus RTU protocols. The Modbus Client on the north side can directly access the Modbus Gateway program on the gateway device to connect to the instruments on the south side.

Enable

To enable the Modbus Gateway functionality, a connection from ETH to COM will be added by default.





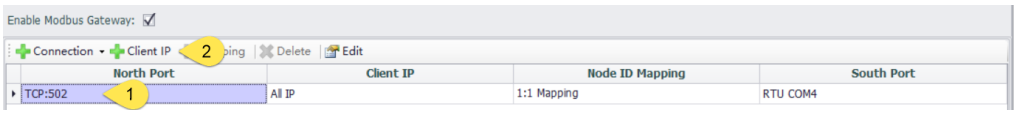
Default Connection Parameters Description

Parameters	Description
North - direction port	The port type used by the client to send requests, TCP:502 means the requests are sent through the TCP port to access the Modbus Gateway using port number 502
Client IP	The IP address of the requesting client. If there are no special restrictions, all IP addresses will be allowed to access

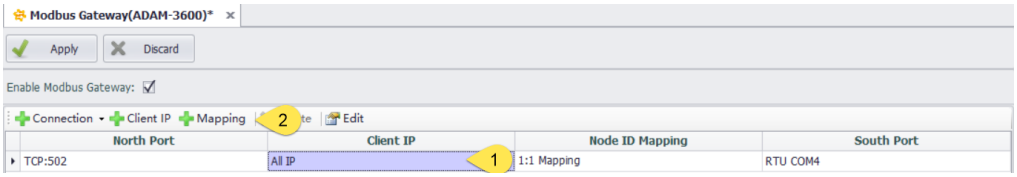
Parameters	Description
Node IP mapping	The mapping relationship between the requesting client's ID and the south-facing instrument's ID, where 1:1 mapping means that if the requesting client's ID is "a", the request will be forwarded to the instrument with the ID of "a" in the south-facing connection
South - direction port	The port type used to connect to the actual instruments

Configuration Instruction

1. Add



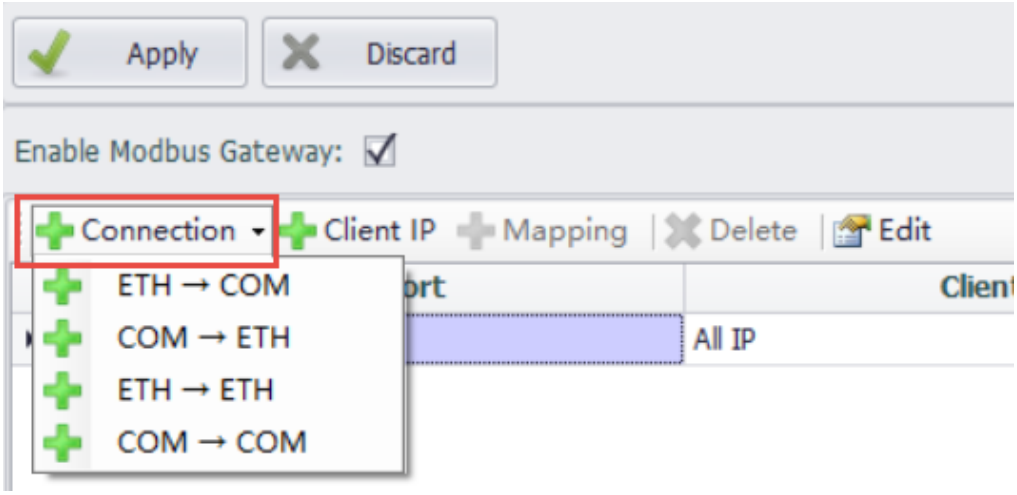
When the cursor selects the northbound port, a new connection can be added, and different client IPs can be added under the same northbound port



When the cursor selects any one of the client IP, node ID mapping, or southbound port, a new connection can be added, or a new client IP or node ID mapping and southbound port can be added

2. Connection

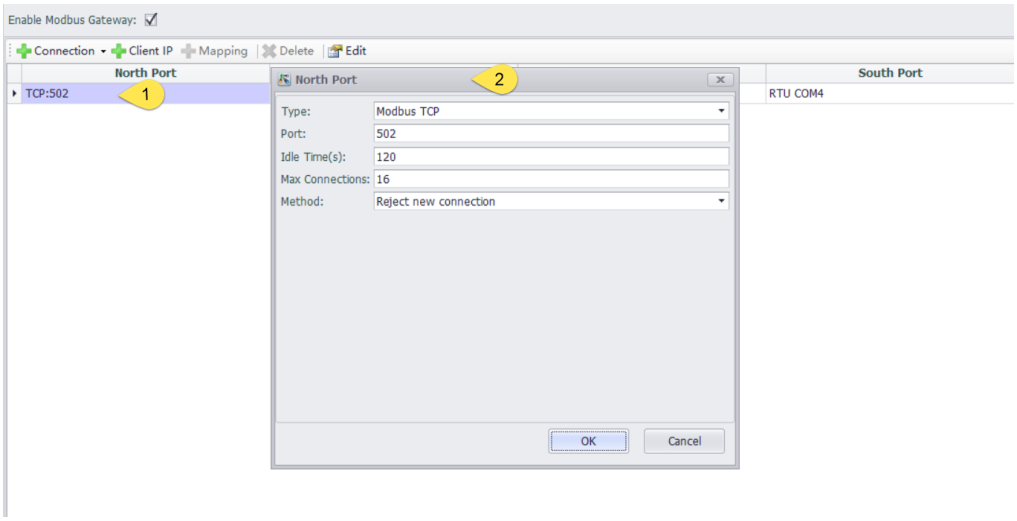
There are four types of connection methods



Connection type	Description
ETH—>COM	Convert the northbound network requests to southbound serial requests
COM—>ETH	Convert the northbound serial requests to southbound network requests
ETH—>ETH	Convert the northbound network requests to southbound network requests
COM—>COM	Convert the northbound serial requests to southbound serial requests

3. NorthPort

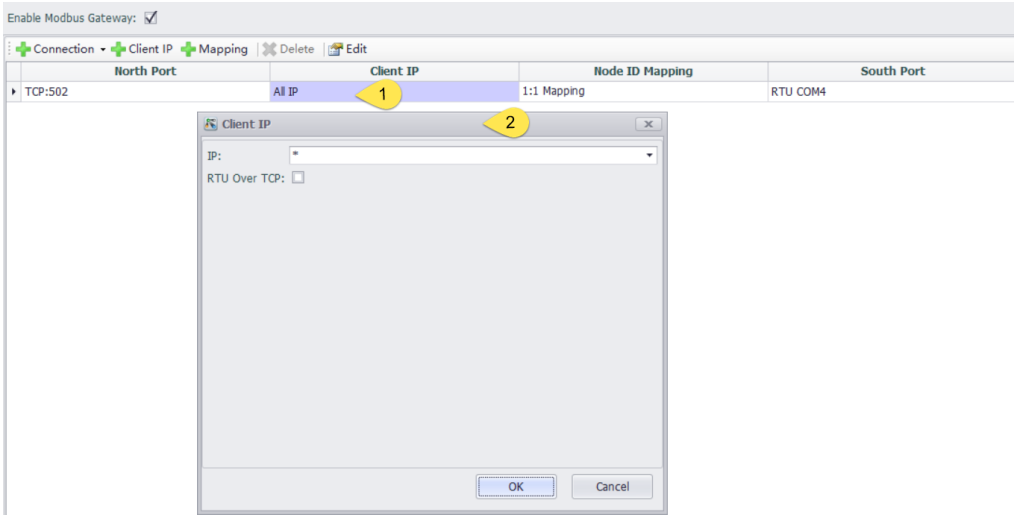
Double-click the northbound port of a specific connection to access the northbound port settings



Parameters	Description
Type	The type of Modbus request：Modbus TCP/ Modbus UDP / Modbus RTU / Modbus ASCII
Port	The port number needs to be set only when using Modbus TCP or Modbus UDP for access
Idle time	The maximum idle time of a specific connection
Max Connection	The maximum number of connections allowed by Modbus Gateway
When the maximum number of connections is exceeded	he strategy when the number of connections exceeds the maximum: refuse connection / drop the earliest connection

4. Client IP

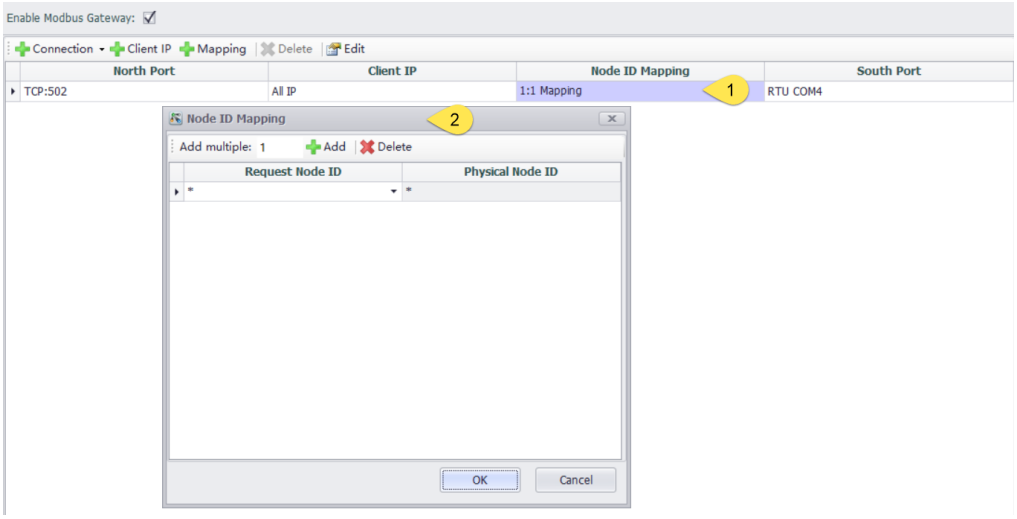
Double-click the client IP of a specific connection to access the client IP settings



Parameters	Description
IP	Allowed client IP addresses. Using an asterisk (*) allows all IP addresses, while specifying a single IP or an IP range is also possible
RTU Over TCP	After selecting this option, the protocol type for northbound requests will be Modbus RTU Over TCP

5. Node ID mapping

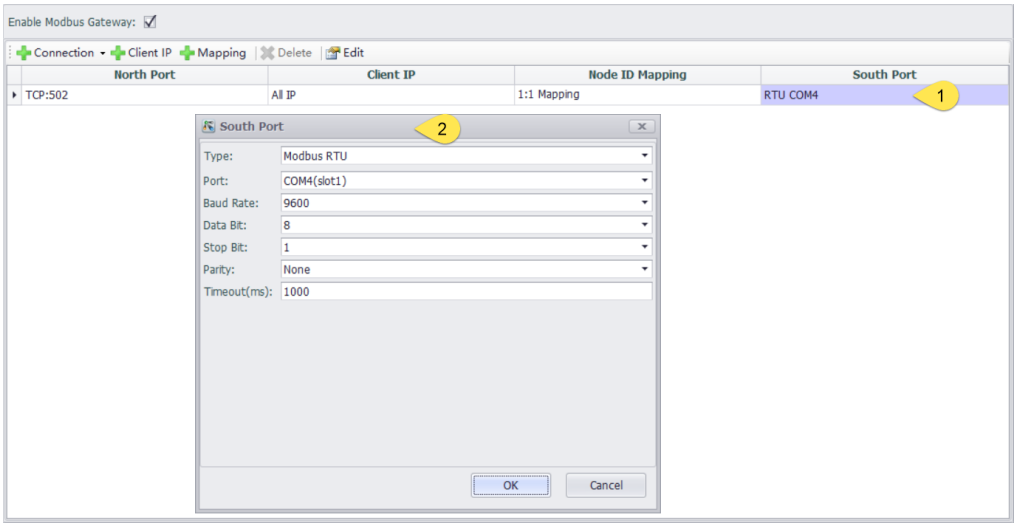
Double-click the node ID mapping of a specific connection to access the node ID mapping settings. Using an asterisk (*) represents no ID conversion, meaning a 1:1 mapping



Parameters	Description
Add multiple	By default, each click on add will increase the number of ID mappings by one. Clicking add on an empty field allows you to add multiple ID mappings at once
Request Node ID	The node ID of the northbound client when sending requests
The actual node ID	The actual ID of the instrument on the southbound side

6. South Port

Double-click the southbound port of a specific connection to access the southbound settings



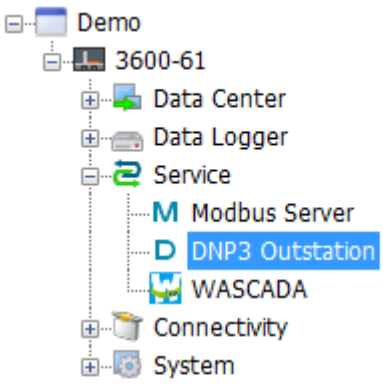
Parameters	Description
Type	The Modbus protocol type used by the southbound instrument：Modbus TCP/ Modbus UDP / Modbus RTU / Modbus ASCII
Serial number	The serial port used to connect the gateway to the southbound instrument
Timeout	The timeout time for southbound requests

DNP3 Server

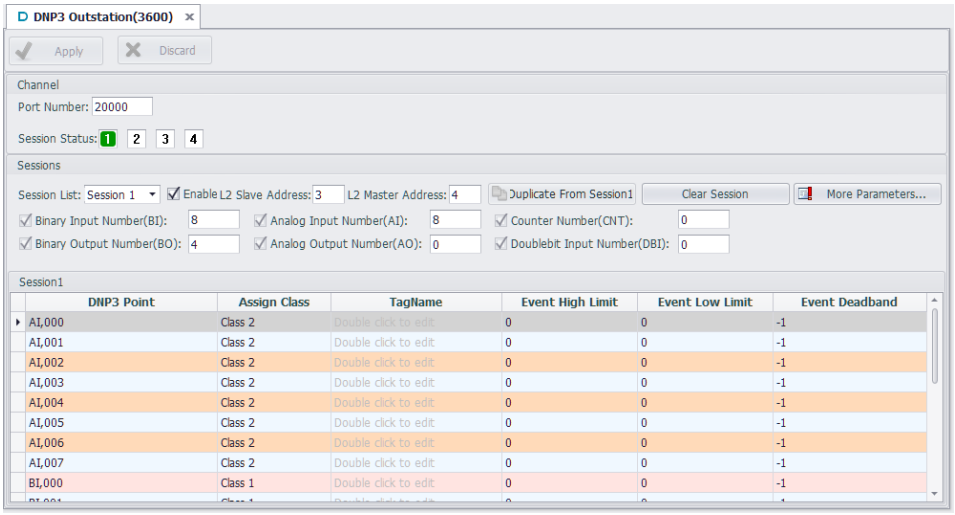
ADAM-3600 can work as DNP3 Outstation (hereinafter referred to as DNP3 server) to exchange data with DNP3 Master of HMI/SCADA (hereinafter referred to as DNP3 client). Current version of DNP3 server has passed DNP3 Level 2 test.

Here will explain the application of DNP3 Outstation in detail.

1. Double-click “DNP3 Outstation” under “Service” item in the left menu tree to pop up the configuration interface.



2. The main configuration interface of DNP3 server is shown as below. Some terms appeared here should be explained:



- Channel:

It represents the media of DNP3 server to communicate with the outside. Current version of DNP3 server only supports Ethernet communication which indicates TCP/IP network communication protocol by default.

Slave Station: It is DNP3 server address. DNP3 protocol specifies that source address and target address of DLL should be set. If users are not quite familiar with this part, please keep the default settings.

Port number: It is the port number of TCP/IP communication on DNP3 server. The default number is 20000.

- Session:

Here the supported number of sessions means at most 4 DNP3 clients are supported to communicate with DNP3 server at the same time. Users should set an appropriate number of sessions based on real

needs to avoid extra idle sessions, so as to less burden the CPU and improve the operating efficiency of EdgeLink.

Enable: Users need to tick “Enable” option to give the right to DNP3 client to access this session.

Master Station: It is DNP3 client address. DNP3 protocol specifies that source address and target address of DLL should be set. If users are not quite familiar with this part, please keep the default settings.

- Database:

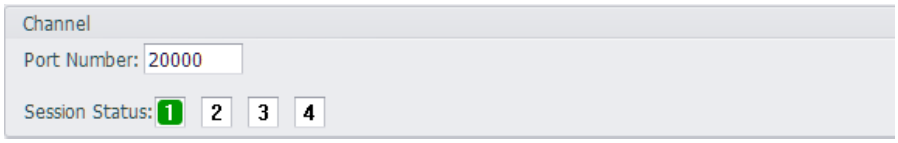
Each session has an independent database, allowing users to classify DNP3 points and configure their properties based on the pre-configured tags and DNP3 points mapped to DNP3 server.

> Note: Please keep the total number of DNP points in all sessions less than 2000 so as to ensure the operating efficiency of EdgeLink.

3. Next will describe the detailed settings of each term.
   - Channel Setting

     Session Status: There are in all 4 sessions here. When any of them is enabled, it will turn green to show its status: read-only.

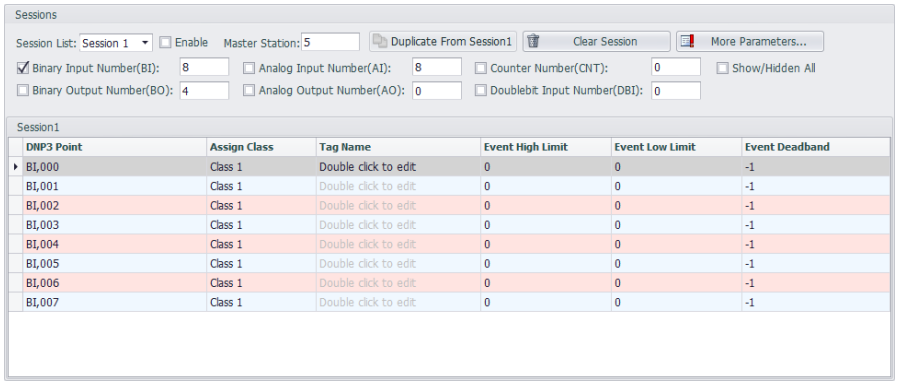
     See the below screenshot.



- Session Setting

  Before starting to edit a session, users should select a session from the drop-down list. The default setting is Session 1. Please tick “Enable” box first,

  then choose whether to show and use 6 categories of DNP3 points. The box before each category allows users to select to show or hide points in the editing interface below; while the box after allows users to set the number of DNP3 points. The studio provides 8 BIs, 8 AIs and 4 BOs by default, and all BI points are shown in the editing interface. “Show/Hide All” determines whether to show all points in each category in the editing interface, to avoid a long list which may in turn affect operation convenience of users. See the below screenshot:



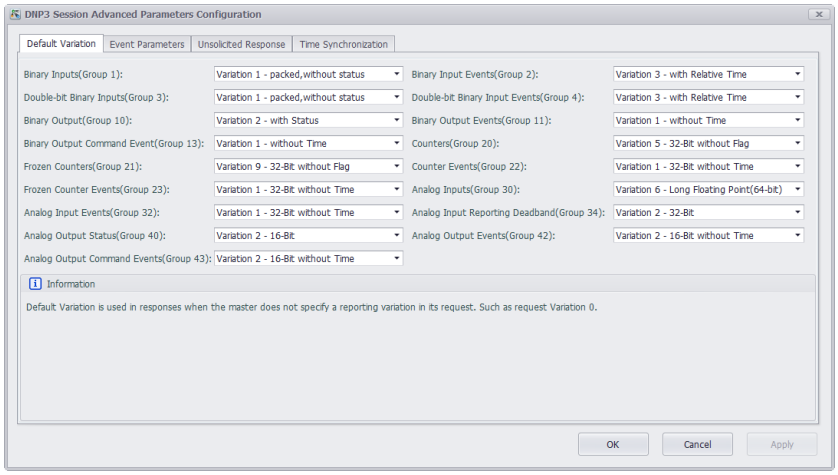
When users want to configure multiple sessions which are basically similar, please click this button to clone session 1.

When users make too many configuration errors, please click this button to clear the session and re-start editing. Note: This operation can’t be undone, please operate with care.

For advanced users who want to customize DNP3 service, please click this button to pop up “DNP3 Session Advanced Parameters Configuration” page which includes four part:

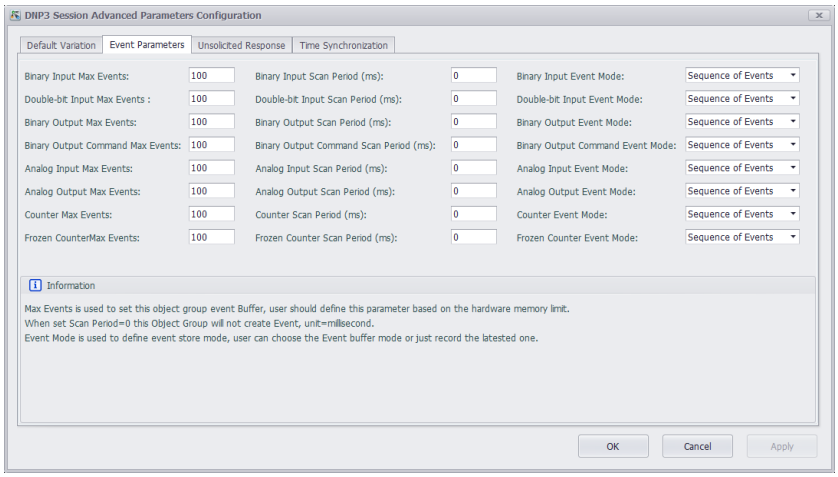
1. [Default Variation]

   Click this tab to show the default data type of each DNP3 group. “Information” box provides the related description and remarks. For more detailed information, please refer to Appendix A DNP3 data object library — object descriptions in DNP3 protocol (This manual refers to 2012 version of DNP3 protocol. Different version may vary in chapter arrangements).



2. [Event Parameters]

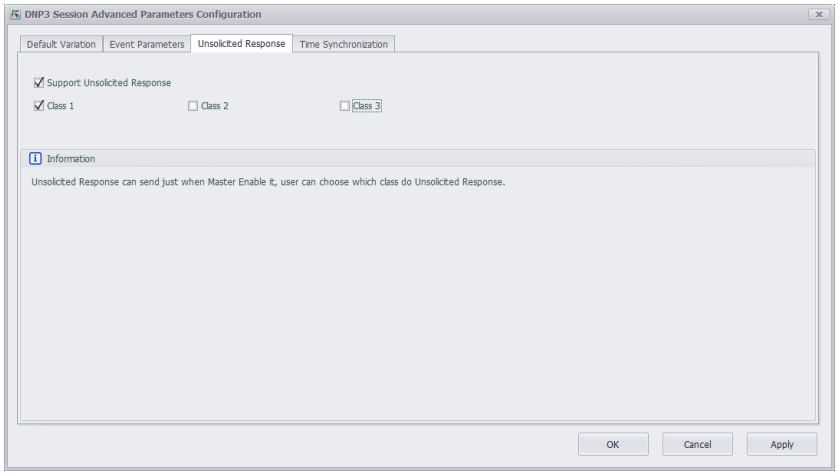
   Click this tab to configure the behavior pattern parameters of the events created by DNP3 point groups. “Information” box provides the related description and remarks. For more detailed information, please refer to 4.1.5.2 Events in DNP3 protocol.



3. [Unsolicited Response]

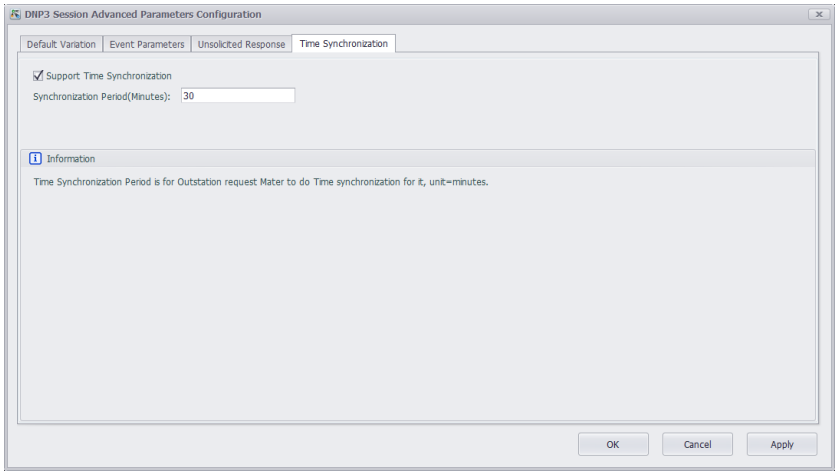
   Click this tab to choose to enable the unsolicited response function of DNP3 server based on the premise that DNP3 client actively enables this function of DNP3 server. Users

can select the class (Class 1, Class 2 and Class 3) to implement this function. “Information” box provides the related description and remarks. For more detailed information, please refer to 4.6 Unsolicited Responses in DNP3 protocol.



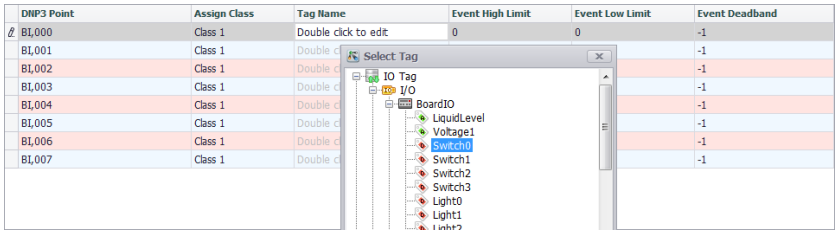
4. [Time Synchronization]

   DNP3 protocol supports time synchronization function by default. Click this tab to choose whether to enable this function on DNP3 client end. If the box is ticked, the default setting is 30 minutes, which means the synchronization will be carried out every 30 minutes. The length of synchronization time depends on the requirements of time precision in users’ application. “Information” box provides the related description and remarks. For more detailed information, please refer to 10.3 Time Synchronization in DNP3 protocol.



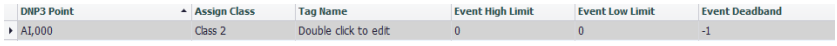
- [Database] Editing of Session

1. DNP3 point in each session should be associated with a tag. Double-click on a cell in “Tag Name” column to add a tag.



2. After the association, the changes of “Switch0” will be sent to [BI0] of DNP3 point. Columns of “Event High Limit”, “Event Low Limit” and “Event Deadband” are only effective for Analog Input; while for other columns, please keep the default settings.

3. For analog input event of DNP3 point, DNP3 server provides the following three settings: “Event High Limit”, “Event Low Limit” and “Event Deadband”. Here, users who set AI event can adjust its event parameters so as to trigger an AI event.



DNP3 Point	Assign Class	Tag Name	Event High Limit	Event Low Limit	Event Deadband
AI,000	Class 2	Double click to edit	0	0	-1

4. The above shows the basic parameter settings of DNP3 server. If advanced users need to configure more parameters, please contact Advantech technical support staff to get more detailed answers.

WASCADA Service

WASCADA protocol is a private communication protocol of WebAccess which can directly access all tags on RTU through TCP connection with the help of WACADA service, with no address mapping needed (such as Modbus service). In addition, the tags supporting periodic data storage will be capable of resuming broken transmission through WASCADA service.

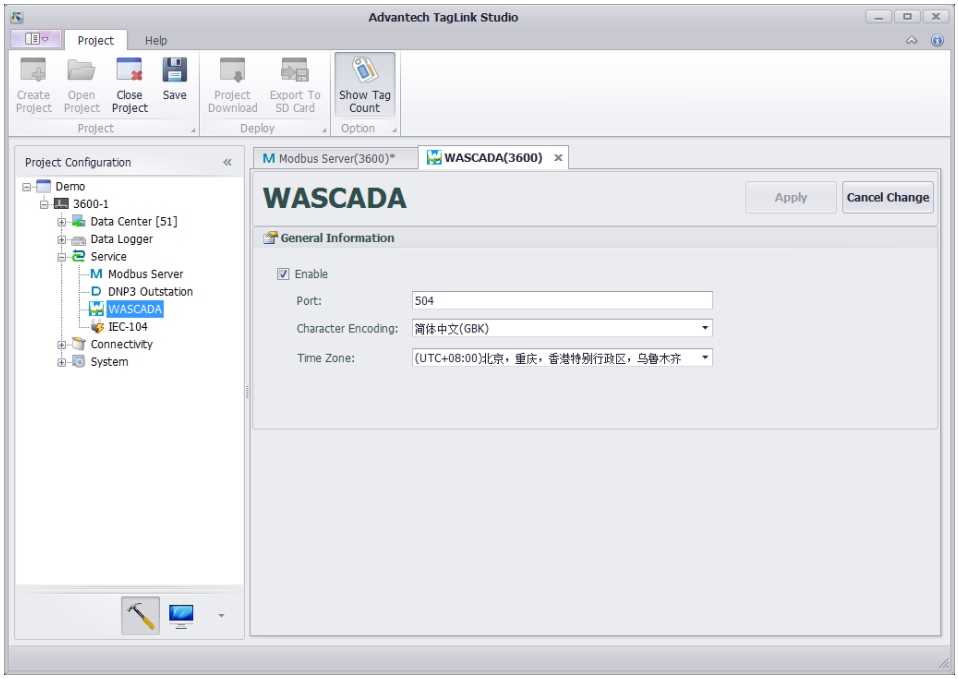
Basic Configuration of WASCADA

WASCADA service is enabled by default. Barring special circumstances, please do not disable it.

WASCADA has three configuration options:

1. Port: Set the port WASCADA listens on. The default setting is 504.
2. Character Encoding: Select the character encoding of WebAccess from the drop-down list. Please set it base on the real character encoding used by WebAccess, otherwise parse error may occur when it comes to a non-Chinese tag name. If WebAccess is the simplified Chinese version, please keep the default setting “Simplified Chinese (GBK)”.
3. Time Zone: Select the time zone for WebAccess server. Sometimes, the time zone of WebAccess server may be different from that of RTU devices. In

order to keep the consistency of data time stamp, please set the correct time zone here.



Add RTU Tag on WebAccess

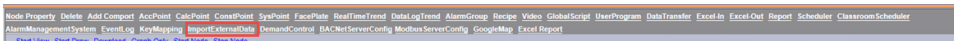
There are two ways to add a tag to WebAccess:

- Import a RTU project file;
- Add manually.

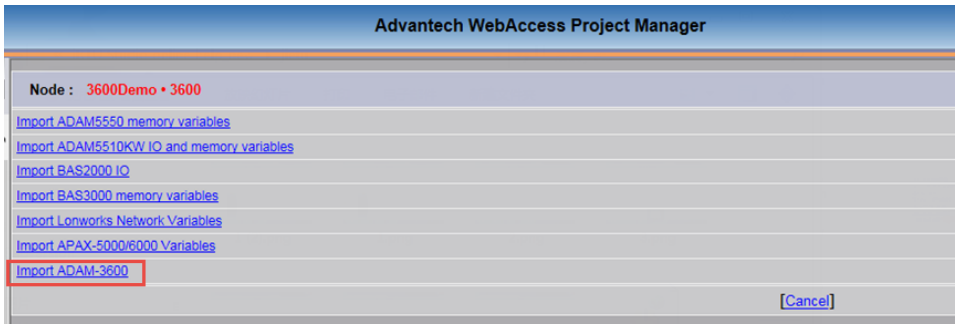
1. Import a RTU project

   Only the new version WebAccess offers the function of importing a RTU project . If your WebAccess does not support this function, please download the new version or install the function expansion package.

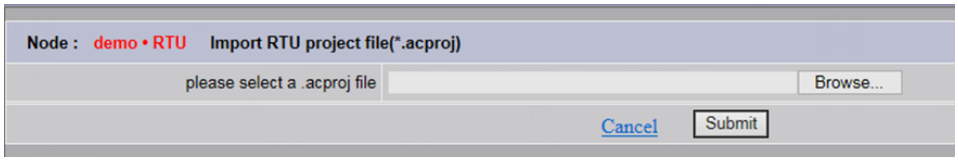
   1.1 Open Advantech WebAccess Project Manager. Then enter the SCADA node property page and click “ImportExternalData” as shown below.



1.2 If your WebAccess supports importing a RTU project file, the option of “Import EdgeLink” should be listed here. Click it to enter the import page.

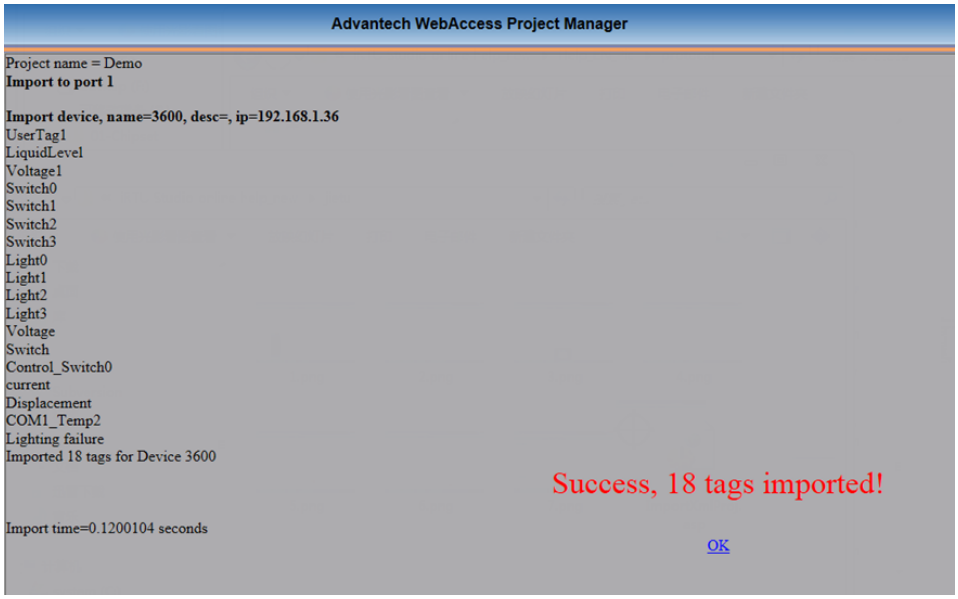


1.3 Click “Browse” button on this page to select a RTU project file with an extension of .acproj, then click “Submit” button as shown below.

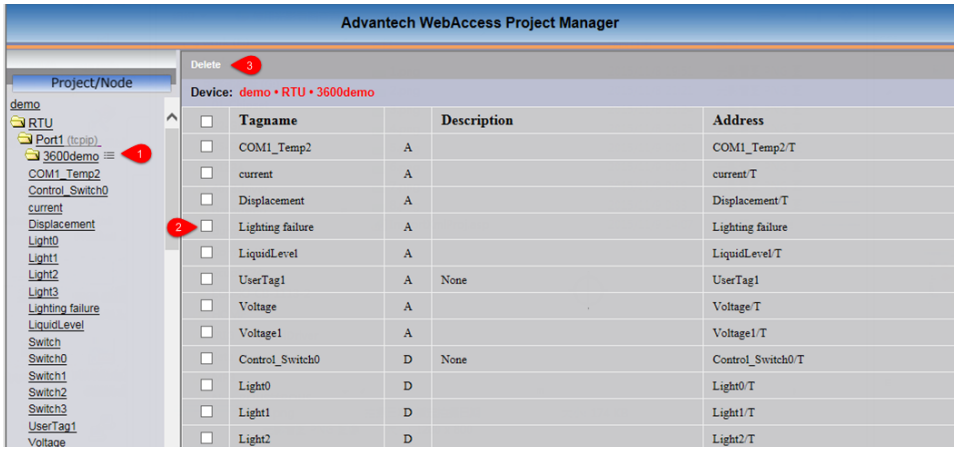


1.4 The page displays “File uploading, please wait…”, which means the selected project file with an extension of .acproj is being uploaded.

1.5 After the upload, the import will be automatically started. When the file has been imported, a window will pop up, showing the information of a successful import and the number of imported tags.



1.6 Delete the unnecessary tags. The import process imports all the tags, some of which are usually unnecessary since they may cause unwanted data traffic, so users need to delete these unuseful tags. Delete method: Please firstly locate the imported device node from the project node, then find the node list icon on its right. [1] Click the icon to open the tag list of the device; [2] Tick the tags to be deleted; [3] Click “Delete” button on the top left of the page to complete the delete operation.

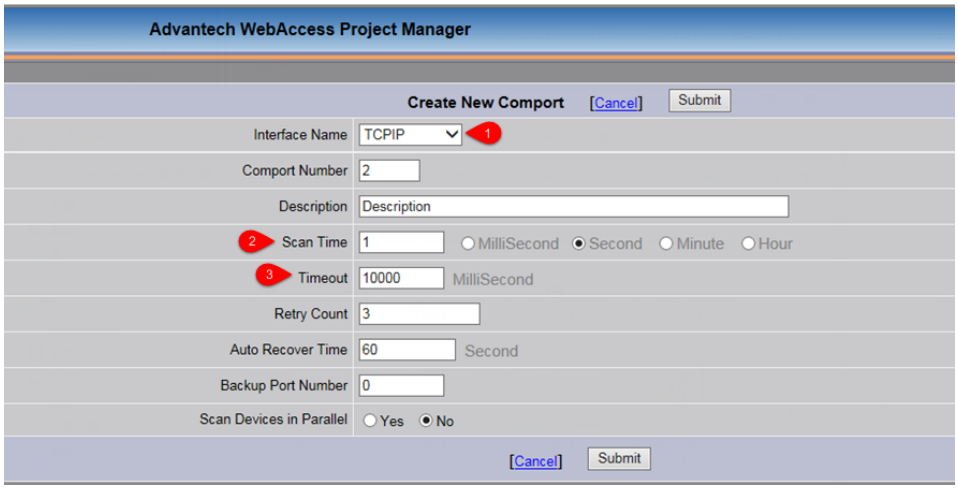


2. Add manually.

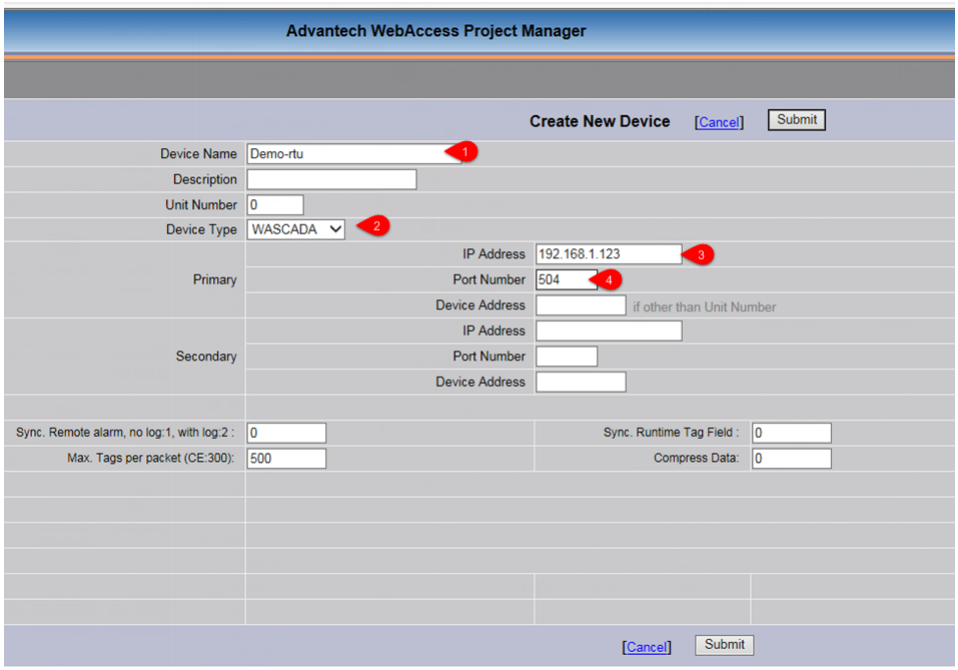
This method is only applicable to two circumstances: a. The installed WebAccess does not support the function of importing a RTU project file; b. Users want to adjust some parameters after the project file has been imported.

2.1 Create a new SCADA node (If users want to add a new device to the existing SCADA node, please ignore this step).

2.2 When users create a new comport on the newly-created SCADA node, the following three places should be noticed: [1] The interface name should be TCPIP; [2] Users should set the scan time based on real needs, and the time should not be too short. The default value of 1 second is not useful at most circumstances, so please reset it. [3] The timeout value is set to 1000 milliseconds by default, which is applicable to LAN communication. As for Internet or wireless cellular network communication which has a long transmission delay of link data, 1000 milliseconds is not appropriate any more. Users should modify it to 10000 milliseconds (10 seconds), so as to avoid connection failure due to bad network communication.



2.3 Create a new device for the new comport. The following options should be set: [1] The device name which should be the distinguished name of the RTU by WebAccess. If the RTU is connected with WebAccess through active connection (please refer to “Active Connection”), the device name here should be the same as the distinguished name of WhereIAm in active connection settings; [2] The device type should be set to “WASCADA”; [3] For IP Address, please fill in the real IP address of RTU. If the RTU is connected with WebAccess through active connection, please leave this box blank; [4] The port number is set to 504 by default. It should be consistent with the port number of WASCADA configured in RTU project. For the rest setting options, please leave them unchanged.

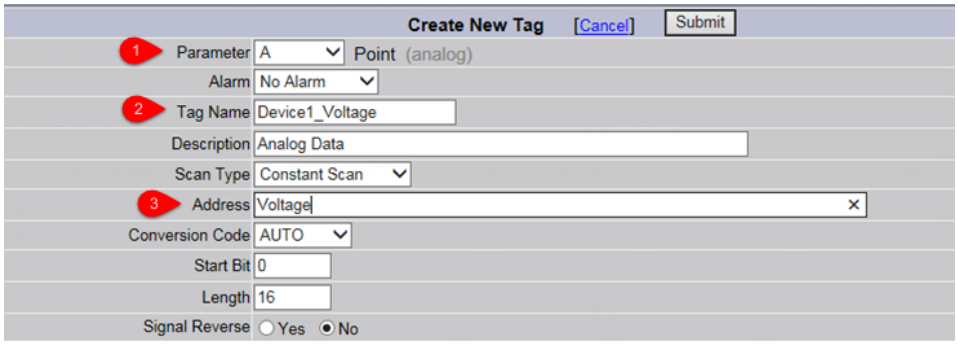


2.4 Create a new tag for the new device. [1] For “Parameter” option, “A” refers to analog tags on RTU; “B” refers to discrete tags on RTU; the tags of “Text” type are currently not supported; [2] The tag name should be the same as the tag name used in SCADA on RTU. This tag name is globally unique in SCADA node; [3] For “Address” option, users should input the tag name on RTU. If this tag is configured for periodic storage on RTU, “/T” can be added after the tag name (for example, “Voltage/T”), which means the function of resuming broken transmission is supported.

Description of resuming broken transmission: For tags with a “/T” suffix, if “Log Data” is configured to “Yes”, WebAccess will reconnect to read the stored data logged on the tag during disconnection to complete the local historical trend data record of SCADA. It should be noted that, the stored data

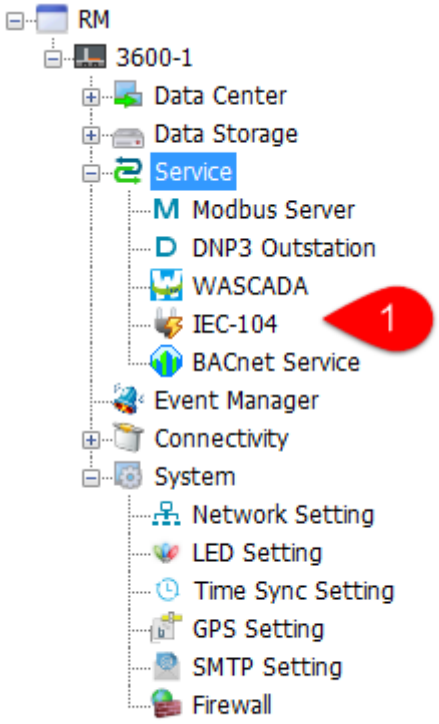
mentioned above could only include the data of minute, hour and day precision. In other words, when users want to view the data during disconnection and the time precision of the historical trend graph is as accurate as second for example, no data curve will be displayed in this graph.

For the configurations of other parameters, please refer to “WebAccess User Manual”.

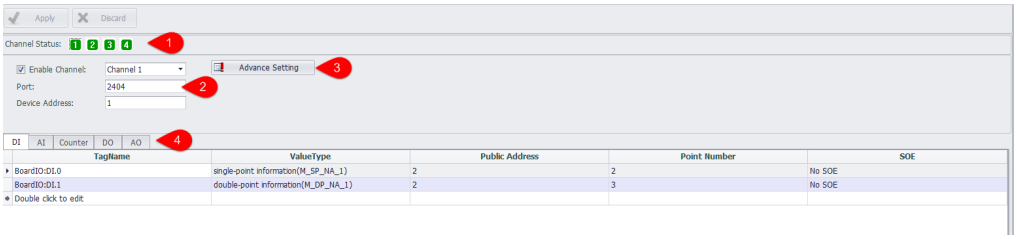


IEC-104 Server

Double click the IEC-104 in the protocol service to open the IEC104 server settings interface.



Main Interface



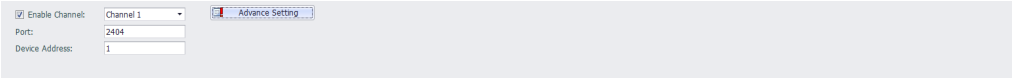
Users can configure up to 4 IEC-104 channels in EdgeLink. Each channel parameter needs to be configured independently.

1. The user can choose to enable or not enable the channel. The channel enabled in the channel state is

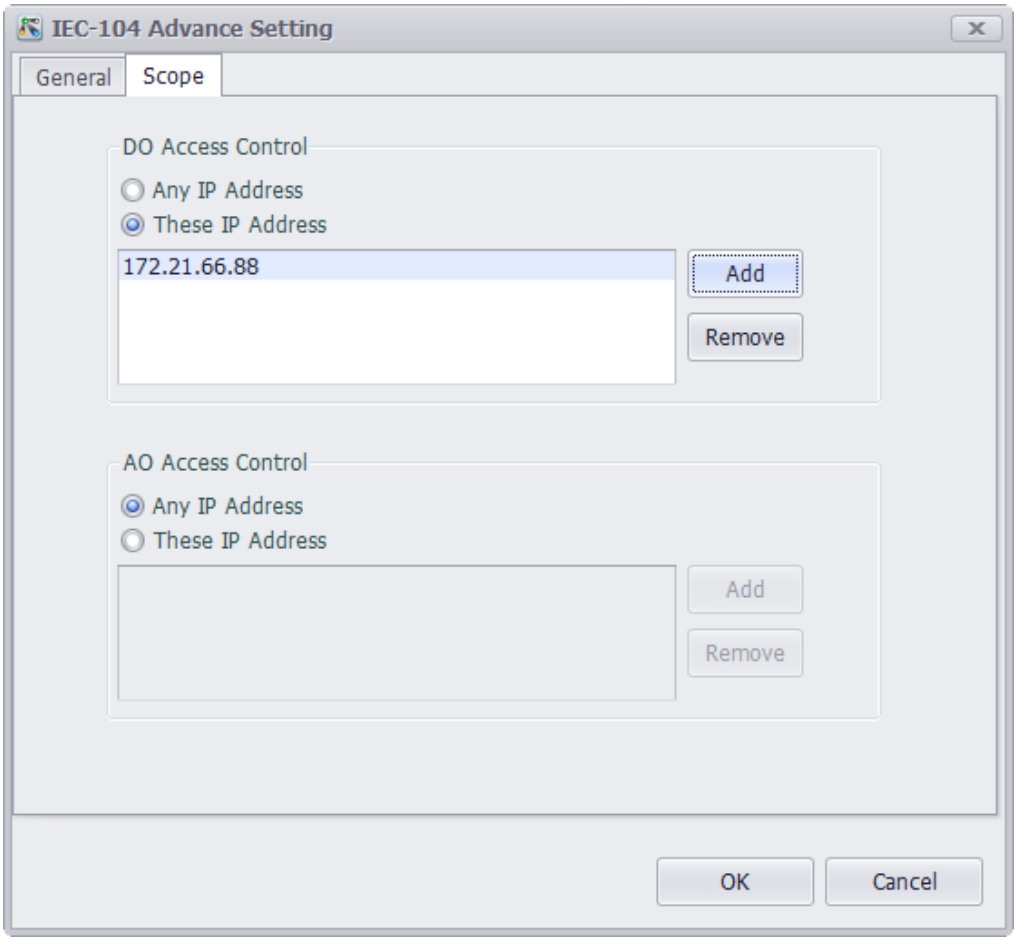
a green background and not enabled is a white background.

2. The channel parameters that need to be configured by the user are placed in the middle area of the interface.
3. At the bottom of the interface is the tag corresponding table, including DI, AI, Counter, DO, AO five types of data tags.

Channel parameter configuration

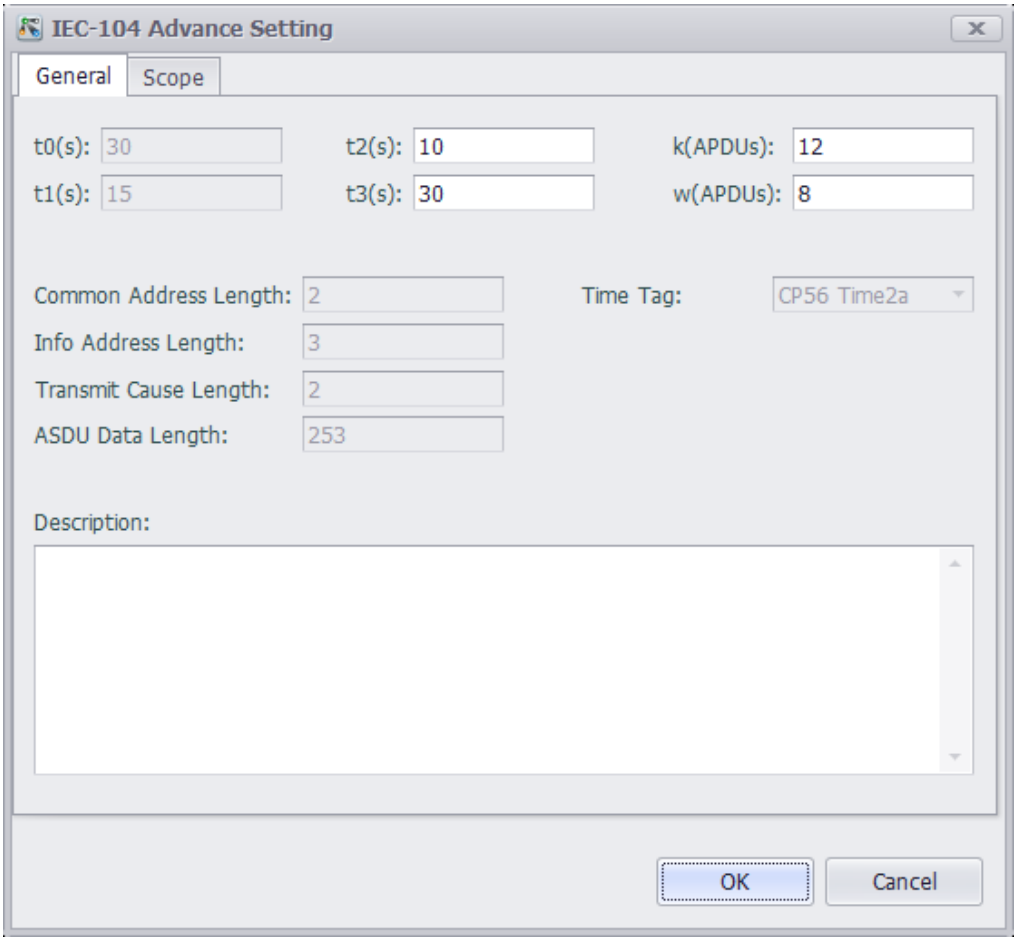


1. Enable channel: drop box can choose to switch channels, and can also choose whether to enable this channel.
2. Port:the default is 2404, and each channel needs to have a different port number.
3. Advanced parameters: set other properties of IEC-104.
4. Device address: defaults to 1, the public address in the data tag configuration should match the device address of the channel. When the device address changes, the public address in the data tag configuration is automatically updated.



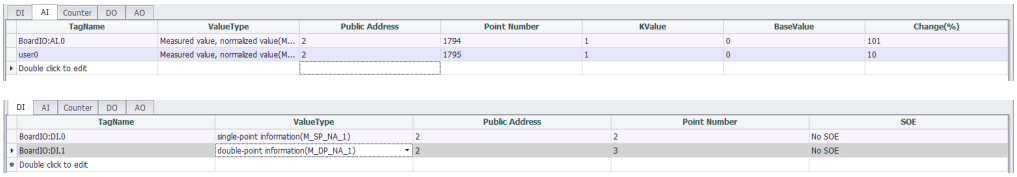
Users can set to allow only some IPs to modify the values of DO and AO in IEC-104.

1. When checking check box, do not limit the changes.
2. When unchecked, only allow IP in the list below to modify DO and AO value.
3. DO and AO values are not allowed to modify when the list below is empty.



1. t0: Timeout of connection establishment. (Not editable)
2. t1: Timeout of sending or testing APDU. (Not editable)
3. t2: A timeout that is confirmed when no data message is received, t2 <t1.
4. t3: Timeout of sending test frame in long idle state.
5. K: The maximum difference between the sending status variable and the received sequence number.
6. W: The acknowledgment is given after receiving the APD of the I-format.
7. Time stamp format: defaults to CP56 Time2a.(Not editable)

Data Tag Configuration



DI | AI | Counter | DO | AO

TagName	ValueType	Public Address	Point Number	KValue	BaseValue	Change(%)
BoardIO:AI.0	Measured value, normalized value(M...	2	1794	1	0	101
user0	Measured value, normalized value(M...	2	1795	1	0	10
Double click to edit						

DI | AI | Counter | DO | AO

TagName	ValueType	Public Address	Point Number	SOE
BoardIO:DI.0	single-point information(M_SP_NA_1)	2	2	No SOE
BoardIO:DI.1	double-point information(M_DP_NA_1)	2	3	No SOE
Double click to edit				

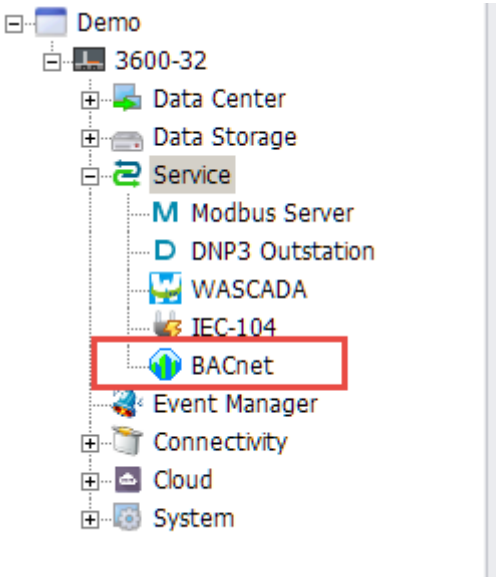
1. TagName: The name of the tag created in the Utility.
2. ValueType: The numeric type of the variable.
3. Public address: the public address to which the variable belongs should be filled with the same value as the device address.
4. Point Number: the corresponding variable number.
5. KValue, BaseValue: AI: engineering value = BaseValue + acquisition value * KValue, AO: export value = (engineering value - BaseValue) / KValue.
6. Change: this variable is greater than this percentage when uploaded to the server.
7. SOE: records the time at which the failure occurred and the type of event.

BACnet Server

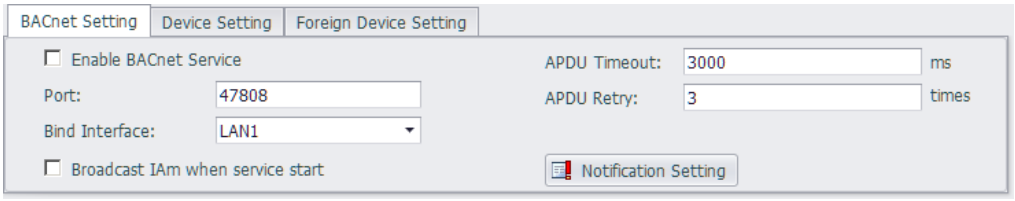
EdgeLink can work as BACnet Server to exchange data with BACnet Client of HMI/SCADA. Current version of BACnet server is designed to conform to BACnet Advanced Application Controller (B-AAC) level.

Here will explain the application of BACnet Server in detail.

1. Double-click “BACnet Server” under “Service” item in the left menu tree to pop up the configuration interface.

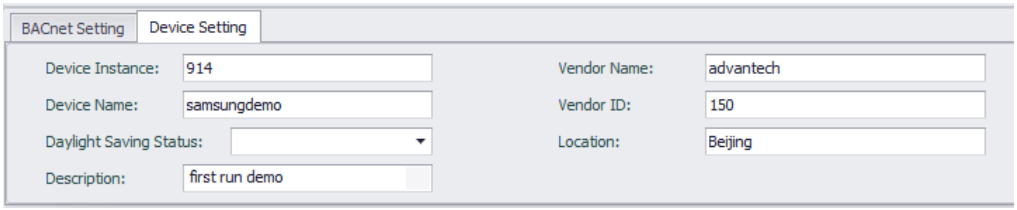


The main configuration interface of BACnet server is shown as below.



- BACnet Setting: To define the parameters of BACnet IP Server. Current version of BACnet server only supports TCP/IP network communication protocol by default.

```
Port: It is the port number of TCP/IP communication

Bind Interface: EdgeLink has 2 LAN Port, user should

Broadcast IAm when service start[Checkbox]: To confi

APDU Timeout: To define the timeout value of APDU re

APDU Retry: To define the retry times of APDU reques

APDU Segment Timeout: To define the timeout of APDU
```



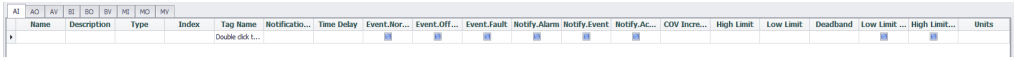
- Device Setting: To define the properties of this device object. Please make sure the device instance is the unique in one whole BACnet network.

```
Device Instance: As the property [Object_Identifier]

Device Name: As the property of [Object_Name] of thi
```

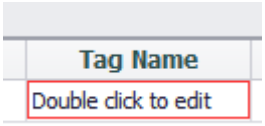
```
Daylight saving status: As the Property of [Daylight
Description: As the Property of [Description] of thi
Vendor Name: As the Property of [Vendor_Name] of thi
Vendor ID: As the Property of [Vendor_Identifier] of
Location: As the Property of [Location] of this devi
```

Next will describe the detailed settings of each object.

Note: Please keep the total number of BACnet Server Objects less than 3000 so as to ensure the operating efficiency of EdgeLink.

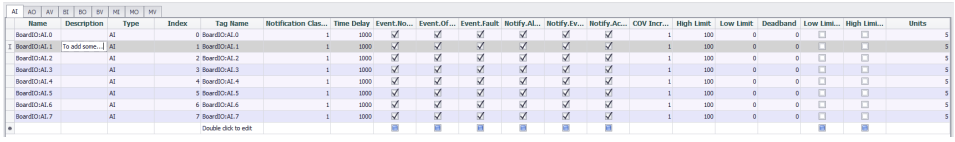


- Add new BACnet object

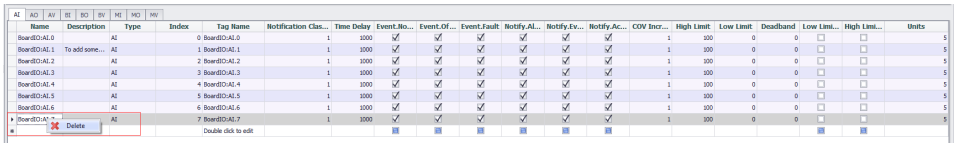
  User can add new BACnet object by [Double click to edit], then will mapping an EdgeLink Tag to this BACnet Object, and the system will auto create the object instance index for you, please keep the continuity of the index, and the system will start from index 0.

- Update BACnet obejct

  User can update and edit the existed BACnet obejct, some property should left click to edit, and some property should do double click to edit such as re-link a new EdgeLink Tag.

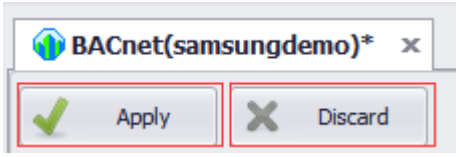
- Delete BACnet obejct



User can delete the existed BACnet obejct, select one or more lines and then right click to call [delete] popup menu out then to delete it.

Note: When appear the [*] in the title, please save or cancel your operation by the button on the left top.

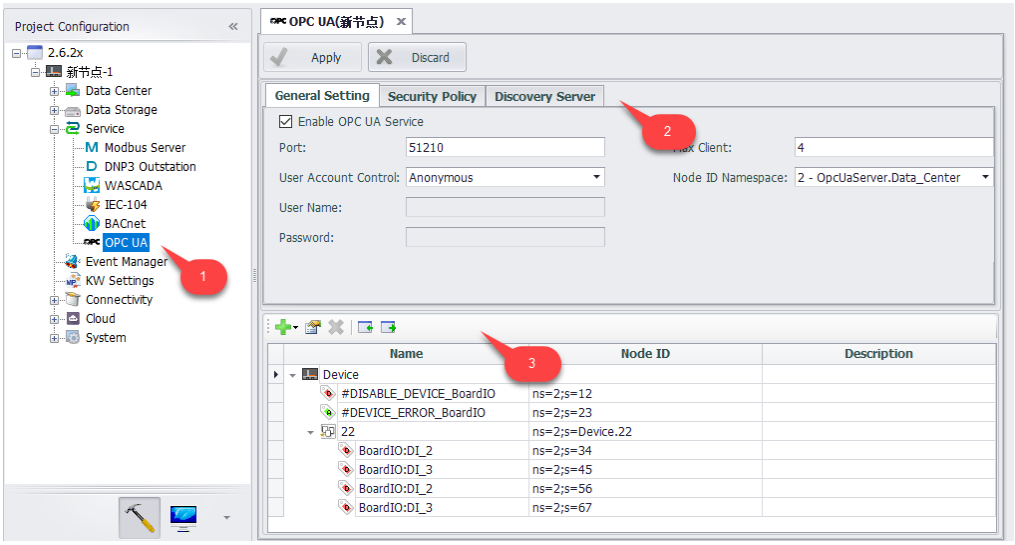
- Apply and discard your operation



OPC UA Server

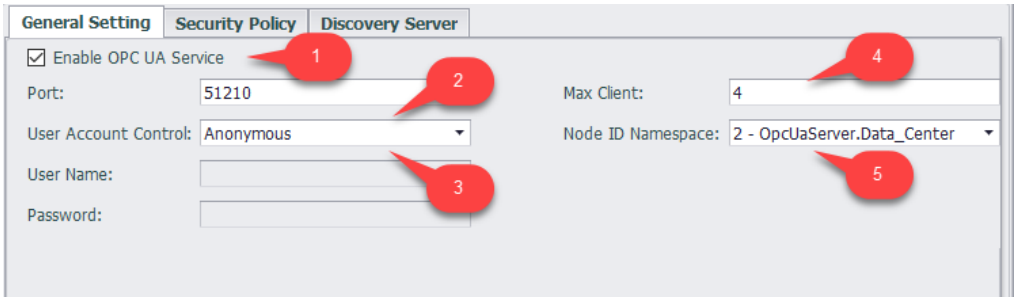
The OPC Unified Architecture is a standard defined by the OPC Foundation and is a modern industrial automation communication protocol. It is an open standard that traditional local applications, industrial Internet of Things, and industrial 4.0 applications and platforms are increasingly using for data collection and control. The EdgeLink Gateway Appliance as an OPC UA server can seamlessly connect to OPC UA Client applications running on any operating system.

Interface Settings



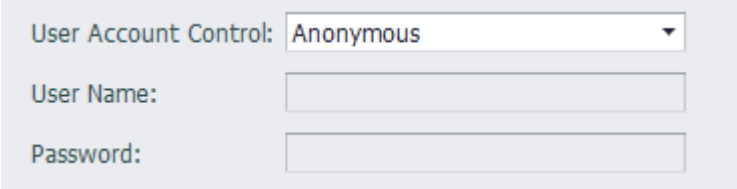
1. The user can click on the OPC UA node under the protocol service to enter the configuration interface.
2. The general settings and security policies of the OPC UA server on the device can be configured in the OPC UA configuration interface.
3. The configured tags in the device can be added to the OPC UA server.

General Settings

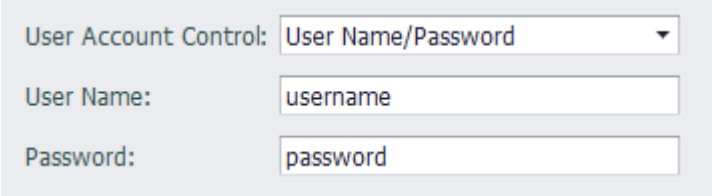


1. The user can choose to enable or disable the OPC UA service. The OPC UA configuration document is not generated when the service is not enabled.
2. Port: The port number of the OPC UA server on the device. The default is 4840.
3. User account control: The server allows the client to access the server anonymously or to verify the username and password when accessing.

   Anonymous: The default connection mode. The server allows the client to create a connection anonymously without the need to configure a username and password.

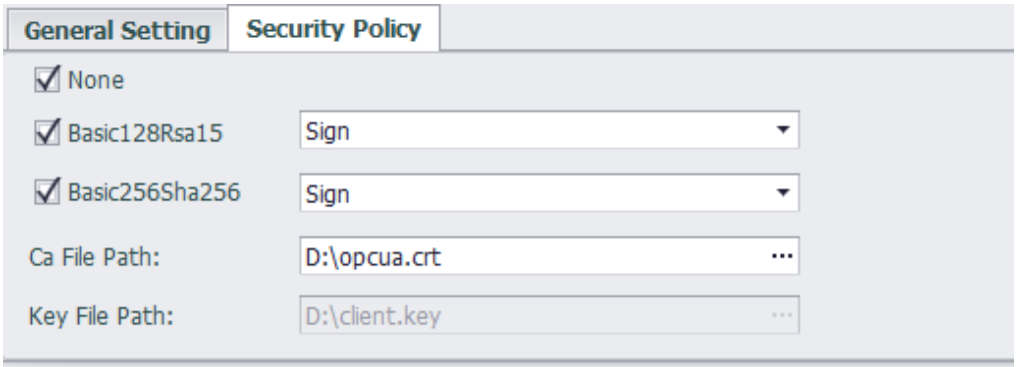


   User Name/Password: The client needs to configure the username and password when creating the connection. The username must be entered and the password can be empty.



4. Max Client：A maximum of several clients are allowed to connect to the server at the same time.
5. Node ID Namespace：Index of the node namespace
    0. OPC UA Namespace
    1. Local Server
    2. OpcUaServer.Data_Center

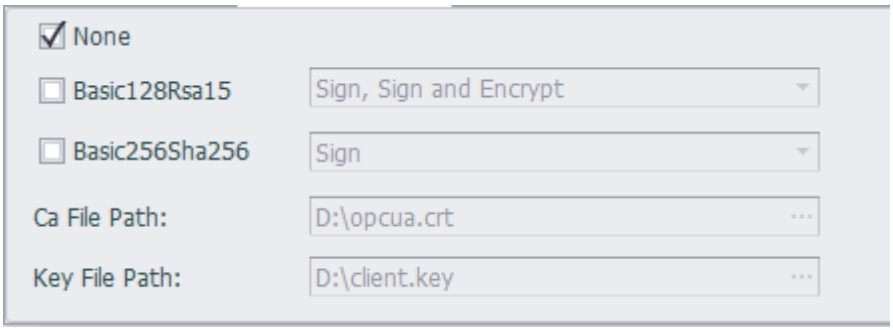
Security Policies



EdgeLink’s OPC UA server supports None/Basic128RSA15/Basic256Sha256 three security policies, which can be flexibly applied to different occasions.

After selecting Basic128RSA15 and Basic256Sha256, you need to select the message security mode for each of these two security policies. The message security mode has two types: “Sign”, “Sign and Encrypt”.

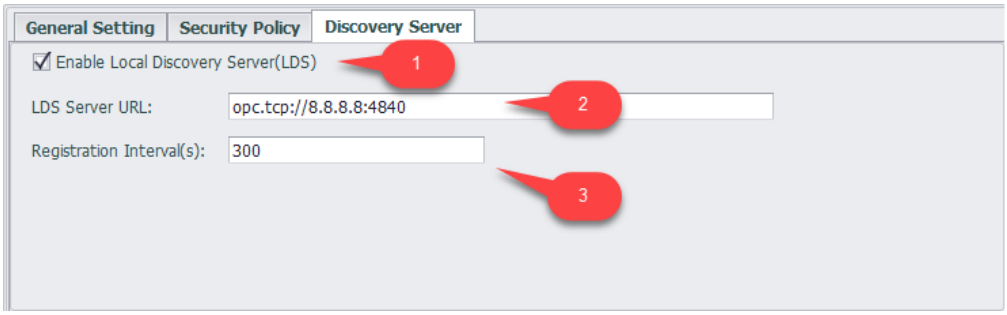
1. When only the message security mode is “Sign”, you need to select the CA file to download to the device.
2. When at least one security policy selects the message security mode as “Sign and Encrypt”, you need to select the CA file and the Key file to download to the device.



If neither Basic128RSA15 nor Basic256Sha256 is checked, the security policy is preset to “None”.

Local Discovery Server（LDS）

The Local Discovery Server (LDS) is a DiscoveryServer that maintains a list of all OPC UA Servers and Gateways available on the host/PC that it runs on, and is the OPC UA equivalent to the OPC Classic OPCENUM interface.



1. Enable LDS
2. LDS Server URL：The address of the LDS server
3. Registration Interval：The interval for registering the OPC UA server with the Local Discovery Server, in seconds.

HDA

First, save the data that needs to be read using historical data to the local data record, refer to DataLogger

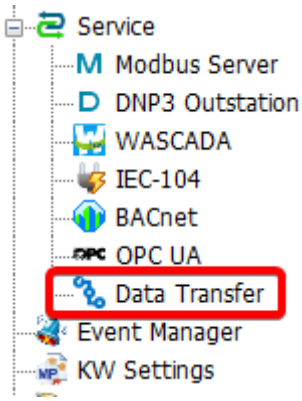
Then, add the corresponding data (tags) to the point table on OPCUA Server

Data Transfer

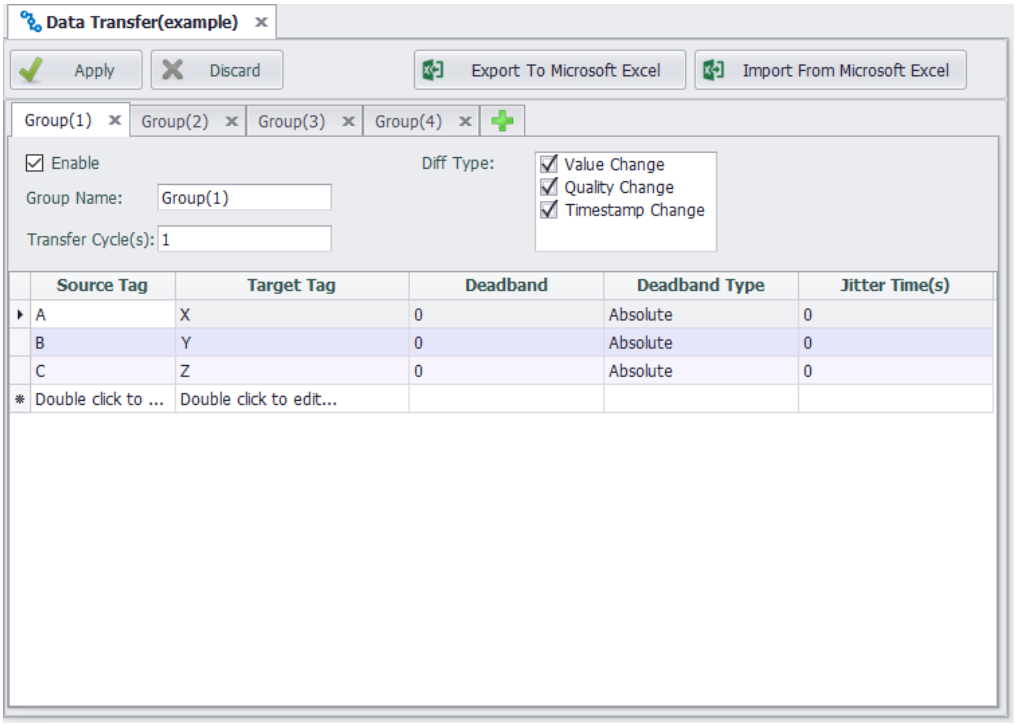
Data Transfer is used to write the value of a specified tag to another tag, according to the preset cycle and tag change detection criteria.

Configuration

1. The user can click the `Data Transfer` node under the protocol service to enter the configuration page.



2. The configuration page of `Data Transfer` is shown in the figure below. Up to 4 groups can be configured, and each group can have a different cycle and change detection configuration. If you have more points, you can use Export/Import Excel function to assist in editing.

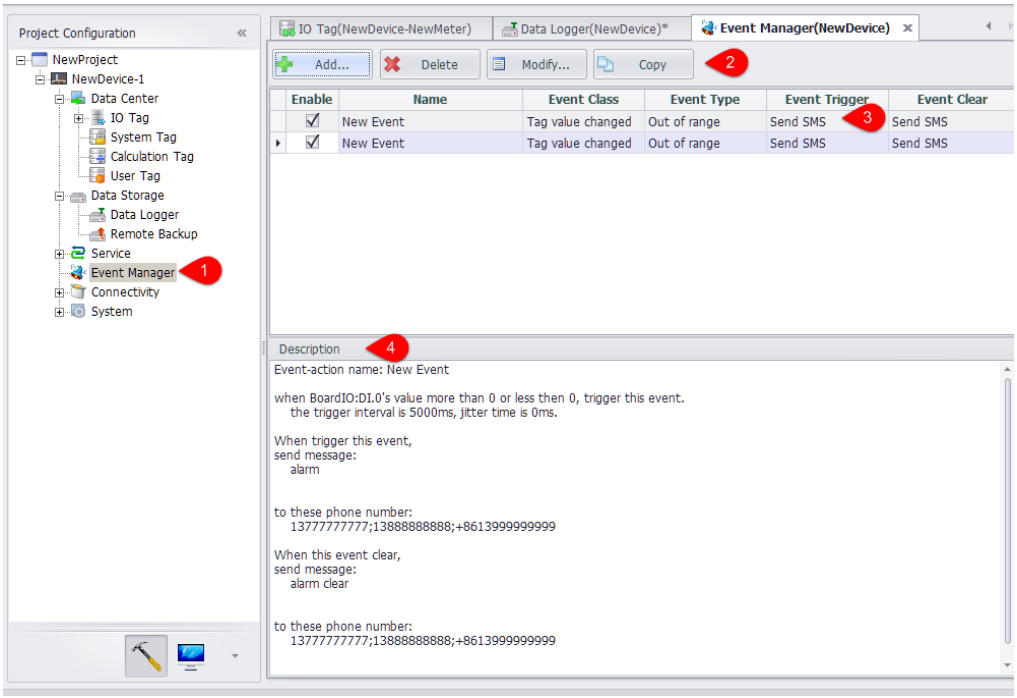


According to the configuration in the above figure, the `Data Transfer` program will transfer the tag values (A=>X, B=>Y, C=>Z) per second, or on detection of any change of the source tag's value, quality, and time stamp.

Event Management

Event management pages allow users to set trigger conditions for events. Trigger events when conditions are met; The event is removed when the state transitions from the satisfaction condition to the non-satisfying condition.

Event Management Page

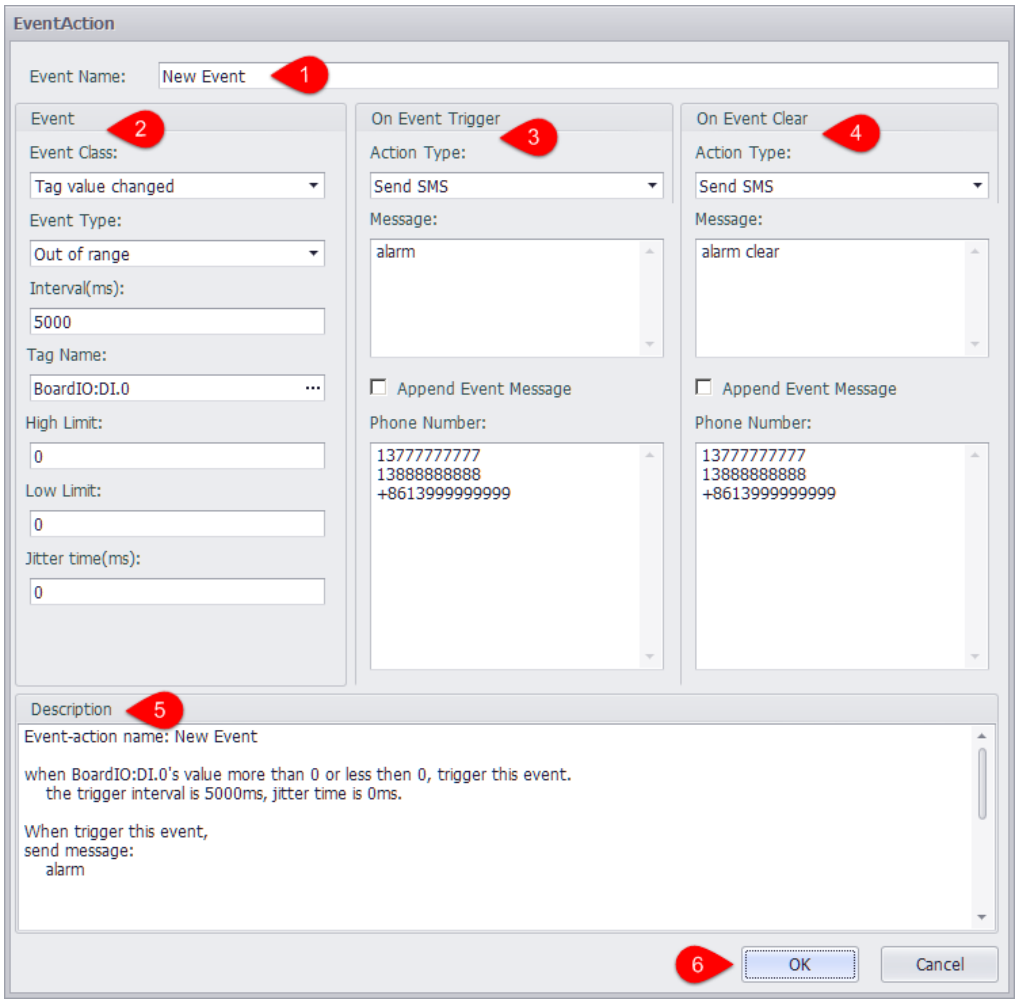


1. Double click the “event management” node to open the edit page.
2. You can add, delete, modify, or copy an event.
    - Add: pop-up the event edit page, create a new event
    - Delete: delete the selected events
    - Modify: pop-up the event edit page, modify the selected event

- Copy: copy the selected event and add it to the event list.

3. The time you have added will be displayed in the list.
4. You can set whether this event is enabled when the device is running by clicking the “Enable” column of the selection box.
5. When you select an event in the list, the description of the event will be displayed in the description box.
6. After setting up, you need to click the “apply” button to save the settings.

Event Edit Page



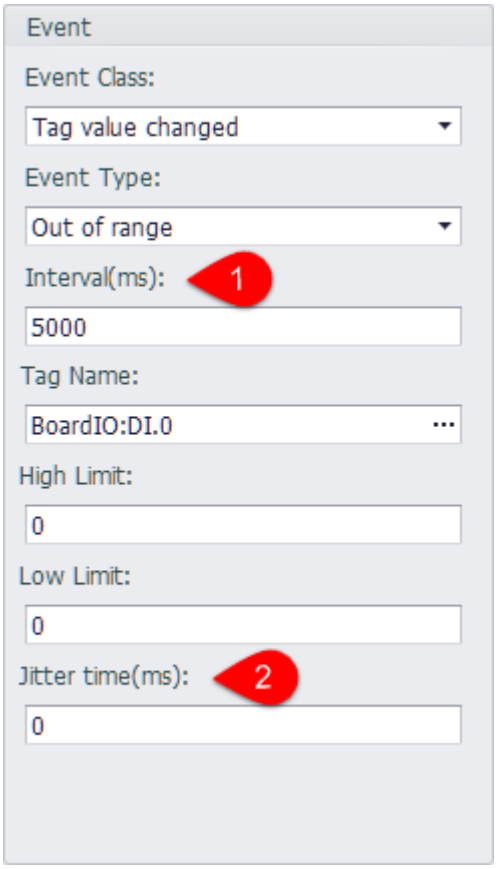
1. Edit event name.

2. The event parameters can be determined by selecting the event type and the specific time type.
3. Perform processing actions when an event is triggered.
4. You can also edit the actions that are performed when the event is lifted.
5. As with the event management page, the description of the event is refreshed in real-time in the description box.
6. When the settings are complete, click OK to save the settings.

Supported Events

Tag Value Change

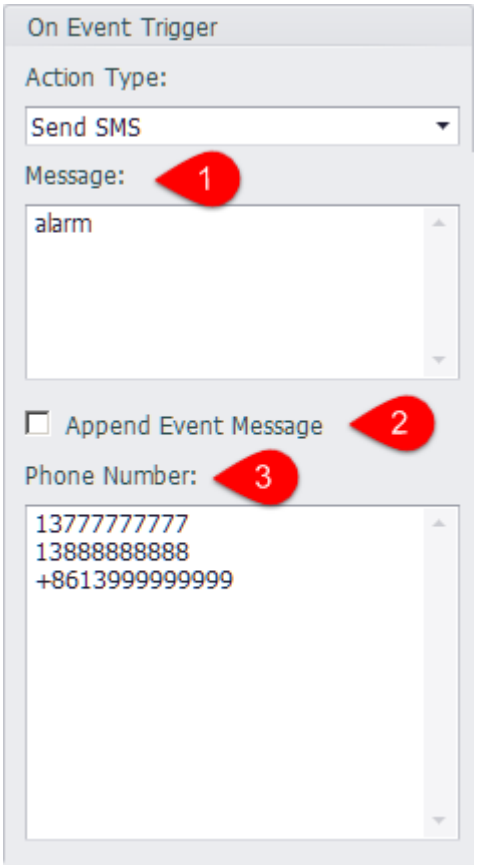
Currently support tag value change events. You can monitor the tag value out of range and tag quality is not good two cases.



1. Interval means that the same event is not triggered within an interval after an event has been triggered.
2. Jitter time means that the tag value exceeds the range or the quality is not good for the duration of time is less than the jitter time, then the event is not triggered.

Supported Actions

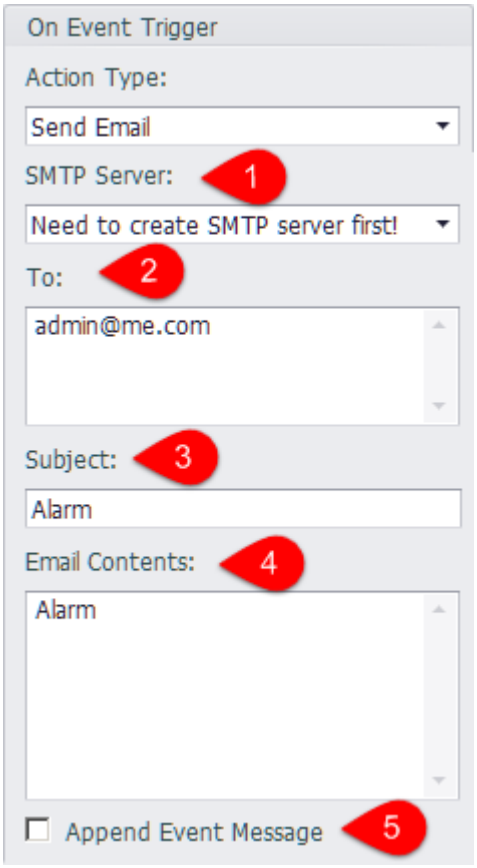
- Send messages: supports sending SMS messages to designated mobile phone numbers



1. Text messages to send to the phone.
2. The details of the event can be added at the end of the text message after

   Tag Name: #BATCH_WRITE_BoardIO
   Value: “current value”
   Quality: “current tag quality”
   Time Stamp: “timing of event”
3. After the event is triggered, the message will be sent to the number in this text box. If there are multiple numbers, it should be wrapped or separated by the ‘;’ semicolon.

- Send mail: supports sending an alert message to the specified mailbox via the SMTP server.

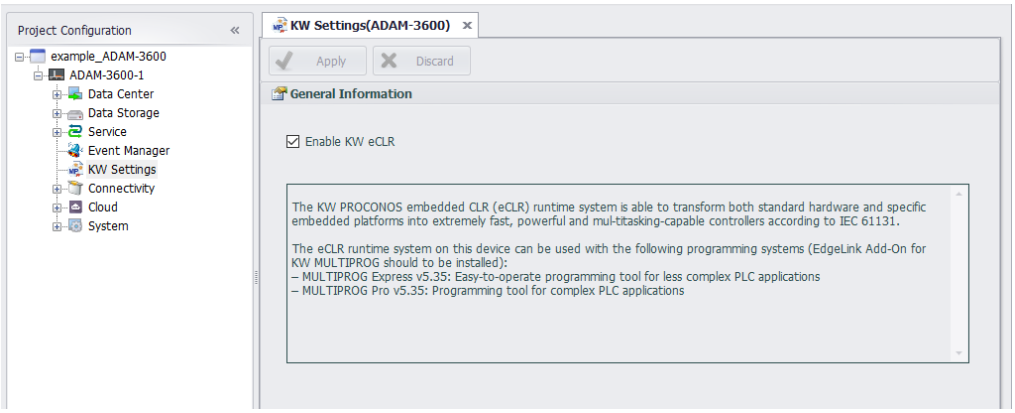


1. Select a configured SMTP server, if not configured, please refer to the SMTP server configuration section of this document.
2. Please enter the standard mail format for the recipients section. If there are multiple recipients, please enter or use ‘; ‘separation.
3. Topic of alarm email.
4. Contents of the alarm message to be sent.
5. The details of the event can be added at the end of the email:

   Tag Name: #BATCH_WRITE_BoardIO
   Value: “current value”
   Quality: “current tag quality”
   Time Stamp: “timing of event”

KW Settings

The KW PROCONOS embedded CLR (eCLR) runtime system is able to transform both standard hardware and specific embedded platforms into extremely fast, powerful and mul-titasking-capable controllers according to IEC 61131.



“KW Settings” allows the user to configure the start and stop of the KW function. When “Enable KW eCLR” is checked, eclr will be enabled when the device starts. If it is not checked, eclr will not be enabled.

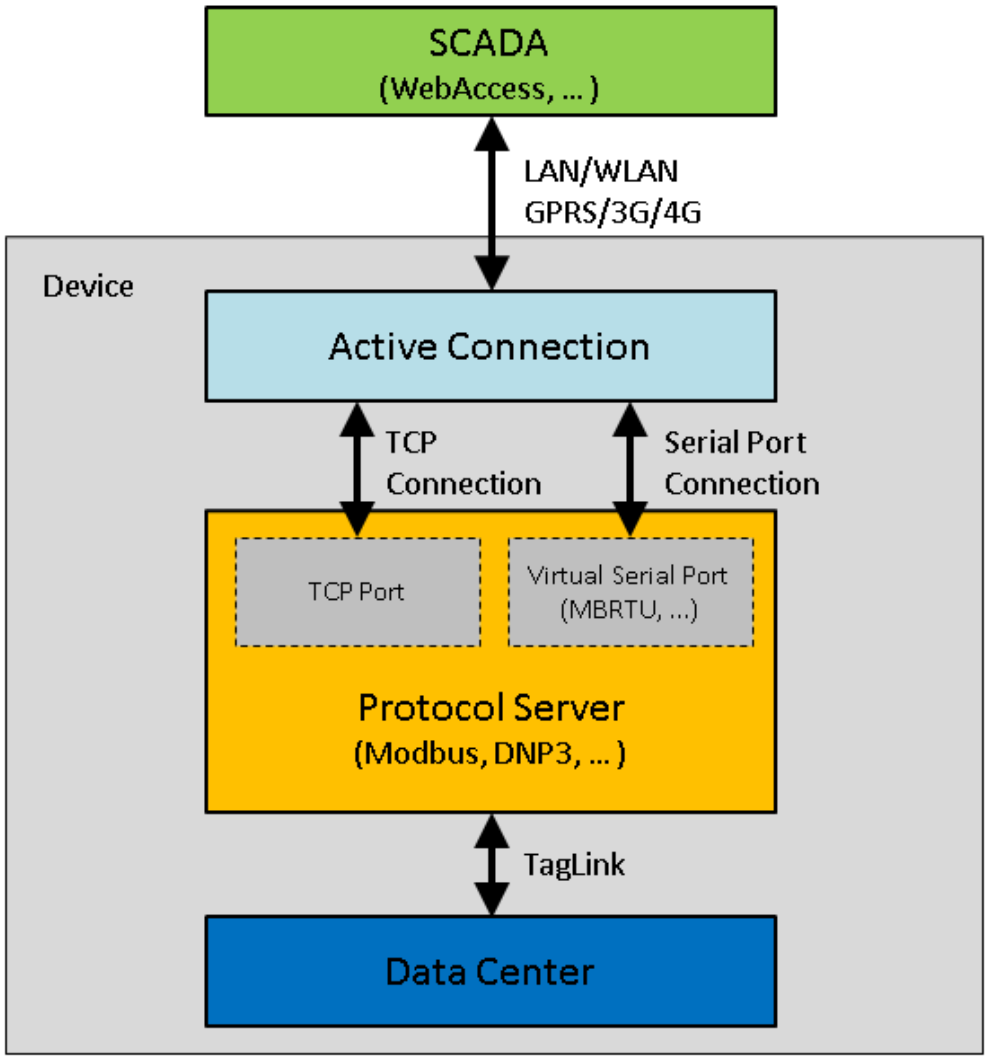
Connectivity Settings

The connectivity settings include the configuration of some additional external connection functions of EdgeLink, such as Active Connection, Serial Port Bridge, and third-party VPN connections.

Active Connection

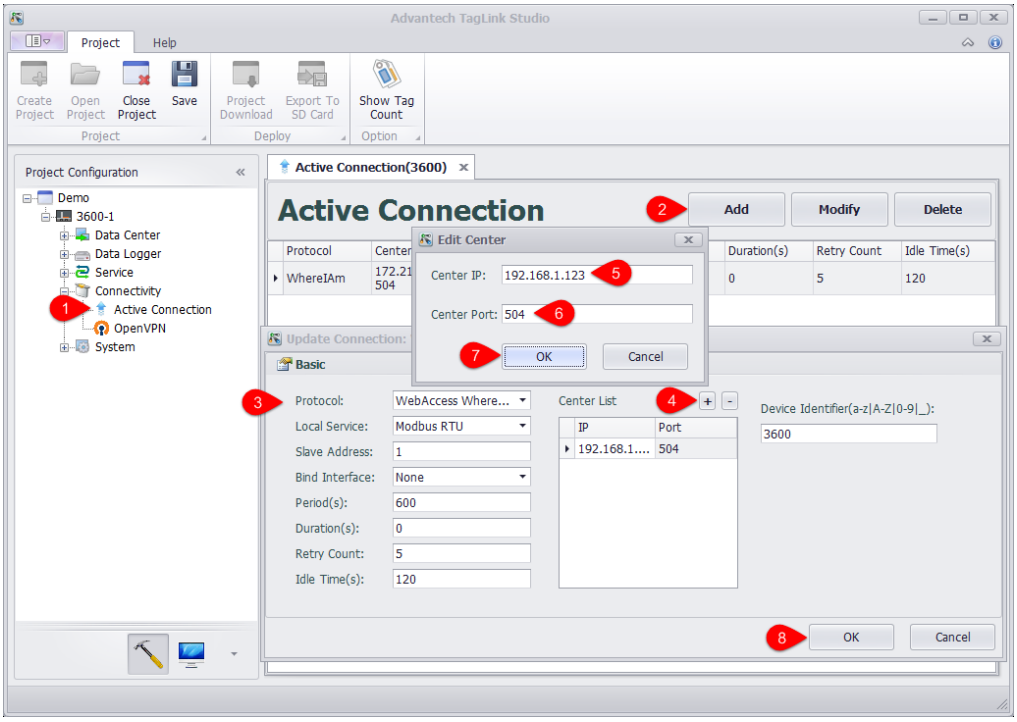
The main application scenario of active connection: RTU can directly access SCADA center, while the latter has no direct access to the former. RTU connected via cellular wireless connection or RTU behind the firewall is such kind of situation. In this case, the traditional TCP connection created by SCADA is not applicable any more. It should be the responsibility of RTU to actively connect with SCADA which will access data in future through this connection.

The fundamentals of active connection is illustrated in the below figure. In active connection, two connections will be established: one is the connection with a service of the device over TCP port or virtual serial port, which is called upward connection; the other is the connection with SCADA center, which is called downward connection. After the establishment, active connection will perform the data forwarding between two connections. Downward connection adopts the standard TCP connection, so it can support all protocols that listens on TCP port, including Modbus TCP, NDP3, etc; while upward connection supports two protocols: one is WhereIAm protocol, used to connect with WebAccess; the other is DTU protocol of FourFaith, used to realize the connection with the server which supports four faith DTU. More upward connection protocols will be added in future.



Active Connection Settings

In active connection page, the items that should be configured include upward connection protocol, downward connection service, center list of upward connection as well as some related parameters. Please follow the below steps to add an active connection:



1. Locate “Active Connection” in “Connectivity” in the left tree menu, and then double-click it to open the configuration page.
2. Click “Add” button to add an active connection
3. Set the related parameters of active connection, including:
    - Protocol: Select the upward connection protocol from the drop-down list. “WebAccess WhereIAm” is used to connect with WebAccess server, while “DTU - Four Faith PROT” is used to connect with four faith DTU server. Different protocol requires users to set different parameters in the lower right corner of the page. For WhereIAm protocol, users only need to set one parameter: “Device Identifier” which should be consistent with the device name in WebAccess project so as to make sure

WebAccess can correctly identify every connected device.

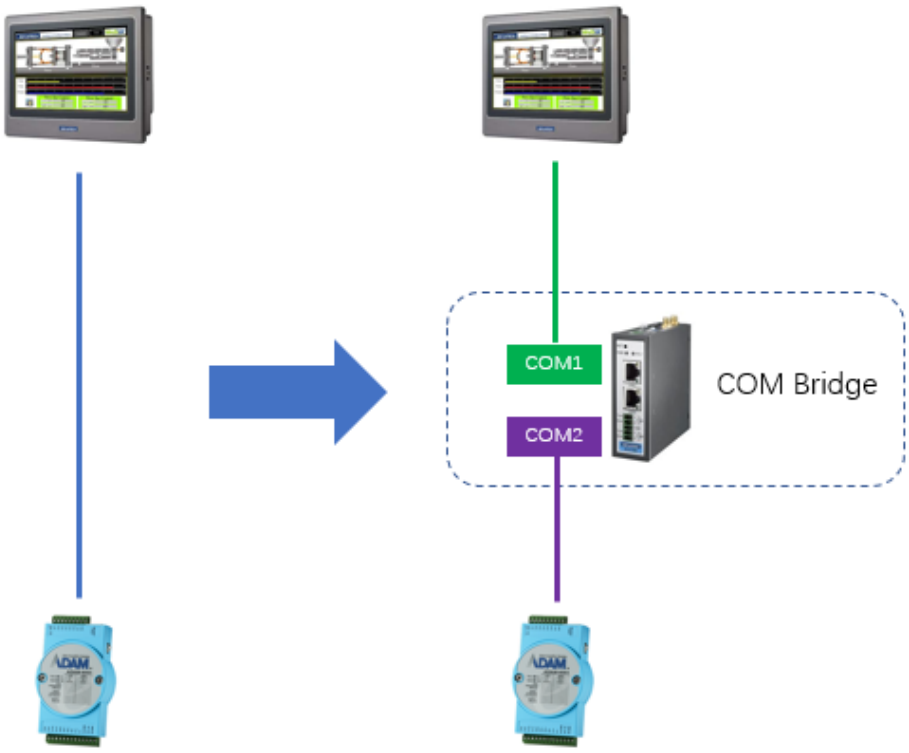
- Local Service: Select the downward connection service from the drop-down list. “Modbus RTU” means to connect with Modubus RTU through the virtual serial port, while other options realize the connection through TCP connection.
- Salve Address: This item is only available when “Local Service” is set to “Modbus RTU”. It specifies the slave address of Modbus RTU.
- Bind Interface: Specify the communication port of active connection. “None” means no port is binded. This parameter is typically used when a device has multiple network connections, the data channel of active connection should be explicitly specified to avoid the uncertainties of the system default route. For example, if “Cellular” option is selected, only cellular wireless network can be applied to data transmission.
- Period (s): Set the time interval for active connection to establish a second upward connection.
- Duration (s): Set the time duration before the upward connection is disconnected. “0” means the connection will never be actively disconnected after it is established.

- Retry Count: Set the retry times after an upward connection is failed. If the count is exceeded, active connection will never try to reconnect again until the next period comes.
- Idle Time (s): After an upward connection is established, if there is no data transmission within the specified idle time, active connection will disconnect and try to reconnect. “0” means no idle time is set.

4. Click “+” button to add center IP and center port of the upward connection.
5. Enter a center IP, which can be either an IP address or a domain name address.
6. Enter a center port. If WebAccess is used, this item is usually set to 504 by default.
7. Click “OK” button to add the center information to “Center List”. Repeat steps 4~7 to add more centers. Each active connection can support at most 5 centers.
8. Click “OK” button to add this new connection to active connection list.

Serial Port Bridge

Serial Port Bridge is mainly used to add a gateway for data acquisition while retaining the existing serial port connection logic. As shown in the figure below, a gateway is added between the HMI and the end device, by bridging the serial ports in the gateway, the original HMI data acquisition is not affected, and the gateway can also read data from the end device..



Principle

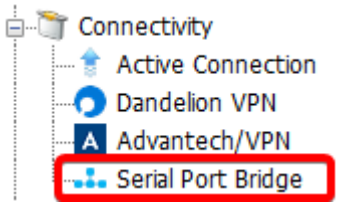
The serial port bridge program will open two serial ports, one is the slave port connected with the upper master station, and the other is the master port connected with the lower-level end device. When the serial port bridge

program receives a request from the upper master station from the slave station port, it will forward the data message to the master station port, accept the response data of the end device, and return it from the slave station port to the upper master station.

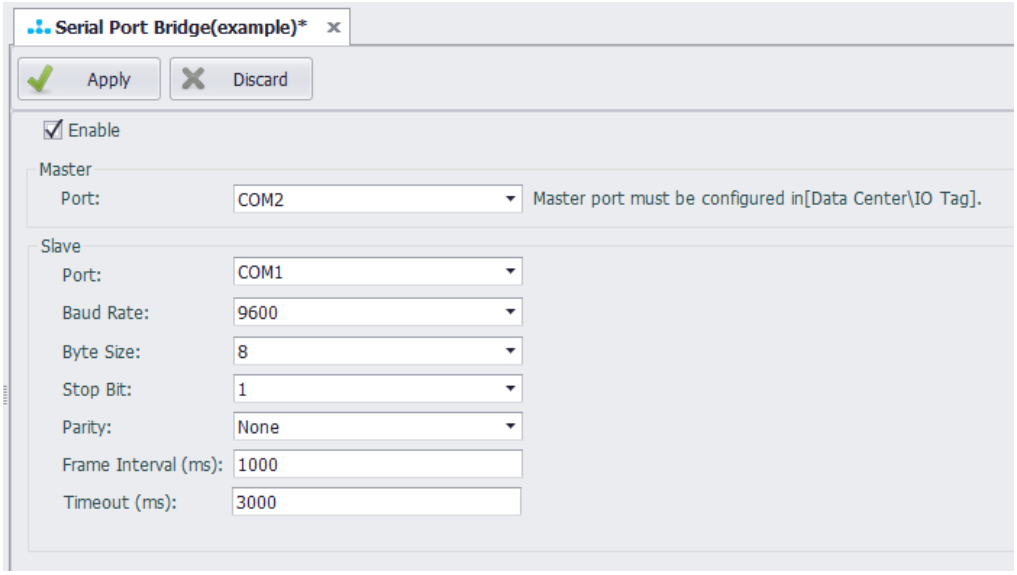
Because the serial port is an exclusive resource, in order to realize that the data center of the gateway and the upper master station can collect data from a lower-level collected device at the same time, the serial port bridge program needs to share the same master port with the data center, using time-sharing multiplexing. Because the master station port is used in time-sharing, the scan time of the data center and the upper master station should be coordinated when using the serial port bridge program, otherwise the data acquisition result will be affected.

Settings

The serial port bridge function is located in the connection settings of the project configuration tree, as shown in the following figure:



Double-click the serial port bridge setting item in the project configuration tree to open the serial port bridge configuration page, and click “Enable” to configure the serial port bridge.



Parameters:

- **Master - Port**: select a serial port that has been configured in the data center for acquisition.
- **Slave - Port**: select a serial port that has not been added to the data center and is not occupied by other applications to be used as a slave port.
- **Baud Rate/Byte Size/Stop Bit/Parity**: set according to the actual connection with the upper master station.
- **Frame interval (ms)**: specify the minimum interval for data requests from the upper master station, in milliseconds. The serial port bridge program will split the complete data message received from the slave station port according to this setting parameter.
- **Timeout (ms)**: specify the timeout time of waiting for response from the end device, the unit is milliseconds. After the serial port bridge program forwards the message, if the waiting time for a response exceeds this set parameter, it is considered

that the end device has no response. At this time, the serial port bridge program will release the occupation of the master port so that the data center can continue to do data acquisition.

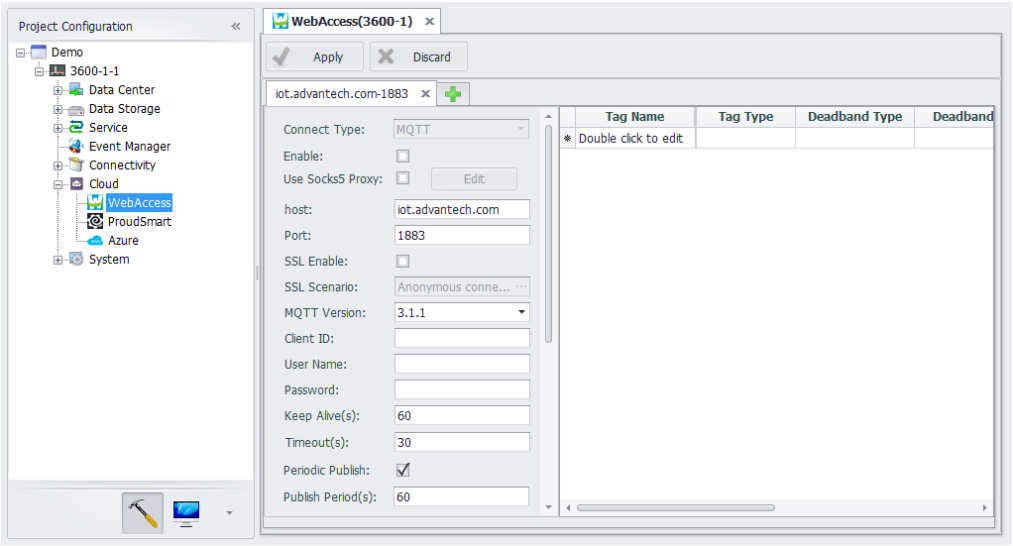
Cloud Service

EdgeLink can communicate with the IoT center device on the cloud via the MQTT protocol. Currently, EdgeLink supports communication with IoT center of Baidu cloud, Azure and other cloud service providers.

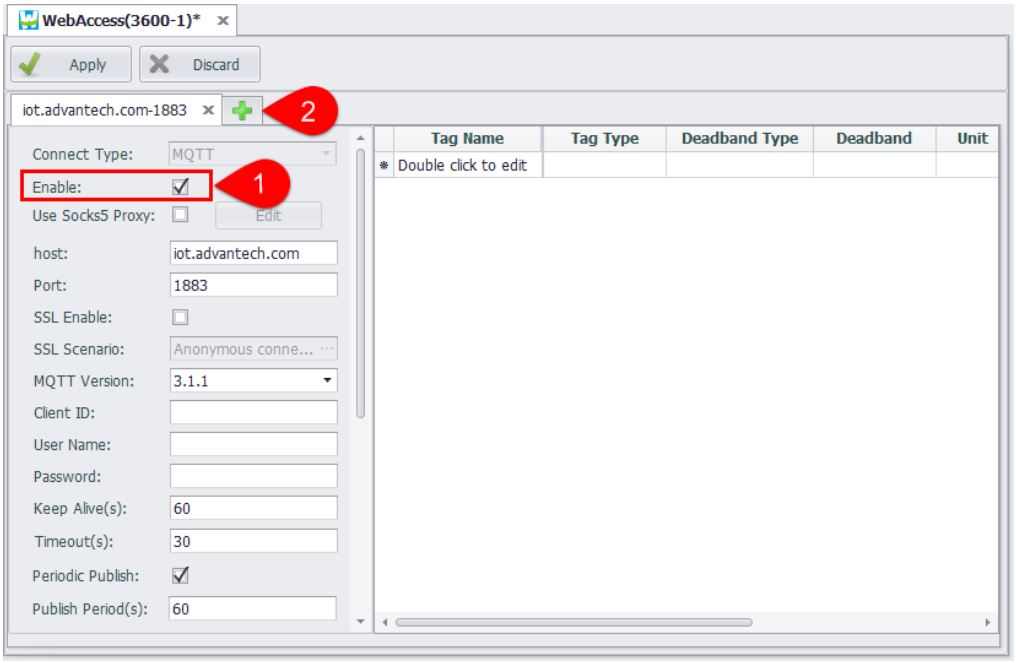
In EdgeLink Studio, users can configure devices on the cloud service page to upload device tag information to the IoT Center, and support uploading to multiple different types of IoT centers.

Users need to configure IoT center connection properties and upload conditions, receive service attributes, tags to be uploaded and other information.

According to different connection types, EdgeLink supports multiple cloud services, which configure corresponding connection information respectively.



Basic Configuration



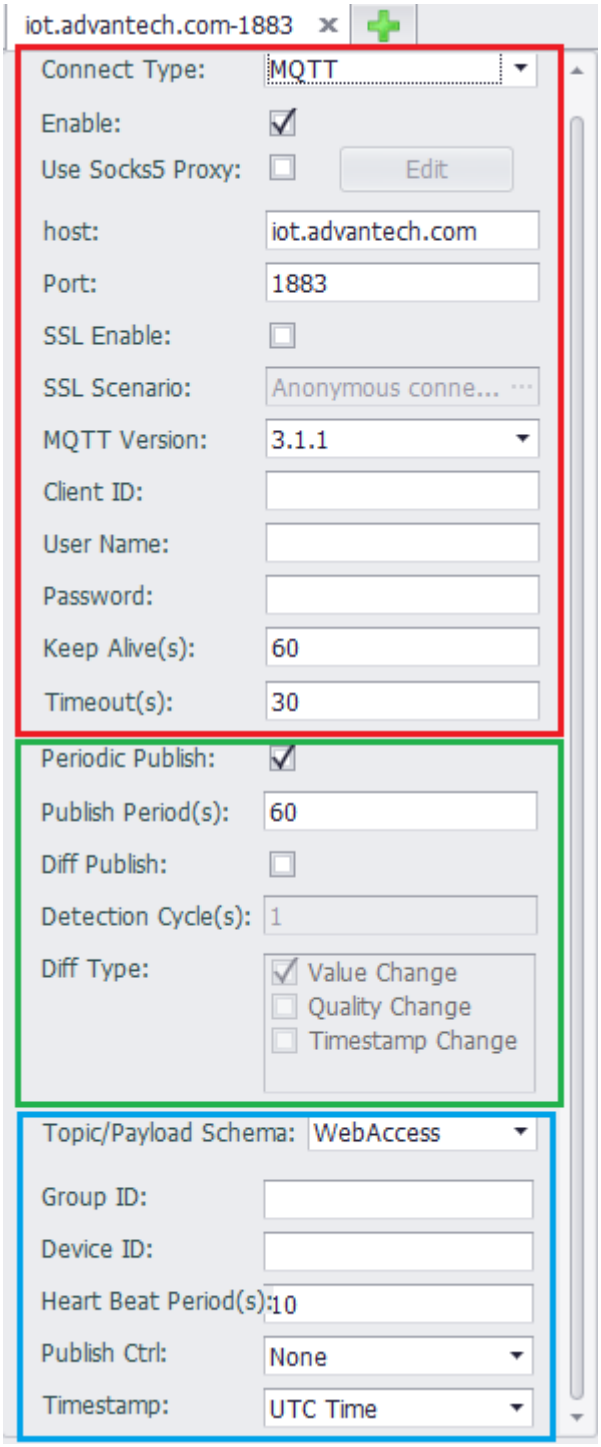
1. For the configuration to take effect, users must check “**Enable**“. This switch can be used reasonably during the debugging phase to test multiple connections added in the same cloud service type.
2. Click the “+” button on the right of the main page to add multiple connections to the cloud service. Each cloud service type allows up to 4 connections to be added.

Cloud Connection Properties and Upload Conditions

EdgeLink uses the standard MQTT protocol specification to connect to cloud services, so most cloud service types have the same configuration interface in the MQTT connection settings section. The Azure IoT Hub is an exception. Because Microsoft uses connection string configuration to provide user login credentials, the Azure

IoT Hub connection configuration will be different. See the Azure IoT Hub configuration page for details.

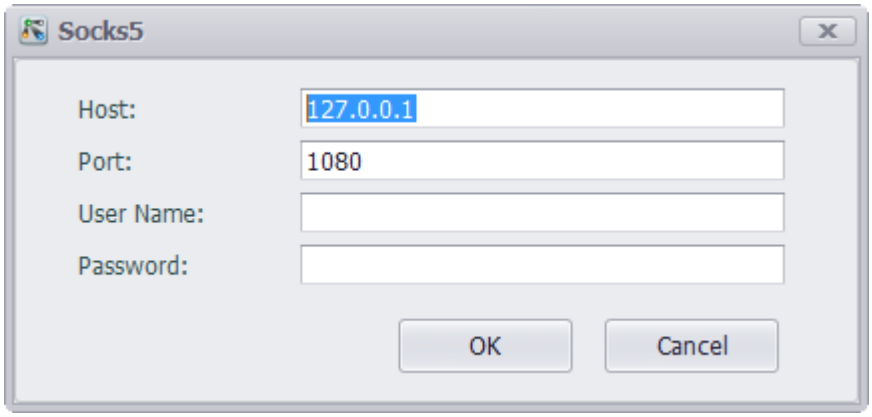
As shown in the following figure, the MQTT configuration interface, the red frame is the configuration information connected to the broker, the green frame is the configuration information of the data upload, and the blue frame is the configuration information specific to each cloud service type. This section will be described in detail on the description page for each cloud service type.



Connection Configuration Section

- **Use Socks5 Proxy** - If the device is used in a network environment that requires a proxy server to connect to the MQTT Broker, then the SOCKS5 proxy needs to be enabled. Click the Enable check

box and then click the “Edit” button to set the SOCKS server information in the pop-up box. As shown below, you can set the IP address, port number, user name and password of the SOCKS5 proxy server.

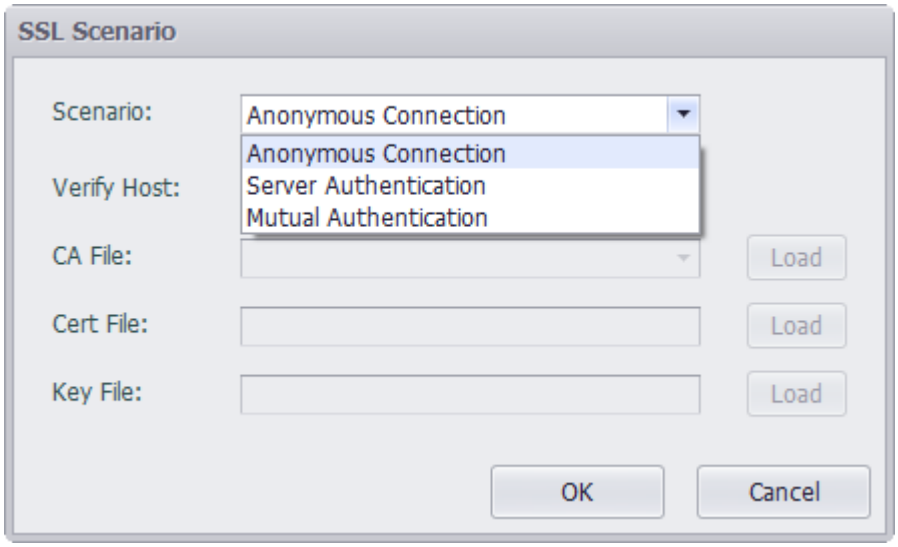


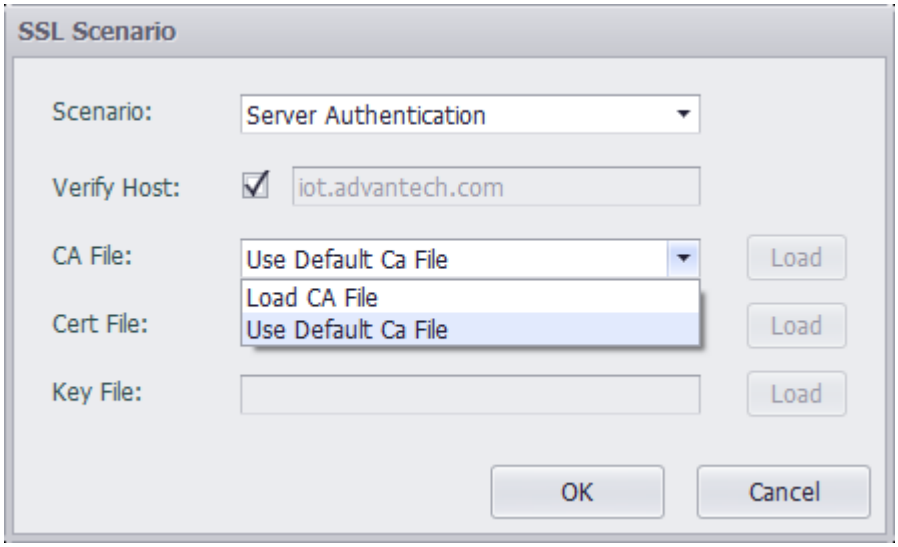
- **Host** - The IP or domain name of entering the MQTT Broker.
- **Port** - Enter the listener port number of the MQTT Broker. By default, the unencrypted TCP port is 1883 and the encrypted TLS port is 8883. EdgeLink does not currently support WebSocket connections.
- **SSL Enable** - If the Broker requires an SSL/TLS connection, then SSL needs to be enabled and selected from three authentication methods depending on the configuration provided by the Broker:

    1. Anonymous connection: Only encrypted connections are provided, and the communicating parties do not verify the identity.
    2. Server authentication: The device side verifies the authenticity of the cloud server, and the cloud

server is required to provide the CA file. EdgeLink comes with some public server certificate files. If you are connected to a public cloud, you can try to use the default CA file. If you use a self-signed certificate for your own server, you will not be able to authenticate with a third-party certificate authority. In this case, in addition to loading the CA file to the device, you need to cancel the verification host name, otherwise the connection will not succeed. set up.

3. Mutual authentication: The difference from the server-side authentication is that in this case, the cloud server needs to verify the identity of the device. In this case, in addition to processing the CA file of the server, the certificate file and the key file of the device need to be loaded. When the cloud server is connected, the device side will authenticate with the cloud server side.





- **MQTT Version** - Specify the version of the MQTT specification that the communication parties follow. Generally, the default version 3.1.1 can be used. If the Broker has special requirements, it can be configured according to its requirements.
- **Client ID** - Client ID is used by the Broker to distinguish multiple clients connected to it. Please enter a unique client ID here. If the Broker supports it, you can leave it blank for automatic distribution by the Broker.
- **User Name** - The username used to connect to the Broker, please follow the instructions of the Broker. If you are configuring a connection to WISE-PaaS, you can leave it blank here. The WISE-PaaS protocol plugin will get the corresponding username and password through the DCCS API.
- **Password** - The password used to connect to the Broker.

- **Keep Alive** - The unit is seconds. According to the MQTT protocol, when there is no communication between the device and the Broker within a certain period of time, the MQTT PING message must be sent to the Broker to maintain the connection. The setting of this parameter should be determined according to the actual project needs and combined with the configuration of the Broker.
- **Timeout**. The unit is in seconds. Define the maximum time interval for the client to send information to the cloud.

Data Upload Configuration Section

There are two modes of data uploading. One is regular upload, that is, to report all the tag instant data in the tag list on the right side at a fixed time interval; the other is change upload. In this mode, the program checks the change of the tag with the configured detection period and detection condition, and uploads the real-time data of the changed tag when the tag change is detected.

Both the regular upload and change upload modes can be enabled at the same time, or only one of them can be enabled. The recommended configuration method is to enable regular upload and change upload at the same time. The detection period of the change upload is set to a shorter time, and the period of the periodic upload is set longer, so that the data can be considered in real time and effective, and reduce bandwidth usage.

- **Periodic Upload**: The enable switch of periodic upload.
- **Publish Period**: Select the upload cycle for data during periodic uploads.
- **Diff Upload**: The enable switch of change upload.
- **Detection Cycle**: Specify the detection period for detecting tag changes.
- **Diff Type**: Select to detect parameter changes for tags. Optional parameters include tag value, quality, and timestamp. The detection of the change of the tag value is affected by the three parameters of the threshold type, the Deadband and the jitter time configured in the tag table. For details, see the tag table configuration description below.

Tag Table Configuration

The tag table is used to add the data center tags to the MQTT connection. Each connection can have its own tag table configuration to meet the needs of different cloud servers.

Tag Name	Alias	Tag Type	Deadband	Deadband Type	Unit	Jitter Time(s)	Decimal Digits	Description
#WLAN0_SIGNAL...		analog	0	Absolute		0	2	SYSTEMTAG_WLAN0_SIGNAL_NOISE
#WLAN0_SIGNAL...		analog	0	Absolute		0	2	SYSTEMTAG_WLAN0_SIGNAL_BITRATE
#ICDM_COM1_SC...		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_COM1_SCORE
#ICDM_COM2_SC...		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_COM2_SCORE
#ICDM_COM3_SC...		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_COM3_SCORE
#ICDM_LAN1_SC...		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_LAN1_SCORE
#ICDM_LAN1_LINK		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_LAN1_LINK
#ICDM_LAN2_SC...		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_LAN2_SCORE
#ICDM_LAN2_LINK		analog	0	Absolute		0	2	SYSTEMTAG_ICDM_LAN2_LINK
#GPS_LATITUDE		analog	0	Absolute		0	2	SYSTEMTAG_GPS_LATITUDE
#GPS_LONGITUDE		analog	0	Absolute		0	2	SYSTEMTAG_GPS_LONGITUDE
#GPS_ALTITUDE		analog	0	Absolute		0	2	SYSTEMTAG_GPS_ALTITUDE
#GPS_SPEED		analog	0	Absolute		0	2	SYSTEMTAG_GPS_SPEED
#GPS_COURSE		analog	0	Absolute		0	2	SYSTEMTAG_GPS_COURSE
#GPS_SATELLITE		analog	0	Absolute		0	2	SYSTEMTAG_GPS_SATELLITE
#SYS_BATTERY_...		analog	0	Absolute		0	2	SYSTEMTAG_SYS_BATTERY_LOW
#SYS_TIME_SEC...		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_SECOND
#SYS_TIME_MIN...		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_MINUTE
#SYS_TIME_HOUR		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_HOUR
#SYS_TIME_DAY		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_DAY
#SYS_TIME_MONTH		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_MONTH
#SYS_TIME_YEAR		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_YEAR
#SYS_TIME_WDAY		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_WDAY
#SYS_TIME_YDAY		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_YDAY
#SYS_TIME_ISDST		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_ISDST
#SYS_TIME_GMT...		analog	0	Absolute		0	2	SYSTEMTAG_SYS_TIME_GMT_OFFSET

- **Tag Name**: Double-click this field to add or select a tag in the device.
- **Alias**: Set the name when uploading data. Use the tag name as the data name when the alias is empty.
- **Tag Type**: Displays the data type of the tag. This item is a read-only item and cannot be modified in this tag table. If you need to modify it, please modify the original tag attribute in the data center.
- **Deadband Type**: Used to configure the change detection method of tag values. There are two ways: absolute value and percentage. When the type is configured as an absolute value, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the *Deadband*, and if it is exceeded, the tag is considered to have changed; When the type is configured as a percentage, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the last uploaded tag value. If the change exceeds the *Deadband*, the tag is considered to have changed.
- **Deadband**: Used to specify the Deadband value of the tag detection. The value change of the tag does not trigger the tag value change within the threshold.
- **Unit**: Read-only item, when the Deadband type is percentage, a percent sign is displayed to distinguish

it from the absolute value.

- **Jitter time**: The unit is second. When the detected tag value exceeds *Deadband*, verification of *jitter time* will start. When the tag value is detected as exceeding the *Deadband* within the specified *jitter time*, it will be finally judged as a little value change, and the changed value will be uploaded at this time, otherwise it will be judged as tag value jitter. Not uploaded.
- **Decimal Digits**: The number of digits after the decimal tag for specifying the analog tag value. The default is 2. When the actual tag value has only one integer value, you can set this field to 0 to save data traffic.
- **Description**: The description of the tag. This item is a read-only item and cannot be modified in this tag table. If you need to modify it, please modify the original tag attribute in the data center.

EdgeSync 360/EdgeHub

precondition：

1. *The prerequisite for establishing a connection between a gateway and EdgeSync 360/EdgeHub is to create a device in EdgeSync 360/EdgeHub and obtain a connection string*

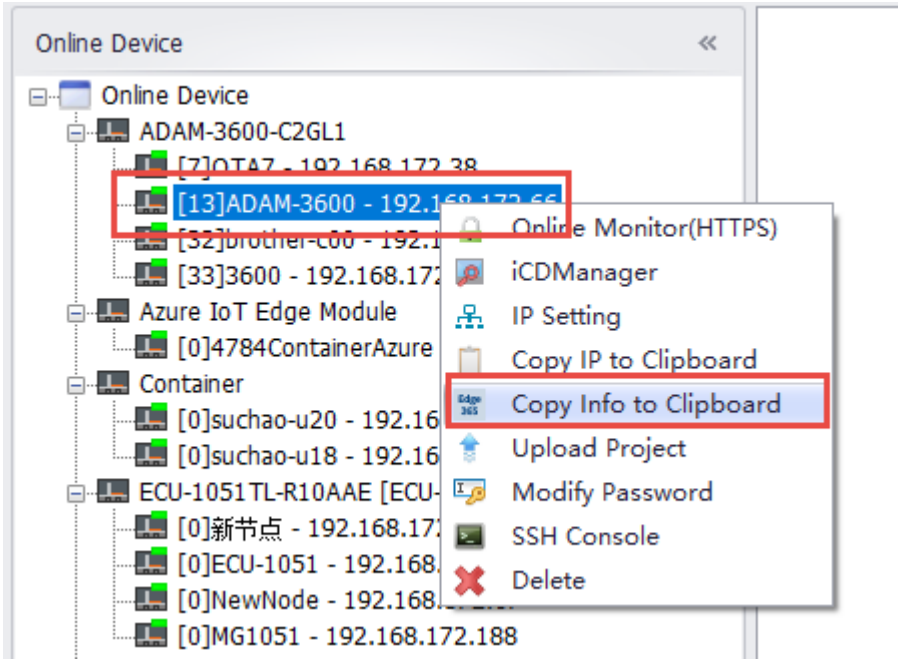
2. *The prerequisite for downloading a project or upgrading an image for a gateway through EdgeSync 360/EdgeHub is that a connection between the gateway and EdgeSync 360/EdgeHub has already been established*

function list：

- Obtaining the connection string in EdgeHub
- Establishing a connection between a gateway and EdgeHub
- Uploading data to EdgeHub
- Downloading projects to the gateway through EdgeHub
- Upgrading the image on the gateway through EdgeHub

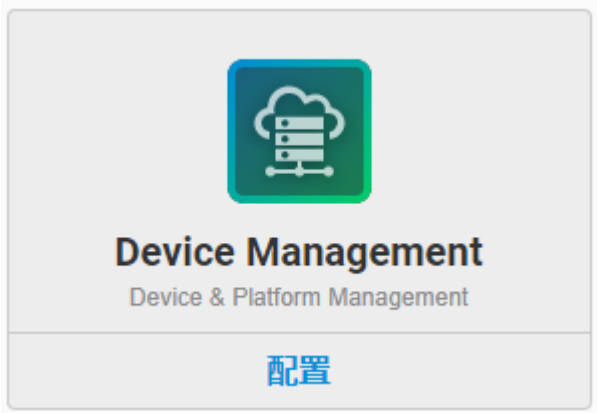
the steps of get connection string ：

1. In EdgeLink Studio, select the online page for the gateway you want to add to EdgeSync 360/EdgeHub, right-click, and choose “Copy device information to clipboard”

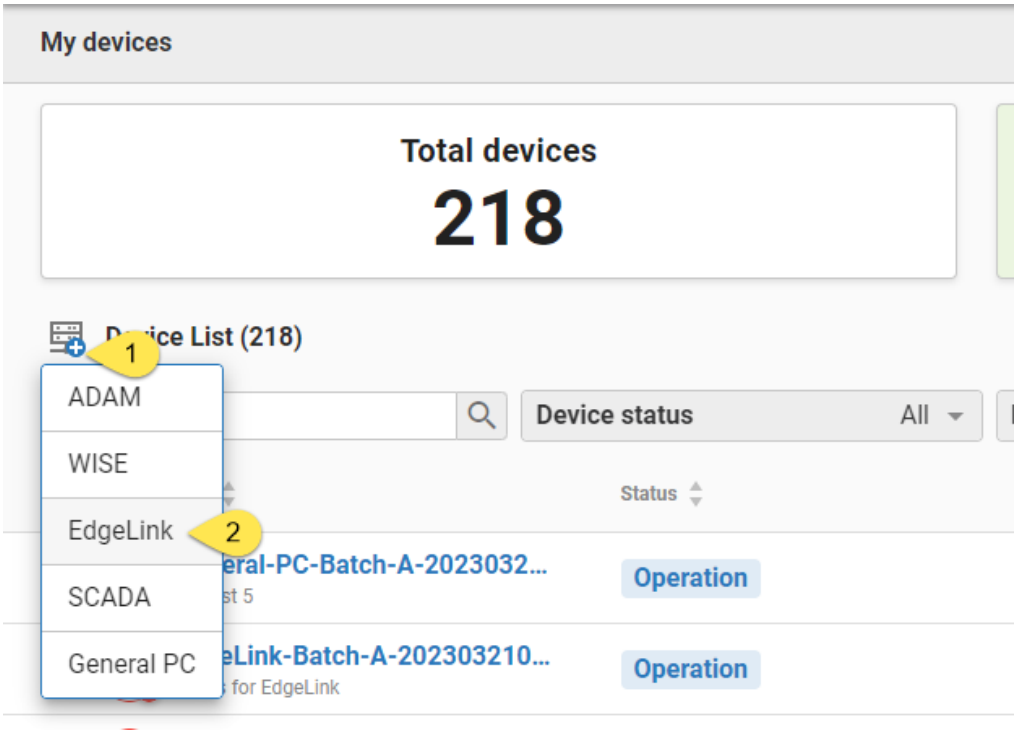


2. Open the EdgeSync 360/EdgeHub login page, enter your username and password to log in

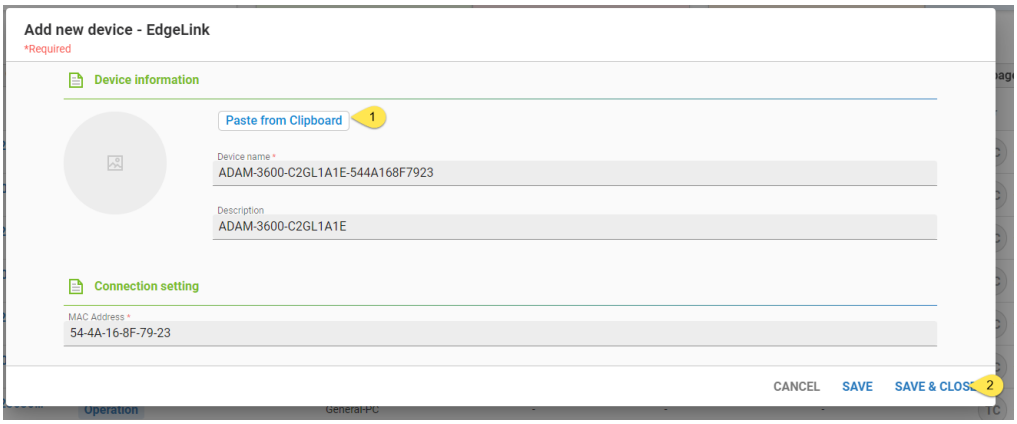
3. Device Management



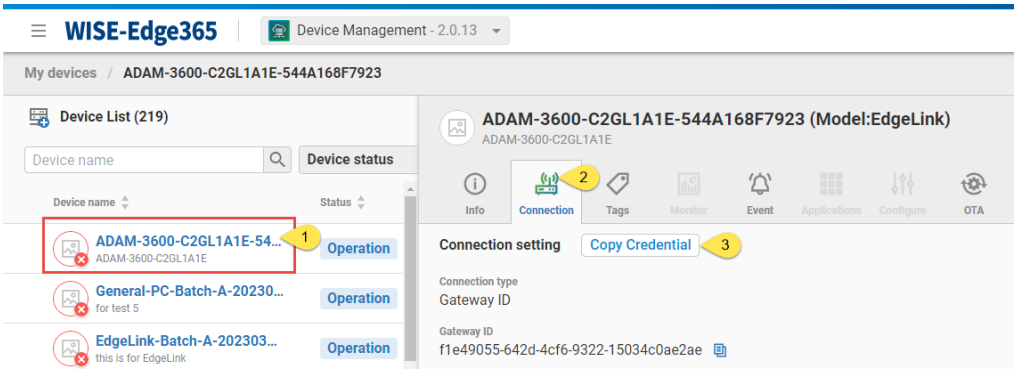
4. Select the option to add an EdgeLink device



5. Paste from Clipboard

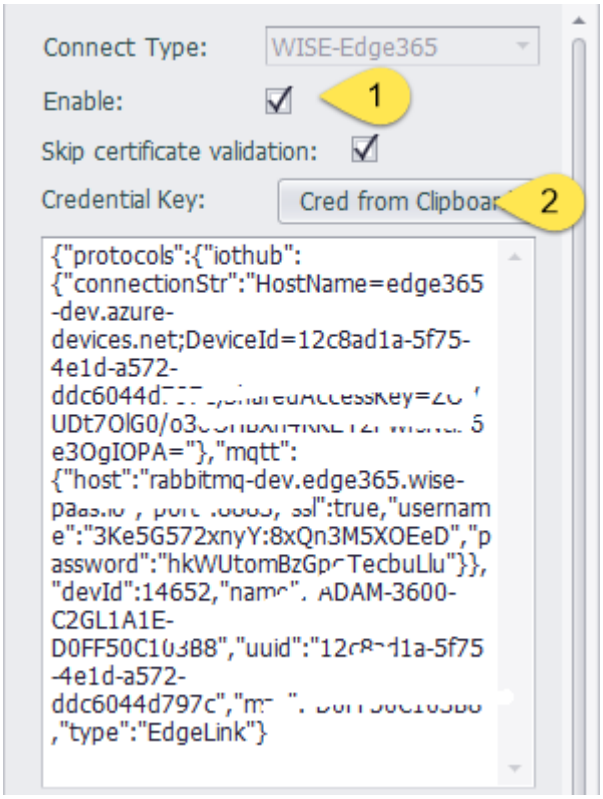


6. Click on the newly added device, and the device information will appear on the right side. Copy the “Credential” to the clipboard

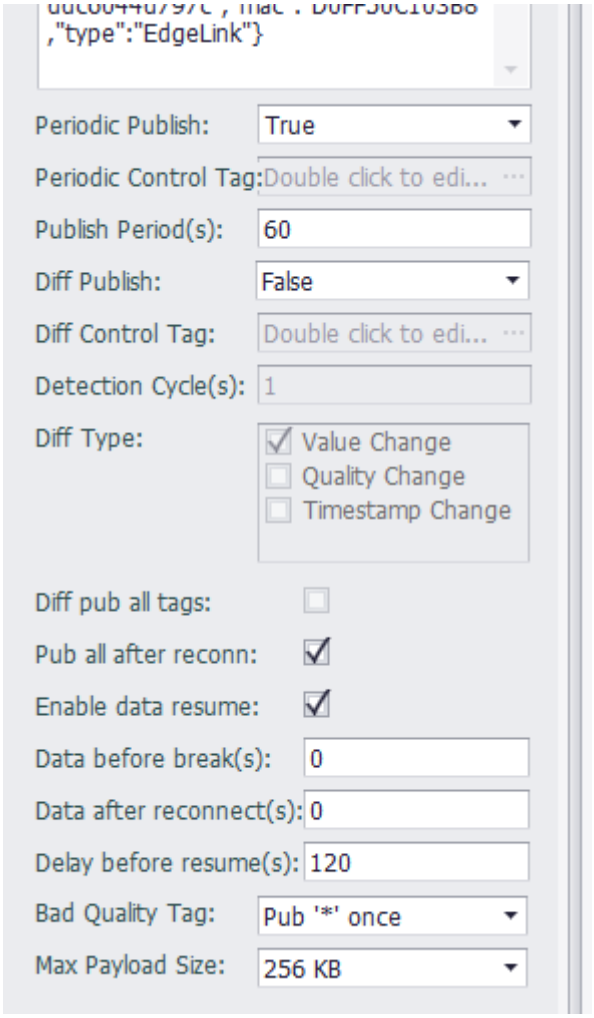


Establishing a connection between a gateway and EdgeHub：

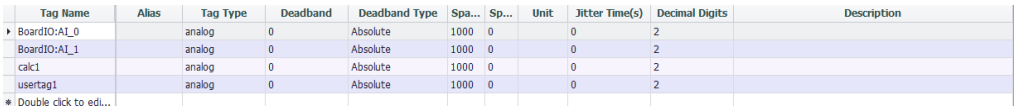
1. Open the EdgeLink Studio project configuration page for EdgeSync 360/EdgeHub by selecting “Project” > “Cloud Service” > “Advantech” > “EdgeSync 360/EdgeHub”, and enable the connection
2. Paste the “Credential Key” into the corresponding field



3. Configure connection parameter, parameter description

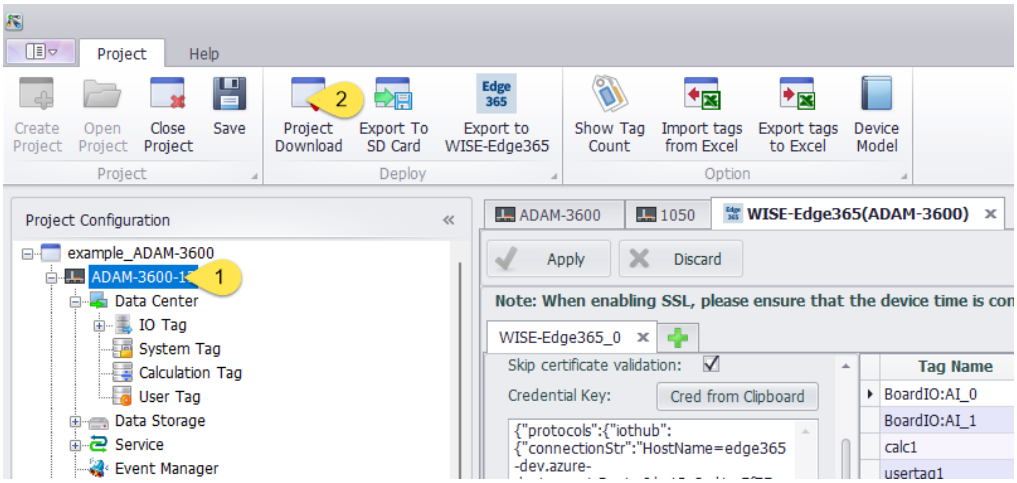


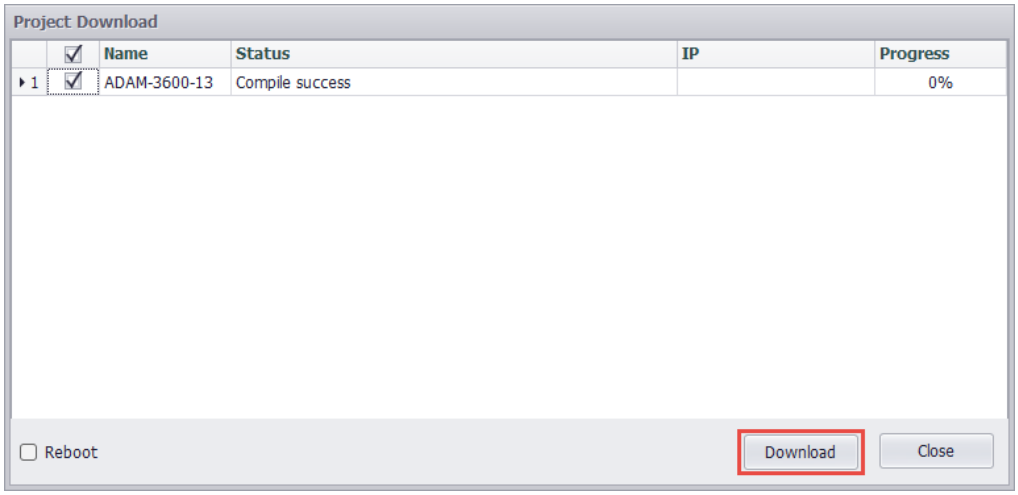
4. Configure tag point, the parameter description of tag



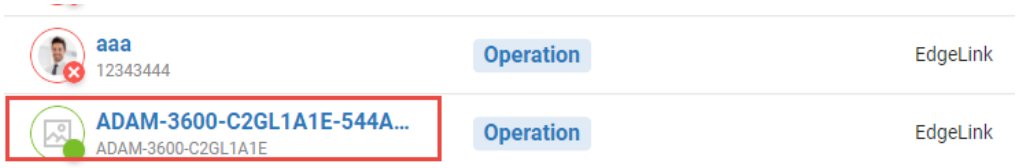
Tag Name	Alias	Tag Type	Deadband	Deadband Type	Spa...	Sp...	Unit	Jitter Time(s)	Decimal Digits	Description
BoardIO:AI_0		analog	0	Absolute	1000	0		0	2	
BoardIO:AI_1		analog	0	Absolute	1000	0		0	2	
calc1		analog	0	Absolute	1000	0		0	2	
usertag1		analog	0	Absolute	1000	0		0	2	
Double click to edi...										

5. Download the project file to the gateway





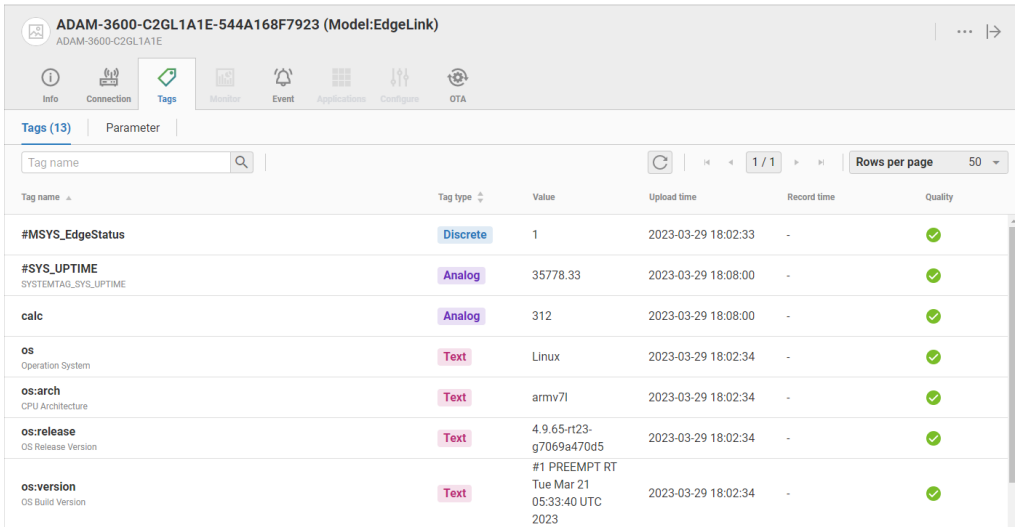
6. View the device as online in EdgeHub



Uploading data to EdgeHub

The gateway is already online in EdgeSync 360/EdgeHub

1. Click the online gateway–> Tags



2. For more detailed instructions on additional features, please refer to the relevant documentation of

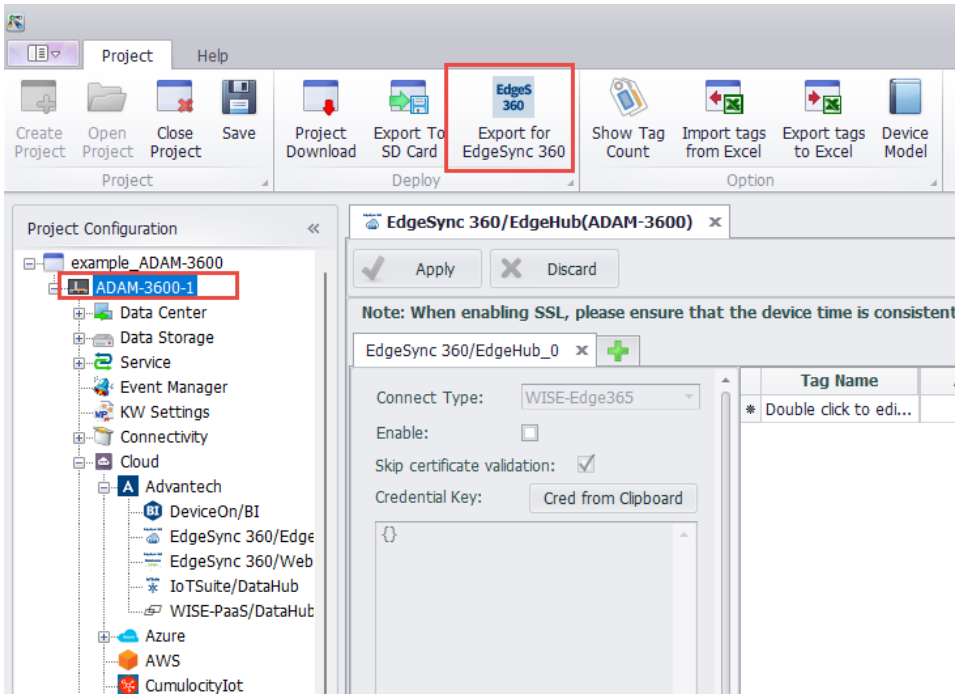
EdgeSync 360/EdgeHub

Downloading Edgelink-Studio generated project files to the gateway through EdgeHub

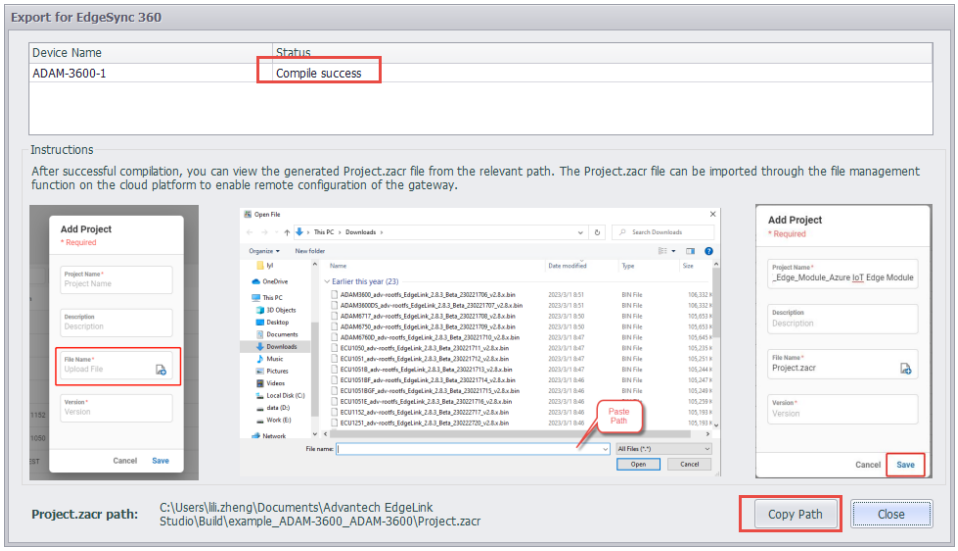
1. Uploading project files to EdgeSync 360/EdgeHub

   Method 1：Uploading project files to EdgeSync 360/EdgeHub through EdgeLink Studio

   step 1. Save the project and click “Export for EdgeSync 360”



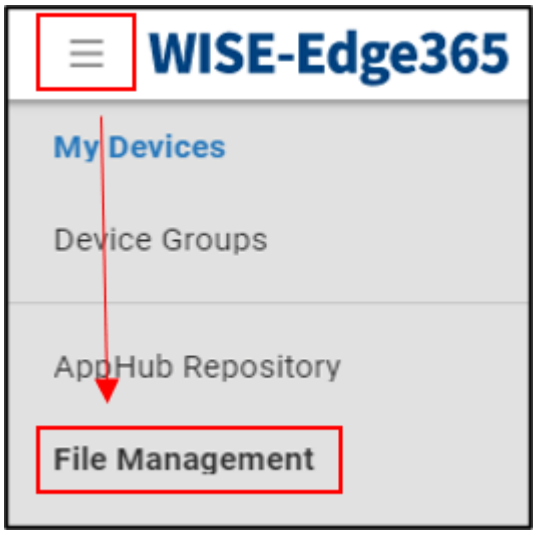
   step 2. After seeing the “Compile success” message, click “Copy Path”



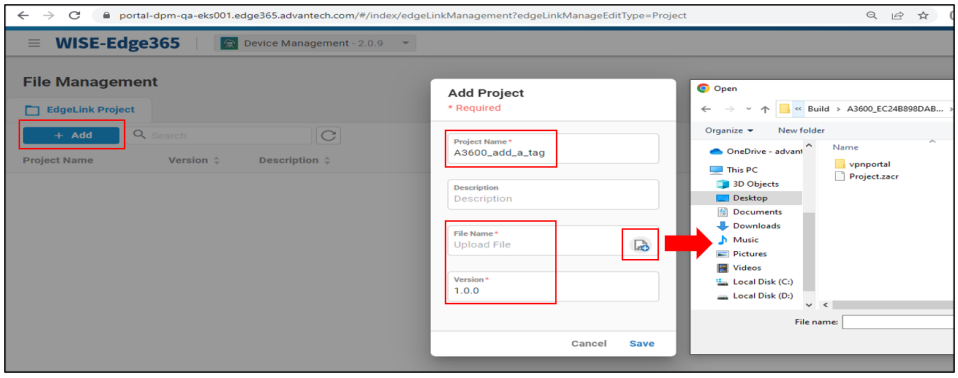
step 3. Navigate to the project loading interface in EdgeSync 360/EdgeHub

Method 2：Directly add the project file generated by EdgeLink Studio to EdgeSync 360/EdgeHub

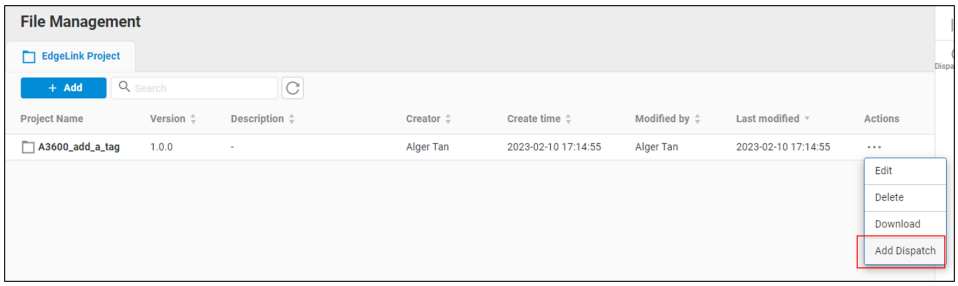
step 1. Click on “File Management” in the EdgeSync 360/EdgeHub interface



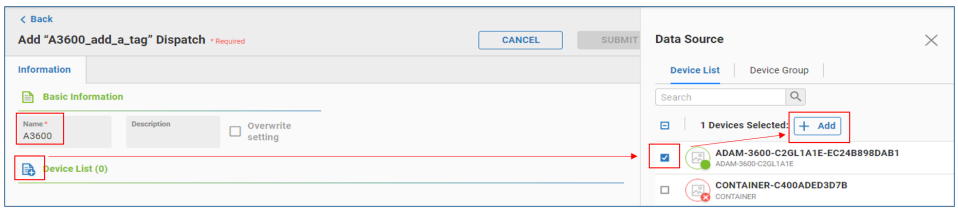
step 2. Add the project file



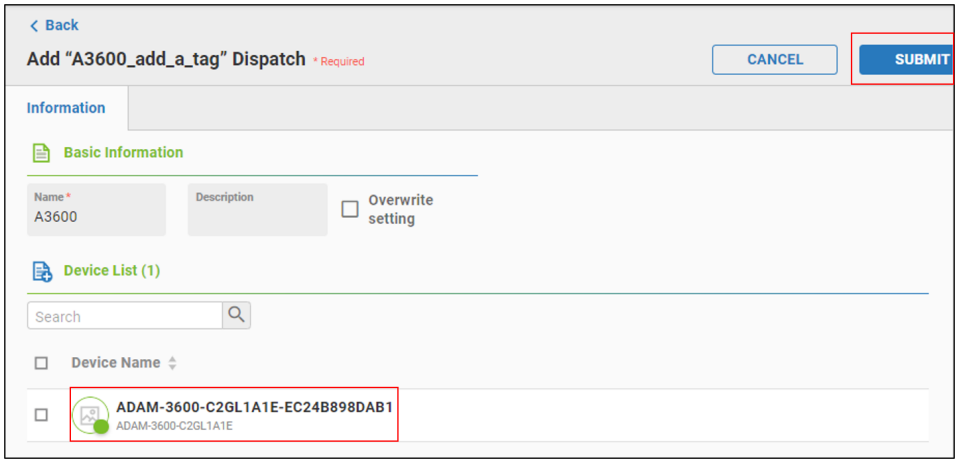
2. Find the corresponding project file in EdgeSync 360/EdgeHub and click Add Dispatch



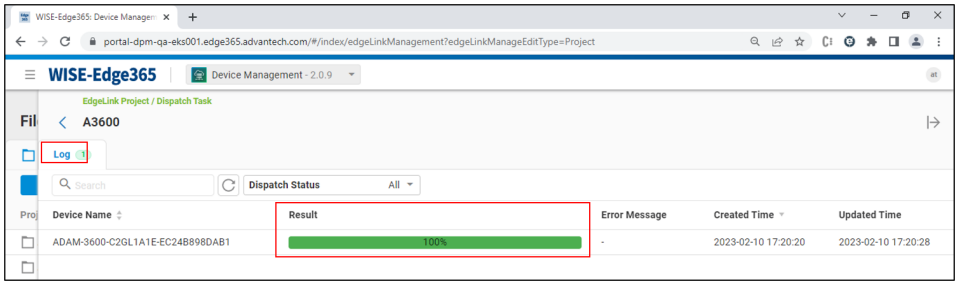
3. Add a Dispatch, enter a dispatch name, and select the corresponding device



4. Click "Submit" to confirm and submit the dispatch

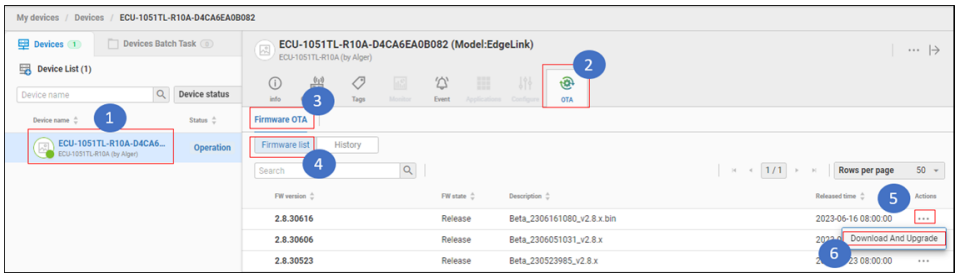


5. View the dispatch results

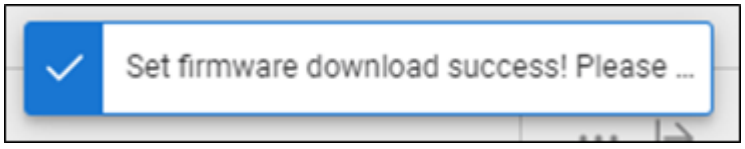


Upgrading the image on the gateway through EdgeHub

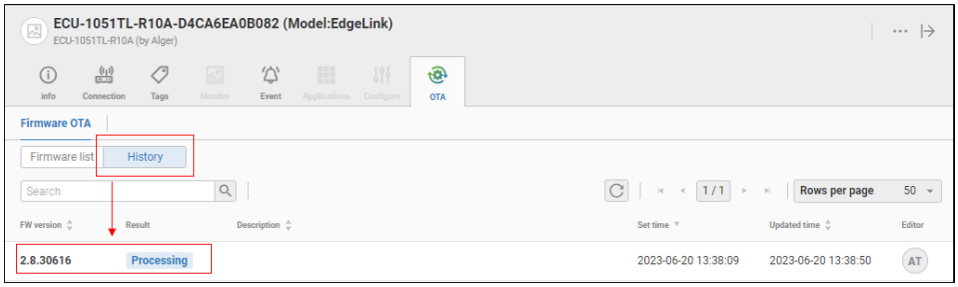
1. Confirm that the device is online and click to enter the functional page.
2. Select the “OTA” feature
3. Click on “Firmware list” under “Firmware OTA” to view all files available for upgrade
4. Click on the “…” behind “2.8.30616” and select “Download And Upgrade”



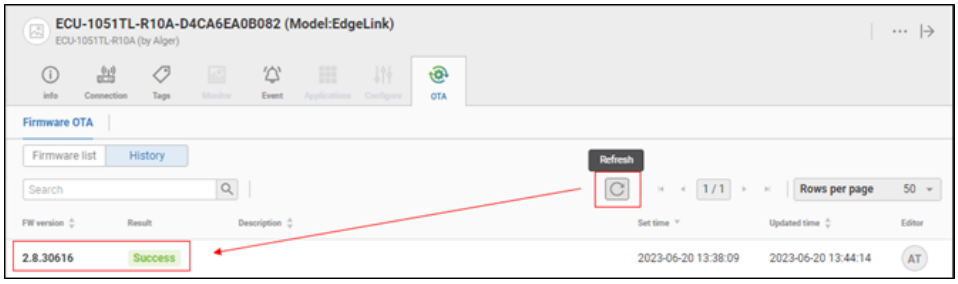
5. You will see the message “Set firmware download success…”



6. At this point, the user can click on “History” under “Firmware OTA” to view the current upgrade status



7. Click on the “Refresh” button to refresh the current upgrade status until you see “Success”, which means the upgrade was successful



parameter description

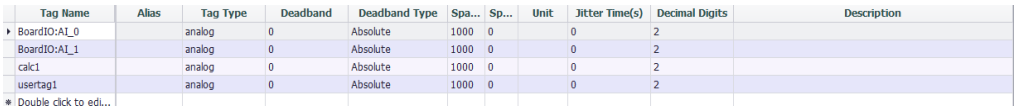
parameter	parameter description
`Connection Type`	MQTT type
`Enable`	Check the box to activate the connection for the current page, and the current page configuration will take effect
`skip certificate validation`	Check the box to skip the certificate validation

parameter	parameter description
`Periodic Publish`	Periodic Upload Mode: Enable, Disable, and start by tag
`Periodic Publish`	Periodic Upload Mode: Enable, Disable, and start by tag
`Periodic Control Tag`	Select the periodic upload control tag. Upload data when the value of the point is not 0; do not upload data when the value of the point is 0
`Publish Period`	Periodic Upload Period, units seconds
`Diff Publish`	Trigger Upload Mode: Enable, Disable, and start by tag Upload
`Diff Control Tag`	Select the trigger upload control tag. Upload data when the value of the point is not 0; do not upload data when the value of the point is 0
`Detection Cycle`	Detection Period for tag Change Detection
`Diff Type`	the type of Diff Publish

parameter	parameter description
`Diff pub all tags`	pub all tags in list when Diff Publish
`Pub all after reconn`	When EdgeLink establishes a connection with the cloud, does it upload the current values of all points once to the cloud, with enabling sending and disabling not sending? The default setting is enabling sending
`Enable data resume`	Enable switch for resume upload from break
`Data before break`	Default: 0, resume uploading data from the most recent n seconds before the disconnection
`Data after reconnect`	Default: 0, resume uploading data until the most recent n seconds after the reconnection
`Delay before resume`	Default: 120, resume uploading data after an interval of n seconds after the reconnection

parameter	parameter description
`Bad Quality Tag`	Upload mode for Tag Quality not equal to 0 (GOOD) : Pub * once; Pub * always; Still pub value; Don't pub

the parameter description of tag



Tag Name	Alias	Tag Type	Deadband	Deadband Type	Spa...	Sp...	Unit	Jitter Time(s)	Decimal Digits	Description
BoardIO:AI_0		analog	0	Absolute	1000	0		0	2	
BoardIO:AI_1		analog	0	Absolute	1000	0		0	2	
calc1		analog	0	Absolute	1000	0		0	2	
usertag1		analog	0	Absolute	1000	0		0	2	
Double click to edi...										

- **Tag Name**: Double-click this field to add or select a tag in the device.
- **Alias**: Set the name when uploading data. Use the tag name as the data name when the alias is empty.
- **Tag Type**: Displays the data type of the tag. This item is a read-only item and cannot be modified in this tag table. If you need to modify it, please modify the original tag attribute in the data center.
- **Deadband Type**: Used to configure the change detection method of tag values. There are two ways: absolute value and percentage. When the type is configured as an absolute value, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the *Deadband*, and if it is exceeded, the tag is considered to have changed; When the

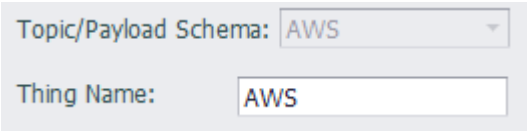
type is configured as a percentage, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the last uploaded tag value. If the change exceeds the *Deadband*, the tag is considered to have changed.

- **Deadband**: Used to specify the Deadband value of the tag detection. The value change of the tag does not trigger the tag value change within the threshold.
- **Unit**: Read-only item, when the Deadband type is percentage, a percent sign is displayed to distinguish it from the absolute value.
- **Jitter time**: The unit is second. When the detected tag value exceeds *Deadband*, verification of *jitter time* will start. When the tag value is detected as exceeding the *Deadband* within the specified *jitter time*, it will be finally judged as a little value change, and the changed value will be uploaded at this time, otherwise it will be judged as tag value jitter. Not uploaded.
- **Decimal Digits**: The number of digits after the decimal tag for specifying the analog tag value. The default is 2. When the actual tag value has only one integer value, you can set this field to 0 to save data traffic.
- **Description**: The description of the tag. This item is a read-only item and cannot be modified in this tag

table. If you need to modify it, please modify the original tag attribute in the data center.

AWS

The AWS Cloud Service Plugin supports connecting to Amazon AWS IoT to upload tag values to the cloud.



- **Thing Name**: Specify the corresponding ‘things’ name on this device on AWS IoT.

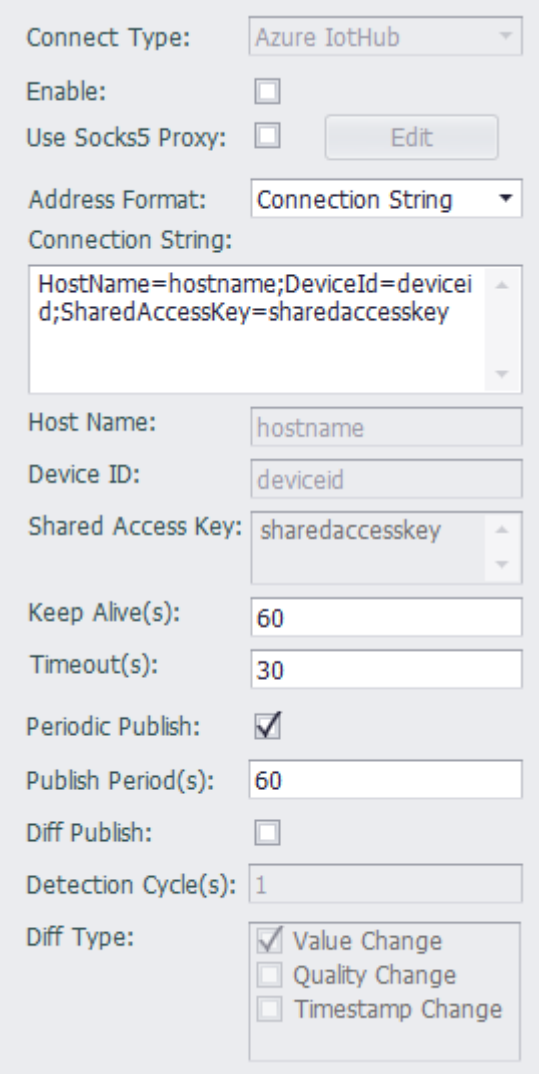
Others

Tag List

resume

export/import

Azure IoT Hub



When connecting to the Microsoft Azure cloud, the connection type must be Azure IoTHub, and the client needs to configure the connection string provided by the cloud.

Users can directly edit the connection string, or generate a connection string by setting the attributes: Host Name, Device ID, and shared Access Key.

Since v2.8.1, the bottom layer of EdgeLink uses the Microsoft Azure IoT SDK to connect to the Azure IoT

Hub, so the communication-related parameters other than the connection string do not need to be set.

If you are using this plugin in the environment of an IoT Edge-launched EdgeLink Container, you do not have to enable resumable uploads, as IoT Edge will cache the transferred data.

This plugin supports the following Direct Method, please note that method names are case sensitive.

1. GetVersion - Get EdgeLink version information

Method Name: `GetVersion`

Parameters: none

Return Value: JSON object, where the `Result` parameter indicates whether the call result is successful or not, `Success` indicates success, and `Error` indicates failure. The content of the `Content` parameter in the successful result is the EdgeLink version information, and the content of the `Error` parameter in the failure result indicates the reason for the failure. Please refer to the return value example below.

Example of return value when the call is successful:

```
{
    "Result": "Success",
    "Content": "ADAM-3600-C2GL1A1E Standard Edition ima
}
```

Example of return value when the call fails:

```
{
    "Result": "Error",
    "Error": "fail to read version file"
}
```

Remarks: None

2. PubAllTags - Publish all tag values in the tag list at once

Method Name: `PubAllTags`

Parameters: none

Return Value: None

Remarks: After the gateway receives this method call, it will immediately publish a message containing the current values of all tags in the tag list. Please note that the content of the message will not be returned from the direct method, but will be published to the data topic.

2. ReadTag - Read tag value

Method Name: `ReadTag`

Parameters: JSON object, including an array of tag names and related read parameters, where the `tags` parameter is a string array, including all the tag names that need to be read; the `value_as_string` parameter is a boolean value, used for control tags Whether the value is returned as a string, the default value is `false`, i.e. not returned as a string.

Example: The following call parameters will read three tags named tag1, tag2 and tag3 and return the tag value

as a string.

```
{
    "tags": ["tag1","tag2","tag3"],
    "value_as_string": true
}
```

Return Value: JSON object, where the `tags` parameter is the object type, including all requested tag values, each object parameter corresponds to a tag, the parameter name is the tag name, and the parameter value is the tag value.

Example:

When there is no `value_as_string` in the calling parameter or its value is false, an example of the return value is as follows:

```
{
    "tags": {
        "tag1": false,
        "tag2": 3.1415926,
        "tag3": 1.28
    }
}
```

When there is `value_as_string` in the call parameter and its value is true, an example of the return value is as follows:

```
{
    "tags": {
        "tag1": "0",
        "tag2": "3.1415926",
        "tag3": "1.28"
    }
}
```

Remarks: None

2. WriteTag - Write tag value

Method Name: `WriteTag`

Parameters: JSON object, including all the tag values to be modified, each object parameter corresponds to a tag, the parameter name is the tag name, the parameter value is the tag value, the tag value can be a string type or can is a numeric type or a boolean type.

Example:

```
{
    "tag1": false,
    "tag2": "3.1415926",
    "tag3": 1.28
}
```

Return Value: JSON object, where the `Result` parameter indicates whether the call result is successful or not, `Success` indicates success, and `Error` indicates failure. The successful result has no additional parameters, and the `Error` parameter in the failed result indicates the reason for the failure. Please refer to the return value example below.

Example of return value when the call is successful:

```
{
    "Result": "Success"
}
```

Example of return value when the call fails:

```
{
    "Result": "Error",
    "Error": "Cannot found tag handle!"
}
```

Others

Tag List

resume

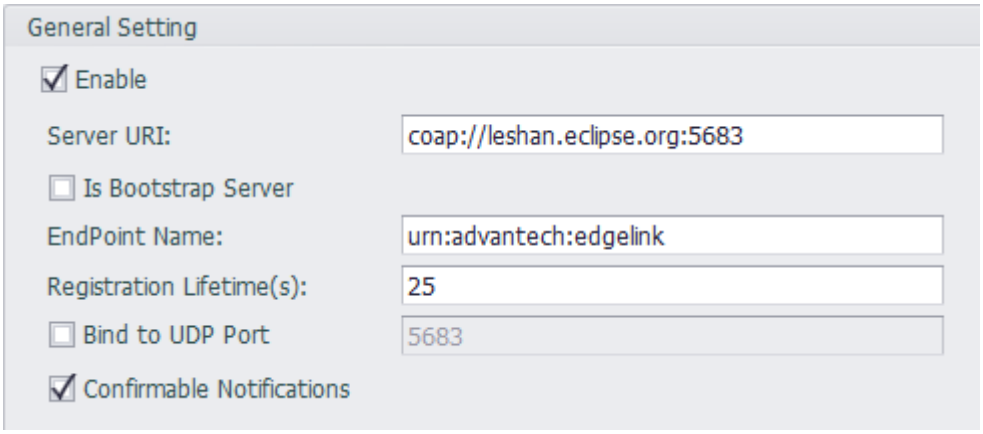
export/import

LwM2M

The LwM2M cloud service plug-in is used to support the OMA Lightweight M2M protocol to implement remote management of devices on the cloud platform. See Supported Objects and Resources for the capability of this plug-in.

Settings

General Settings

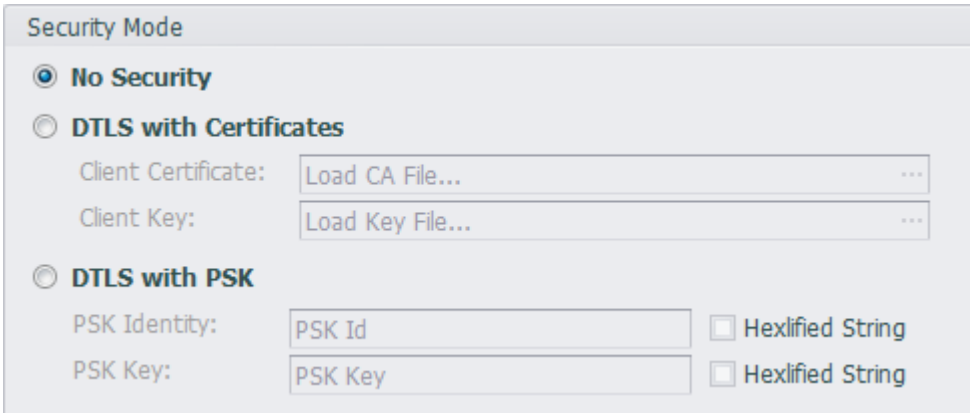


- **Enable**: Check to enable this plugin
- **Server URI**: Enter the full URI of the server.
- **Is Bootstrap Server**: If the `Server URI` related to a Bootstrap Server, it should be checked here.
- **EndPoint Name**: Enter the end point name of this device. This name should be named according to the management rules of the server.
- **Registration Lifetime(s)**: Specify how often this device is registered with the server, in seconds.
- **Band to UDP Port**: Check this box and fill in the value of 1 ~ 65534 to band the Lightweight M2M

device to the specified port.

- **Confirmable Notifications**: Lightweight M2M messages can be sent as a Non-confirmable or as a Confirmable message, you can specify the behavior of the client by this option.

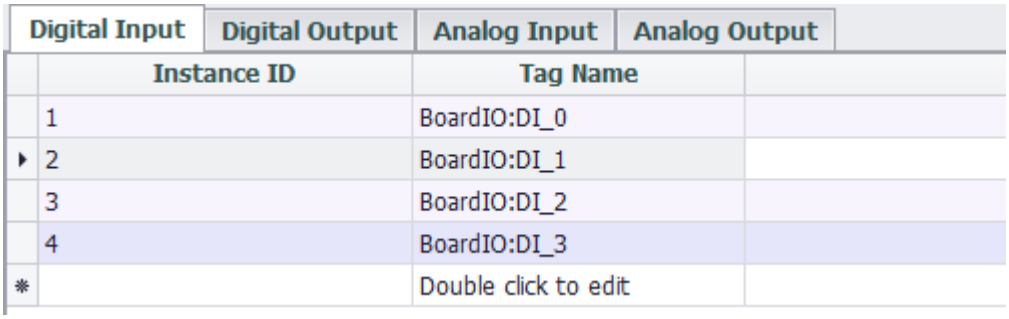
Security Mode



- **No Security**：Select this option to use an in-secure connection. In this case, the `Server URI` should be filled with `coap://` instead of the address starting with `coaps://`. Conversely, if you choose the two security options below, then the `Server URI` should be filled with the address starting with `coaps://`.
- **DTLS with Certificates**：Use a secure connection for a given client certificate. Load the client certificate file in the `Client Certificate` and load the client certificate key file in the `Client Key`.
- **DTLS with PSK**：Use the secure connection of the given PSK method. Please fill in the PSK string in `PSK Identity`. If the string is a hexadecimal format string, please check the `Hexlified String` option. Fill

the `PSK Key` with the PSK key and check the `Hexlified String` option as appropriate.

Tag List Settings



Currently, you can map the tag to the four I/O objects defined by the IPSO (Digital Input, Digital Output, Analog Input, Analog Output). In the four types of tag lists, double-click the tag name field and select the tag to be mapped in the dialog, then the tag will be added to the tag list.

The default `Instance ID` is automatically incremented, you can click the `Instance ID` field to modify it.

Supported Objects and Resources

```
<td><b>Object<b></td>
<td><b>Object ID<b></td>
<td><b>Resource<b></td>
<td><b>Resource ID<b></td>
```

```
<td rowspan="6">LwM2M Security</td>
<td rowspan="6">0</td>
<td>LWM2M Server URI</td>
<td>0</td>
```

```
<td>Bootstrap-Server</td>
<td>1</td>
```

```
<td>Security Mode</td>
<td>2</td>
```

```
<td>Public Key or Identity</td>
<td>3</td>
```

```
<td>Server Public Key</td>
<td>4</td>
```

```
<td>Secret Key</td>
<td>5</td>
```

```
<td rowspan="9">LwM2M Server</td>
<td rowspan="9">1</td>
<td>Short Server ID</td>
<td>0</td>
```

```
<td>Lifetime</td>
<td>1</td>
```

```
<td>Default Minimum Period</td>
<td>2</td>
```

```
<td>Default Maximum Period</td>
<td>3</td>
```

```
<td>Disable</td>
<td>4</td>
```

```
<td>Disable Timeout</td>
<td>5</td>
```

```
<td>Notification Storing When Disabled or Offline</td
<td>6</td>
```

```
<td>Binding</td>
<td>7</td>
```

```
<td>Registration Update Trigger</td>
<td>8</td>
```

```
<td rowspan="11">Device</td>
<td rowspan="11">3</td>
<td>Manufacturer</td>
<td>0</td>
```

```
<td>Model Number</td>
<td>1</td>
```

```
<td>Serial Number</td>
<td>2</td>
```

```
<td>Reboot</td>
<td>4</td>
```

```
<td>Error Code</td>
<td>11</td>
```

```
<td>Current Time</td>
<td>13</td>
```

```
<td>UTC Offset</td>
<td>14</td>
```

```
<td>Timezone</td>
<td>15</td>
```

```
<td>Supported Binding and Modes</td>
<td>16</td>
```

```
<td>Device Type</td>
<td>17</td>
```

```
<td>Software Version</td>
<td>19</td>
```

```
<td rowspan="2">IPSO Digital Input</td>
<td rowspan="2">3200</td>
<td>Digital Input State </td>
<td>5500</td>
```

```
<td>Application Type</td>
<td>5750</td>
```

```
<td rowspan="2">IPSO Digital Output </td>
<td rowspan="2">3201</td>
<td>Digital Output State</td>
<td>5550</td>
```

```
  <td>Application Type</td>
  <td>5750</td>
```

```
  <td rowspan="2">IPSO Analogue Input</td>
  <td rowspan="2">3202</td>
  <td>Analog Input Current Value</td>
  <td>5600</td>
```

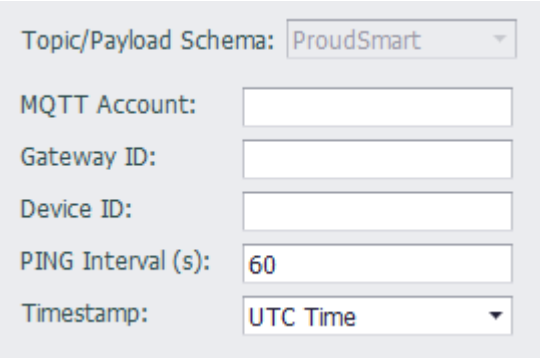
```
  <td>Application Type</td>
  <td>5750</td>
```

```
  <td rowspan="2">IPSO Analogue Output</td>
  <td rowspan="2">3203</td>
  <td>Analog Output Current Value</td>
  <td>5650</td>
```

```
  <td>Application Type</td>
  <td>5750</td>
```

Proud Smart

When connecting to the ProudSmart Cloud server, you need to configure the connection properties of the receiving server.



- **MQTT Account**: MQTT account name. Required field.
- **Gateway ID**: The name of the gateway to use for the connection. Required field.
- **Device ID**: The device name of the project in ProudSmart Cloud. Required field.
- **PING Interval**: The interval at which the server sends a PING command.
- **Timestamp**: This option is used to control the timestamp representation format in the published message. UTC Time is expressed in UTC time and Local Time is represented in the local time of the device. For example, if the time zone of the device is set to East 8 (ie, Beijing time), the message is sent at 11:30:45 on January 1, 2018 Beijing time, then UTC

Time will be 2018-01-01T03:30:45+0000, and the Local Time will be 2018-01-01T11:30:45+0800.

Others

Tag List

resume

export/import

Simple MQTT

Simple MQTT provides a simple topic / load scheme in which topics can be defined by the user to test and verify MQTT data communications or to be applied to cloud services that require simple development. In addition to tag data upload and modification, Simple MQTT also supports the ability of the server to deliver messages of a specific topic to perform the specified commands for special application extensions.

The default simple MQTT publishing data payload format is as follows:

```
{
    "d":[
        {
            "tag":"AI.0",
            "value":12.00,
            "quality":0
        },
        {
            "tag":"AI.1",
            "value":12.00,
            "quality":0
        }
    ],
    "ts":"2017-12-22T08:05:20+0000"
}
```

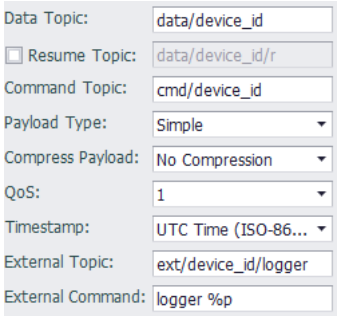
- Among them
- “d” represents an array object that contains all reported tag information. Each tag is represented by an object. Its properties are as follows:

Attributes	Introductions
tag	tag name
value	tag current value
Quality	tag current quality value (selectable via parameter switch)

- “ts” is the timestamp of the message and follows the ISO 8601 standard.

> The data retransmission of the disconnected SimpleMQTT packet is exactly the same as the data packet format of the real-time data.The difference is that the time stamp is obtained from the data record, not the current time.

Parameter settings



- **Data Topic**: Required fields that specify topics for publishing real-time data. To facilitate parsing of data packets from different devices on the cloud server, it is recommended to add the device unique identifier to the topic when setting this topic.
- **Resume Topic**: Optional, specifies the topic for publishing resuming data. If this field is not set, then the topic specified in `Data Topic` will be used.
- **Command Topic**: Optional, specifies the subject to receive the command. Publishing data from the cloud server to the topic can modify the tag value on the device. The format of the data is the same as the publishing format except that “d” is changed to “w”. There can be no timestamp data in the write packet (that is, ts). If this field is not filled in, the device will not accept the command to modify the value of the cloud service.

The example of modifying the value of a packet is as follows: The following packet will write the value of AO_1 as 12.88 and the value of AO_2 as 18.76.

```
json { "w":[ { "tag":"AO_1", "value":12.88 }, { "tag":"AO_2", "value":18.76 } ], "ts":"2017-12-
```

- **Payload Type**: This option is used to control the payload format.
- `Simple`: The default payload type, no quality field in payload
- `Simple with quality`: The default payload type with quality field in payload
- `Compact`: The compact payload type as below.
  `{"ts":1451649600512, "values":{"tag1":"value1", "tag2":"value2"}}`
- **Compress Payload**: This option controls whether to use GZIP to compress the message payload. By default, the payload is not compressed. If this option is set to GZIP compression, you must make sure that the cloud platform also uses the same GZIP method for decompression. At the same time, the `cmd` payload must also be GZIP compressed message content.
- **QoS**: This option is used to control the quality of service used when publishing messages. The default value is QoS 1.
- `QoS 0`: Distributed at most once, the distribution of messages depends on the capabilities of the underlying network. The recipient will not send a response and the sender will not retry. The message may or may not be delivered at all.
- `QoS 1`: Distribute at least once, the quality of service ensures that the message is delivered at least once.
- `QoS 2`: Distribute only once, which is the highest level of quality of service, and message loss and duplication are unacceptable. There is an additional overhead in using this quality of service level.
- **Timestamp**: This option is used to set the timestamp format in the published message.
- `UTC Time (ISO-8601)`: UTC time in ISO-8601 format，such as `2018-01-01T03:30:45+0000`
- `Local Time (ISO-8601)`: Local time in ISO-8601 format, such as`2018-01-01T11:30:45+0800`
- `UNIX Time`: UNIX time stamp format, such as `1600058903`
- `UNIX Time w/ MS`: UNIX time stamp format with millisecond, such as `1600058903001`

- **External Topic**: This option is used to set the topic for external command. If set, the device will subscribe this topic, and will execute the command specified in “External Command” when the message arrived.
- **External Command**: This option is used combined with the “External Topic”, to specify the command line to be executed when message arrived. For example: `logger %p`, this command will output the message payload to syslog when it is executed。
  The command line can have arguments, the following patterns supported in the command line:
  - %t: Topic, this pattern will be substitute by the topic when executing.
  - %p: Payload, this pattern will be substitute by the payload when executing.
  - %pf: Payload file, this pattern will be substitute by a file contains the payload when executing.

  > Note: Don’t use `newline` or one of `|, &, ;, <, >, (, ), {, }` in the command string, and because of the MQTT application is running as unprivileged user, please don’t specify any command needs to run in privileged mode.

Others

Tag List

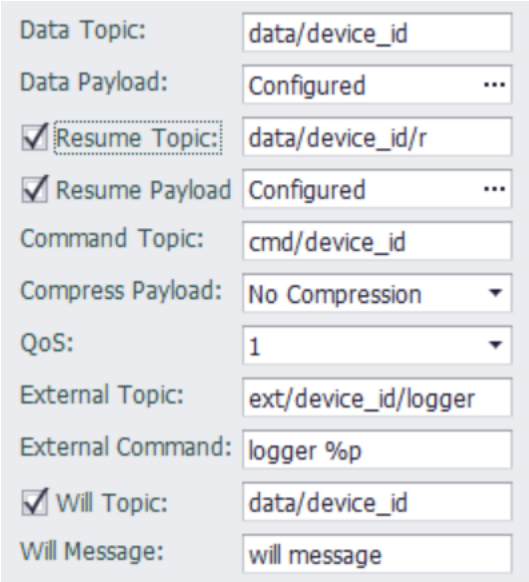
resume

export/import

Custom MQTT

Custom MQTT provides a customized topic / payload scheme in which topic / payload can be defined by the user to test and verify MQTT data communications or to be applied to cloud services that require customized development. In addition to tag data upload and modification, Custom MQTT also supports the ability of the server to deliver messages of a specific topic to perform the specified commands for special application extensions.

Parameter settings



- **Data Topic**: Required fields that specify topics for publishing real-time data. To facilitate parsing of data packets from different devices on the cloud server, it is recommended to add the device unique identifier to the topic when setting this topic.
- **Data Payload**: Required fields that specify payload for publishing real-time data.

  Payload Configuration instructions
- **Resume Topic**: Optional, specifies the topic for publishing resuming data. If this field is not set, then the topic specified in `Data Topic` will be used.
- **Resume payload**: Optional, specifies the payload for publishing resuming data. If this field is not set, then the load specified in `Data Payload` will be used.

  Payload Configuration instructions
- **Command Topic**: Optional, specifies the subject to receive the command. Publishing data from the cloud server to the topic can modify the tag value on the device. The format of the data is as follows. Tags and Tags value are defined by the user. There can be no timestamp data in the write packet (that is, ts). If this field is not filled in, the device will not accept the command to modify the value of the cloud service.

The example of modifying the value of a packet is as follows: The following packet will write the value of AO_1 as 12.88 and the value of AO_2 as 18.76.

`json { "w":[ { "tag":"AO_1", "value":12.88 }, { "tag":"AO_2", "value":18.76 } ], "ts":"2017-12-`

- **Compress Payload**: This option controls whether to use GZIP to compress the message payload. By default, the payload is not compressed. If this option is set to GZIP compression, you must make sure that the cloud platform also uses the same GZIP method for decompression. At the same time, the `cmd` payload must also be GZIP compressed message content.
- **QoS**: This option is used to control the quality of service used when publishing messages. The default value is QoS 1.
- `QoS 0`: Distributed at most once, the distribution of messages depends on the capabilities of the underlying network. The recipient will not send a response and the sender will not retry. The message may or may not be delivered at all.
- `QoS 1`: Distribute at least once, the quality of service ensures that the message is delivered at least once.
- `QoS 2`: Distribute only once, which is the highest level of quality of service, and message loss and duplication are unacceptable. There is an additional overhead in using this quality of service level.
- **External Topic**: This option is used to set the topic for external command. If set, the device will subscribe this topic, and will execute the command specified in “External Command” when the message arrived.
- **External Command**: This option is used combined with the “External Topic”, to specify the command line to be executed when message arrived. For example: `logger %p`, this command will output the message payload to syslog when it is executed。
  The command line can have arguments, the following patterns supported in the command line:
  - %t: Topic, this pattern will be substitute by the topic when executing.
  - %p: Payload, this pattern will be substitute by the payload when executing.
  - %pf: Payload file, this pattern will be substitute by a file contains the payload when executing.

  > Note: Don’t use `newline` or one of `|, &, ;, <, >, (, ), {, }` in the command string, and because of the MQTT application is running as unprivileged user, please don’t specify any command needs to run in privileged mode.
- **Will Topic**: Optional, specifies the topic for publishing will message.
- **Will message**: Optional, specifies the content for publishing will message.

Others

Tag List

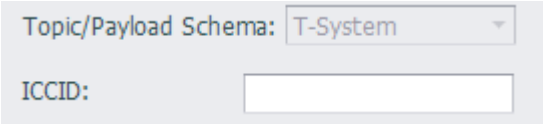
resume

export/import

T-System

Connect to the Cloud Of Thing.

SSL need to Enable，SSL Scenario please chose Server Authentication，Port 8883.



- **ICCID**: Device unique identification ICCID.

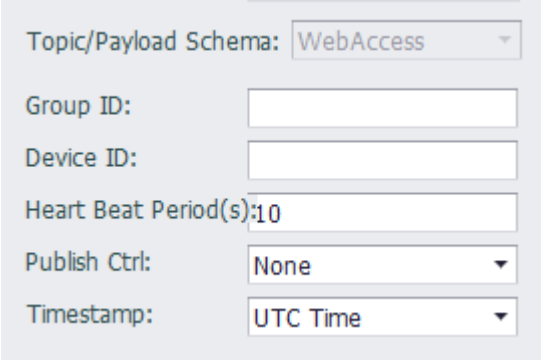
Others

Tag List

resume

export/import

WebAccess



- **Group ID**: The Group ID is a combination of the project name of the WebAccess Cloud and the SCADA name with an underscore “_”, for example: MyProject_MySCADA.
- **Device ID**: The device name of the project in the WebAccess Cloud.
- **Heart Beat Period**: The period during which the client sends heartbeat information to the server.
- **Publish Ctrl**: Choose whether to upload data by Publish Ctrl.
- **Timestamp**: This option is used to set the timestamp representation format in the published message. UTC Time is expressed in UTC time and Local Time is expressed in the local time of the device. For example, if the time zone of the device is set to East 8 (ie, Beijing time), the message is sent at 11:30:45 on January 1, 2018 Beijing time, then UTC Time will be 2018-01-01T03:30:45+0000, and the Local Time will be 2018-01-01T11:30:45+0800.

Others

Tag List

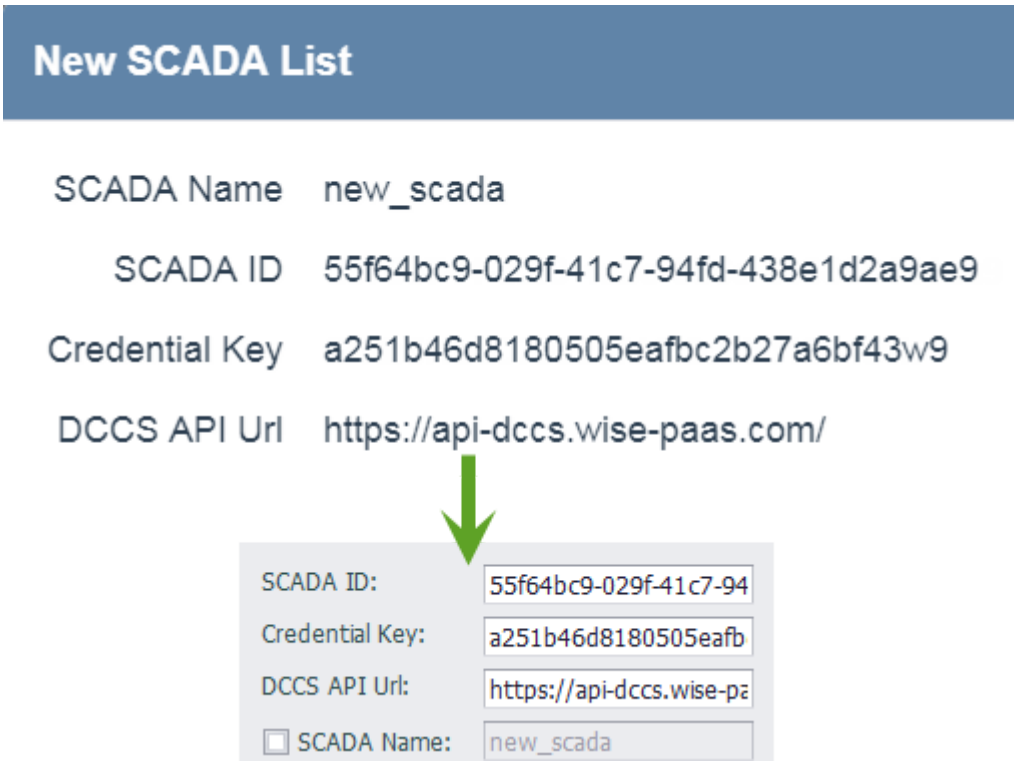
resume

export/import

WISE-PaaS/DataHub

The WISE-PaaS/DataHub plug-in supports sending tag data to WISE-PaaS/DataHub cloud service. It supports device configuration data upload in Plug&Play, and does not support modifying device configuration from cloud.

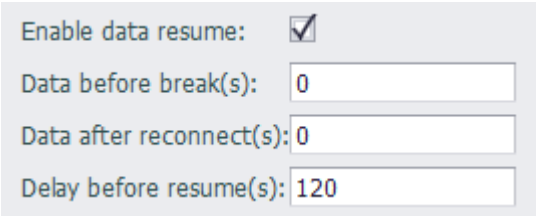
Because the WISE-PaaS/DataHub connection depends on the DCCS API to get the connection parameters, the basic connection parameters in the setting configuration will be ignored. Please copy and paste the `DataHub ID`, `Credential Key` and `DCCS API Url` generated on the website to the the corresponding field as following figure shows.



`SCADA Name` is optional. When not specified, the name of the gateway node configured in the project will be used.

WISE-PaaS/DataHub data uses a sub-device model to upload data. The name of the child device is distinguished by the colon (:) in the tag name or alias. The name before the colon is used as the child device name, and the name after the colon is used as the actual uploaded point name. If there is no colon in the name or alias, `SCADA Name` is used.

Data resume



- **Data before break(s)** :0(default) Cache the data n seconds before disconnection and send it to the server after reconnection
- **Data after reconnect(s)** :0(default) Cache the data n seconds after reconnection and send it to the server after reconnection
- **Delay before resume(s)** :120(default) Wait n seconds after reconnecting to the server before starting data transmission

Others

Tag List

resume

export/import

DeviceOn/BI

The DeviceOn/BI cloud service plugin is used to upload data to the DeviceOn/BI platform.

Because the DeviceOn/BI connection requires the DCCS API to get the connection parameters, the connection parameters in the basic configuration will be ignored. Simply copy and paste the `Gateway ID`, `Credential Key` and `DCCS API Url` generated on the website into the corresponding fields to complete the connection configuration.

`Gateway Name` is optional. When not specified, the name of the gateway node configured in the project will be used.

DeviceOn/BI data uses a sub-device model to upload data. The name of the child device is distinguished by the colon (:) number in the tag name or alias. The name before the colon will be the child device name, and the name after the colon will be the actual uploaded point name. If there is no colon in the name or alias, then `Gateway Name` will be used as the name of the child device.

Others

Tag List

resume

export/import

ThingsBoard

ThingsBoard is an open-source Internet of Things platform for data collection, processing, visualization, and device management. It supports device connectivity through protocols such as MQTT, CoAP, and HTTP, and offers both cloud and on-premise deployment options.

Others

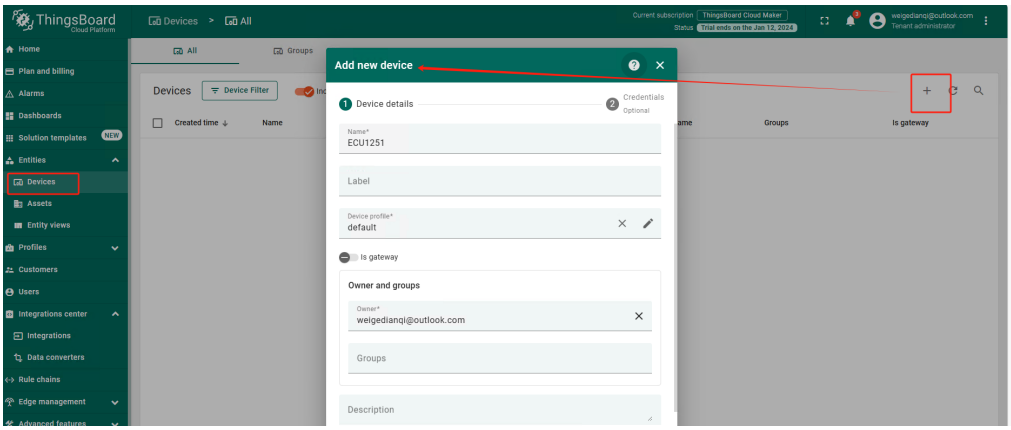
Tag List

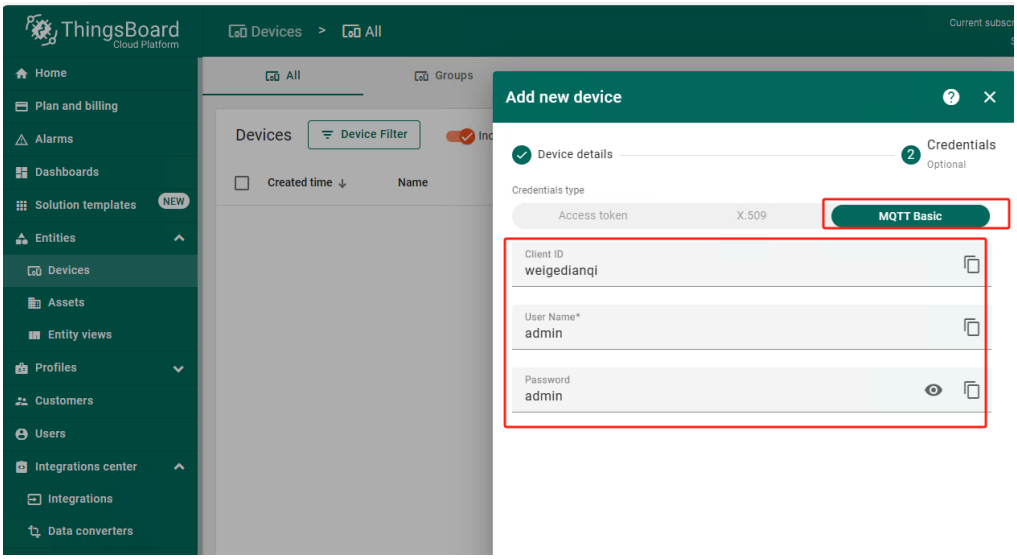
resume

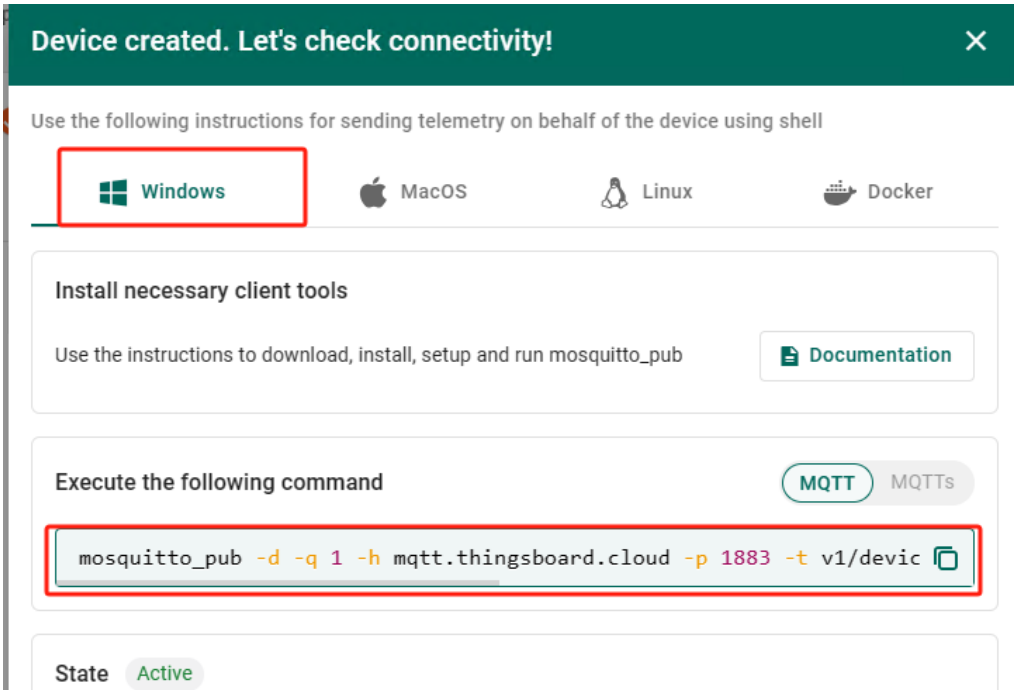
export/import

Steps:

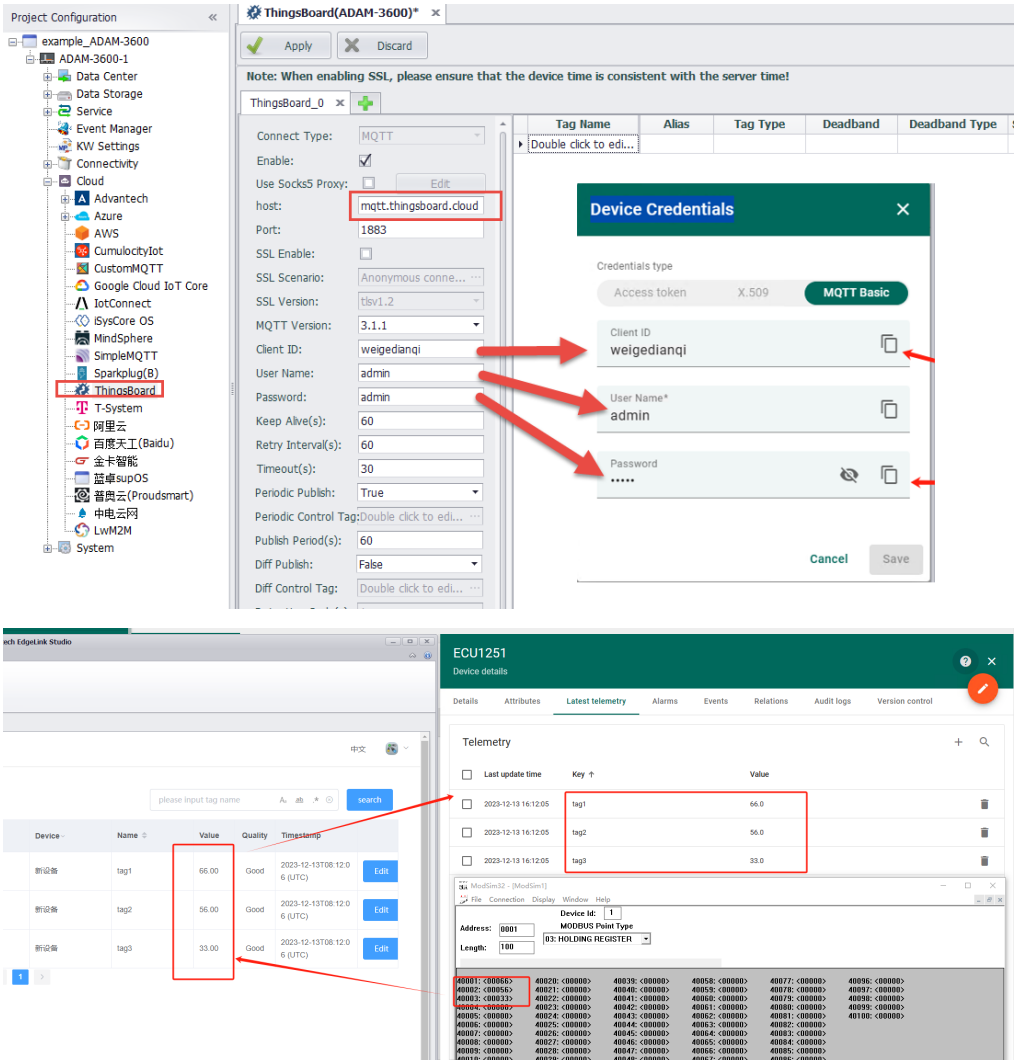
1. Log in to the ThingsBoard server and create a gateway device







2. Connect to ThingsBoard


Project Configuration
example_ADAM-3600
ADAM-3600-1
Data Center
Data Storage
Service
Event Manager
KW Settings
Connectivity
Cloud
Advantech
Azure
AWS
CumulocityIot
CustomMQTT
Google Cloud IoT Core
IotConnect
iSysCore OS
MindSphere
SimpleMQTT
Sparkplug(B)
ThingsBoard
T-System
阿里云
百度天工(Baidu)
金卡智能
蓝卓supOS
普奥云(Proudsmart)
中电云网
LwM2M
System
ThingsBoard(ADAM-3600)*
Apply
Discard
Note: When enabling SSL, please ensure that the device time is consistent with the server time!
ThingsBoard_0
Connect Type: MQTT
Enable:
Use Socks5 Proxy:
host: mqtt.thingsboard.cloud
Port: 1883
SSL Enable:
SSL Scenario: Anonymous conne...
SSL Version: tlsv1.2
MQTT Version: 3.1.1
Client ID: weigedianqi
User Name: admin
Password: admin
Keep Alive(s): 60
Retry Interval(s): 60
Timeout(s): 30
Periodic Publish: True
Periodic Control Tag: Double click to edi...
Publish Period(s): 60
Diff Publish: False
Diff Control Tag: Double click to edi...
Tag Name
Alias
Tag Type
Deadband
Deadband Type
Double click to edi...
Device Credentials
Credentials type
Access token
X.509
MQTT Basic
Client ID
weigedianqi
User Name*
admin
Password
Cancel
Save

ECU1251
Device details
Details
Attributes
Latest telemetry
Alarms
Events
Relations
Audit logs
Version control
Telemetry
Last update time
Key
Value
2023-12-13 16:12:05 tag1 66.0
2023-12-13 16:12:05 tag2 56.0
2023-12-13 16:12:05 tag3 33.0
search
Device
Name
Value
Quality
Timestamp
Edit
Device Id: 1
Address: 0001
Length: 100
MODBUS Point Type
03: HOLDING REGISTER

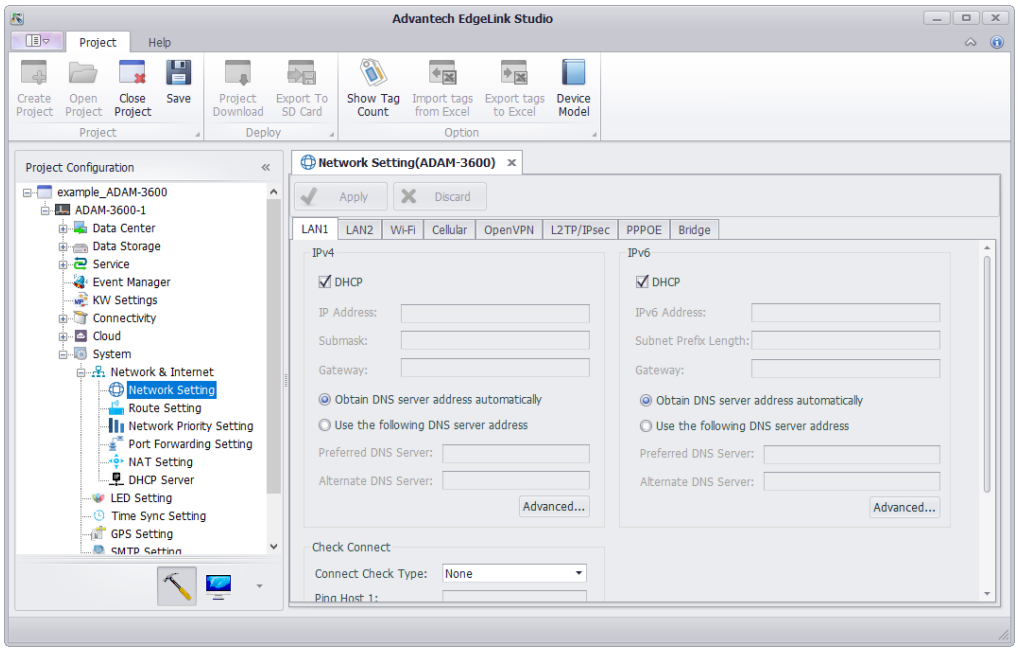
System Setting

System configuration in Advantech EdgeLink Studio includes network, LED, Time Sync, GPS, SMTP and Firewall setting.

Network and Internet

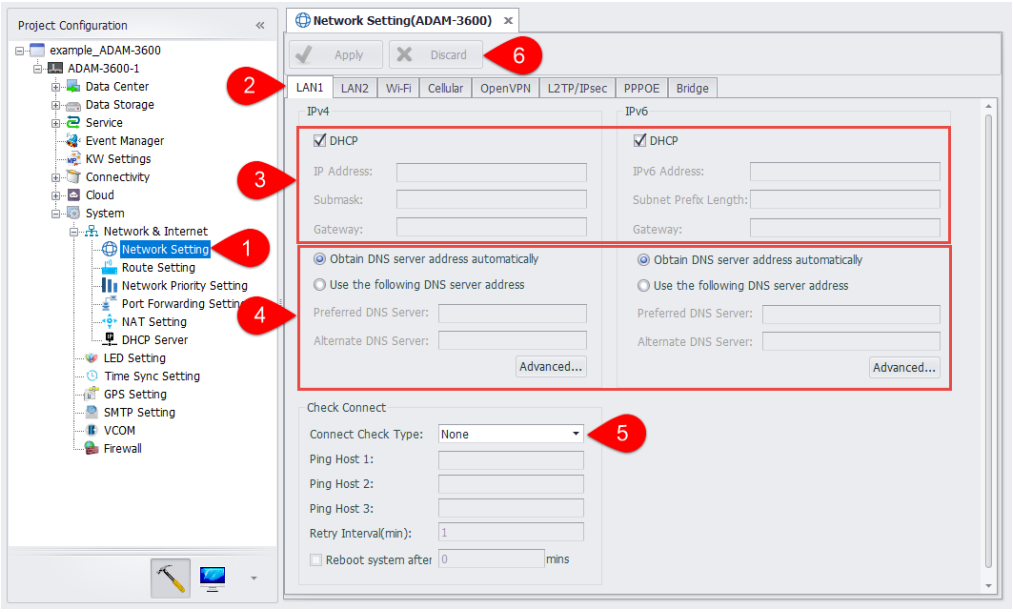
Network Settings

EdgeLink supports two network methods to achieve RTU communication with other devices, namely wired Ethernet transmission and wireless transmission. These two methods can be configured in EdgeLink Studio. In addition, it also includes settings for multiple network environments such as OpenVPN, L2TP / Ipsec, PPPOE, and bridging.

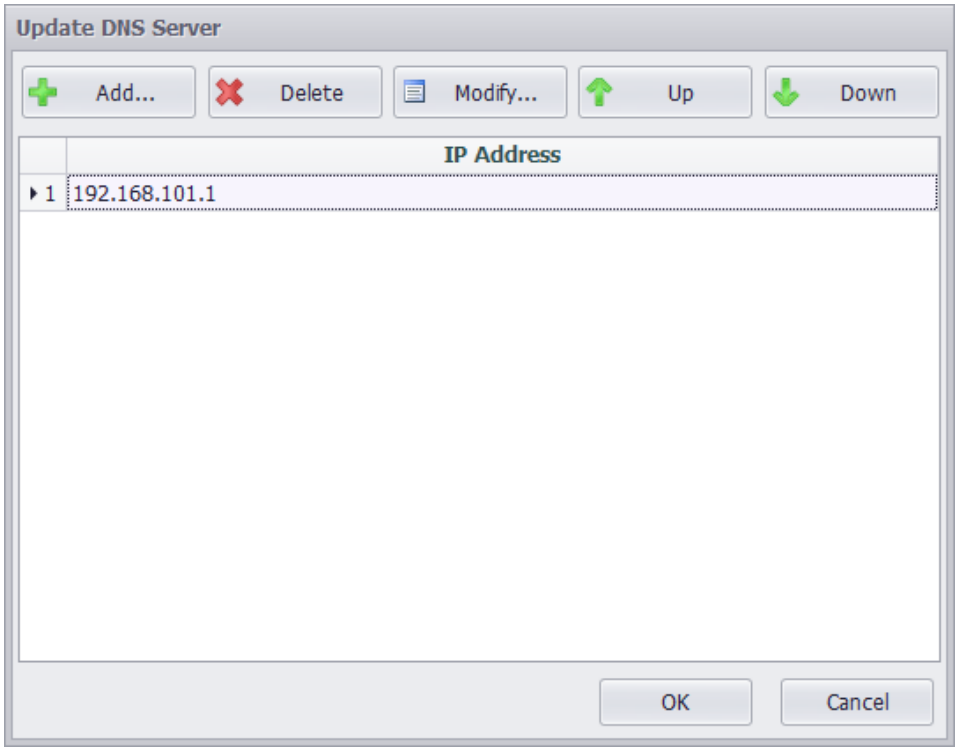


Wired Network Settings

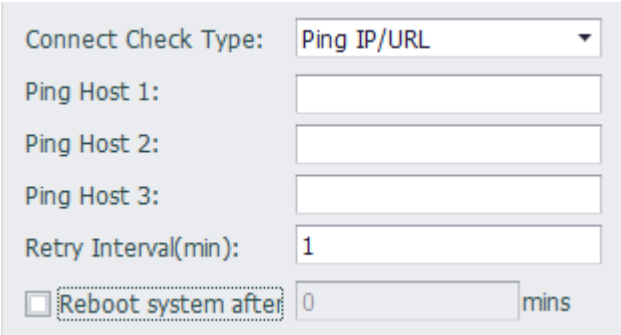
EdgeLink has two Ethernet ports, which can be configured to support IPv4 and IPv6 network modes under the Ethernet network. In both modes, the user can set the RTU to DHCP or fixed IP.



1. Open the “System Settings”-“Network and Internet”-“Network Settings” page.
2. Select to set a wired network information.
3. Check DHCP or uncheck, and write fixed IP information.
4. DNS settings. When selecting “Use the following DNS server address”, in addition to entering “Preferred DNS server” and “Alternate DNS server”, you can click the “Advanced” button to maintain more DNS information in the new window, including adding, deleting, modifying, and sorting. The top DNS server will be used first.



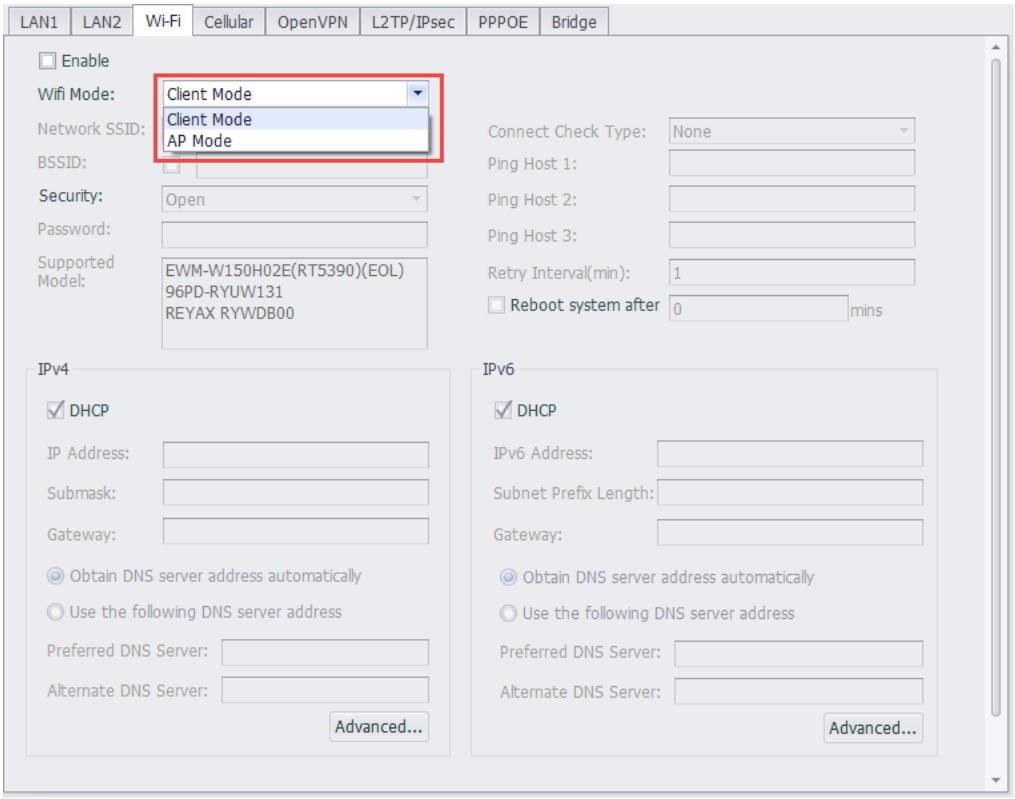
5. Set the network to check the connection information.Users can use the Ping IP / URL mode for network inspection, which requires the user to enter at least one ping target address. RTU will ping these destination addresses every once in a while. If you need to restart the RTU after judging that the connection is disconnected, you can check “Restart Device”, and the RTU will restart after a period of disconnection.



6. Click apply to complete the configuration.

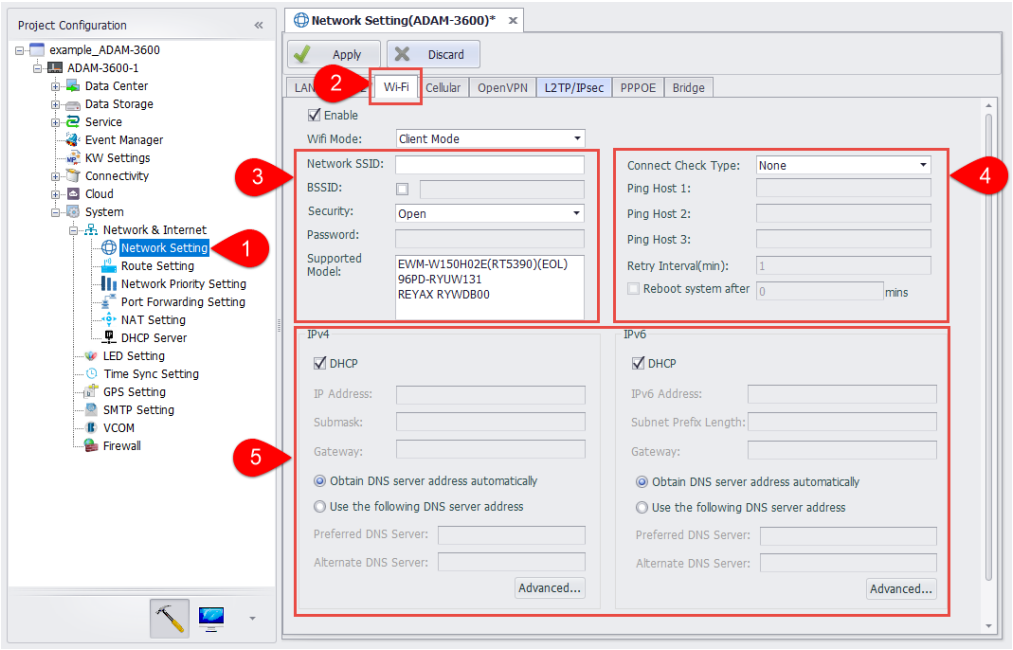
Wifi Network Settings

Wifi network supports two modes: client mode and AP mode, which can be set separately on the Wifi network setting interface.



Client Mode

Similar to the Ethernet port, the Wifi network client mode also supports IPv4 and IPv6 network mode settings. In these two modes, users can set the RTU to DHCP mode or fixed IP mode.



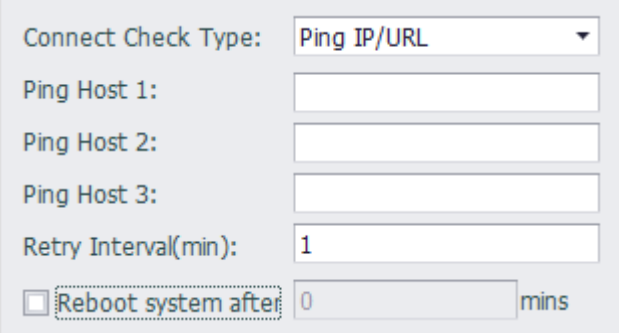
1. Open the “System Settings”-“Network and Internet”-“Network Settings” page.
2. Select to set Wifi network information.
3. Users need to set the SSID name and security of the WLAN to join the network. There are 3 optional security modes for the network:
    1. Open：LAN is open. Users can enter the LAN without a password.
    2. WEP: A type of authentication that encrypts the LAN and requires a password.
    3. WPA/WPA2 PSK：A type of authentication that encrypts the LAN advanced and requires a password.

    If you need to set the function of using the WIFI through the “MAC” address binding, you need to

select the “BSSID” check box on the page, and enter the MAC address of the AP in the text box behind it.

In addition, the page lists the wireless module information supported by the system.

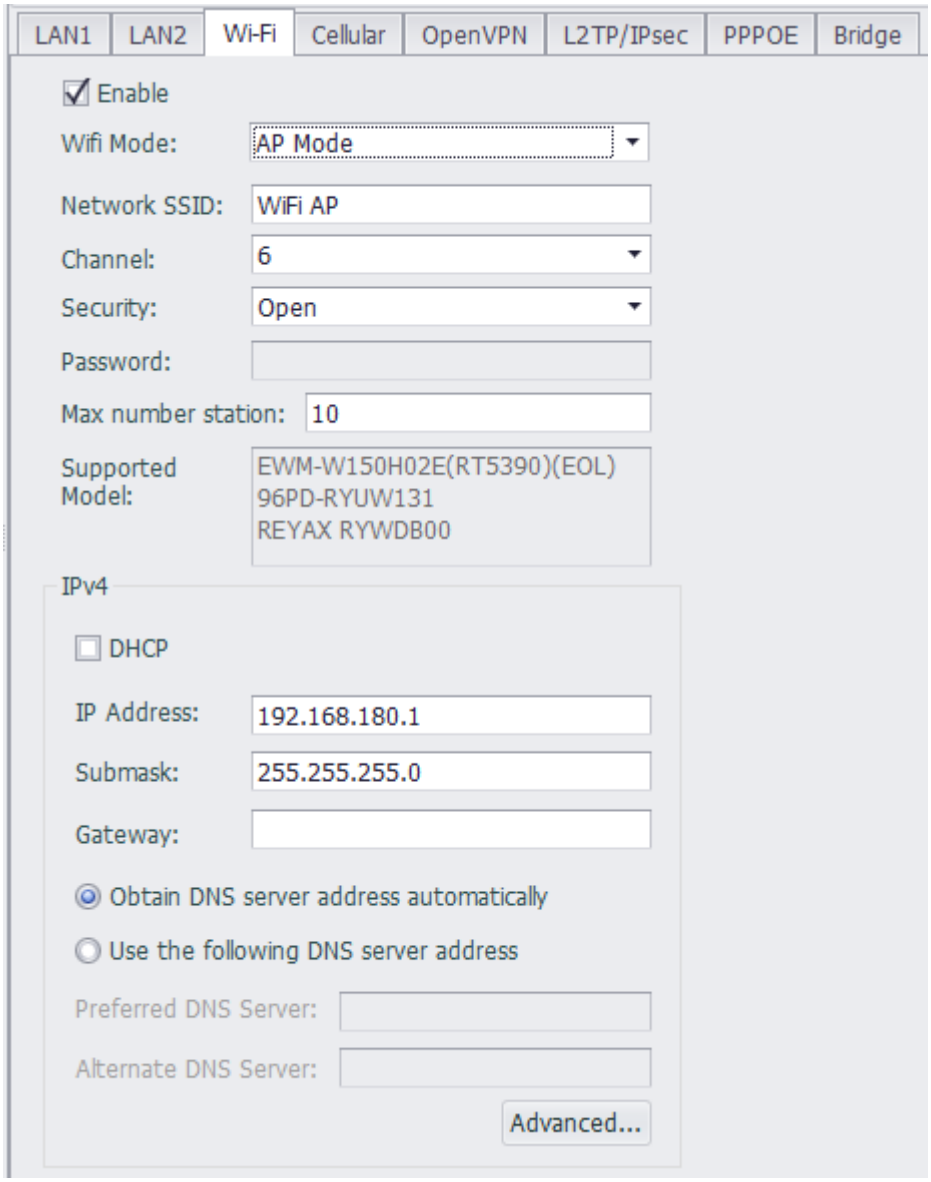
4. Set the network to check the connection information. Similar to the Ethernet port, you can use the Ping IP / URL mode for network inspection, which requires the user to enter at least one ping target address. RTU will ping these destination addresses every once in a while. If you need to restart the RTU after judging that the connection is disconnected, you can check “Restart Device”, and the RTU will restart after a period of disconnection.



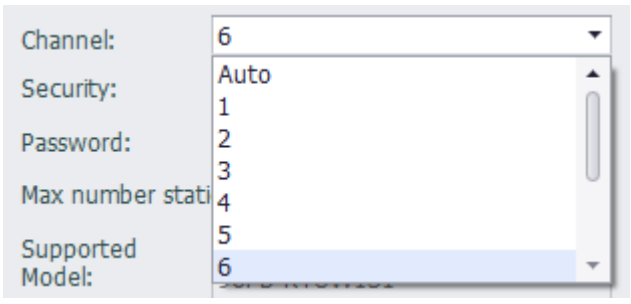
5. Similar to the Ethernet port, users need to check DHCP or not, write fixed IP information, and set the DNS information of the Wifi network.

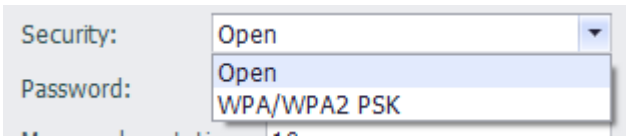
6. Click apply to complete the configuration.

AP Mode

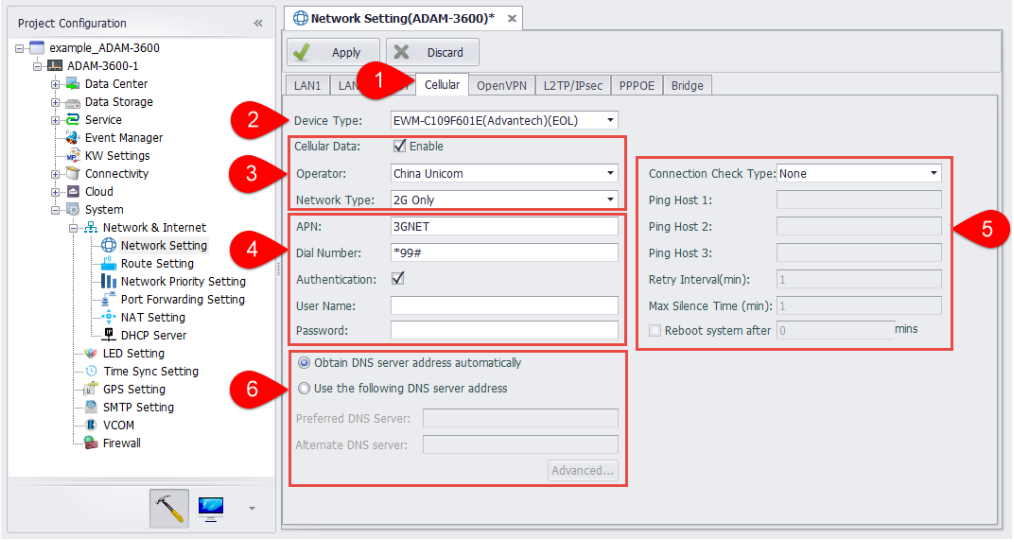


In wifi ap mode, users need to fill in the network SSID, channel, security, password, maximum number of sites, supported wireless modules, IPv4 information.

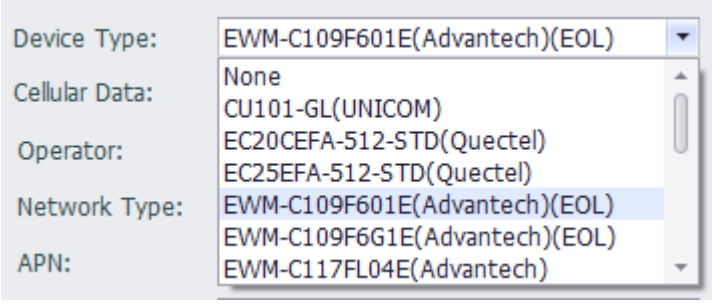




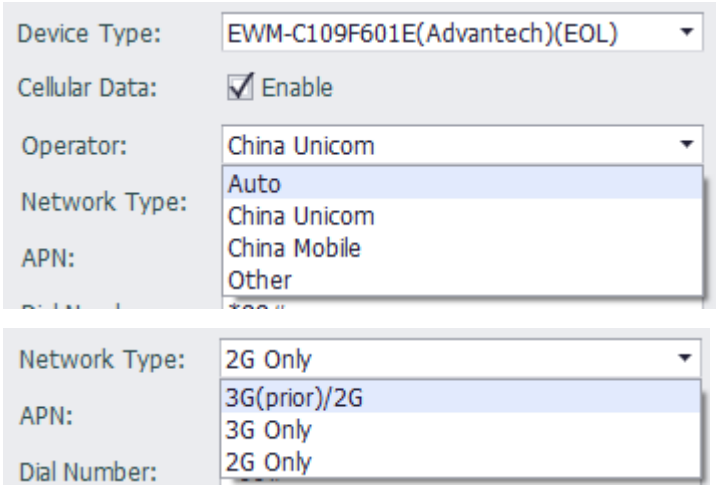
Cellular Network Settings



1. Open the “System Settings”-“Network and Internet”-“Network Settings” page, and select to set Cellular network information.
2. Select the type of wireless data terminal used, that is, the module name. During project compilation, different scripts will be generated according to different terminal types.

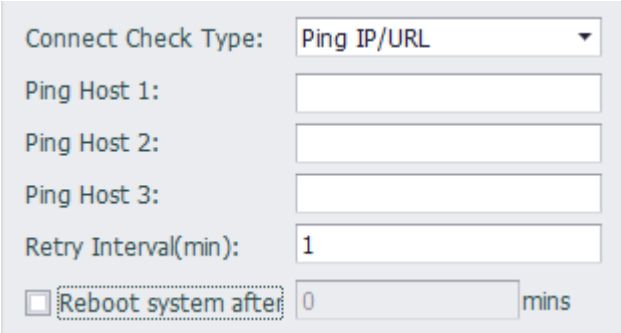


3. Check the “Enable Mobile Data” selection box to enable RTU’s GPRS function. Users can choose the operator supported by the wireless terminal, and can choose to connect to 2G, 3G, 4G mobile networks or wireless private networks.

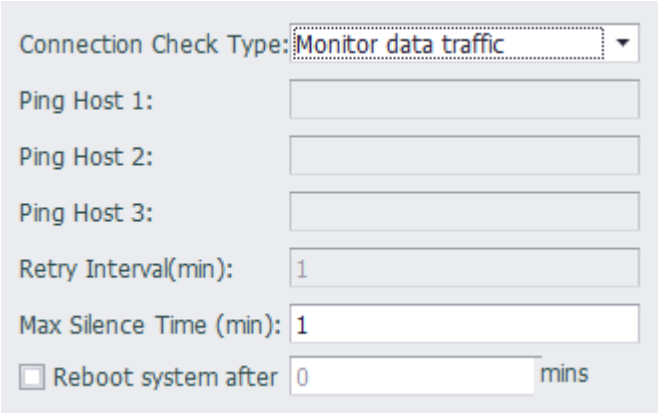


4. Among the operators supported by the wireless terminal, if the user selects “Auto”, the user does not need to enter the information such as APN, connection user name, password, and number; otherwise, the user needs to enter information such as APN, connection user name, password, and number. During project compilation, a set of scripts will be generated for each operator based on the default settings. EdgeLink will select the corresponding script to connect to the network according to the type of sim card inserted.
5. RTU provides two connection judgment mechanisms, Ping IP / URL mode and monitoring data communication mode.
    1. Ping IP / URL mode requires the user to enter at least one ping target address. RTU will ping these destination addresses every once in a while. If you need to restart the RTU after judging that the connection is disconnected, you can check

“Restart Device”, and the RTU will restart after a period of disconnection.



2. In monitoring data communication mode, RTU will monitor the data transmission. If the time for no data transmission exceeds the maximum silence time, the RTU will determine that the connection has been disconnected. If you need to restart the RTU after judging that the connection is disconnected, you can check “Restart Device”, and the RTU will restart after a period of disconnection.



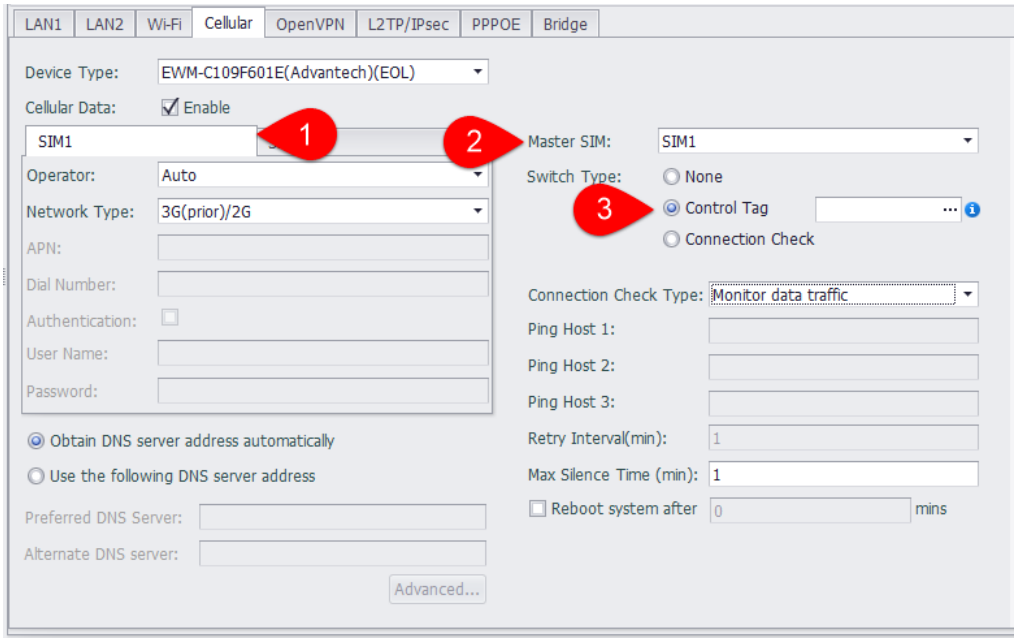
When setting the maximum silence time, please note that the maximum silence time should not be too long, otherwise it will affect the SIM card switching time. At the same time, when enabling “Restart Device”, it is recommended that the

maximum silence time is less than half of the time to restart the device.

6. Set DNS information of GPRS network.
7. Click apply to complete the configuration.

Dual Network Card Configuration

On ADAM-3600-D1GL1 and other devices with dual network card functions, in addition to the above basic settings, you need to configure settings such as dual network card switching mode.



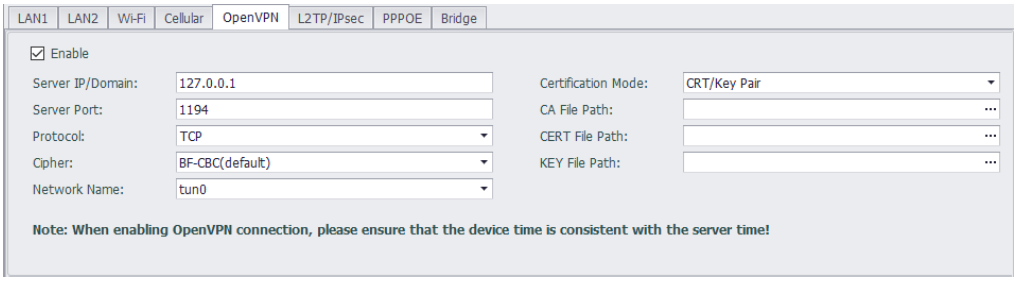
1. Two network cards can be configured with different operators and connection information.
2. Users need to select a network card as the default network card, and the device will connect to the default network card firstly when it starts.
3. Configure the switch mode of the network card

- No switching: No network card switching during operation
- Tag value control: Use the tag value to control the switch of the network card. When the value is 1, switch to the network card 1, and when the value is 2, switch to the network card 2.The rest will not be switched.
- Check the connection: Switch the network card according to the connection judgment mechanism, and switch the network card when the network connection fails.

OpenVPN Settings

OpenVPN can be set up to enable EdgeLink as a client to connect to the VPN server through a virtual private channel. OpenVPN is set in “System Settings”-“Network and Internet”-“Network Settings”-“OpenVPN”.

Basic Settings



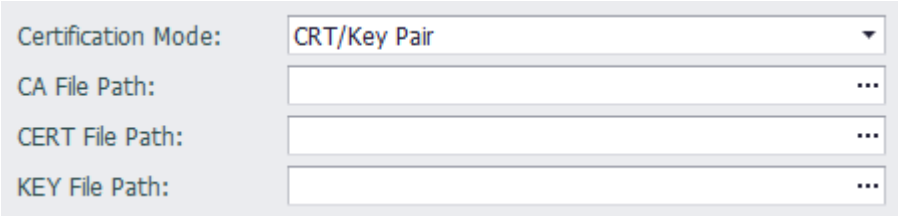
Due to the need to connect to the VPN server, the following attributes need to be configured:

1. Server IP or domain name.

2. The port number used by the VPN connection is 1194 by default.
3. The transmission protocol used can be TCP or UDP.
4. There are three encryption methods for transmission: FB-CBC, AES-128-CBC and DES-EDE3-CBC.

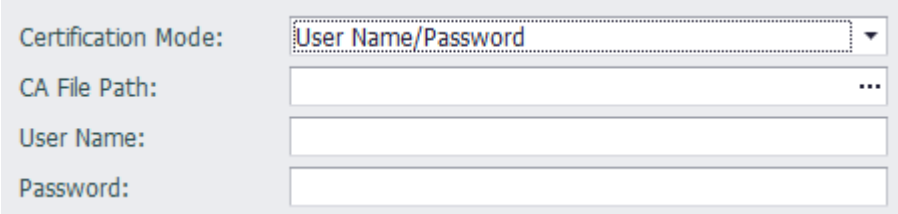
Authentication Mode-CRT / Key Pairing

EdgeLink supports two authentication modes: CRT / Key pairing and username / password.



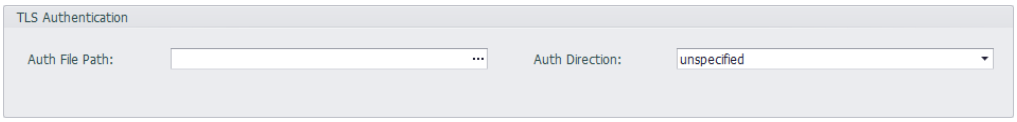
CRT / Key pairing requires the user to put the CA file, CERT file, and KEY file generated on the OpenVPN server on the computer where EdgeLink Studio is located. After loading this page, these three files will be downloaded to EdgeLink when the project is downloaded.

Authentication Mode-Username / Password



When using the user name and password to connect to the OpenVPN server, the CA file generated on the server is also required. It also requires the username and password assigned on the server.

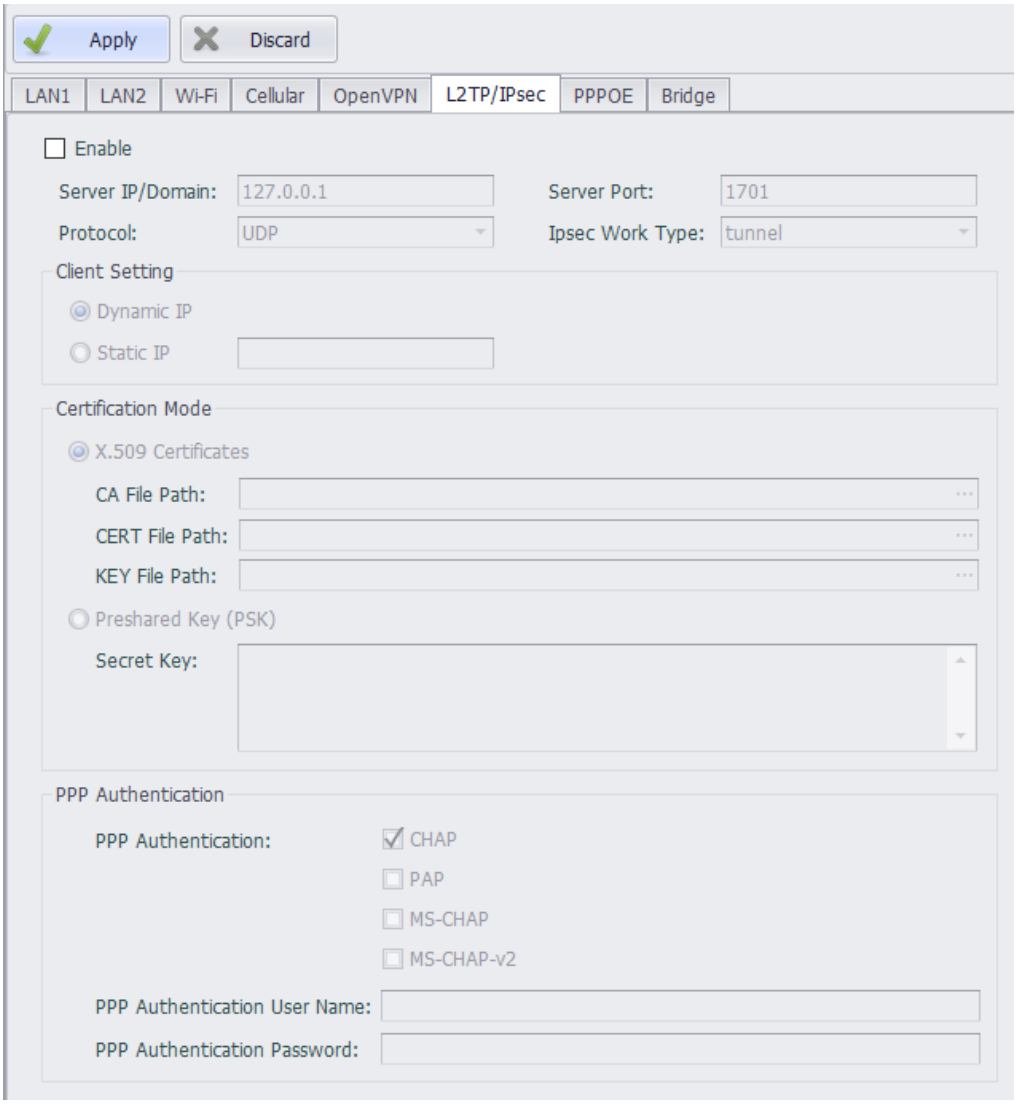
TLS Authentication



1. When the connected OpenVPN server requires TLS authentication, you can enter the path of the authentication file in the authentication file field to enable TLS identity authentication.
2. The value of the authentication direction should be complementary to the OpenVPN server. For example, when the server is “0”, the client should select “1”, or both ends should ignore this value.

L2TP/Ipsec Settings

L2TP / IPsec VPN can be set up to enable EdgeLink as a client to connect to the L2TP / IPsec VPN server through a virtual private channel. Set the L2TP / IPsec VPN in “System Settings”-“Network and Internet”-“Network Settings”-“L2TP / IPsec”.



Basic Settings

Due to the need to connect to the VPN server, users need to configure the following attributes:

1. Server IP or domain name.
2. The port number used by the VPN connection, the default is% any.
3. The transmission protocol used can be TCP or UDP.
4. Ipsec working mode can choose tunnel or transport.

Client Settings

Set the way the client obtains the IP address: Dynamic IP is automatically assigned by the system, and static IP is set by the user.

When setting a static IP, make sure that the corresponding settings on the server side are correct, otherwise you cannot connect.

Authentication Mode

EdgeLink supports two authentication modes: certificate authentication and PSK.

Certificate authentication

Users need to put the CA file, CERT file, and KEY file generated on the OpenVPN server on the computer where EdgeLink Studio is located. After loading this page, these three files will be downloaded to EdgeLink when the project is downloaded.

PSK

Enter the key for authentication.

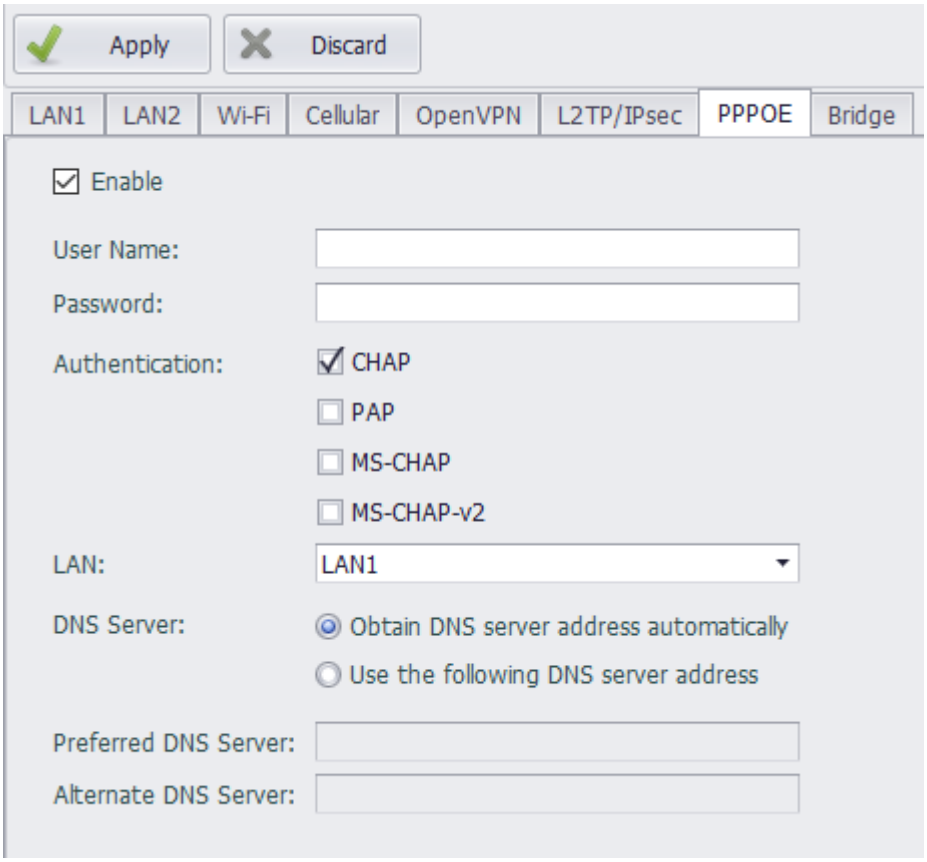
PPP Encryption Authentication

EdgeLink supports three PPP encryption authentication modes: no encryption, chap and pap.

When selecting chap and pap authentication, you need to enter the authentication user name and password. No input is required if you choose no encryption.

PPPOE Settings

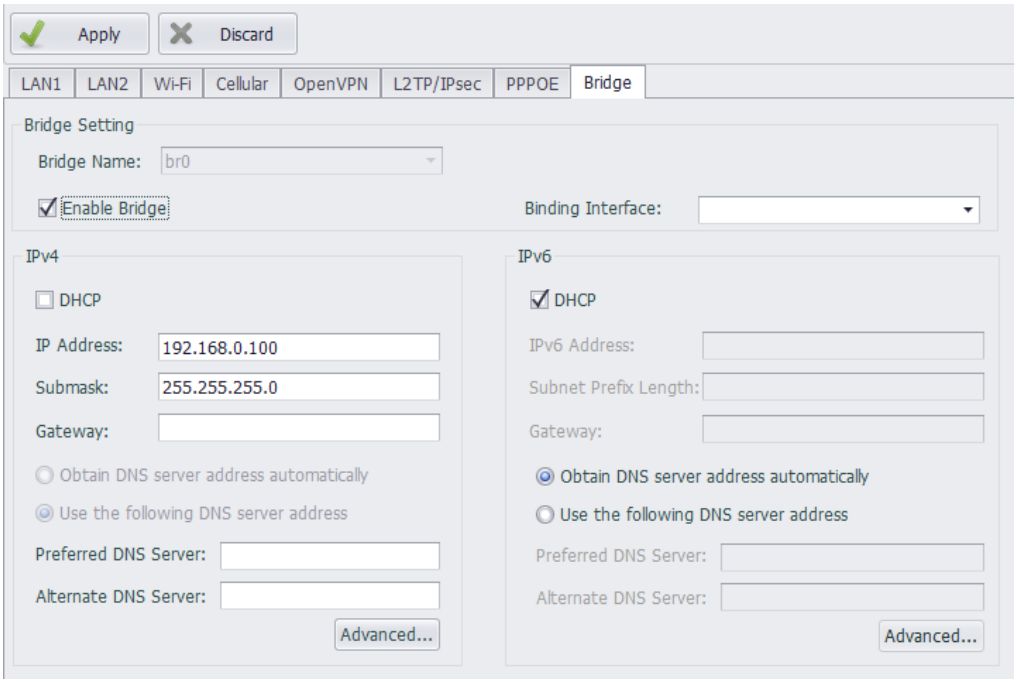
Through the PPPOE setting, the LAN port can be used as a WAN port for dial-up Internet access. Set PPPOE in “System Settings”-“Network and Internet”-“Network Settings”-“PPPOE”.



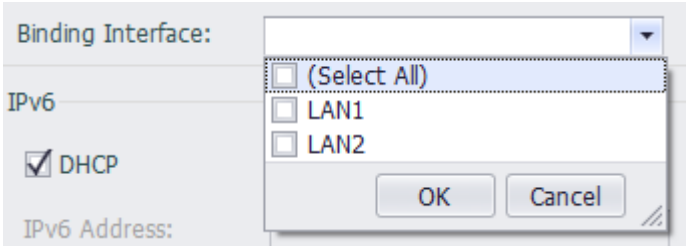
Users need to fill in the PPPOE user name and password, select the authentication method to use (multiple choices), the network port to be set, and set the DNS server information to complete the PPPOE setting.

Network Bridge Settings

Network card bridge setting is supported on EdgeLink non-UNO and WISE710 Linux platforms. Set the network card bridge settings in “System Settings”-“Network and Internet”-“Network Settings”-“Bridge”.

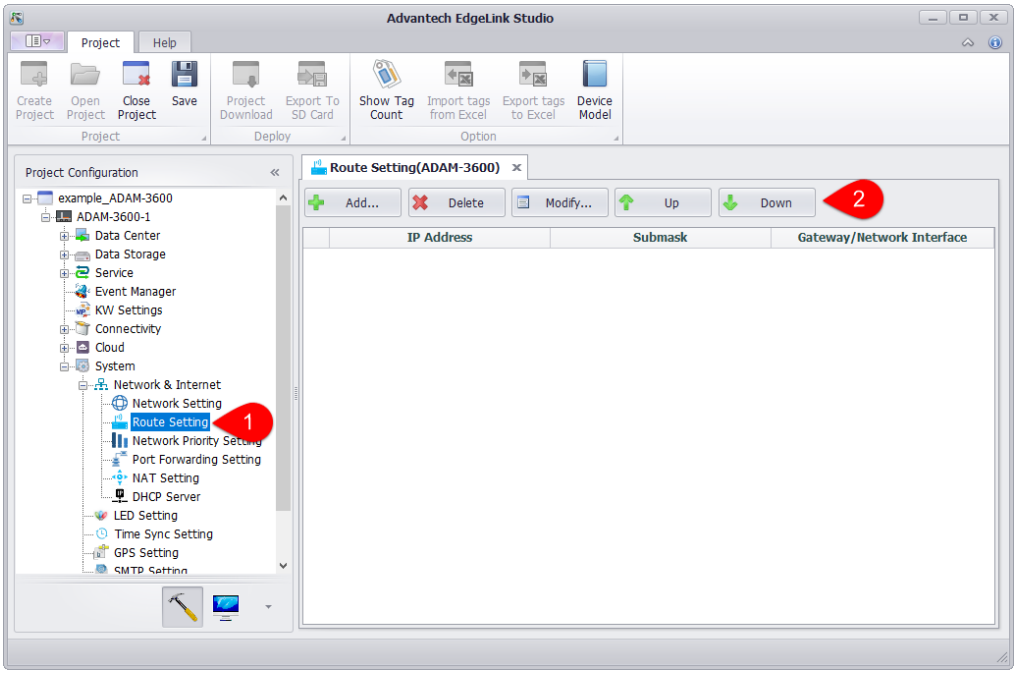


The user needs to check whether to enable the bridge and set the bridge-associated network port and IPv4 and IPv6 information to complete the bridge setup.

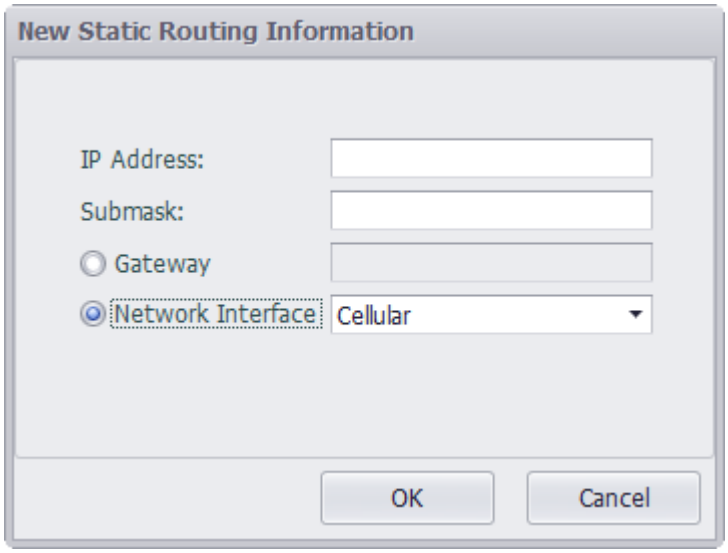


Route Settings

In the case where multiple network cards have a gateway configuration, the preferred routing address will be selected according to the routing sequence set by the route. In the route setting panel, users can add, delete, and modify routing information, and adjust the order of routing information.

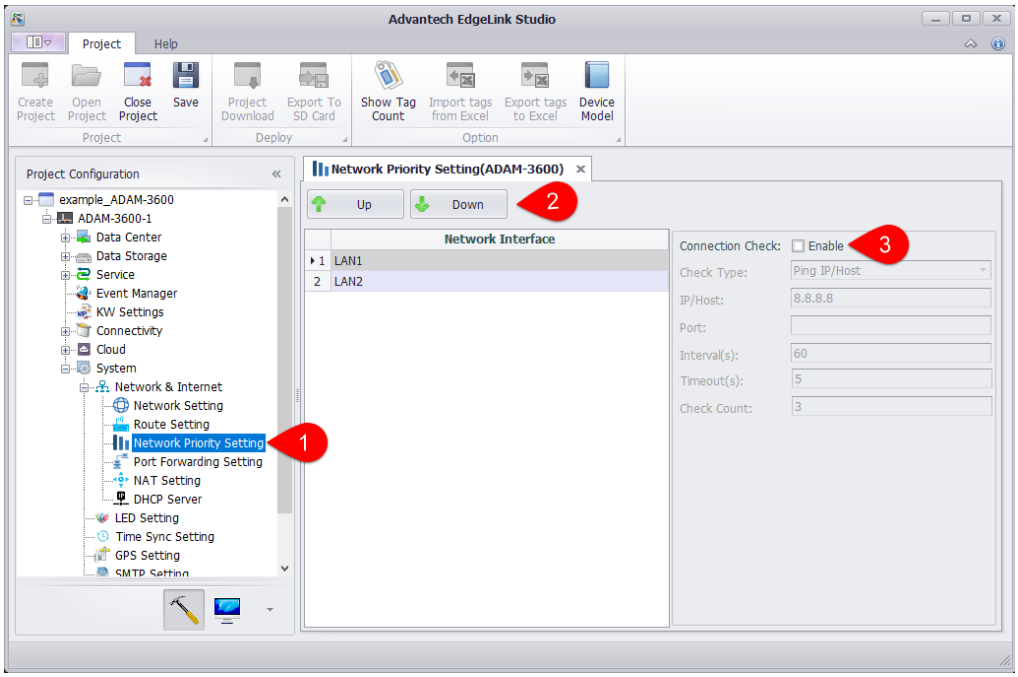


1. Users can add, delete, modify and sort routes on the “System Settings”-“Network and Internet”-“Route Settings” page.
2. Configure routing information. In the routing information editing window, the user can choose to set the gateway or network card.


New Static Routing Information
IP Address:
Submask:
Gateway
Network Interface
Cellular
OK
Cancel

Network Priority Settings

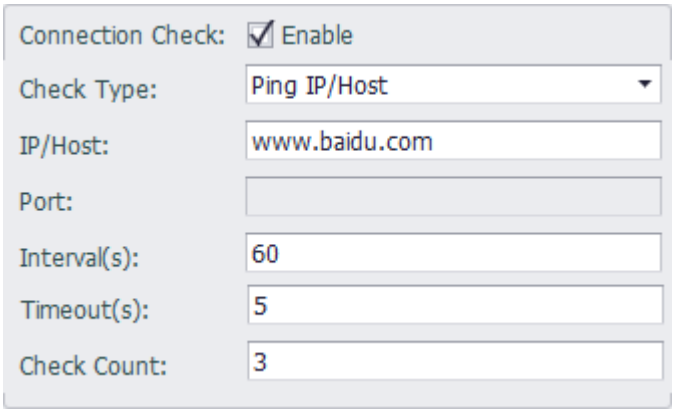
Users can configure the network priority, which is the priority of the default route. The network cards on existing devices are listed in the network priority setting panel, and users can click the sort button to sort.



1. Open the “System Settings”-“Network and Internet”-“Network Priority Settings” page.
2. Select the network card and click the “Move Up” or “Move Down” button to modify the network priority order.
3. Enable connection checking on the network.

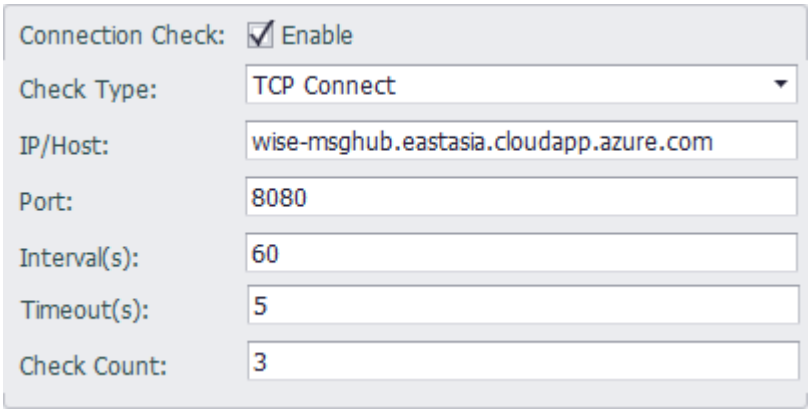
According to the network priority setting, when the high priority network is not available, it will switch to the second priority network and update the routing table;

when the high priority network is restored, switch back to the high priority network and update the routing table .



- Inspection method: Ping IP / Host means to check the network connection by ping, and TCP Connect means to specify the TCP port through TCP protocol connection.
- IP / HOST: Users can fill in IP or Domain. It is recommended to fill in the public network IP / HOST. When setting Domain, if the network card is fixed IP, the user must set up a DNS server.
- Port number: Only TCP Connect requires the port number. Please fill in the corresponding port number.
- Inspection interval: the inspection cycle, in seconds.
- Time-out time: Time-out time when the check fails, in seconds
- Number of inspections: Switch the network card after the inspection failure exceeds this value.

Some servers are not allowed to ping. In this case, users can select TCP Connect as the check method. Taking wise-paas as an example, users can set it as follows:

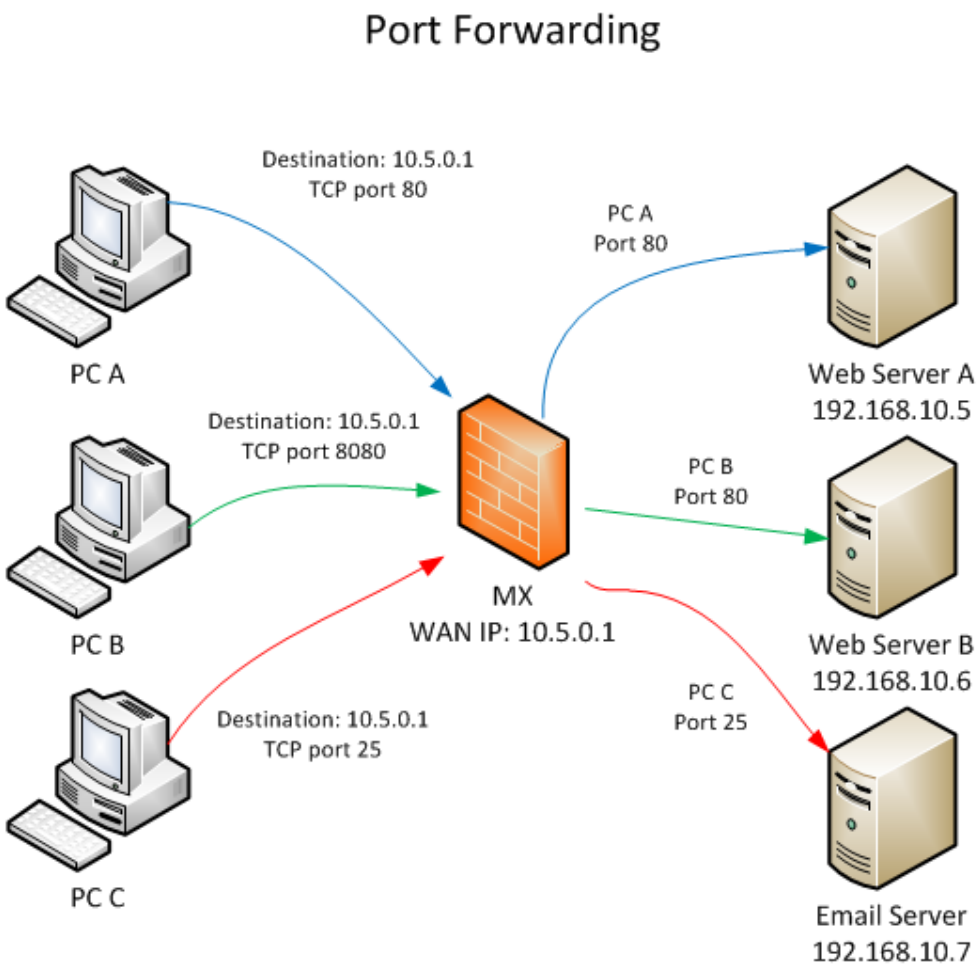

Connection Check:
Enable
Check Type:
TCP Connect
IP/Host:
wise-msghub.eastasia.cloudapp.azure.com
Port:
8080
Interval(s):
60
Timeout(s):
5
Check Count:
3

Gateway Function

When a device is used as a gateway, one network port is used to connect to the external network, and one or more network ports are connected to the internal network. EdgeLink supports port forwarding and NAT to help users manage the network more conveniently.

Port Forwarding

When a device is used as a gateway, the external network user cannot directly access the devices on the internal network. Users can set the mapping between the port of the external network port and the IP address of the internal network device by setting port forwarding on the router. That is, the gateway forwards the request to a specific port of the external network port of the gateway to the device of a specific IP address of the intranet through the intranet port, and the intranet device can be accessed by the external network.



As shown in the above figure, the device will forward the tcp request of port 80 with the external device IP of 10.5.0.1 to port 80 of the intranet device IP 192.168.10.5.

The device will forward the tcp request of port 8080 with the external device IP of 10.5.0.1 to port 80 of the intranet device IP 192.168.10.6.

The device will forward the tcp request of port 25 with the external device IP of 10.5.0.1 to port 80 of the intranet device IP 192.168.10.7.

The configuration in Studio is as follows:

Convert to iptables script as:

```
iptables -t nat -A PREROUTING -d 10.5.0.1 -p tcp --dpor
iptables -t nat -A PREROUTING -d 10.5.0.1 -p tcp --dpor
iptables -t nat -A PREROUTING -d 10.5.0.1 -p tcp --dpor
iptables -t nat -A POSTROUTING -j MASQUERADE
```

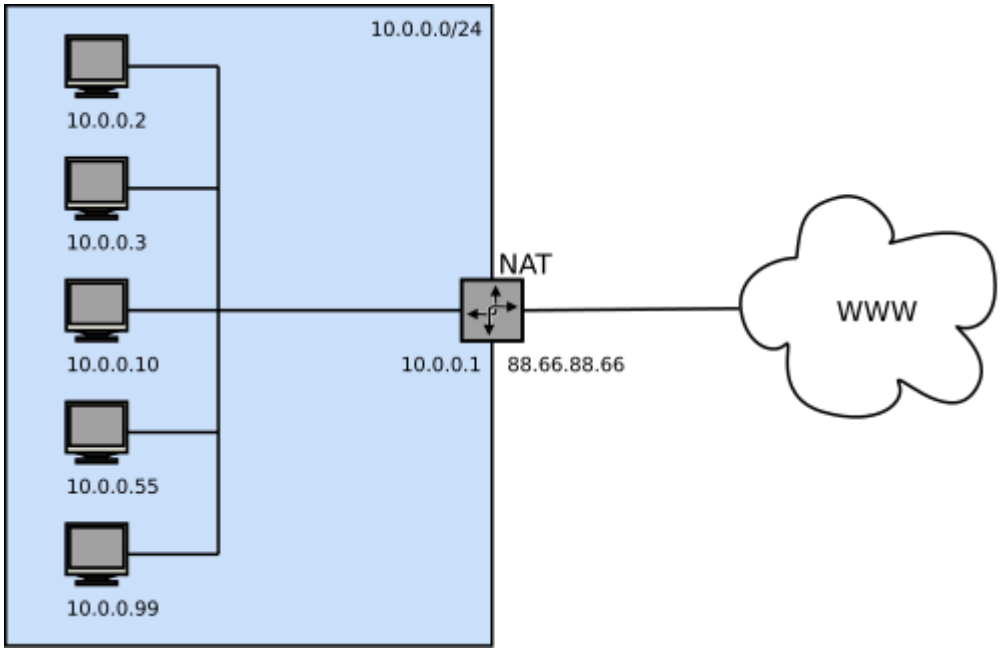
The attributes that users can configure are as follows:

- Enable: When you select Enable, this configuration will be added to forward.sh.
- Protocol: You can choose to support either TCP / UDP or both.
- External - Interface: Select to forward all access or only forward requests from specific network ports.
- External - IP Address: Select to forward only requests for specific IPs.

- External - Port: Set the port number to be forwarded, that is, the port requested by the external network.
- Internal - Dest IP Address: Set the IP address of the intranet device to be forwarded to.
- Internal - Dest Port: Set the port number of the intranet device to be forwarded to.

NAT Function

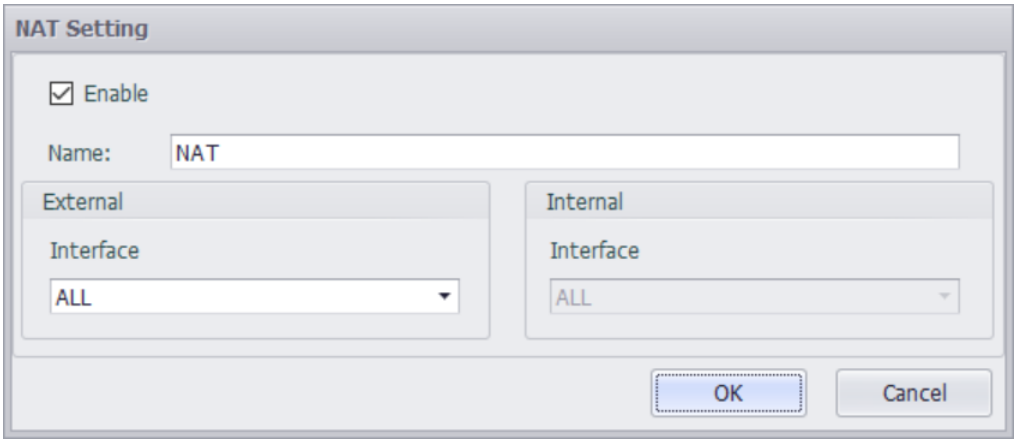
When using the device as a gateway, enable the NAT function to allow the intranet device to access the external network through the gateway.



Convert to iptables script as:

```
iptables -t nat -A POSTROUTING -j MASQUERADE -o eth0
```

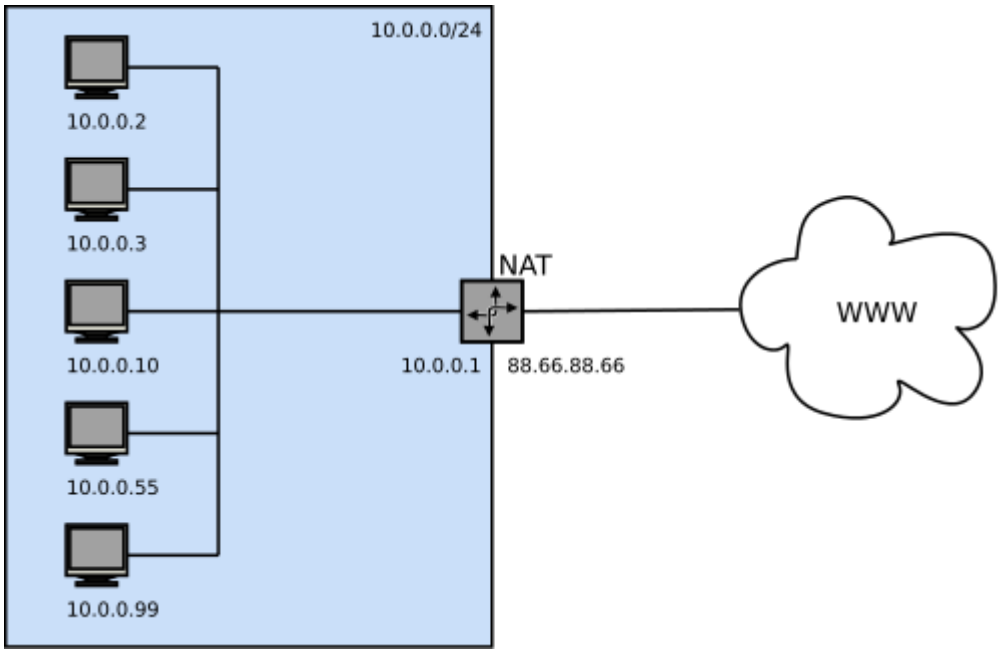
The attributes that users can configure are as follows:



- Enable: When you select Enable, this configuration will be added to nat.sh.
- Name: You can choose to support either TCP / UDP or both.
- External - Interface: Select to allow intranet devices to access the external network through a specific interface of the gateway, or access through all interfaces.

NAT Settings

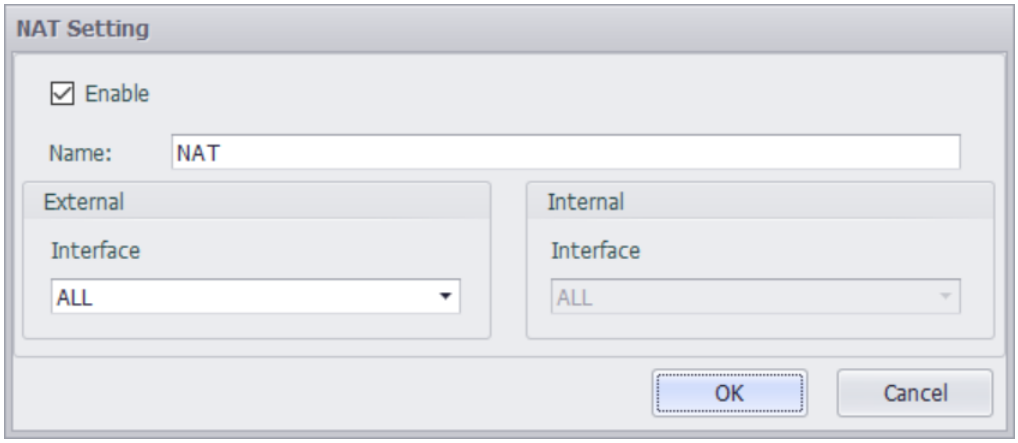
When using the device as a gateway, the NAT function is enabled to allow devices connected to the network card from the internal network to access the external network through the gateway.



Converted to iptables script as:

```
iptables -t nat -A POSTROUTING -j MASQUERADE -o eth0
```

The user can configure the properties as follows:

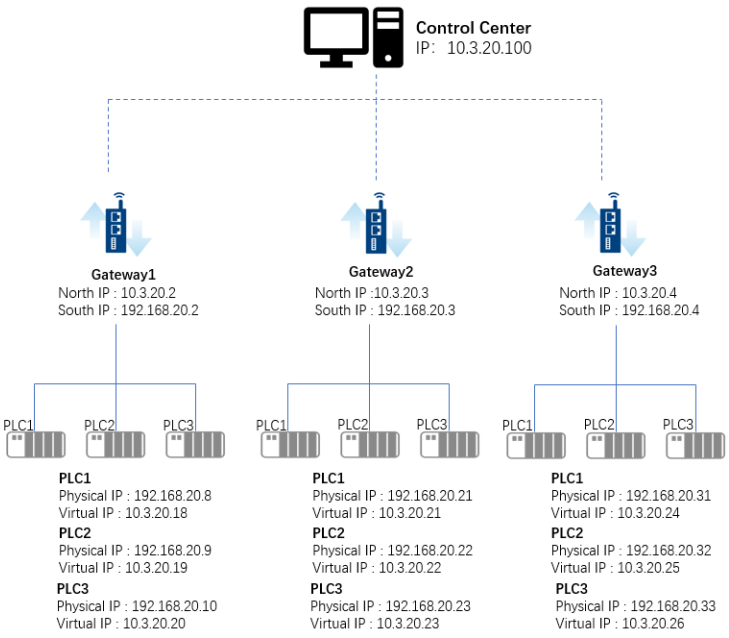


- Enabled: When enabled, this configuration will be added to nat.sh.
- Name: You can choose to support only TCP or UDP or both protocols.
- External network-network port: Select to allow the internal network device to access the external network through the specific network port of the gateway, or can access through all network ports.

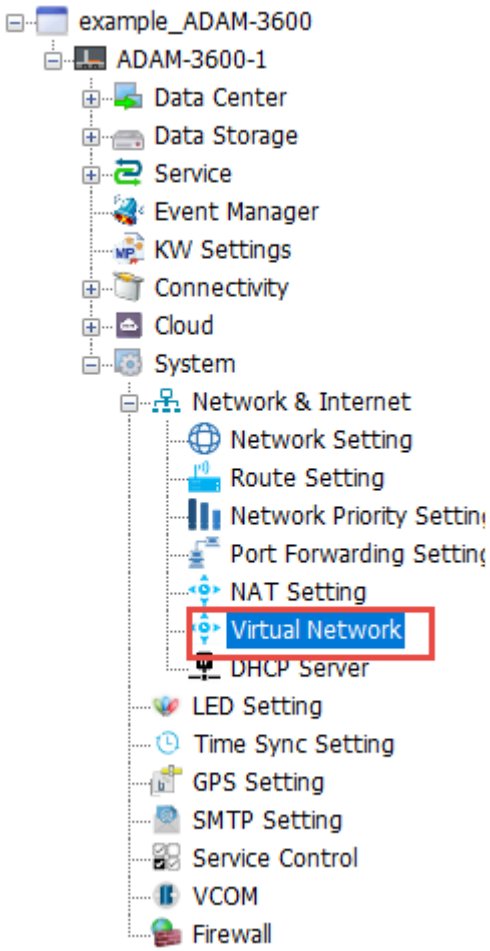
Virtual Network

Virtual network is used for remote operation and maintenance of PLCs. It establishes a network connection from the control center to the terminal PLC through configuration. That is, the control center and the PLC are set up in the same network through a virtual network.

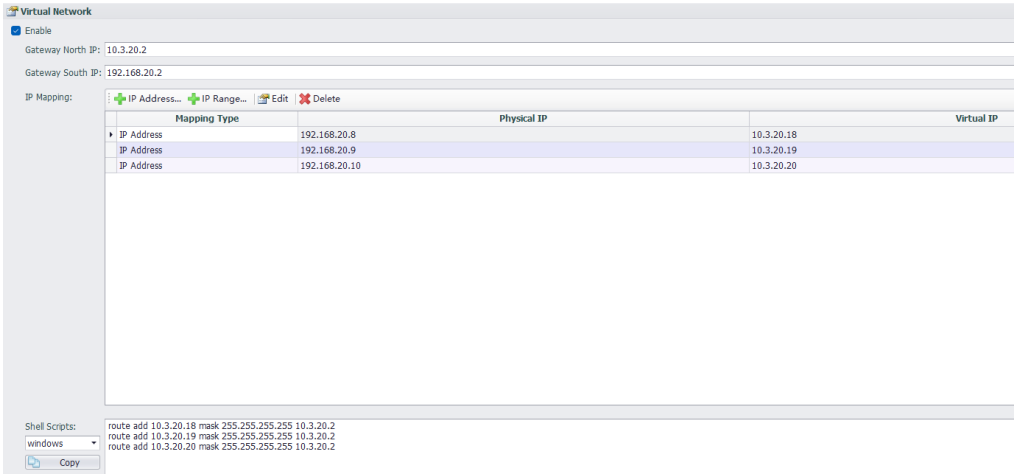
Step 1: First, plan the virtual IP network based on the physical connections and network environment on-site, as shown in the example below:



Step 2: Open the EdgeLink Studio project –> System –> Network and Internet –> Virtual Network

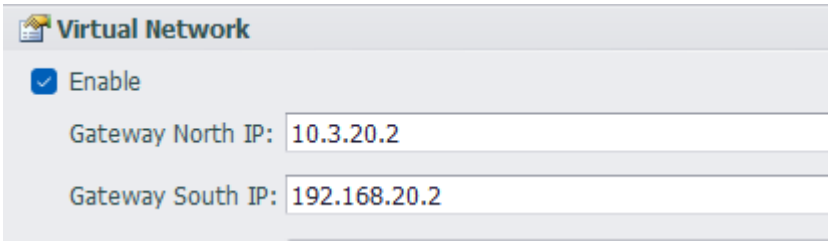


Step 3: Complete the configuration and download the project to the gateway



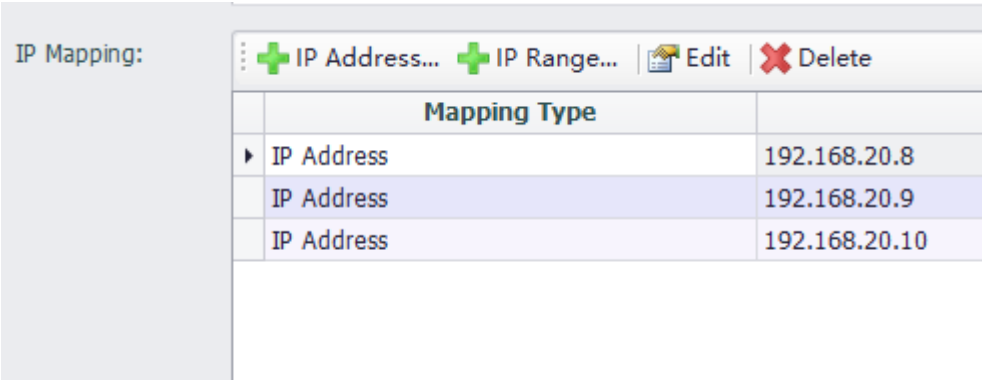
Parameter Description

Basic Configuration

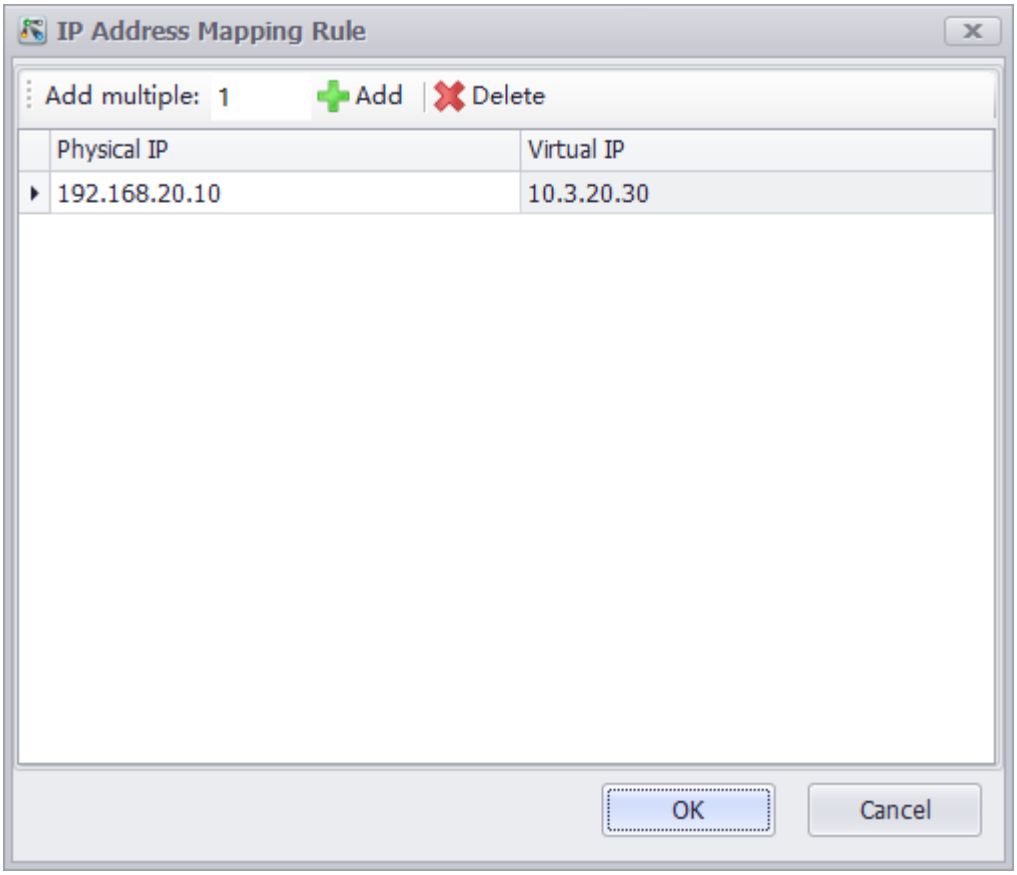


- Enable: Selecting enable will establish a virtual network according to the configuration.
- Gateway North IP: The network IP connecting the gateway to the control center.
- Gateway South IP: The network IP connecting the gateway to the southbound device.

IP Mapping Configuration



- IP Address Mapping: Add the mapping between physical IP and virtual IP (edit IP Address as you need).



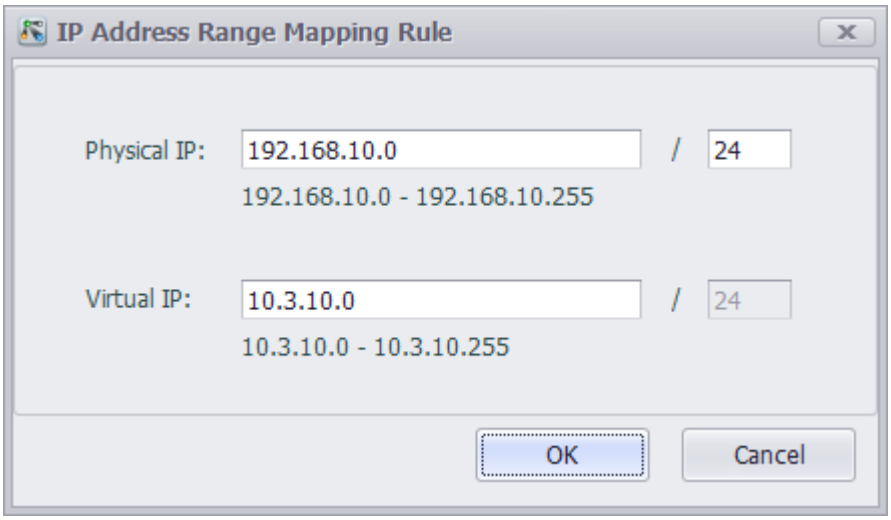
1. Click “Add” to add a mapping relationship.

2. After modifying the number of additions, click “Add” to add multiple mapping relationships at once.

3. Click “OK” to add the mapping relationships to the IP mapping table.

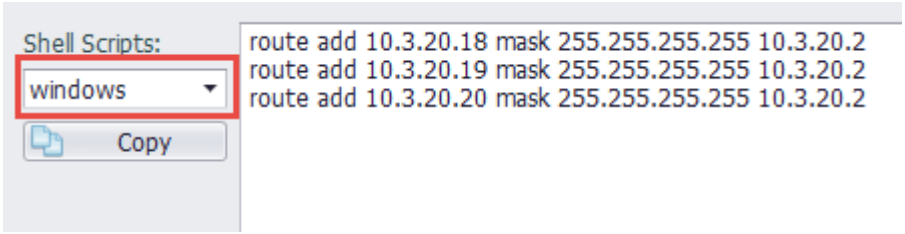
- IP Range Mapping: Edit the IP mapping range.

Edit the network segment and subnet mask bits of the physical IP and virtual IP to adjust the networking range.



- Edit: Edit and modify the IP address mapping rules.
- Delete: Select one or more IP address mappings and click “Delete” to delete them.

Control Center Configuration



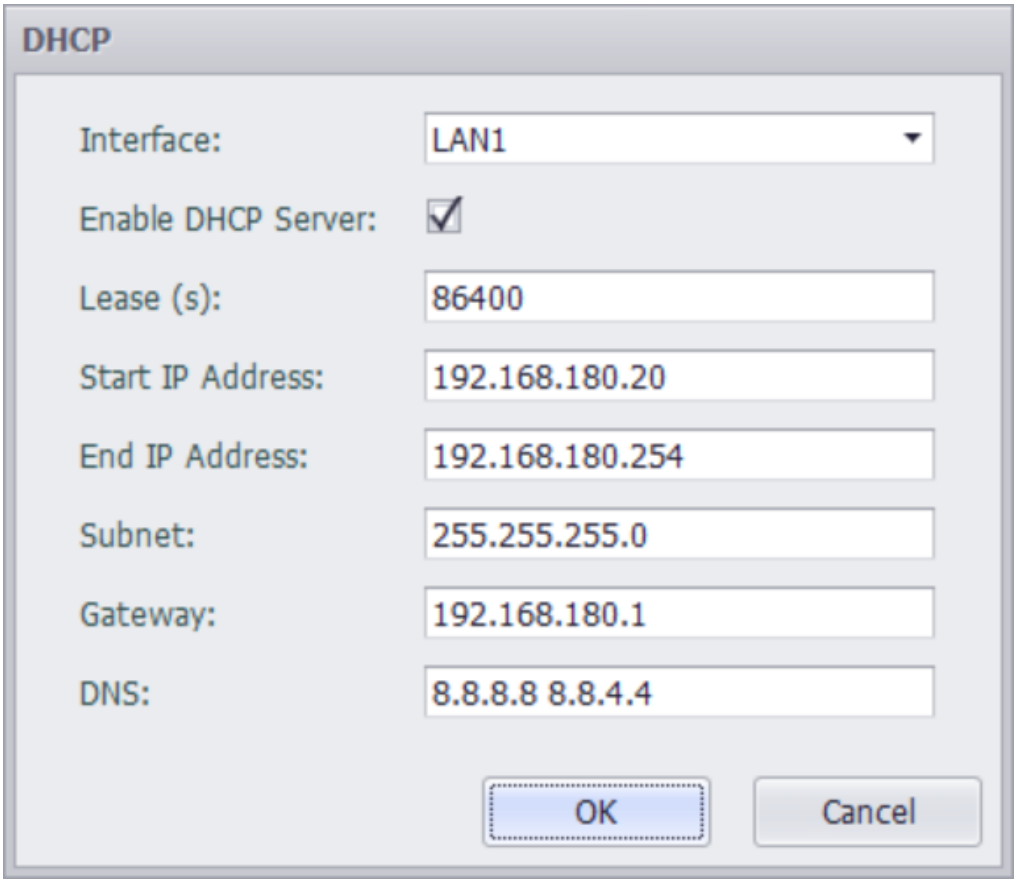
- The control center needs to add corresponding routes to implement the overall virtual networking application. Based on the IP mapping configuration, EdgeLink Studio automatically generates the corresponding control center route script (Windows and Linux versions). Copy this script to the control center computer and execute it on the command line.

DHCP Server Settings

DHCP (Dynamic Host Configuration Protocol) is a network protocol of a local area network. It refers to a range of IP addresses controlled by the server. When the client logs in to the server, it can automatically obtain the IP address and subnet mask assigned by the server. When the WIFI of this device is set to AP mode, users need to configure this service if they want the station connected to the AP to automatically obtain IP address and other related information.

Note: If you use this function on a fixed network card, please ensure that there is only one DHCP service in the whole LAN, otherwise it will cause abnormal IP allocation and make the entire LAN unable to work normally.

The user can configure the properties as follows:



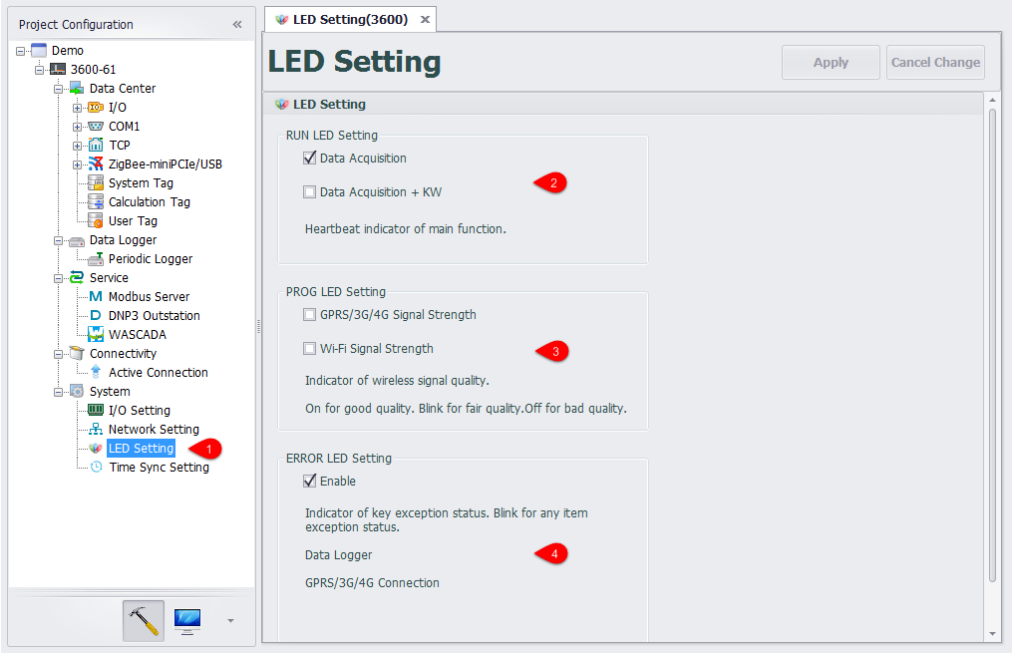
- Network port: Select to enable the DHCP Server function on a network port.
- Enable: Choose whether to enable this configuration.
- Lease time: The lease time of the DHCP server.
- Assign IP start address: Configure the start address of the range of IP addresses assigned by the DHCP server to clients.
- Assign IP end address: Configure the end address of the range of IP addresses assigned by the DHCP server to clients.
- Subnet mask: Configure the subnet mask assigned by the DHCP server to the client.
- Gateway: Configure the gateway assigned by DHCP Server to the client, generally the local IP of DHCP

Server.

- DNS: Configure the DNS address assigned by the DHCP Server to the client. Multiple DNS addresses are separated by spaces.

LED Setting

In this page, users can set the working modes of LED indicators on RTU, including RUN, PROG and ERROR.



1. In the navigation bar, double-click on “LED Setting” of “System Setting” to open the edit page.
2. In the RunLED selection box, you can choose whether the RUN is enabled.

The RUN LED monitors the data acquisition and KW function. When the RUN flickers, it indicates that the main program is running normally.

3. In the ProgLED selection box, you can select whether the PROG is enabled or not.

PROG lamp monitors the intensity of mobile signal or WIFI signal. The long light signal is good, the flicker signal is normal, and the signal is not bright.

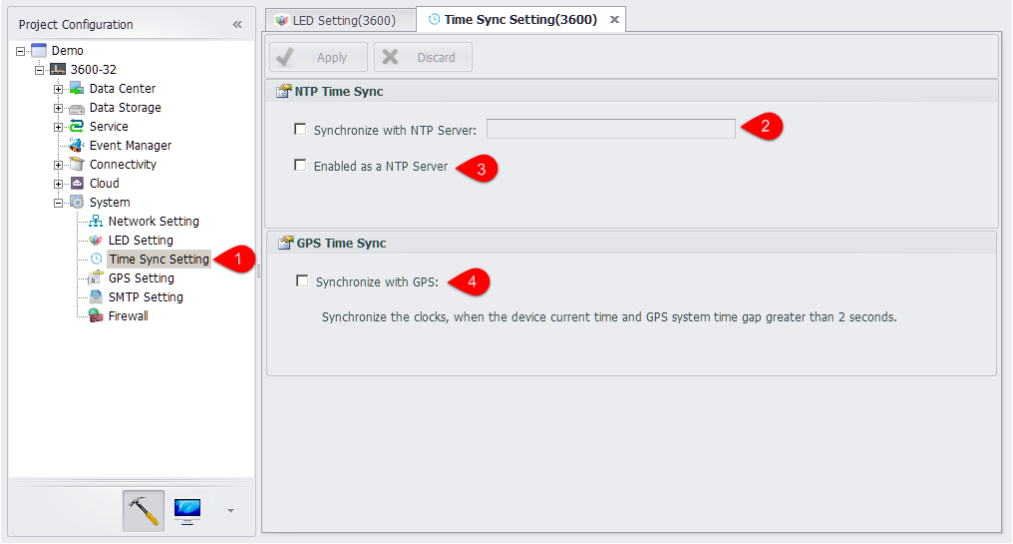
4. In the ErrorLED selection box, you can choose whether the ERROR lamp is enabled.

When it is enabled, it will monitor whether the key modules are connected properly. When a module is abnormal, the ERROR light will flash. The modules that can be monitored include data storage module, mobile module and WIFI module.

When it is not enabled, the ERROR light will not light up, and users can write their own programs to use this light.

Time Sync Setting

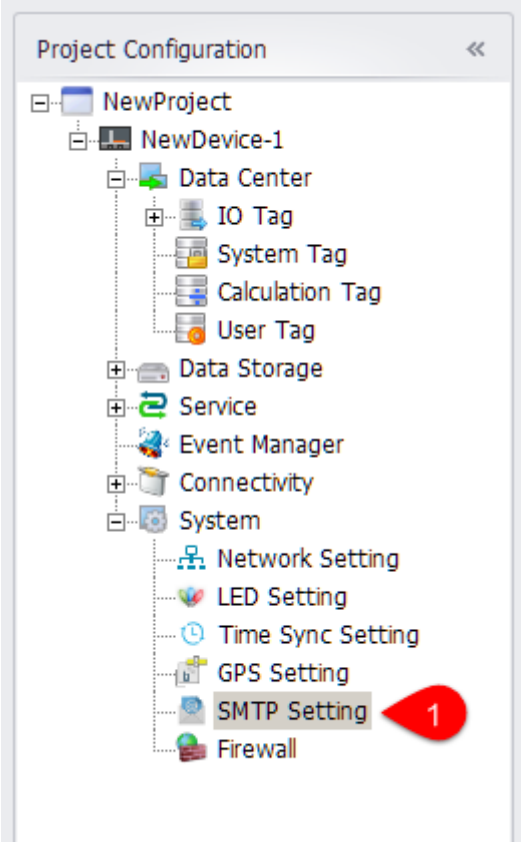
In this page, users can perform the time synchronization settings, making RTU time consistent with another time source. Meanwhile, users can also set RTU as a time synchronization source.



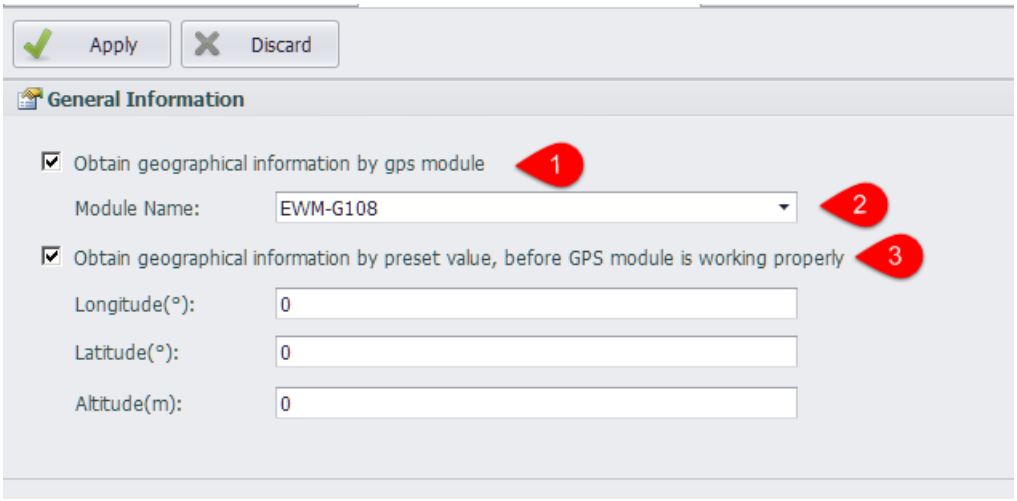
1. Double click the Time Sync Setting in the navigation bar to enter the configuration page.
2. The selection of “synchronization with the NTP server” allows the device to synchronize with a source, and the address of the source can be a domain name or a IP address.
3. Check “serve as a NTP server” to enable the device to be a time synchronization source and other devices to synchronize time with this device.
4. The user can choose to synchronize time through GPS.

GPS Settings

In the GPS settings, you can set the GPS module on RTU.

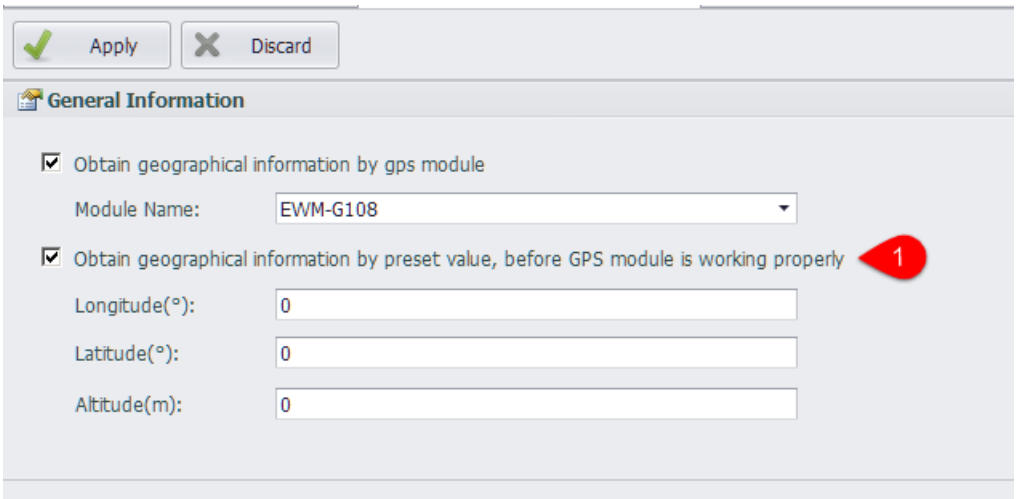


GPS Module



1. Enable: enable the GPS module acquisition function, RTU will collect real-time location information, speed and angle through the GPS module.
2. Module name: the GPS module type that can be selected. The program reads the module information from the configuration file .xml. When the module type is switched, the program sets the other properties as default values.
3. The preset latitude and altitude are used as the initial value before the GPS module works properly.
   Note! After the GPS module is working normally, if the unexpected situation occurs, such as: when the GPS module is pulled out and the GPS search star number is less than 3 stars, the longitude latitude and altitude value will be retained as the last normal value obtained when the position information is not available

GPS Default Mode



1. The user can choose not to use the GPS module, but the preset RTU location information. Users can also choose not to use preset location information, and GPSManager modules will not be started at RTU.

GPS System Tag

After the GPS function is enabled, location information will be stored in the system tag.

#GPS_LATITUDE	Analog	degrees	Latitude for the GPS module
#GPS_LONGITUDE	Analog	degrees	Longitude for the GPS module
#GPS_ALTITUDE	Analog	m	Altitude for the GPS module
#GPS_SPEED	Analog	knots	Speed for the GPS module
#GPS_COURSE	Analog	degrees	Course for the GPS module
#GPS_SATELLITE	Analog		Status of the GPS module: 0-error state, 1-use GPS module working, 2-use a preset location information

The current working state of the GPS module is saved in GPS_SATELLITE

- When the value is 0, the GPSManager module in RTU is not started, or GPSManager is in error mode.
- The GPS module works when the value is 1.
- When the value is 2, the default location information is used to set the GPS _LATITUDE, GPS _LONGITUDE, GPS _ALTITUDE, and the GPS_SPEED and GPS_COURSE values are 0.

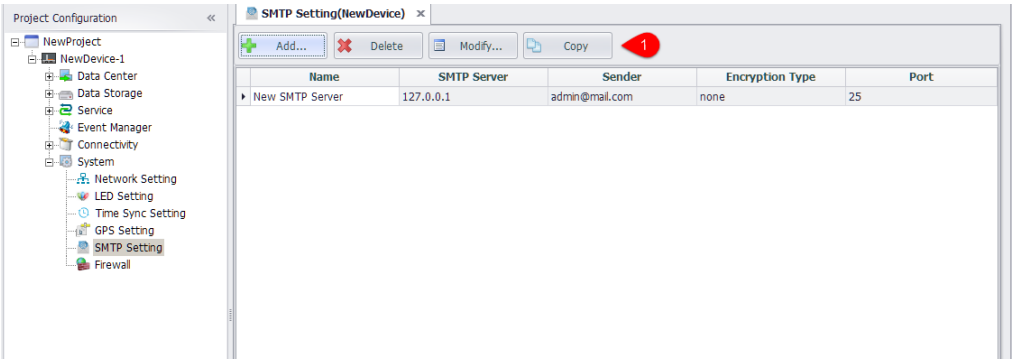
GPS Time Synchronization

After the GPS function is enabled, you can use GPS to synchronize RTU time

1. You can choose at most one time synchronization mode.
2. When the gap between the GPS time and the RTU time is greater than the “calibration interval”, the device time is synchronized with the GPS time.

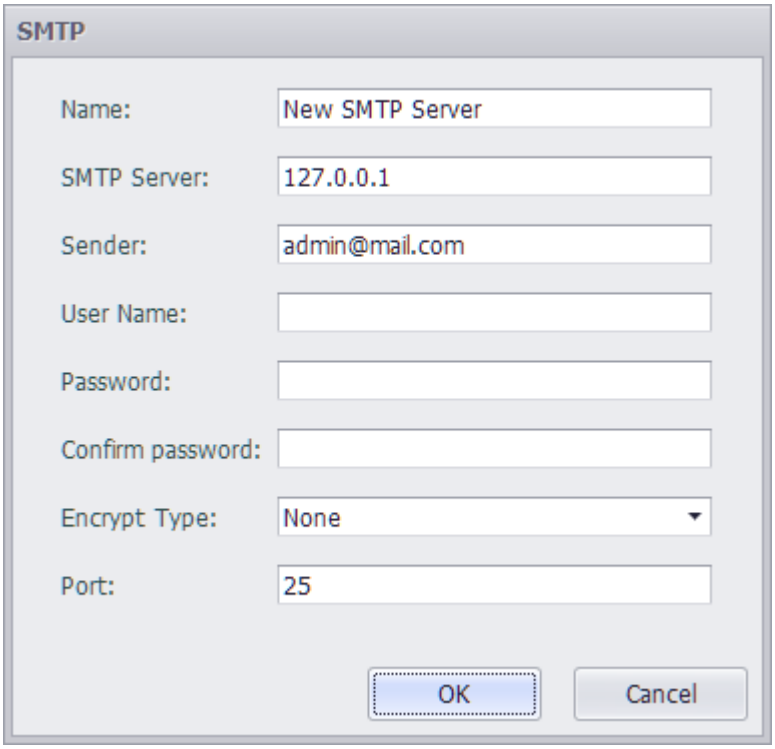
SMTP Settings

In event management, you need to set up SMTP before sending the time message by mail.



1. In the device -> system Settings ->SMTP Settings node double - click to open the edit interface.
2. Users can add, delete, modify SMTP, and copy existing SMTP settings.
3. The existing SMTP Settings are shown in the list, and double-clicking on the selected row can also open the edit interface

SMTP Editor



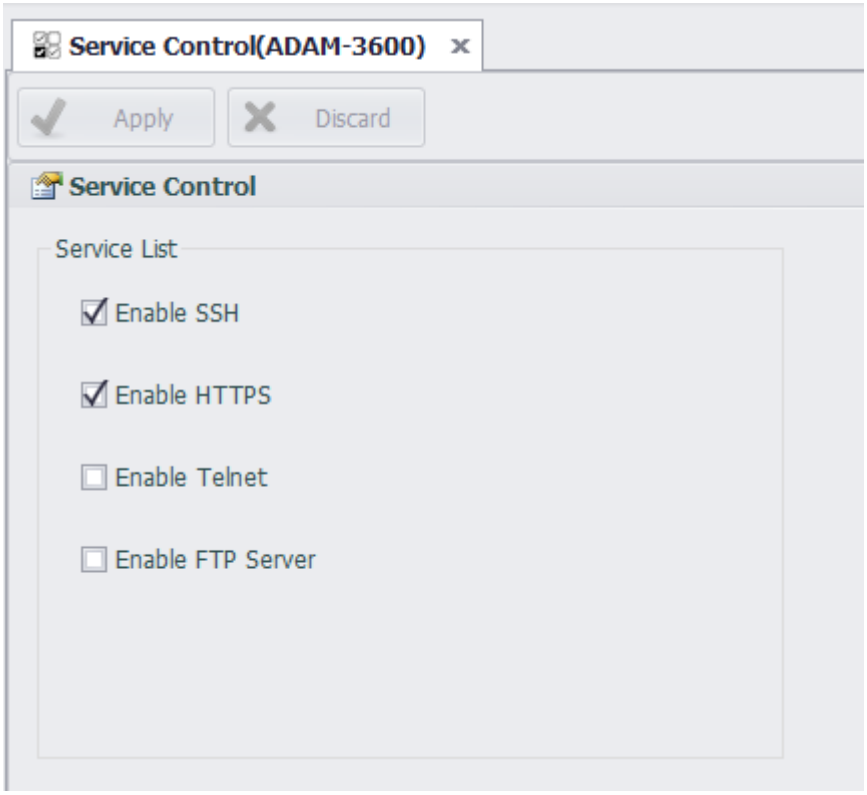
1. SMTP Name: used only in EdgeLink Studio
2. SMTP server: enter IP or domain name
3. Sender: the sender’s mailbox address that is displayed when the message is received
4. User name: the user name needed to connect to the SMTP server
5. Password: the password needed to connect to the SMTP server
6. Confirm password: you need to type in the same password again
7. Encryption mode: you can choose either unencrypted or SSL, TLS two encryption methods
8. When the option is encrypted, the default port is 25. When you select SSL encryption, the default port is 465, and when you select TLS encryption, the default port is 587.

Service Control

Set the following services in system startup or not.

SSH and HTTPS is enabled by default.

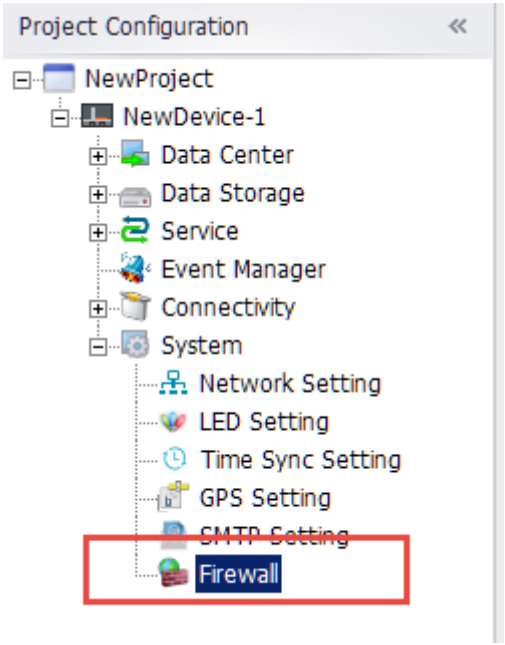
Telnet and FTP server is disabled by default.



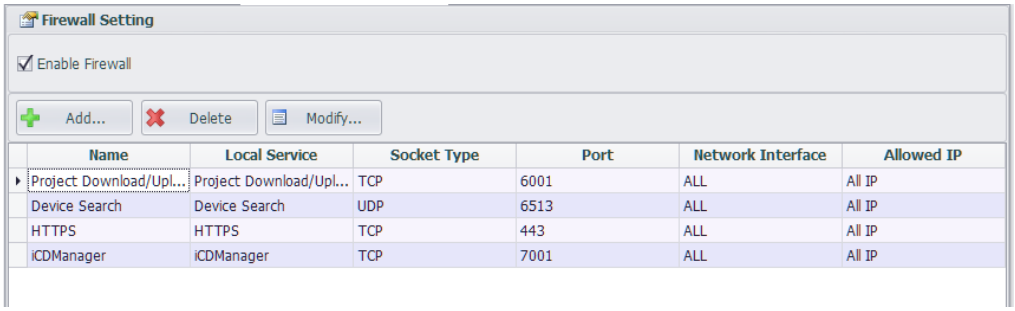
Firewall Settings

In “firewall settings”, you can restrict the network port of the device and only allow the set IP address to access the specified port.

When the firewall is started, only the connections in the firewall list are allowed to access the device.



Firewall List

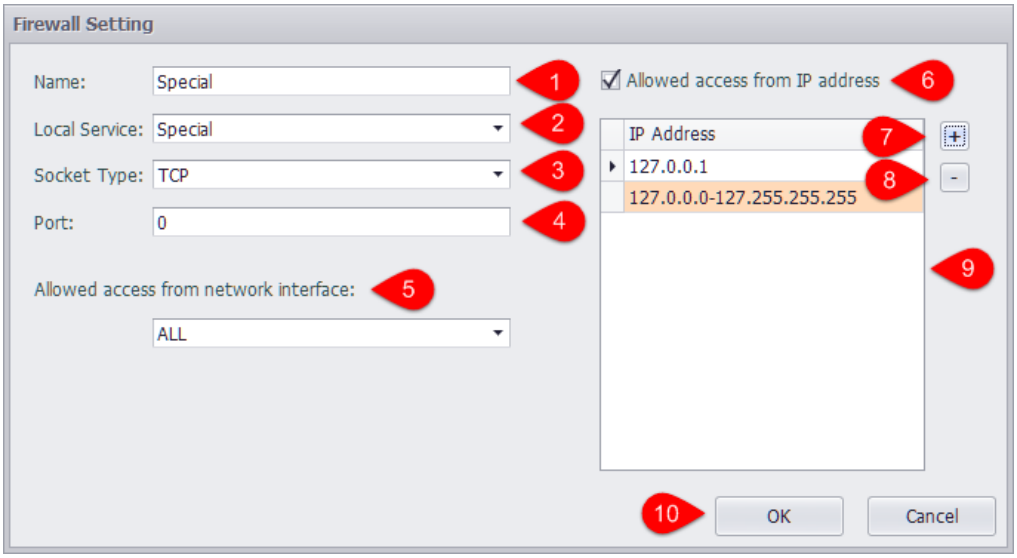


After the new device is built, the firewall will start by default and include “project upload/download”, “search device” and “HTTPS” three local services. “Project

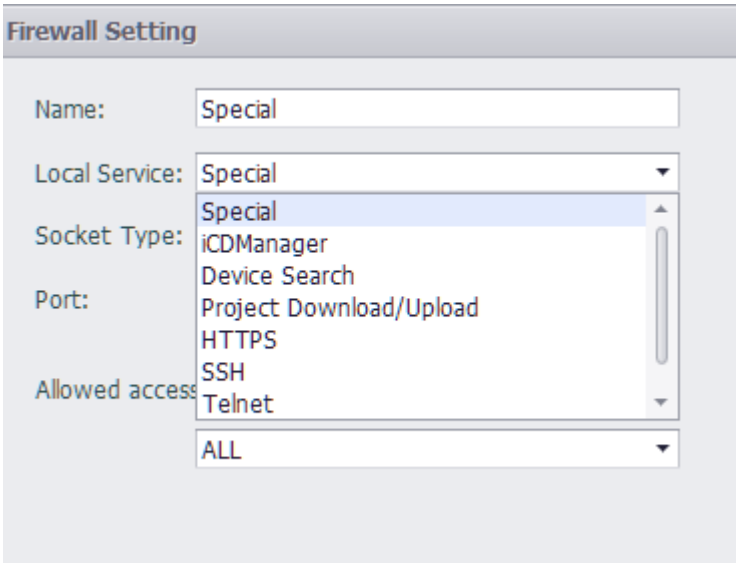
upload/download” and “search device” are required for local services, and at least one of these services needs to be kept.

Add firewall settings

Click the add button in the firewall list interface to add firewall Settings.



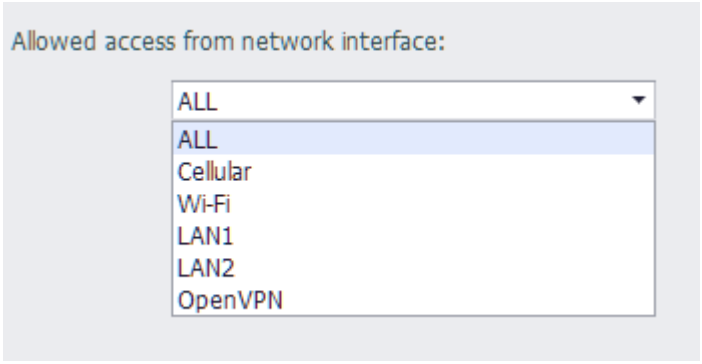
1. The name of this configuration, by default, is the same as the “local service” name, and the user can modify it.
2. Local services include “project upload/download”, “search device”, “HTTPS” and the enabled “Modbus”, “IEC104” and other services. Users can also select “custom” to set.



3. Users can set “TCP” or “UDP” access restrictions.

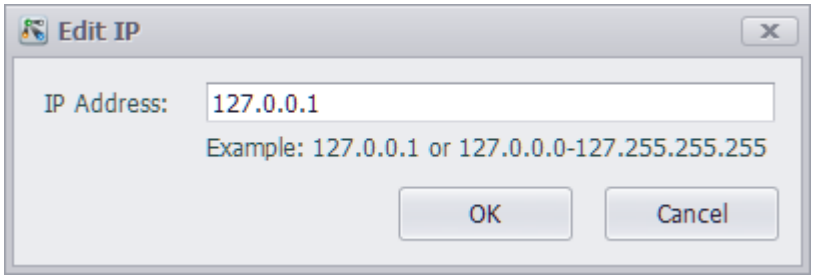
4. Set the port number that allows you to pass through the firewall, in the range of 0-65535.

5. Set to allow specific network access devices.



6. Users can choose to allow all IP access to this device through the previous configuration. You can also choose to only allow specific IP access.

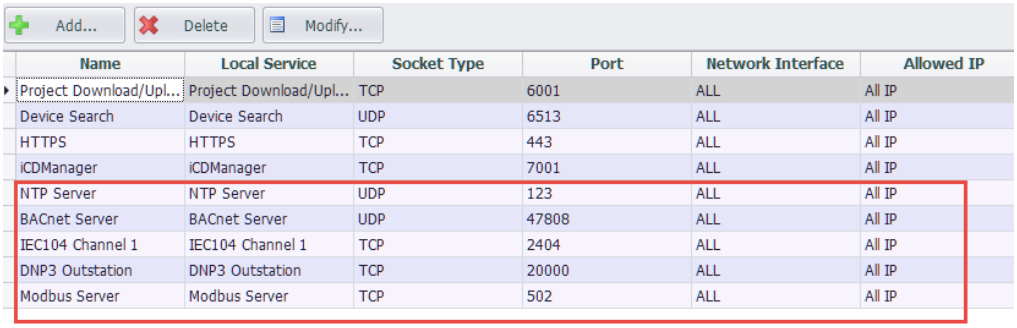
7. Users can click “+” to add the allowed IP address. When you add, you can enter the IP address or IP range.



8. Users can click “-” button to delete the selected IP address.
9. The added IP address or IP range can be displayed in the IP list, and the user can double-click the IP list to edit options.
10. After setting, click “OK” button to save the settings.

Default Settings for Local Services

The firewall contains local services including “Modbus”, “DNP3”, “IEC104”, “BACnet”, “NTP”. These services will add this service when enabled the default settings to the firewall restrictions.When the service is disabled, all relevant settings in the firewall will be removed.

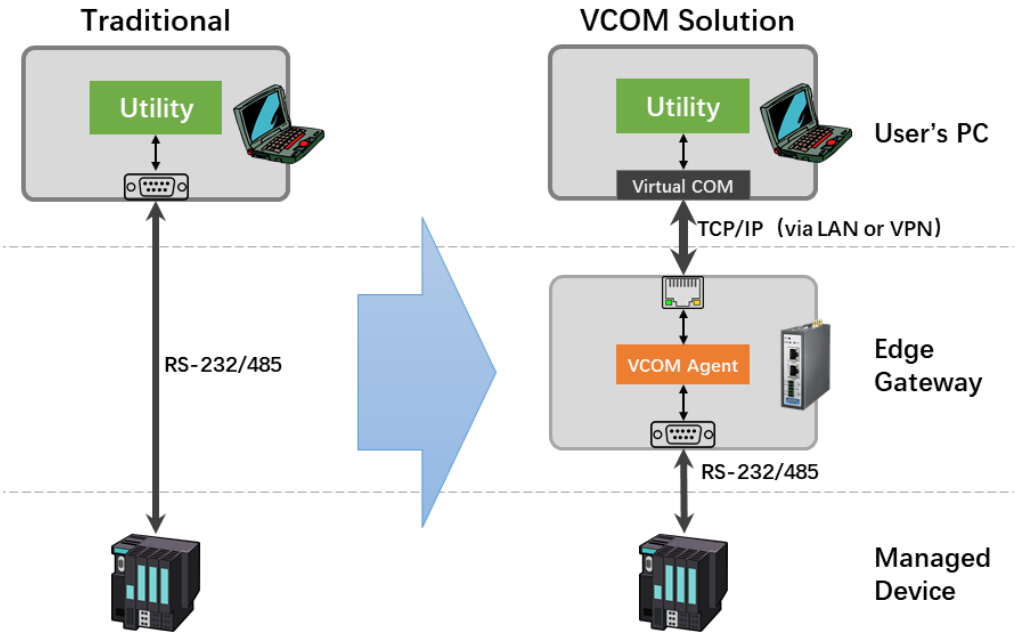


> VCOM Manager Setup File download link:
> https://www.advantech.tw/support/details/utility?id=1-24KJ5E7

VCOM Instructions

1. Introduction

VCOM is Virtual COM, through the VCOM function provided by the gateway, users can map the remote serial port device to the virtual serial port of the PC, as shown in the following figure. In this way, users can directly manage and maintain the device through serial port communication. Generally speaking, the serial port communication software of the managed device can be directly used on the mapped virtual serial port.



When using VCOM, please note the following:

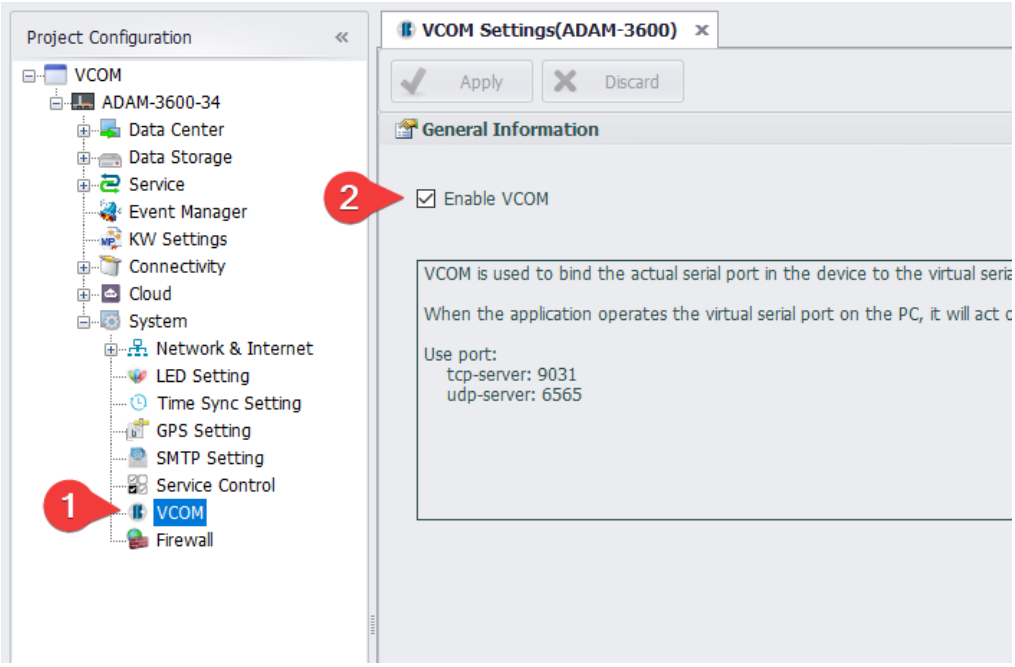
1. The VCOM function is designed for the purpose of remote device maintenance. It is suitable for applications that are not sensitive to communication delay and not long operation time applications, such

as parameter configuration, firmware update, etc. Do not use it as a remote serial server.

2. The delay and stability of the virtual serial port depend on the characteristics of the TCP connection. If the TCP connection is via a cellular wireless network or other high-latency links, please adjust the communication timeout parameters of the serial port device supporting application software.
3. If the serial port on the gateway has been configured as a port occupied by the data acquisition program, then due to the exclusive use of the serial port, after the serial port is bound by VCOM, the data acquisition program will stop data collection until the serial port is unbound, the data collection will be resumed.

2. Enable the VCOM function on the gateway

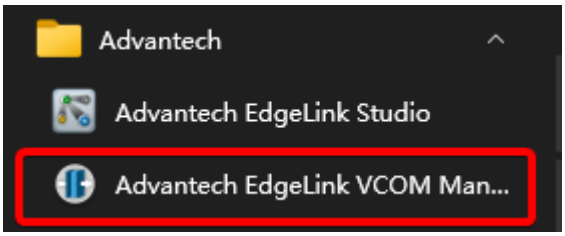
The VCOM function on the gateway is disabled by default. It can be enabled through the VCOM configuration item in the EdgeLink Studio. After downloading the project, the VCOM function can be enabled.



3. VCOM Management Program

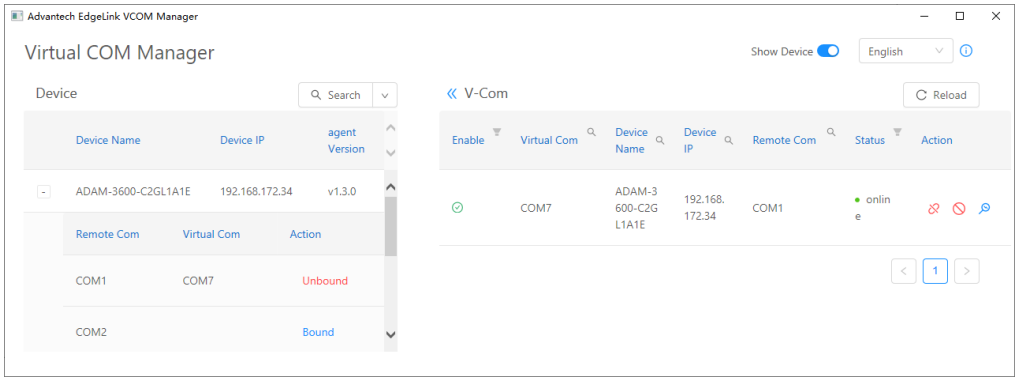
The VCOM management program is an independent installation package. You can download the setup file from this site: https://www.advantech.tw/support/details/utility?id=1-24KJ5E7.

After the installation is complete, you can find the shortcut of the `Advantech EdgeLink VCOM Manager` program in the startup item of the system start menu, as shown in the figure below.



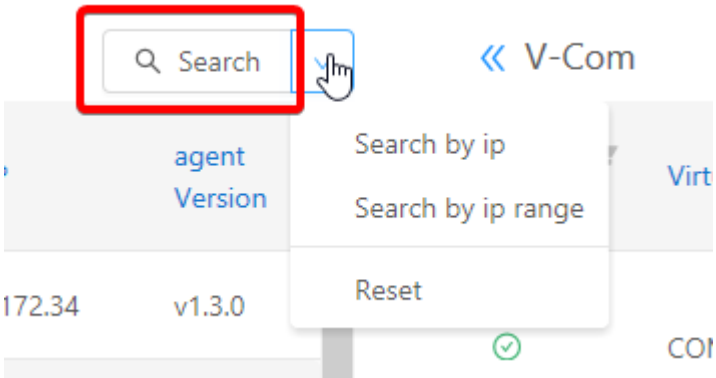
The main interface of the VCOM management program is shown below. The left half shows the information of the online device, including the device name, device IP,

version number of the serial port agent (vcom-agent) and the list of physical serial ports contained in the device. The right half shows the list of virtual serial ports currently created by the management host, including the status of the device serial ports bound to the virtual serial ports.



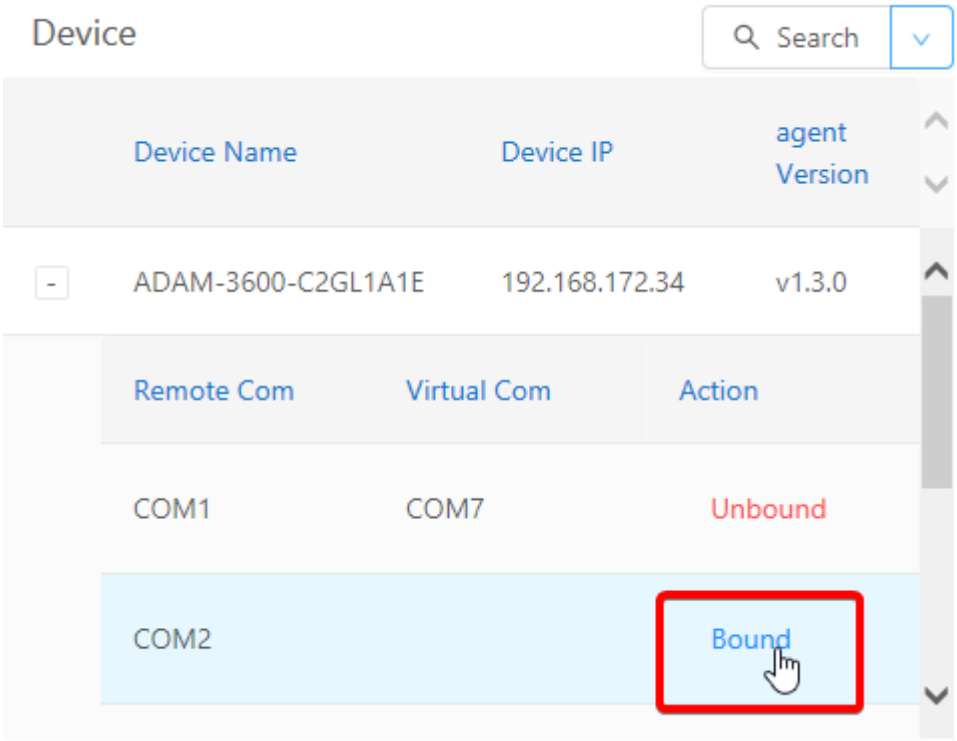
3.1 Searching for online devices

Click the search button on the interface to search for online devices in the local area network that have enabled the VCOM function. If the device is not in the local area network, you can use the drop-down menu to select `Search by IP` or `Search by IP Range`, the `Reset` command in the drop-down menu can be used to clear the current search criteria and device information list.

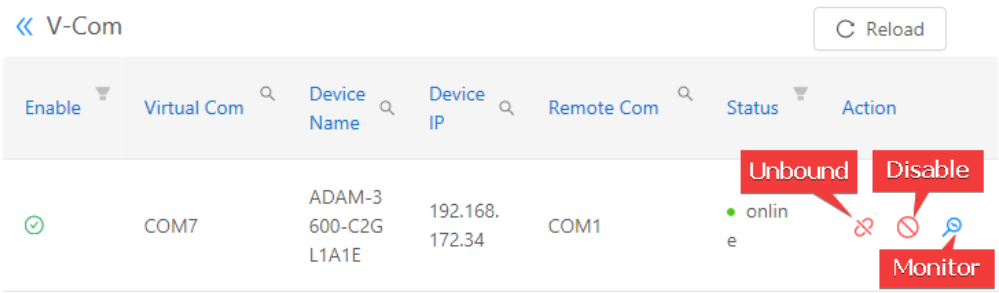


3.2 Bound device serial port

In the device list, click on the left of the target device + sign button, you can see a list of physical serial ports of the device, click on the right side of the serial bind command to complete the binding. During the binding process, the VCOM management program will create a new virtual serial port on the management host (the system will automatically assign an unoccupied serial port number, which cannot be specified manually).



The bound serial port is displayed in the V-Com list on the right side of the main interface, as shown in the figure below.



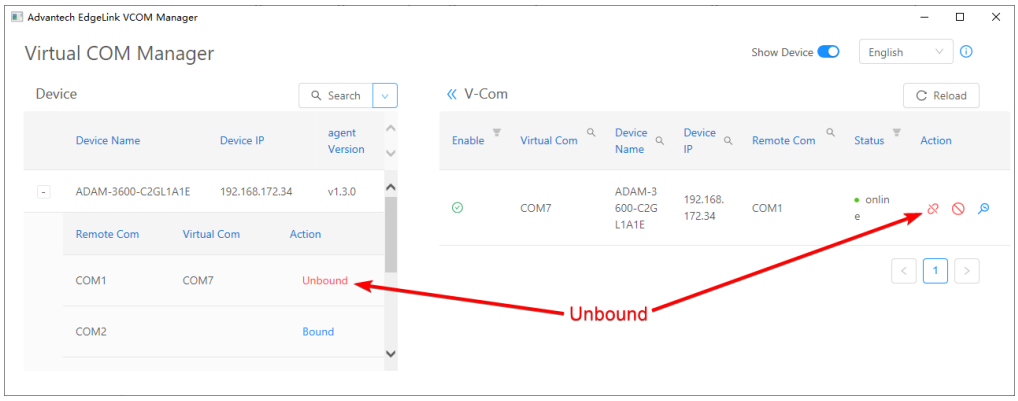
For the virtual serial ports that have been bound, there are three operations to choose: Unbound, Disable and Monitor.

- Unbound: Unbound the virtual serial port and the physical serial port, and delete the virtual serial port from the management host.
- Disable: Unbound the virtual serial port and the physical serial port, but retain the virtual serial port in the management host, which can be re-bound if necessary.
- Monitor: Display the monitoring screen of the virtual serial port, from which you can see the data bytes sent and received by the application program using the serial port for debugging.

3.3 Unbound the serial port

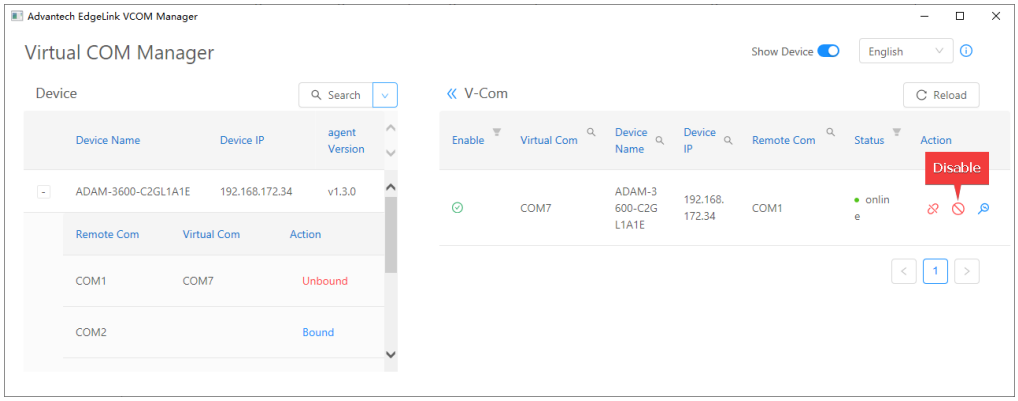
As mentioned above, the VCOM function is designed for the purpose of remote device maintenance. When the remote device maintenance task is completed, the serial port binding should be released in time, otherwise it will affect the normal operation of the data acquisition program.

The unbound operation can be completed by unbounding the corresponding physical serial port in the device list on the left half of the main interface. It can also be done through unbounding the corresponding virtual serial port in the V-Com list on the right half. The results of these two operations are exactly the same, as shown in the figure below.



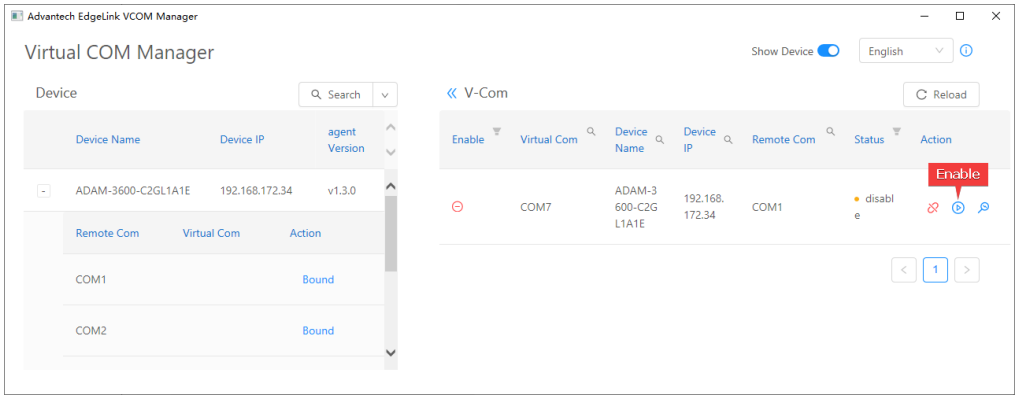
3.4 Disable/Enable serial port bound

If you just want to unbound the serial port temporarily and reserve the virtual serial port for future rebinding, you can use disable, as shown in the figure below.



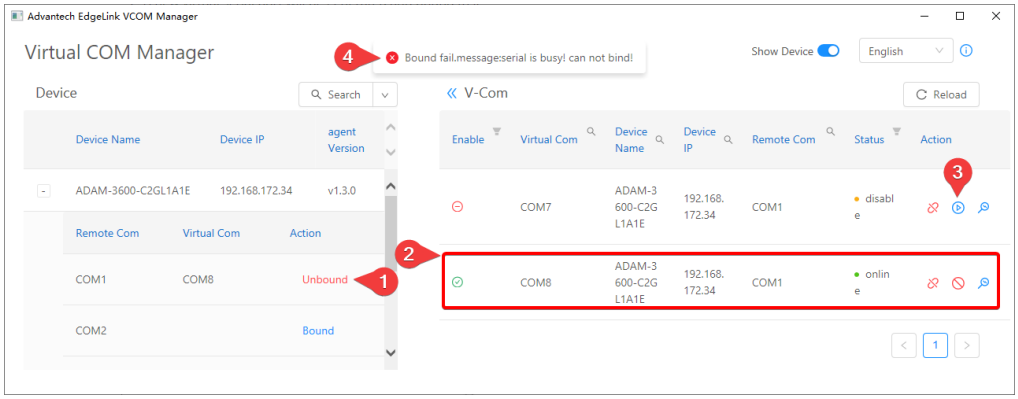
After disabling, the virtual serial port will not disappear, which means that the virtual serial port still exists. But its status information will become `disable`, as shown in the figure below, the original `disable` button will also become

an `enable` button, which is used to rebind the virtual serial port.



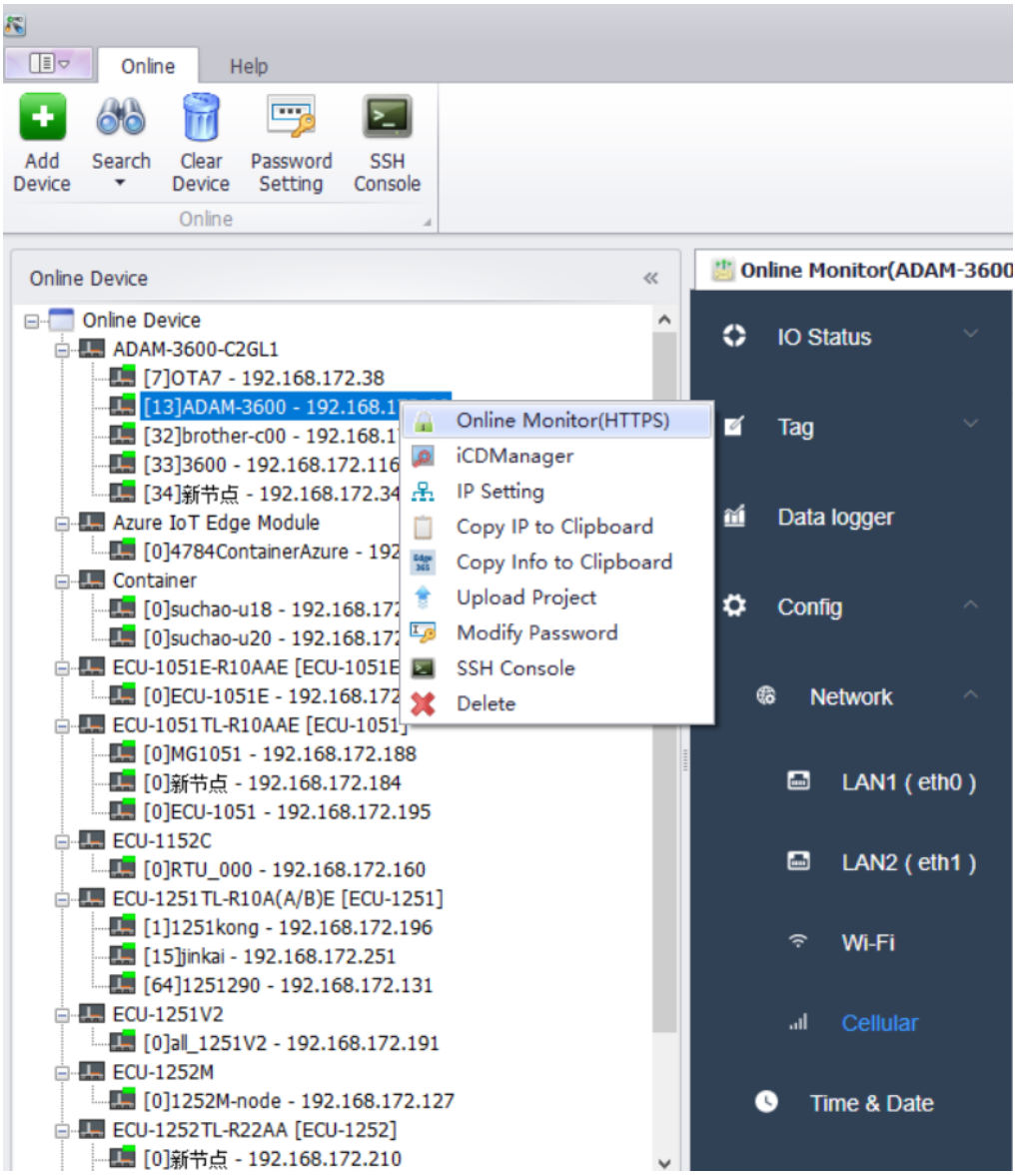
It should be noted that the disabling operation will cause the binding relationship between the physical serial port and the virtual serial port to be released. So when the virtual serial port is disabled, the binding operation on the corresponding physical serial port in the device information interface on the left can be executed. If the binding operation is performed on the physical serial port at this time, it will be bound to a newly generated virtual serial port, as shown in the following figure:

1. Click the `Bind` operation on the physical serial port
2. A new virtual serial port will be generated and bound to it
3. At this time, try to re-enable the previously disabled virtual serial port
4. You will receive an error message indicating that the binding failed, indicating that the physical serial port has been occupied


Advantech EdgeLink VCOM Manager
Virtual COM Manager
4
Bound fail.message:serial is busy! can not bind!
Show Device
English
Device
Search
Device Name
Device IP
agent Version
ADAM-3600-C2GL1A1E
192.168.172.34
v1.3.0
Remote Com
Virtual Com
Action
COM1
COM8
Unbound
COM2
Bound
1
2
V-Com
Reload
Enable
Virtual Com
Device Name
Device IP
Remote Com
Status
Action
COM7
ADAM-3600-C2GL1A1E
192.168.172.34
COM1
disable
COM8
online
3
1

Online Functions

Advantech EdgeLink Studio supports online device operations and has the following main functions:



1. Add Device、Search、Clear Device
2. This password is used for Project download and online login (default password 00000000).
3. Online Monitor:IO Status、Tags、DataLogger、Config、System Log

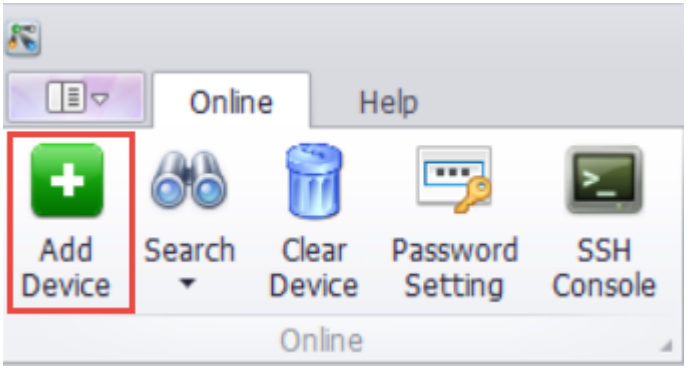
4. Set device IP address online (reboot expired)
5. Copy current device IP address to clipboard
6. Copy the current device information to the clipboard (used when creating the device in Edge365)
7. Upload the current device project to the local computer
8. SSH access
9. iCDManger

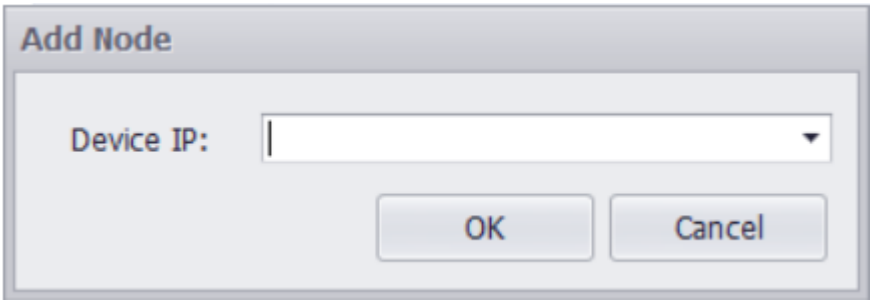
Online Configuration

1. Add Device
2. Search Device
3. Clear Device
4. Password Setting
5. IP settings (reboot expired)
6. Copy the current device IP address to the clipboard
7. Copy the current device information to the clipboard (used when creating the device in Edge365)
8. Upload the current device project to the local computer
9. SSH access
10. iCDManger

Add Device

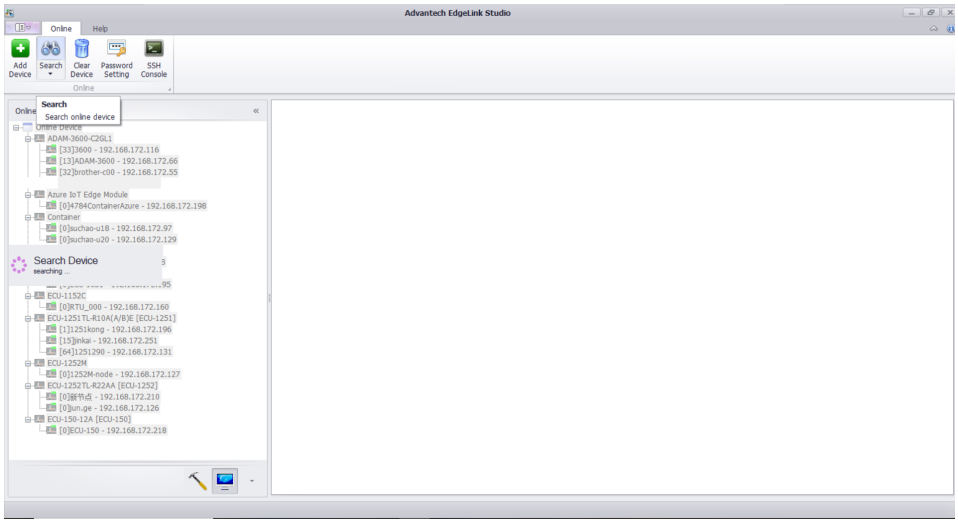
Add devices by IP address, one device at a time



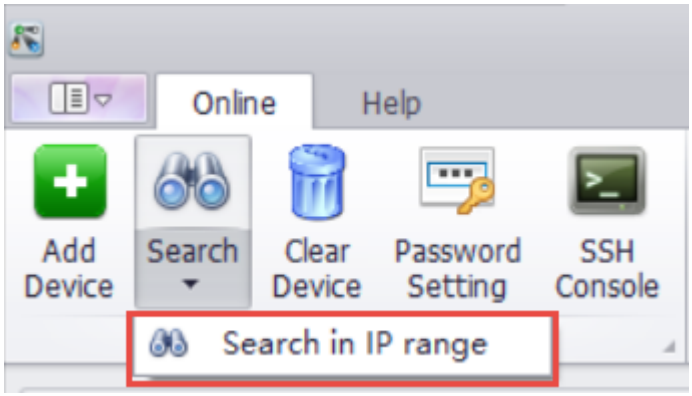


Search Device

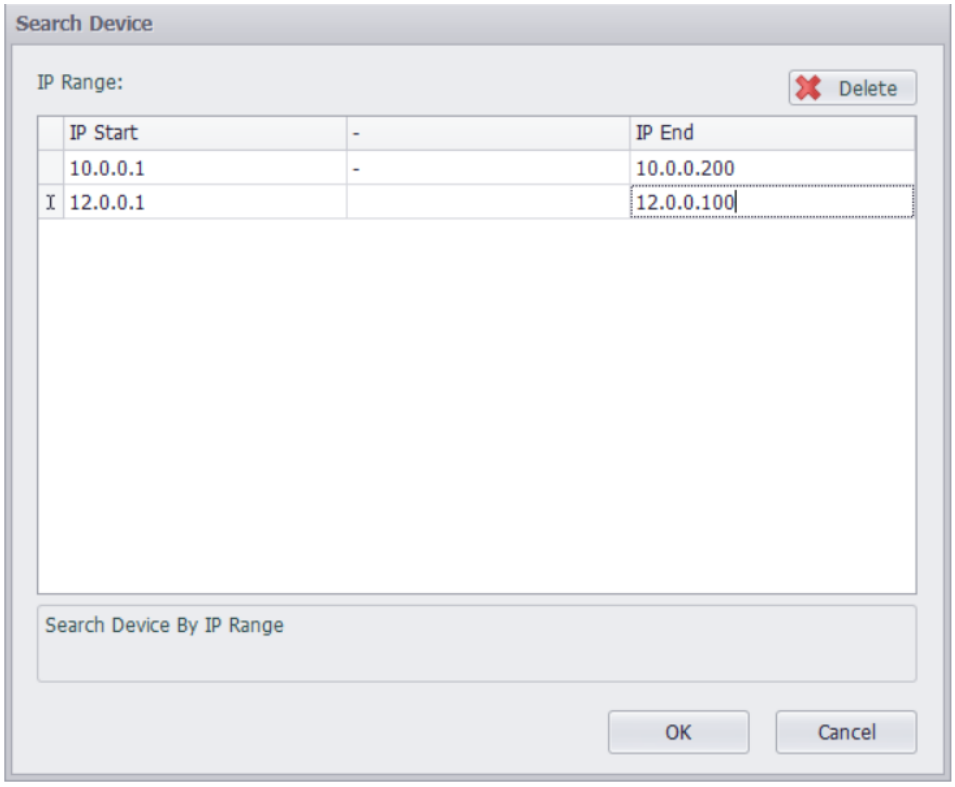
1. Search for all devices in the network and list them in the online list.



2. Users can also choose to search within an IP range when searching.

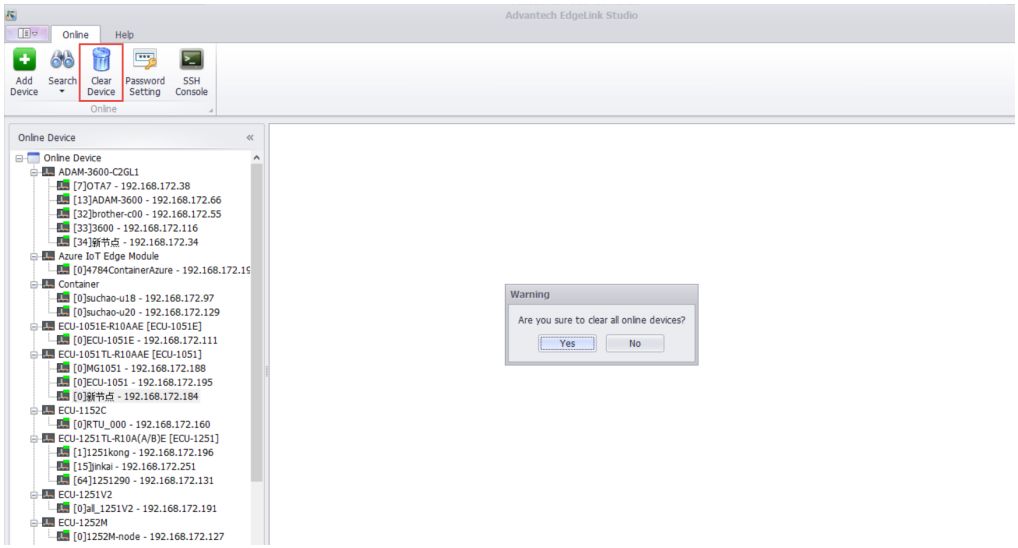


3. Multiple network segments can be added to search at the same time, and the program will send search commands to each IP in the IP range in turn, which can search for devices across the router.


Search Device
IP Range:
Delete
IP Start
-
IP End
10.0.0.1
-
10.0.0.200
12.0.0.1
12.0.0.100
Search Device By IP Range
OK
Cancel

Clear Device

Clear the list of online devices.

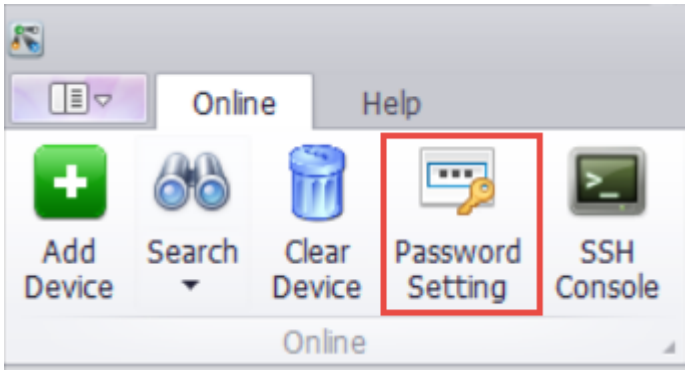


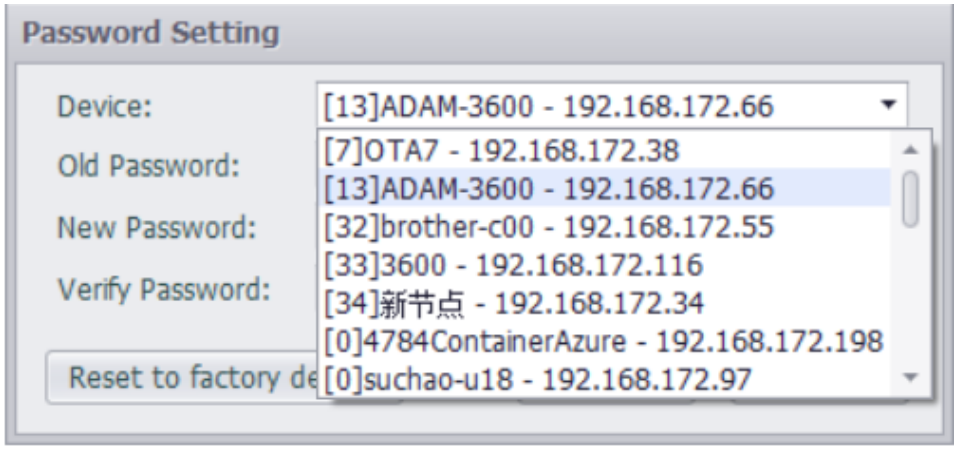
Password Setting

You can set a password for the device, and note that this password is also the download password (default password 00000000).

The first case: any one of the multiple devices is selected to change the password

1. Click Password setting
2. Select the device you want to set up

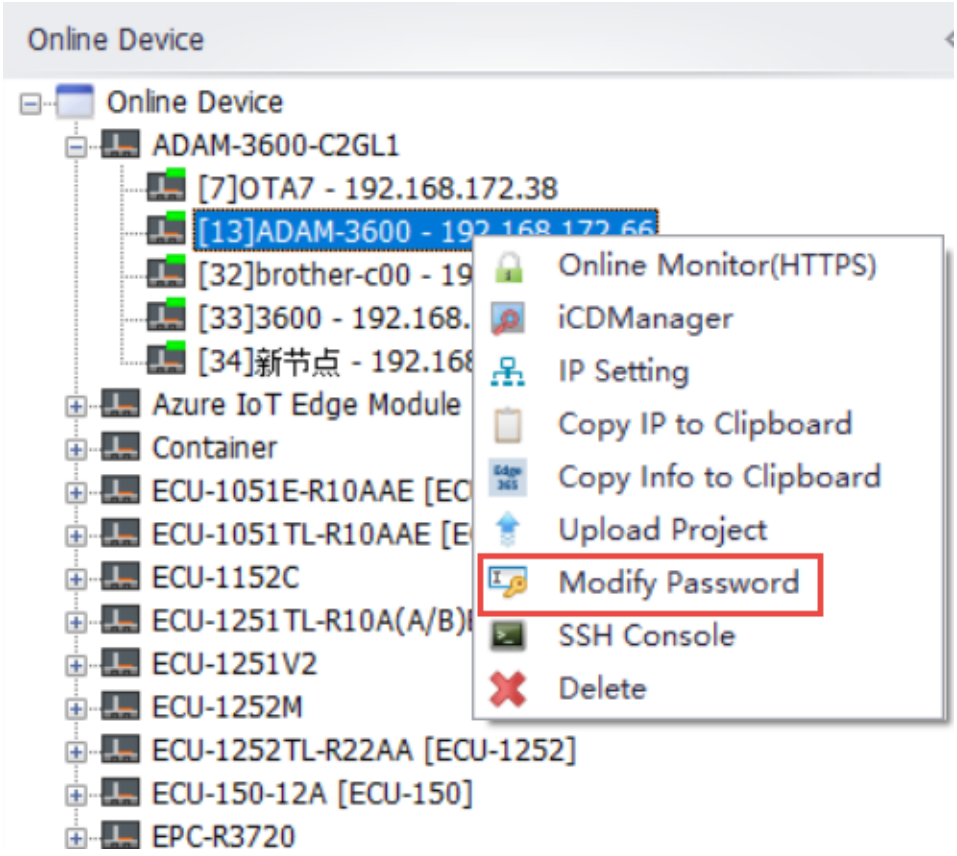




The second case: Right-click on a specific online device and select Change Password to modify the password of the current device

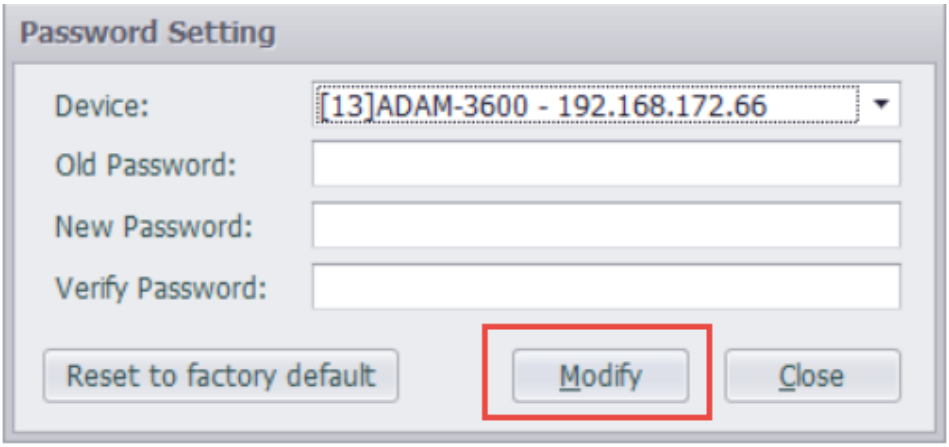
1. Select the device, right-click

2. Select Modify password



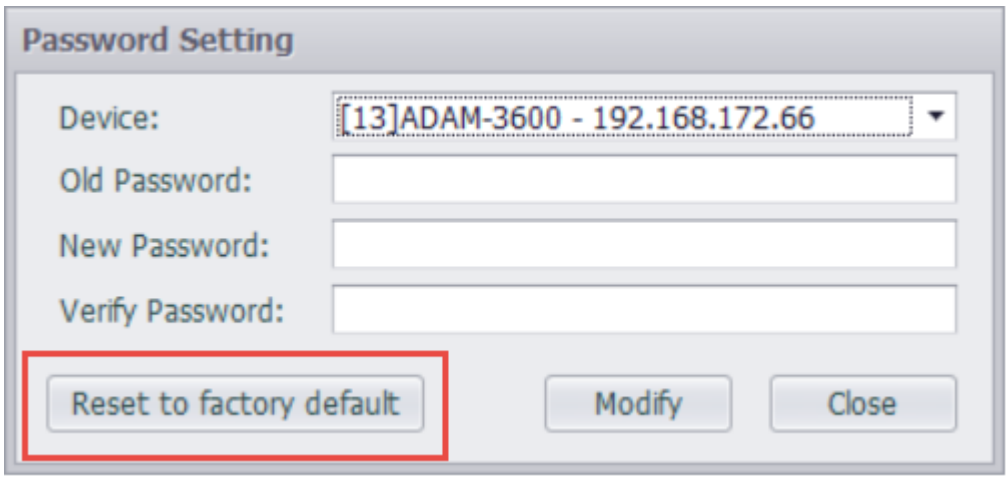
After the above two situations

1. Fill in the old password, new password, and thenconfirm password
2. Click Modify to set a password



Reset to factory default

Click “Reset to factory default” on this interface, after which you need to restart the device within 10 seconds. After restarting, the device’s passcode is restored to its factory state.

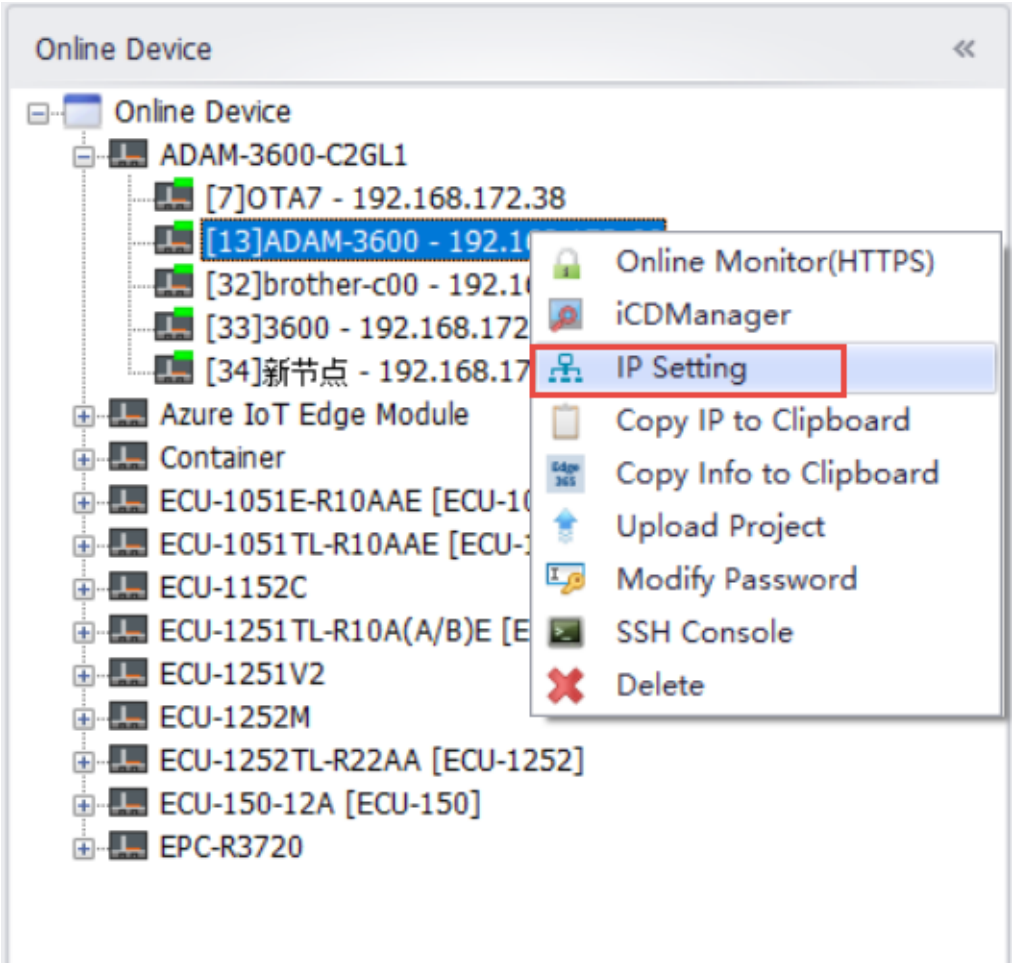


IP Setting

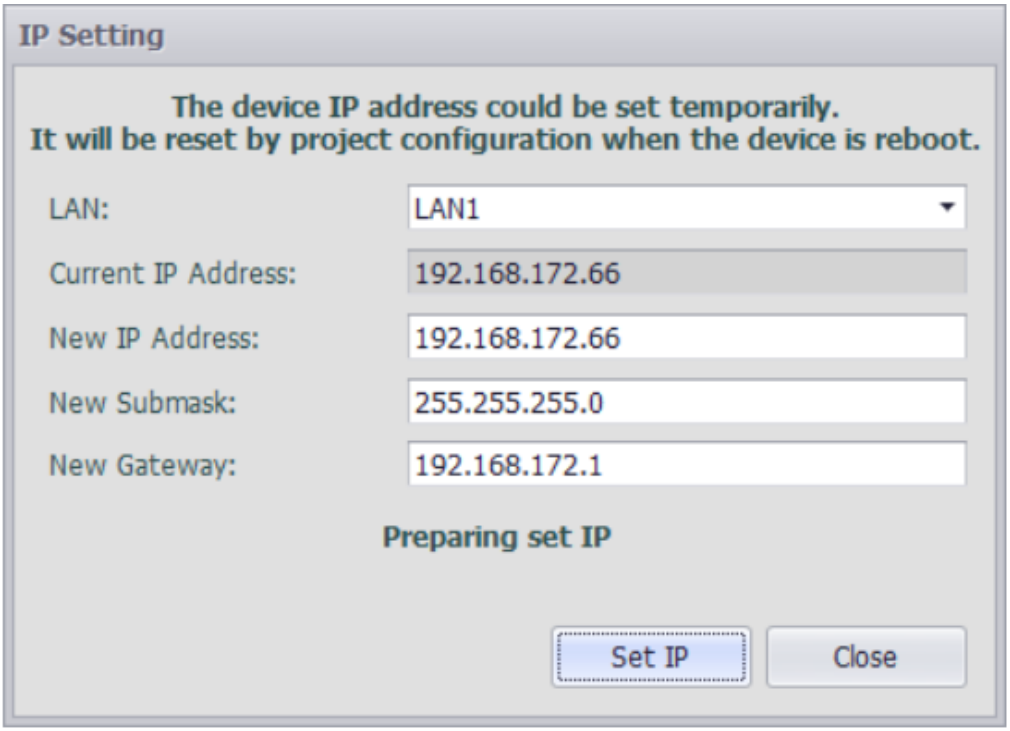
Users can temporarily modify the IP address and subnet mask of the network port of online devices through EdgeLinkStudio. For example, the two network ports of RTU are set to DHCP mode (dynamically assigned IP), but there is no server in the network that can provide DHCP services. At this point, the RTU can be searched, but not accessed by IP. At this time, the user can temporarily set the IP address of the RTU for operations such as downloading projects.

> **Note**：This setting expires after the RTU is rebooted. After restarting, the RTU sets the network port status according to the configuration document

1. Right-click on the online device that has been searched, click Set IP, and open the “Set IP” pop-up box.



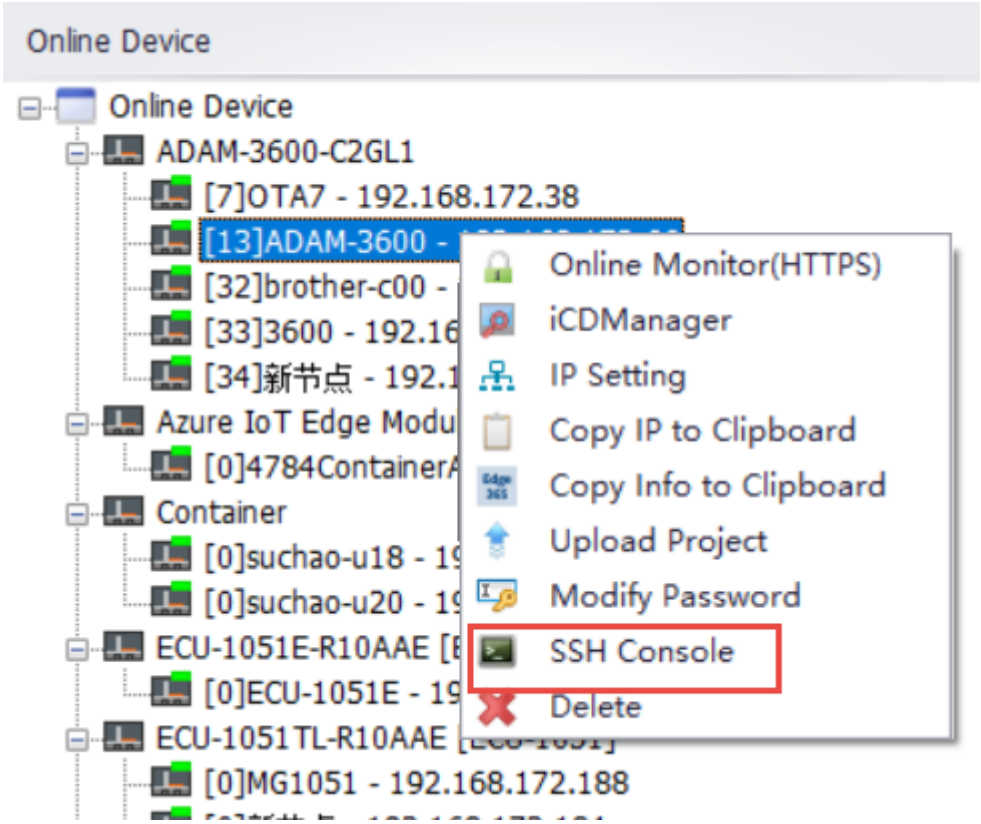
2. In the Set IP pop-up box, the user first selects the network port to be modified, and then enters the new IP address and subnet mask.


IP Setting
The device IP address could be set temporarily.
It will be reset by project configuration when the device is reboot.
LAN:
LAN1
Current IP Address:
192.168.172.66
New IP Address:
192.168.172.66
New Submask:
255.255.255.0
New Gateway:
192.168.172.1
Preparing set IP
Set IP
Close

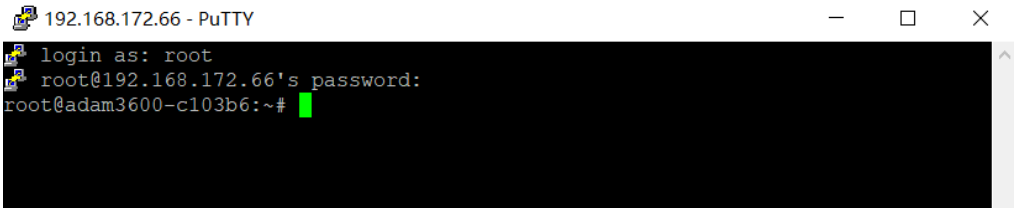
SSH Console

Users can log in directly to the online device via SSH Console in the Online interface.

Sign in to your online device



Right-click on the device in the online device to bring up the toolbar and click the SSH Console button in the toolbar.

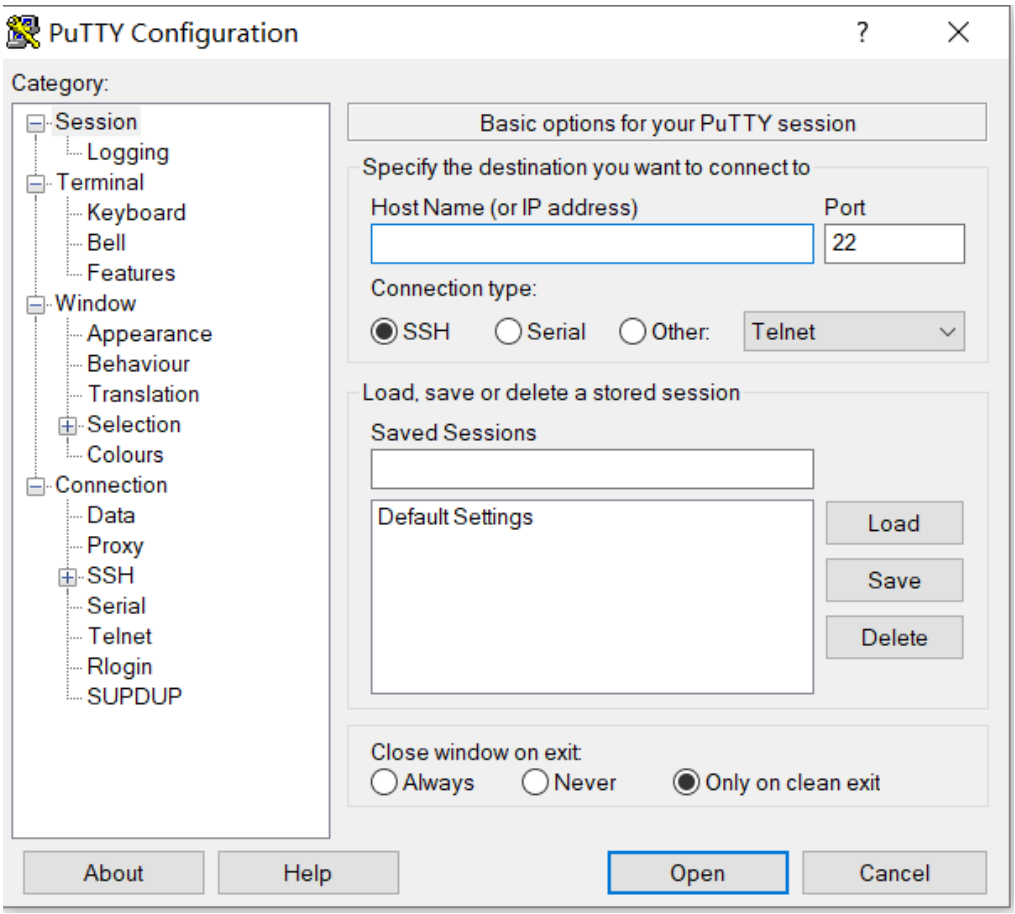


After entering a user name and password, the user can remotely log in to the device's system.

> ! **Note**：EdgeLink Studio uses Putty to connect devices remotely

Log in to the device manually

If you need to set the connection parameters before logging in to the device, you can click the SSH Console button in the upper toolbar.

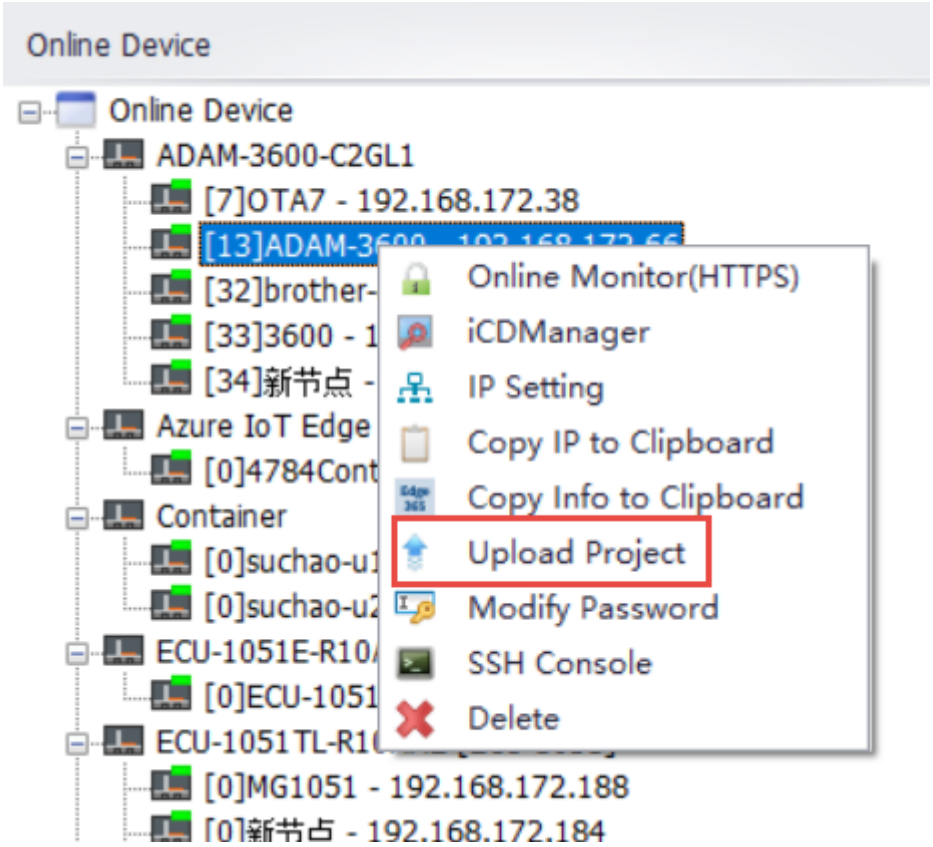


EdgeLink Studio will open Putty's configuration page for users to edit, and click Open to log in to the device after editing.

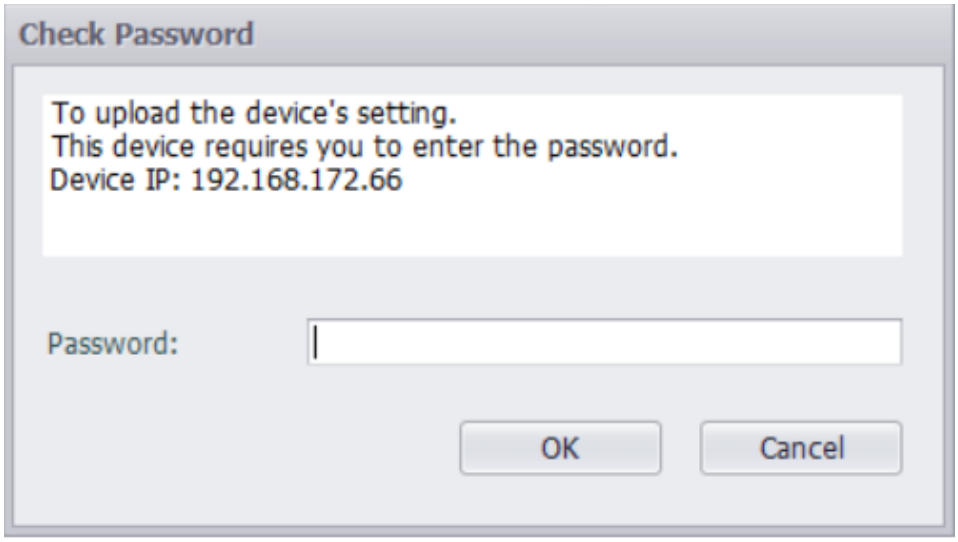
Upload Project

Users can upload the current device project on the device to EdgeLink Studio.

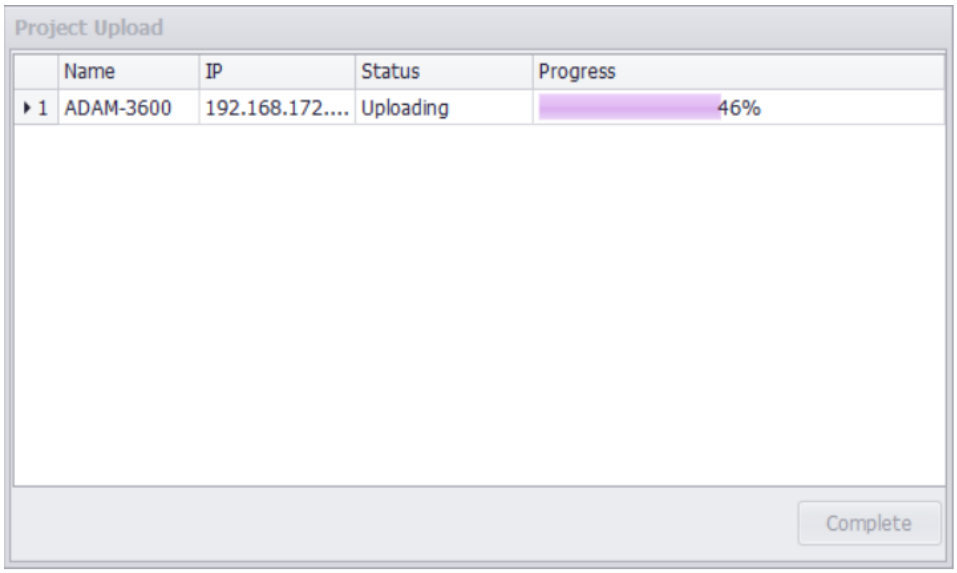
1. Right-click on the already searched device and select “Upload Project” in the Online device list to start uploading device information.



2. Before loading the device information, the user needs to enter the password of the current device and verify that it is correct before uploading.



3. The current upload progress is displayed as a progress bar while uploading.

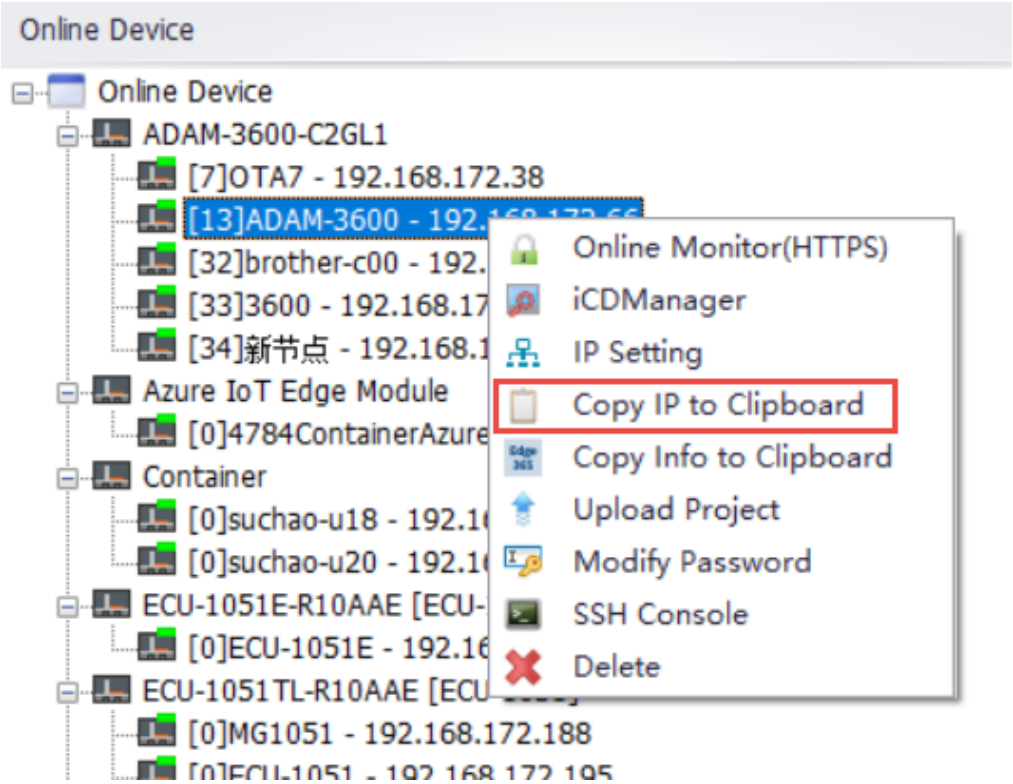


4. When the upload is complete, the uploaded project is displayed in Project Management.
    - At this point, if there are no open projects in Project Management, a new project is created with the uploaded equipment information.
    - If you already have an open project, an attempt is made to save the device information in the existing project after the upload is complete.

Copy Device

Users can copy device information to the pasteboard for later use.

Copy the IP address to Clipboard, for example: 192.168.172.66



Copy the device information to Clipboard, this information is currently used when Edge365 creates an EdgeLink device (supported in versions 2.8.2 and above).

The information format is as follows:

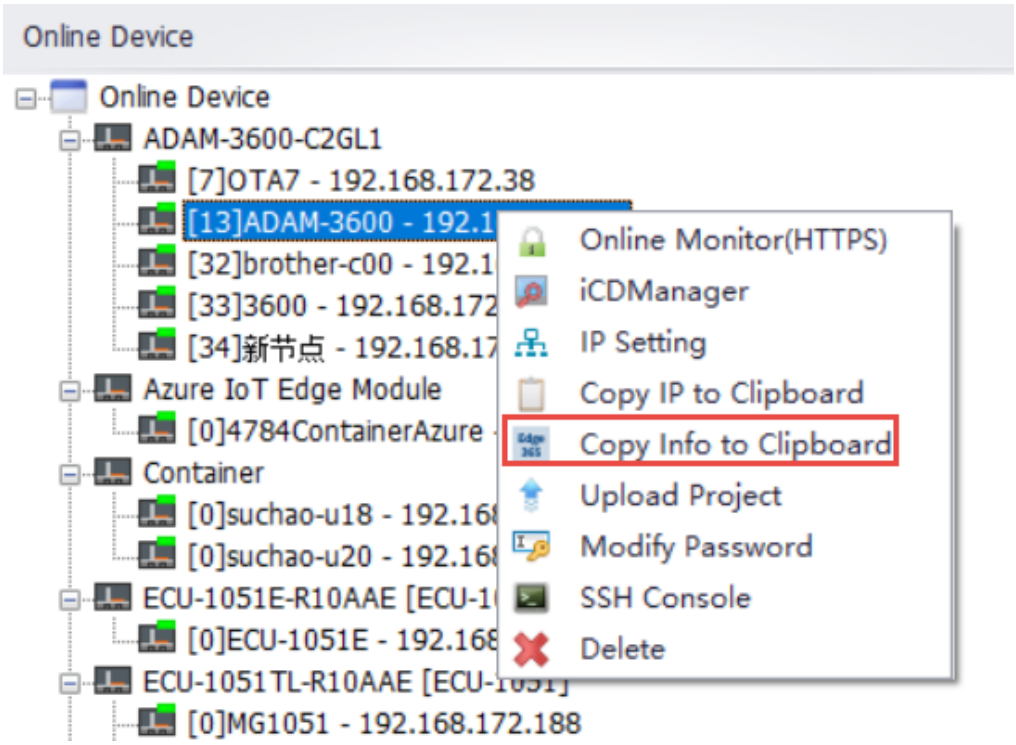
{ “name”: ””,

“description”: ””,

“mac”: ””,

“type”: “EdgeLink”

}



Online Monitor

There are mainly the following functions:

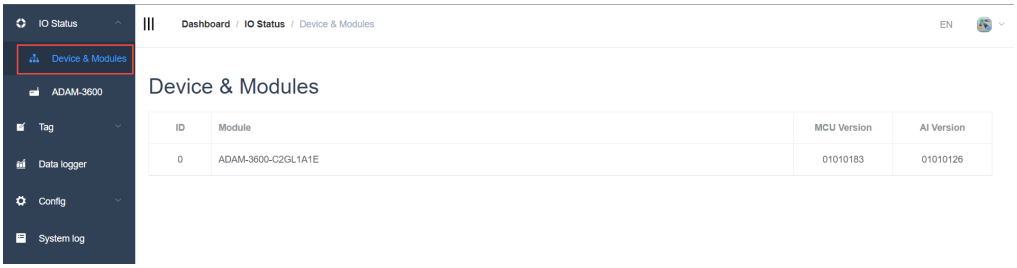
1. IO Stauts：Includes setup and reading of onboard and extended IOs
2. Tags：All tags on the device, including value, quality and timestamp
3. DataLogger：Check historical data online
4. Config：NetWork Setting、Time&Date、remote.it、Image Recovery、Image Update、Reboot
5. System Log： system information

Note: Third-party clients are supported to access through RESTful API, download link of API specification document:Open RESTFul API Specification

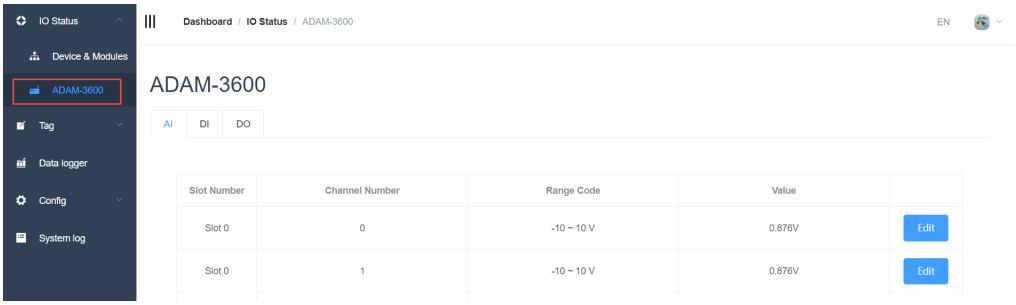
I/O data acquisition and parameter setting

EdgeLink online operation provides on-board and extended I/O data acquisition and setting functions, different I/O modules correspond to different tabs, respectively AI, AO, DI and DO four types.

1. The device displays the current device model, and if there are expansion modules, it will also be listed on this page



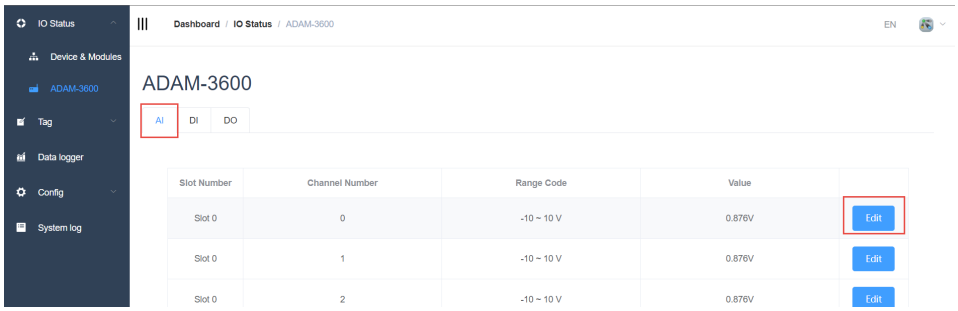
2. Select Current Device to display all IO points on the device



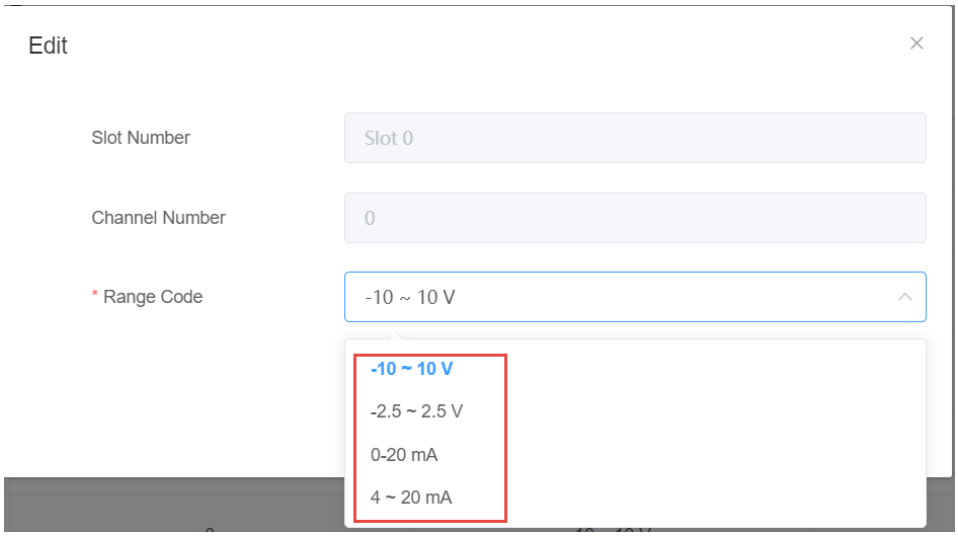
AI data acquisition and parameter setting

The data of the AI module is shown in the figure below. The data form items are as follows:

- Slot number: The module where the AI function block is located, and slot 0 is onboard.
- Channel number: AI channel number.
- Range: The range of AI sampled values.
- Value: The value of the AI.



When you need to configure parameters, click the Edit button

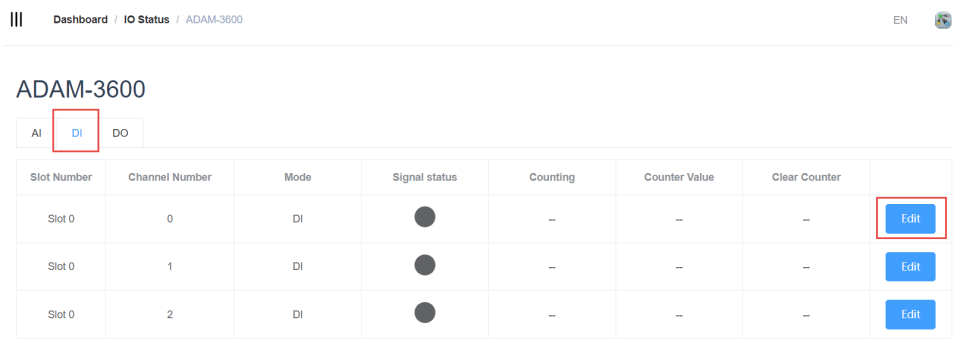


Note: After the parameter is modified, you need to click the Confirm button to take effect

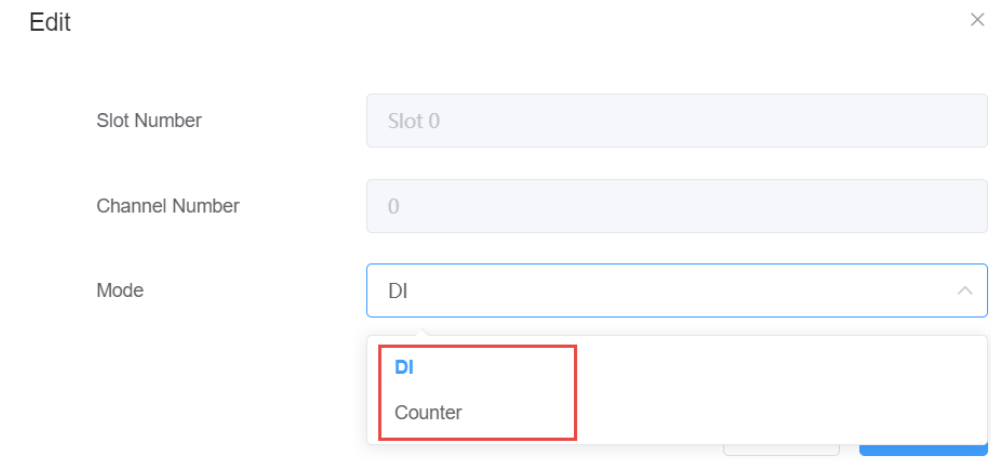
DI data acquisition and parameter setting

The data of the DI module is displayed in the figure below. The data form items are as follows:

- Slot number: The module where the DI function block is located, slot 0 is onboard.
- Channel number: DI channel number.
- Mode: Normal (i.e. DI) or Counter.
- Signal Status: DI port level value.
- Value: In Normal mode, the collected DI value is displayed here; Counter mode, the count value is displayed here.



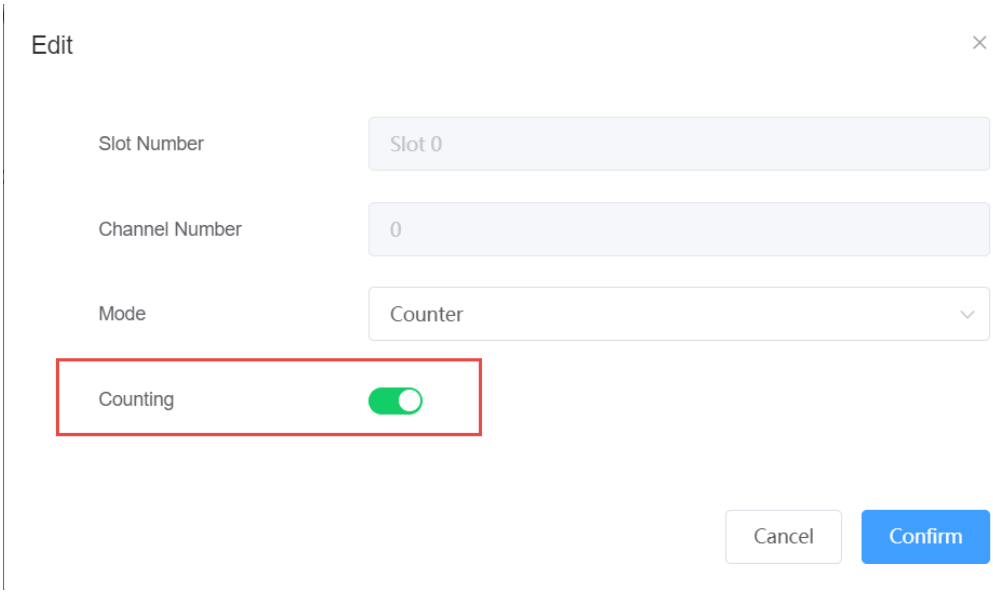
When you need to configure parameters, click the Edit button to set the working mode of this DI channel



When the DI channel operating mode is Counter, you can choose whether to enable Counter counting by starting counting:

Green is enabled, and if enabled, the DI channel is counted if there is an input

Red is not enabled, and DI channels do not count



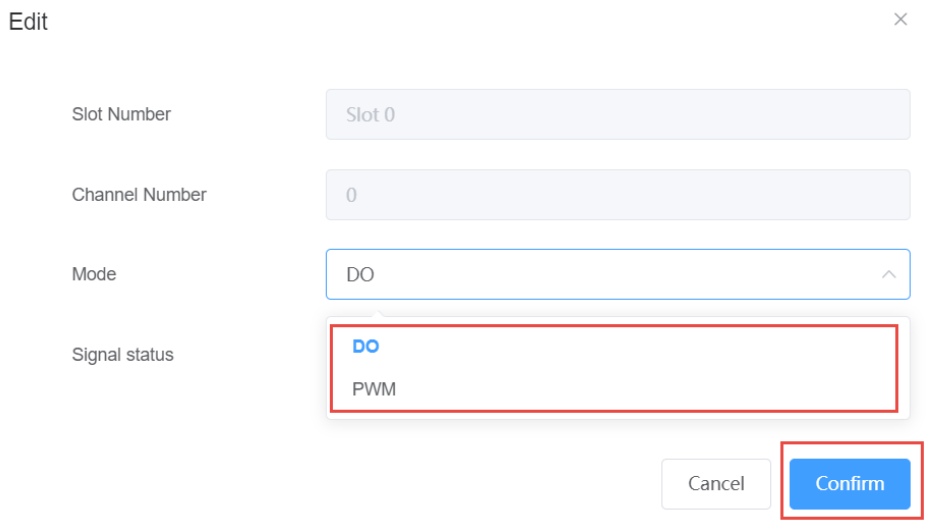
Note: After the parameter is modified, you need to click the Confirm button to take effect

DO data acquisition and parameter setting

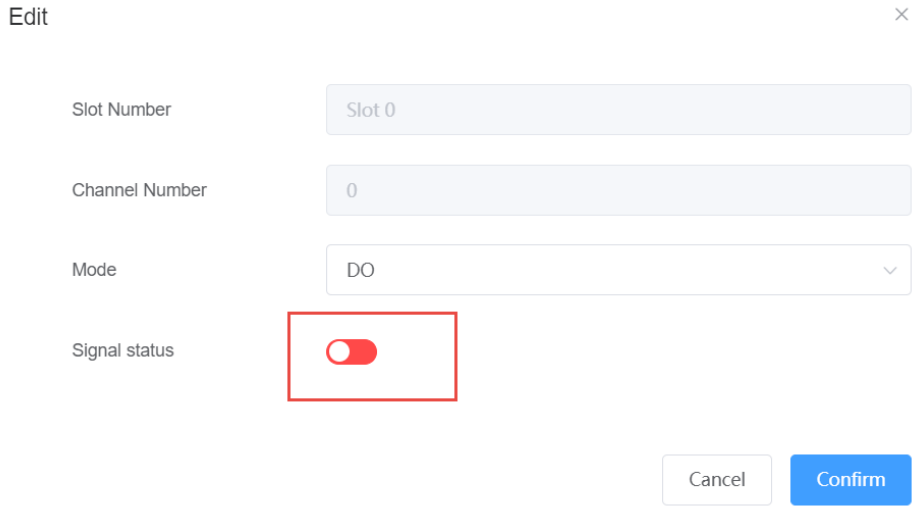
1. The data of the DO module is displayed in the following figure. The data form items are as follows:

- Slot number: The module where the DO function block is located, slot 0 is onboard.
- Channel number: DO channel number.
- Mode: Normal (i.e. DO) or PWM.
- Signal Status: DO port level value.
- Value: When in Normal mode, the output DO value is displayed here; Counter mode, the count value is displayed here.
- Low width: The low level pulse width of the output in PWM mode.
- High width: The high-level pulse width of the output in PWM mode.

If you need to configure, click the Edit button to set the DO channel mode to DO or PWM



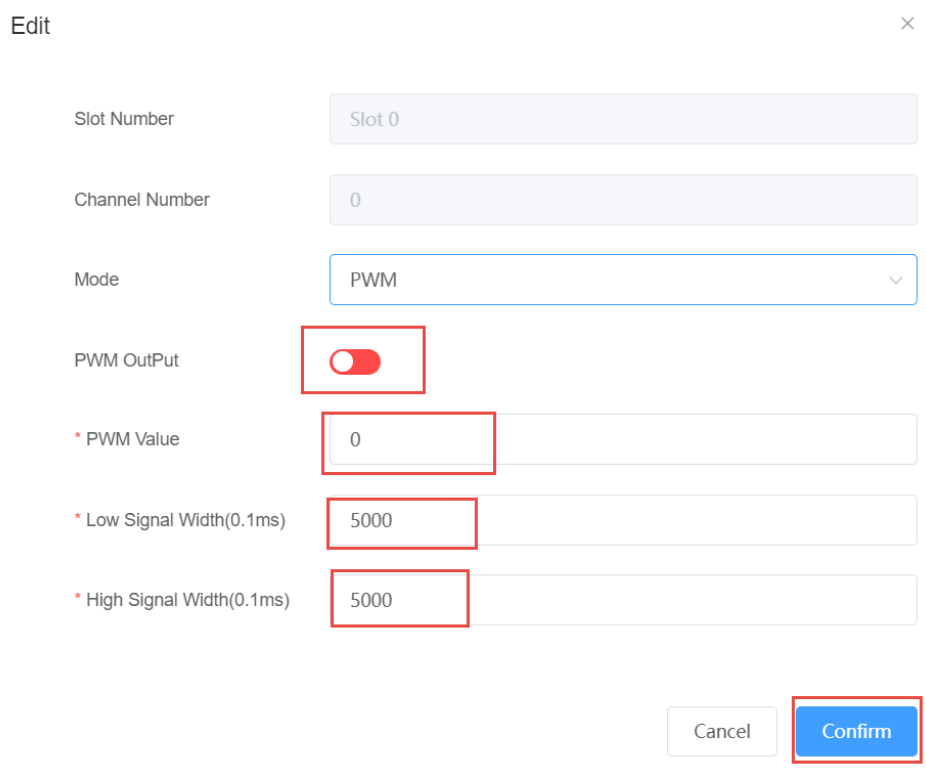
2. DO mode: Set the DO output by clicking the signal status, green is high, red is low.



3. PWM mode:

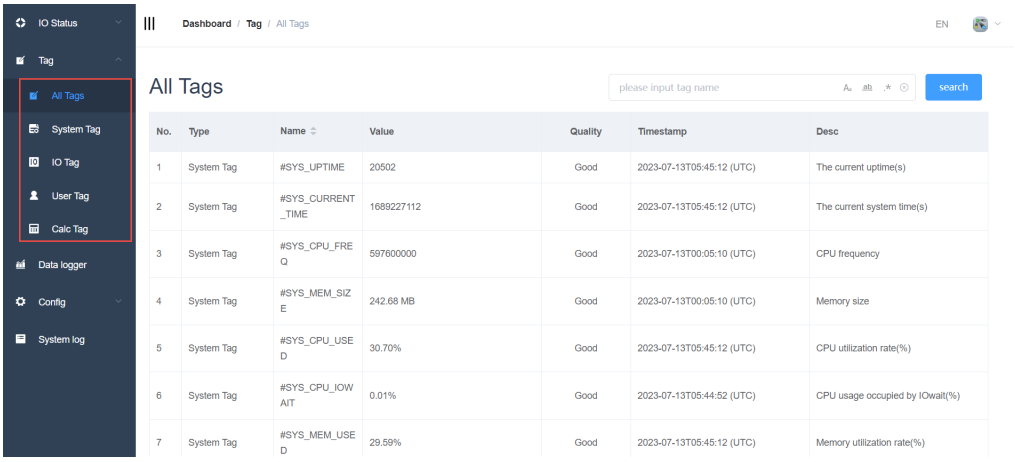
- PWM output: green is enabled, red is not enabled
- PWM value: Set the number of output PWM waveforms, the default is 0, 0 means always output
- Low signal width: The low level pulse width of the output PWM in 0.1ms, and the pulse width is (0.1* number) ms

- High signal width: The high level pulse width of the output PWM is 0.1ms, and the pulse width is (0.1* number) ms



Tags

EdgeLink online operation provides the function of obtaining and setting Tags, different Tag types correspond to different pages, System Tag, IO Tag, User Tagand and Calculation Tag, and support unified viewing of all tags.



Search of Tags：

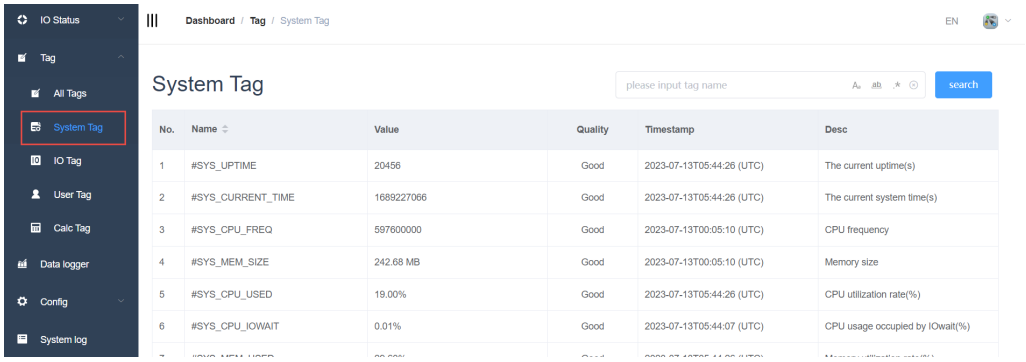
Tag Search

> **Note**
>
> 1. The default number of displayed rows of the page is 10 rows, or you can choose to display the number of rows per page::100000

> 2. The excess part is paginated and displayed, and you can switch to other tags by clicking the number or arrow in the lower right corner

9	System Tag	#SYS_SYSCARD _FREE_SPACE	186.93 MB	Good	2023-07-13T00:05:10 (UTC)	System partition free space
10	System Tag	#SYS_DATACAR D_CAPACITY	7.33 GB	Good	2023-07-13T00:05:10 (UTC)	Data partition capacity

System Tag



Search of Tags：

Tag Search

General system tag description(Read Only)

Name	Description
#SYS_UPTIME	The current uptime(s)
#SYS_CURRENT_TIME	The current system time(s)
#SYS_CPU_FREQ	CPU frequency
#SYS_MEM_SIZE	Memory size(Byte)
#SYS_CPU_USED	CPU utilization rate(%)
#SYS_CPU_IOWAIT	CPU usage occupied by IOwait(%)
#SYS_MEM_USED	Memory utilization rate(%)
#SYS_SYSCARD_CAPACITY	System partition capacity(Byte)

Name	Description
#SYS_SYSCARD_FREE_SPACE	System partition free space(Byte)
#SYS_DATACARD_CAPACITY	Data partition capacity(Byte)
#SYS_DATACARD_FREE_SPACE	Data partition free space(Byte)
#SYS_NODE_ID	Node ID on RTU
#SYS_ROOT_READONLY	Read-only system：0-System Partition Readable and Writable, 1-System Partition Read-Only
#SYS_COM_COUNT	COM count
#SYS_LAN_COUNT	LAN count
#SYS_DEFAULT_IF	Meaning of the value：0-Cant’t find default interface for route, 1-LAN1, 2-LAN2, 3-LAN3, 4-LAN4, 101-WiFi, 201-Cellular
#MOBILE_SIM	0 error 1 READY: MT is not pending for any password 2 SIM PIN: MT is waiting SIM PIN to be given 3 SIM PUK: MT is waiting SIM PUK to be given 4 SIM PIN2: MT is waiting SIM PIN2 to

Name	Description
	be given 5 SIM PUK2: MT is waiting SIM PUK2 to be given 6 PH-NET PIN: MT is waiting network personalization password to be given 7 PH-NETSUB PIN: MT is waiting network subset personalization password to be given 8 PH-SP PIN: MT is waiting service provider personalization password to be given 9 PH-CORP PIN: MT is waiting corporate personalization password to be given 10 PH-SIM PIN: MT is waiting phone to SIM/UICC card password to be given 99 not known
#MOBILE_IP	Celluar device ip
#MOBILE_MNO	Mobile network operator
#MOBILE_MNT	Mobile network type

Name	Description
#MOBILE_MDT	Mobile data traffic
#MOBILE_MPN	Mobile phone number
#MOBILE_SIGNAL_QUALITY	Signal quality of mobile network
#MOBILE_CSQ	Received Signal Strength Indication
#MOBILE_MCC	Mobile Country Code，MCC
#MOBILE_MNC	Mobile Network Code，MNC
#MOBILE_LAC	Location Area Code, LAC
#MOBILE_CID	Cell Tower ID, Cid
#MOBILE_IMSI	IMSI, International Mobile Subscriber Identity
#MOBILE_IMEI	IMEI, International Mobile Equipment Identity
#MOBILE_IMEI_RAW	IMEI raw data
#MOBILE_USBID	mobile modem, usb vendor id, product id
#MOBILE_DATA_DAY	Cellular data, current day used traffic
#MOBILE_DATA_MONTH	Cellular data, current month used traffic

Name	Description
#MOBILE_DATA_YEAR	Cellular data, current year used traffic
#WLAN0_SIGNAL_QUALITY	Signal quality of wlan0
#WLAN0_SIGNAL_LEVEL	Signal level of wlan0
#WLAN0_SIGNAL_NOISE	Signal noise of WLAN0
#WLAN0_SIGNAL_BITRATE	Bit rate of WLAN0
#WLAN0_AP_MAC	MAC or BSSID in Wifi AP mode
#ICDM_COM1_SCORE	COM 1 score
#ICDM_COM2_SCORE	COM 2 score
#ICDM_COM3_SCORE	COM 3 score
#ICDM_LAN1_SCORE	LAN 1 score
#ICDM_LAN1_LINK	LAN 1 link state
#ICDM_LAN2_SCORE	LAN 2 score
#ICDM_LAN2_LINK	LAN 2 link state
#GPS_LATITUDE	Latitude for the GPS module
#GPS_LONGITUDE	Longitude for the GPS module
#GPS_ALTITUDE	Altitude for the GPS module
#GPS_SPEED	Speed for the GPS module

Name	Description
#GPS_COURSE	Course for the GPS module
#GPS_SATELLITE	Status of the GPS module: 0-error state, 1-use GPS module working, 2-use a preset location information
#SYS_BATTERY_LOW	Battery power: 1 indicates that the battery is low, 0 indicates that the battery is normal
#SYS_TIME_SECOND	(0~59, when leap seconds: 60)
#SYS_TIME_MINUTE	Minutes（0~59）
#SYS_TIME_HOUR	Hours (0~23)
#SYS_TIME_DAY	Day (1~31)
#SYS_TIME_MONTH	Month (1~12)
#SYS_TIME_YEAR	Year (for example,2016)
#SYS_TIME_WDAY	Week (0~6, Sunday: 0, Monday to Saturday: 1~6)
#SYS_TIME_YDAY	Number of days from the beginning of the annual January 1st (0~365,January 1st: 0, January 2nd: 1, and so on)

Name	Description
#SYS_TIME_ISDST	Daylight saving time identifier, implementing daylight saving time, the value is positive. Do not implement the time in the summer, the value is 0. Cannot be determined when the value is negative
#SYS_TIME_GMT_OFFSET	The deviation of GMT seconds and local time, the eastern time zone is positive and negative for West Zone, such as China, should be 28800
#DATALOG_ENABLE	Enable Datalogger storage when the value is 1, and stop storage when the value is 0
#DATALOG_ERROR	When the value of DATALOG_ERROR is 0, it means that there is no error in the program. Check the manual for other error code information
#SYS_MAC_LAN1	MAC address of lan1

Name	Description
#SYS_MAC_LAN2	MAC address of lan2
#SYS_TFCARD_CAPACITY	TF card capacity(Byte)
#SYS_TFCARD_FREE_SPACE	TF card root partition free space(Byte)
#SYS_SDCARD_CAPACITY	SD card capacity(Byte),the value is 0 if there is no SD card
#SYS_SDCARD_FREE_SPACE	SD card free space(Byte),the value is 0 if there is no SD card
#SYS_DNP3_AI_POLLED_COUNTER	The number of times AI data was polled in DNP3 Outstation
#MQTTStatus_WISE-Edge365_0	0- Not connected; 1- Connecting; 2- Connected, subscribing to topics; 3- Connected，the topics is subscribed

Special system tag description

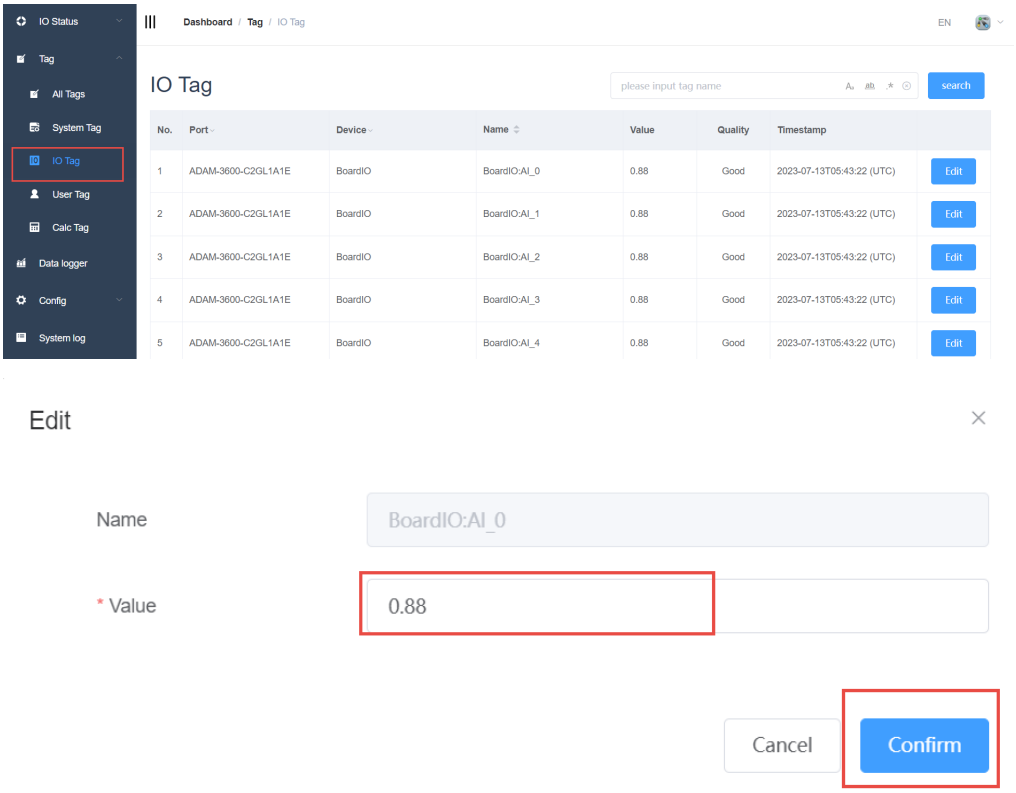
- **#DATALOG_ENABLE** ： Read-write, enabling DataLogger storage when the value is 1 and stopping the DataLogger storage when the value is 0
- **#DATALOG_ERROR** ： Read-only, 0—The program runs normally, other error codes need to be found in the

DataLogger manual section

- **#DISABLE_DEVICE_MeterName** ： Read-write, each meter in the DataCenter has its own tag, distinguished by the name of the meter. 0—meter available, 1—meter not available. For example, if the meter name is Test Device 1, there will be a corresponding system tag #DISABLE_DEVICE_ Test Device 1, through which the meter can be disabled or started
- **#BATCH_WRITE_MeterName** ： Read-write, each meter in the DataCenter has its own tag, distinguished by the name of the meter. 0—meter single point write, 1—meter batch write. For example, if the name of the meter is testdevice1, there will be a corresponding system point #BATCH_WRITE_ testdevice1, through which the writing method of the meter can be set
- **#DEVICE_ERROR_MeterName** ： Read-only, each meter in the DataCenter has its own tag, distinguished by the name of the meter. The error code when the current meter is collecting errors. For example, if the instrument name is TestDevice1, there will be a corresponding system tag #DEVICE_ERROR_TestDevice1, through which the current meter collection status can be viewed
- **#DISABLE_PORT_PortName** ： Read-write, each port has its own tag, 0—port available, 1-disable port. For example, the COM1 port will have a corresponding system tag #DISABLE_PORT_COM1, through which the port can be turned on or disabled

IO Tag reading and setting

Support the reading and setting of IO tags, for the tags that need to be edited, you can click the edit button at the end of the corresponding point to enter the editing interface:

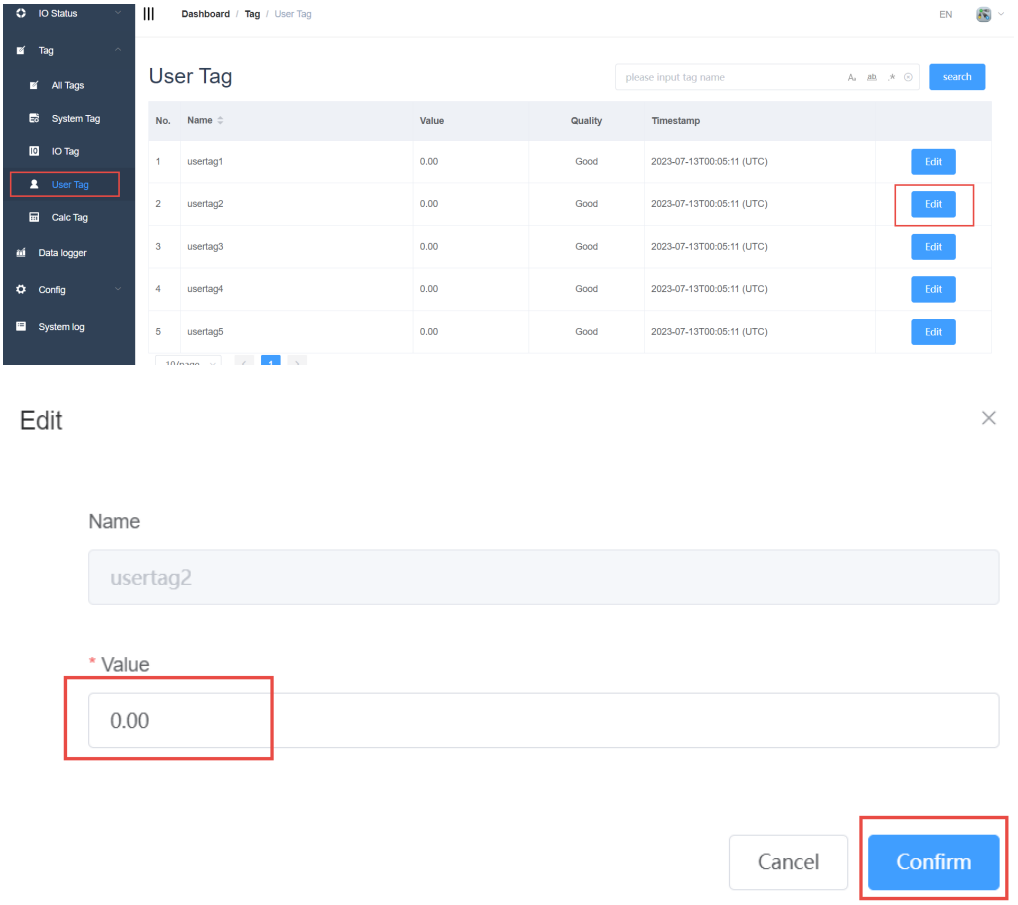


Search of Tags：

Tag Search

User Tag

User Tag support the reading and setting of user-defined points, click the edit button to enter the editing interface:

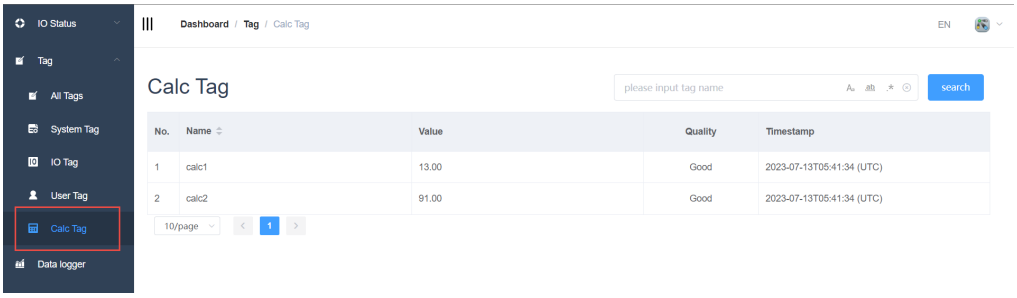


Search of Tags：

Tag Search

Calculate Tag

Read of Calculate Tag

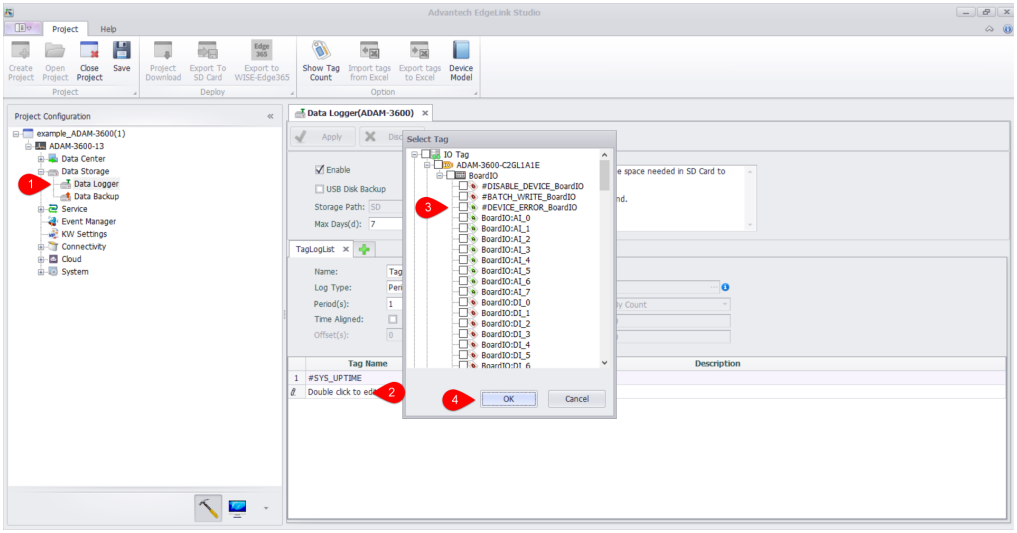


Search of Tags：

Tag Search

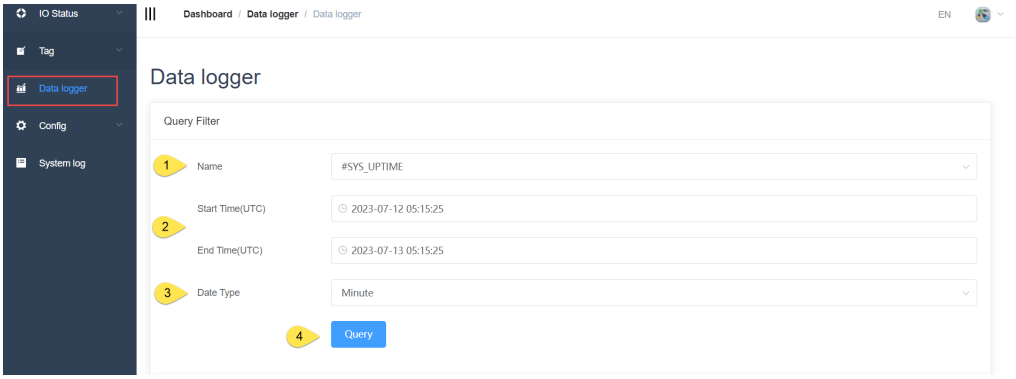
DataLogger

Users can view historical data stored on the device. First, the user needs to configure the “DataLogger” in the project interface.



After downloading the project to the device, you can view the stored data on the “DataLogger” page of the online.

The query properties are as follows:

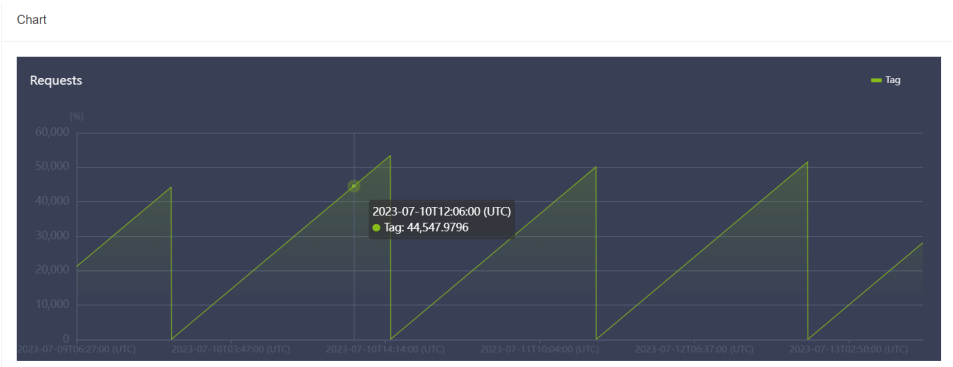


1. Select the tag name
2. Select the start time and end time of the data storage
3. Select the statistics time of the query, select: minutes/hours/days/all data

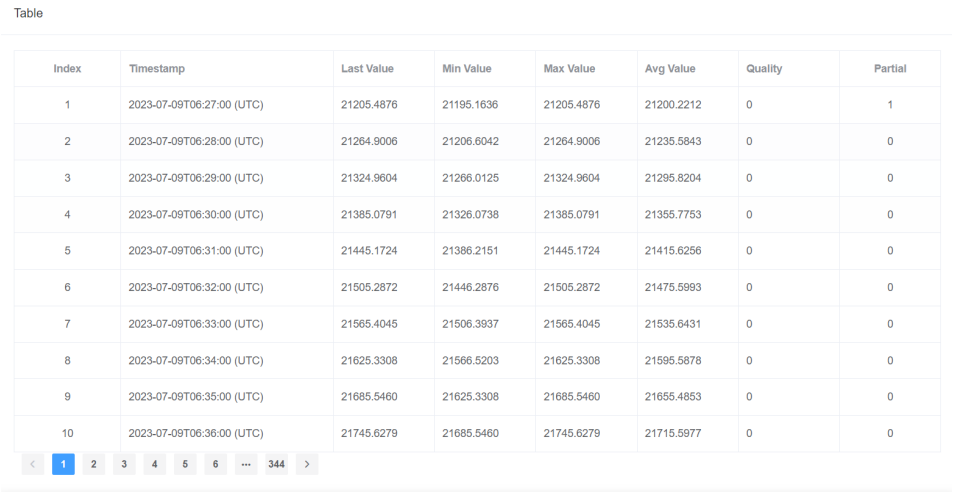
4. Click Quary

Users can view data in three ways

1. Chart:



2. Table:

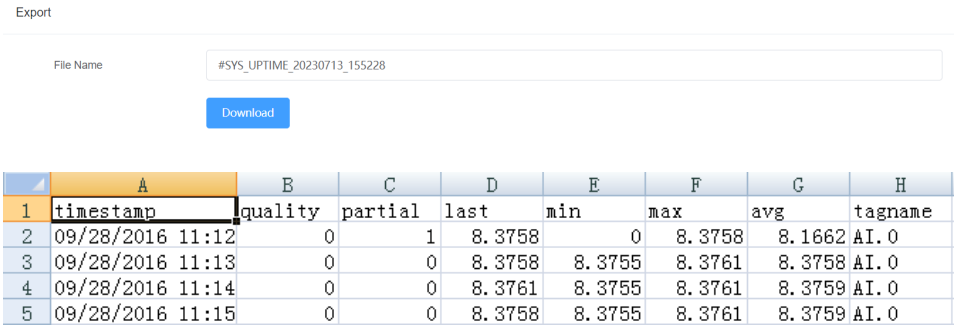


Table

Index	Timestamp	Last Value	Min Value	Max Value	Avg Value	Quality	Partial
1	2023-07-09T06:27:00 (UTC)	21205.4876	21195.1636	21205.4876	21200.2212	0	1
2	2023-07-09T06:28:00 (UTC)	21264.9006	21206.6042	21264.9006	21235.5843	0	0
3	2023-07-09T06:29:00 (UTC)	21324.9604	21266.0125	21324.9604	21295.8204	0	0
4	2023-07-09T06:30:00 (UTC)	21385.0791	21326.0738	21385.0791	21355.7753	0	0
5	2023-07-09T06:31:00 (UTC)	21445.1724	21386.2151	21445.1724	21415.6256	0	0
6	2023-07-09T06:32:00 (UTC)	21505.2872	21446.2876	21505.2872	21475.5993	0	0
7	2023-07-09T06:33:00 (UTC)	21565.4045	21506.3937	21565.4045	21535.6431	0	0
8	2023-07-09T06:34:00 (UTC)	21625.3308	21566.5203	21625.3308	21595.5878	0	0
9	2023-07-09T06:35:00 (UTC)	21685.5460	21625.3308	21685.5460	21655.4853	0	0
10	2023-07-09T06:36:00 (UTC)	21745.6279	21685.5460	21745.6279	21715.5977	0	0

‹ 1 2 3 4 5 6 ··· 344 ›

3. Output to Excel document and download, users can download the document in the browser, this feature is not supported in Studio temporarily.

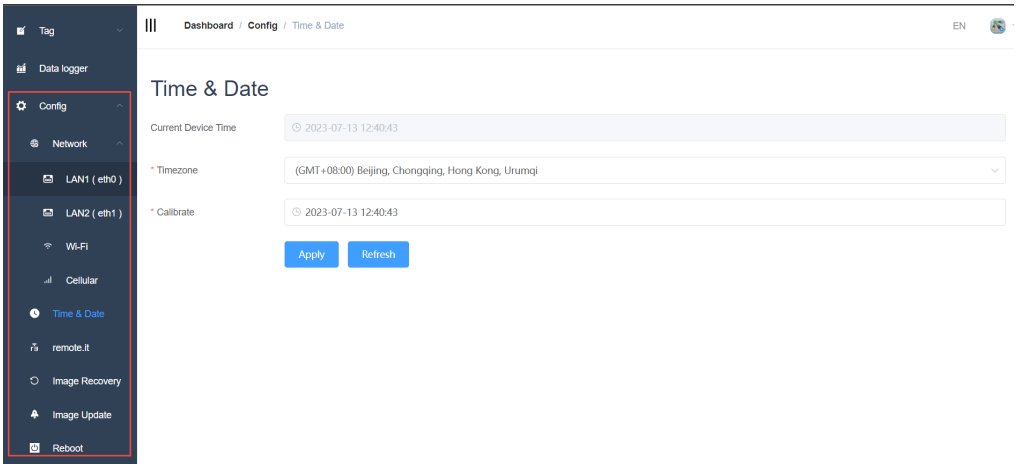


	A	B	C	D	E	F	G	H
1	timestamp	quality	partial	last	min	max	avg	tagname
2	09/28/2016 11:12	0	1	8.3758	0	8.3758	8.1662	AI.0
3	09/28/2016 11:13	0	0	8.3758	8.3755	8.3761	8.3758	AI.0
4	09/28/2016 11:14	0	0	8.3761	8.3755	8.3761	8.3759	AI.0
5	09/28/2016 11:15	0	0	8.3758	8.3755	8.3761	8.3759	AI.0

Config

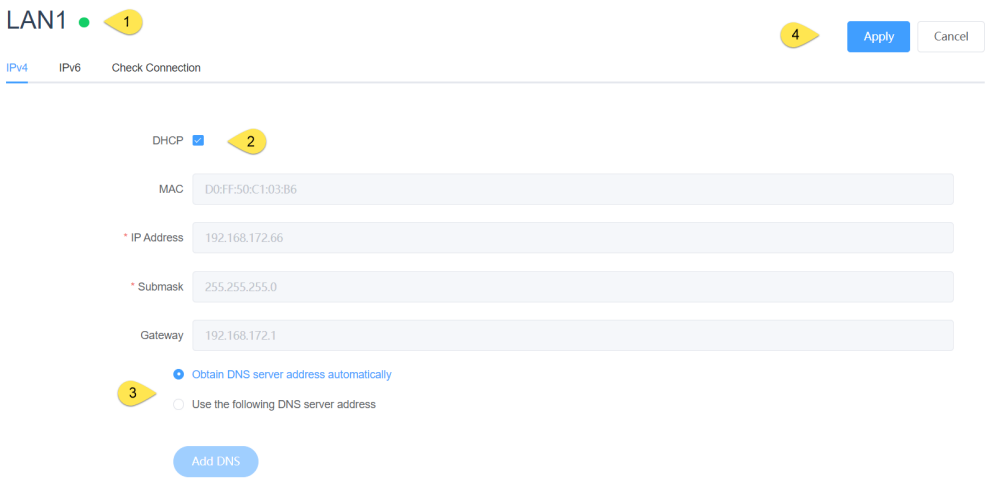
There are mainly the following functions:

1. Network Setting
2. Time and Date
3. remote.it
4. Image Recovery
5. Image Update
6. Reboot



LAN

General



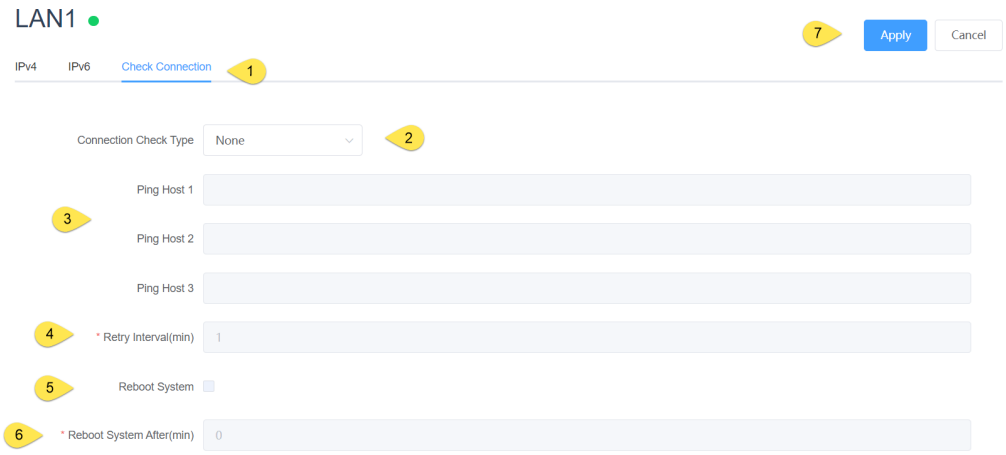
1. led status

status	description
green	The network is connected
yellow	A network cable was detected, but not connected to the network
red	The network cable is unplugged

2. When checked, it is DHCP mode, and when it is unchecked, it is static IP mode, and you can set the IP address, subnet mask, and gateway
3. DNS servers can be obtained automatically or added manually
4. Effective after apply

Check Connection

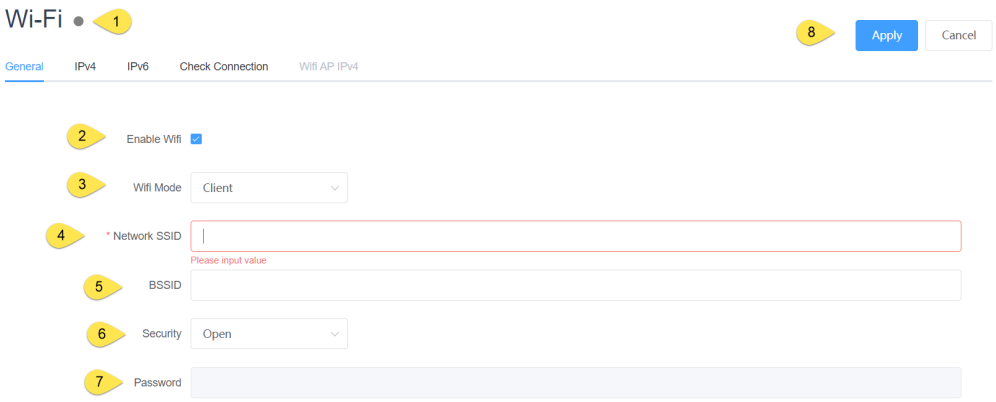
The connection mechanism is checked in order to make the network recoverable through some attempts in case the network is not available, including rebooting the network card and rebooting the device (customer choice)



1. Swtich to Check Connection
2. Select the connection judgment mechanism, which currently supports Ping IP/URL
3. Ping host(1) Please fill in the IP or URL that can be accessed under normal network conditions
4. Retry interval: The interval between ping commands
5. Check whether to restart the device
6. How long to restart the device when checking that the network cannot be connected and the network card cannot be restored by turning it back on
7. Effective after apply

Configure of Wifi

General



1. led status

Status	Description
grey	The module is unplugged
green	The module has been detected and a network connection has been established
red	Module detected but no network connection is established

2. Whether Wifi networks are enabled

3. Mode：Client or AP

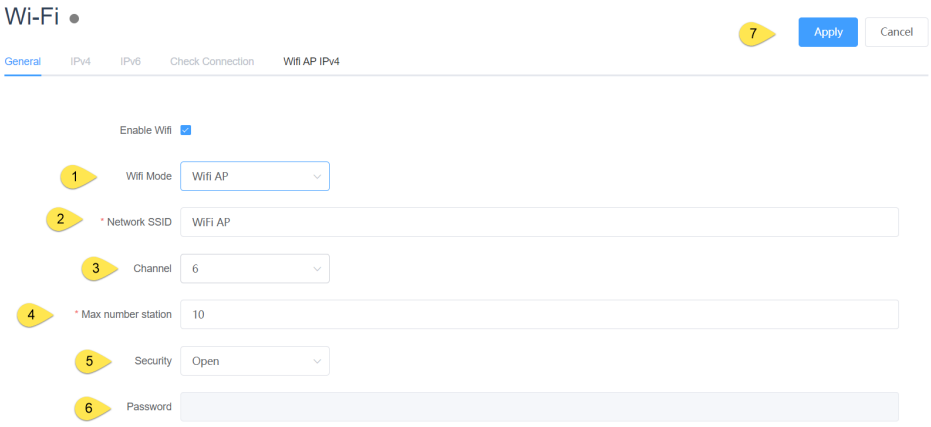
Client Mode

4. The SSID of the network that the Wifi module connects to in Client mode

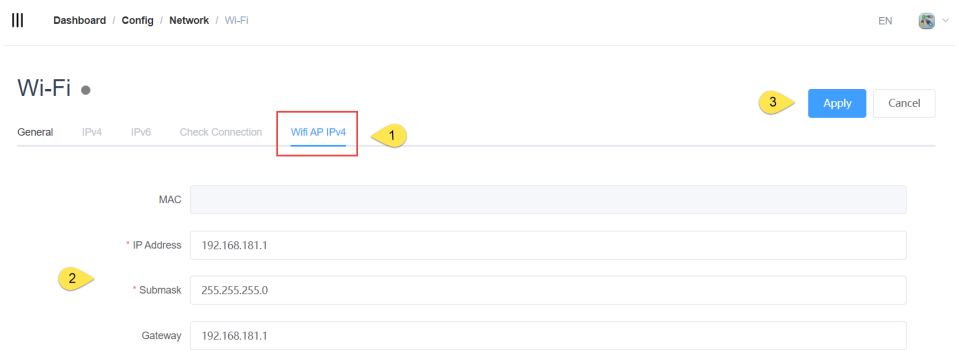
5. BSSID:Optional. Fill in this field when you need to connect to a specific AP.

6. Security：Open、WEP、WPA/WPA2 PSK
7. Password
8. Effective after apply

AP Mode



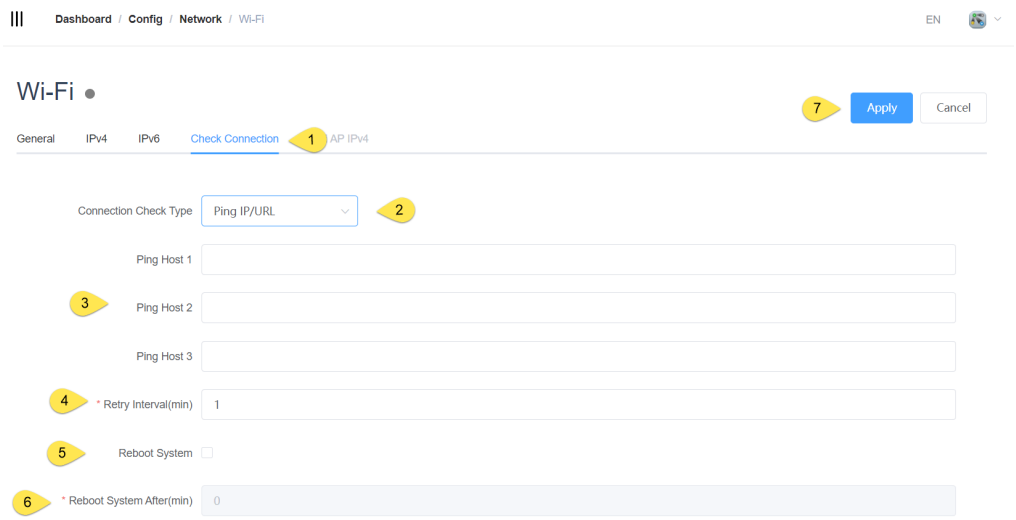
1. select Wifi AP Mode
2. The SSID is a unique identifier for a wireless network that is used to distinguish it from other nearby networks.
3. Channel: Defaults to 6 and depends on the module.
4. Maximum number of stations: This refers to the maximum number of clients that the AP allows to connect to it.
5. Security：Open、WPA/WPA2 PSK
6. Password：Password for AP
7. Effective after apply



1. select Wifi AP IPv4
2. set up the IP range to be allocated to clients in AP mode
3. Effective after apply

检查连接（Client模式）

The connection mechanism is checked in order to make the network recoverable through some attempts in case the network is not available, including rebooting the network card and rebooting the device (customer choice)

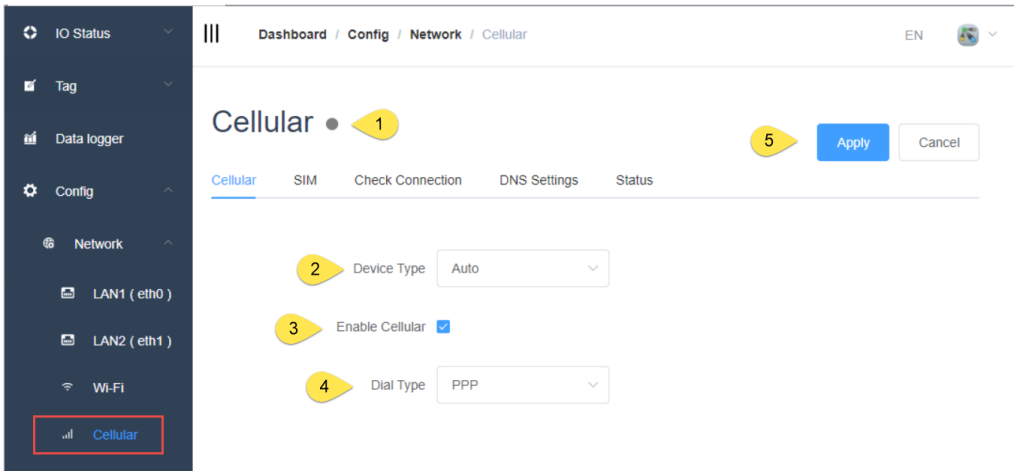


1. Swtich to Check Connection

2. Select the connection judgment mechanism, which currently supports Ping IP/URL
3. Ping host(1) Please fill in the IP or URL that can be accessed under normal network conditions
4. Retry interval: The interval between ping commands
5. Check whether to restart the device
6. How long to restart the device when checking that the network cannot be connected and the network card cannot be restored by turning it back on
7. Effective after apply

Celluar Configuration

General



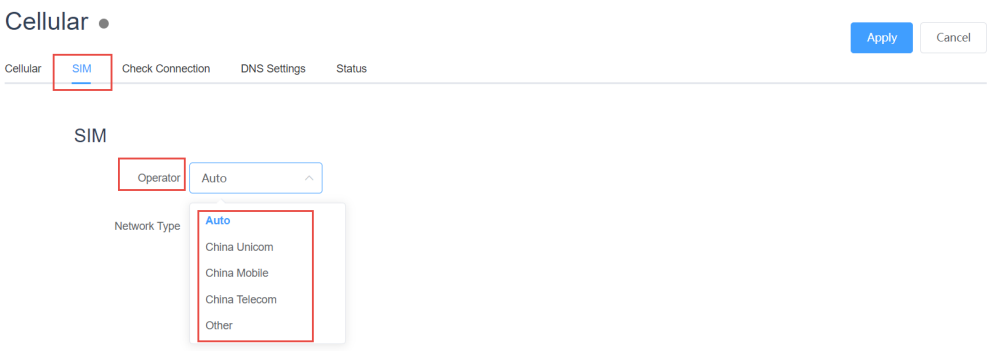
1. Led Status

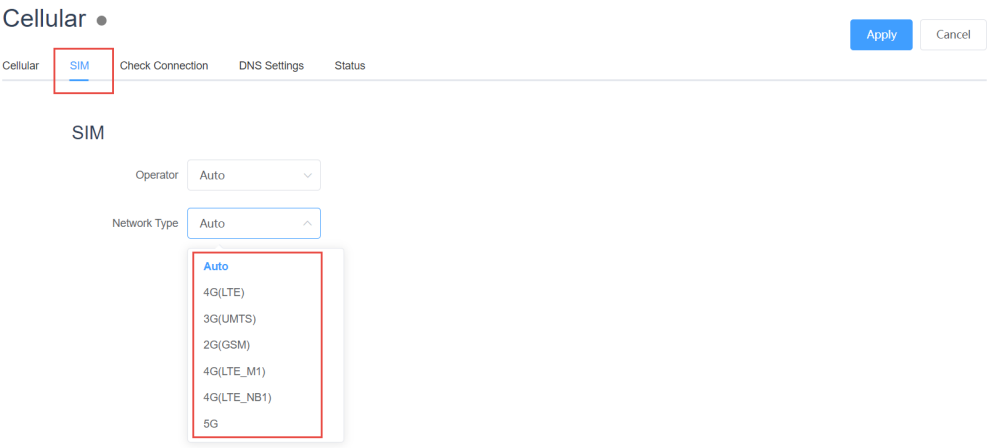
Status	Description
grey	The module is unplugged
green	The module has been detected and a network connection has been established
red	Module detected but no network connection is established

2. Select Module Auto or None
3. Whether cellular networks are enabled
4. Dialing type: PPP or QMI (depending on module)
5. Effective after apply

SIM

The default is Auto mode, which can be configured separately if needed

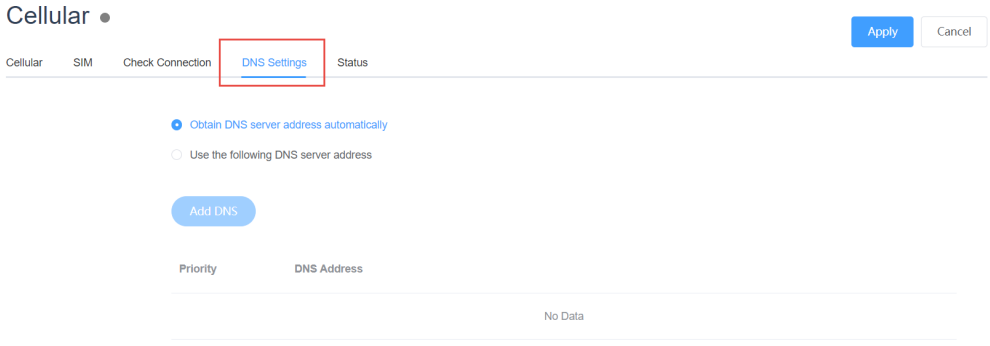




Effective after apply

DNS

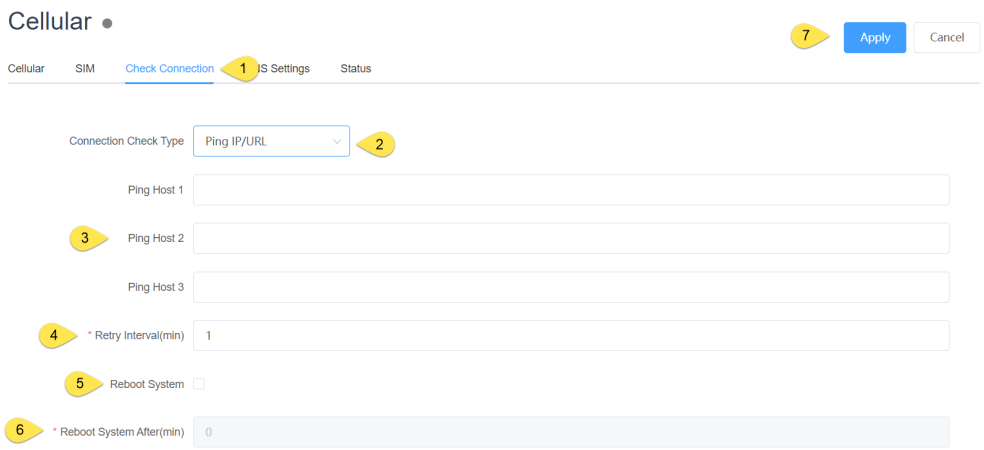
The default is to obtain DNS automatically, or you can configure it manually



Effective after apply

Check Connection

The connection mechanism is checked in order to make the network recoverable through some attempts in case the network is not available, including rebooting the network card and rebooting the device (customer choice)

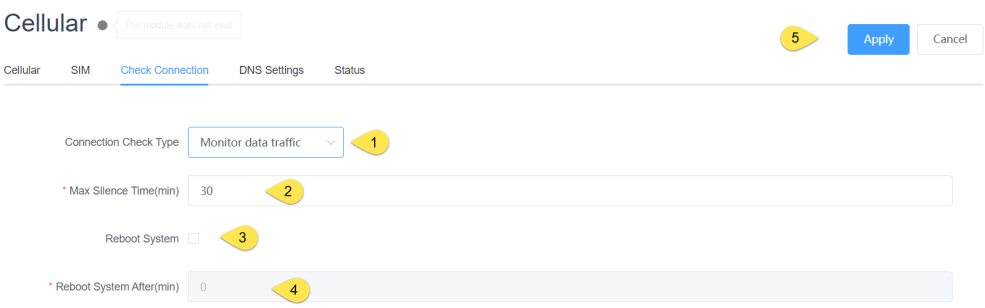


1. Swtich to Check Connection
2. Select the connection judgment mechanism, which currently supports Ping IP/URL and Monitor data traffic

Ping IP/URL Mode

```
3. Ping host(1\2\3) Please fill in the IP or URL that c
4. Retry interval: The interval between ping commands
5. Check whether to restart the device
6. How long to restart the device when checking that th
7. Effective after apply
```

Monitor data traffic Mode

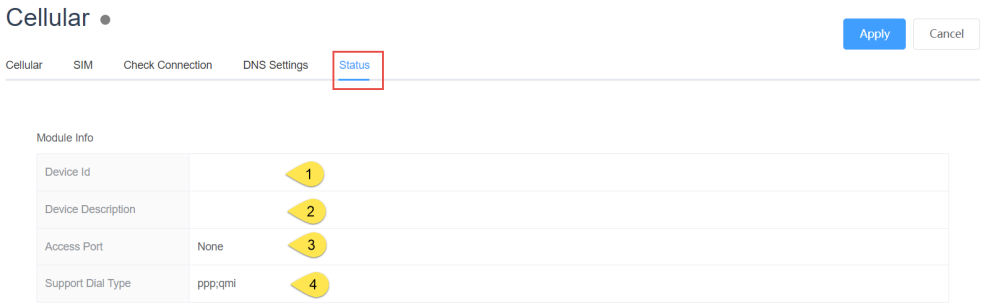



```
1. Choose Monitor data traffic Mode

2. The maximum silence time is the time that no traffic

3. Check whether to restart the device

4. How long to restart the device when checking that th

5. Effective after apply
```

Status

View module status online, divided into two parts, one is module status and the other is Celluar information, including dial-up and network status

Module Status

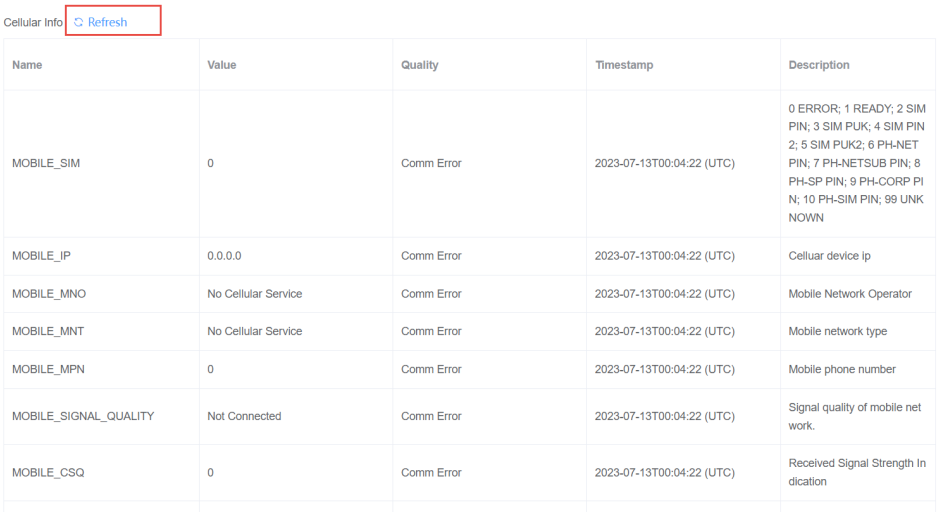


1. Device Id
2. Module Description
3. Access Port

4. Dial Type

Celluar Status

Cellular-related system tag, in order to avoid traffic waste, please click the “Refresh” button to update the current status every time you view it



Name	Value	Quality	Timestamp	Description
MOBILE_SIM	0	Comm Error	2023-07-13T00:04:22 (UTC)	0 ERROR; 1 READY; 2 SIM PIN; 3 SIM PUK; 4 SIM PIN 2; 5 SIM PUK2; 6 PH-NET PIN; 7 PH-NETSUB PIN; 8 PH-SP PIN; 9 PH-CORP PIN; 10 PH-SIM PIN; 99 UNKNOWN
MOBILE_IP	0.0.0.0	Comm Error	2023-07-13T00:04:22 (UTC)	Celluar device ip
MOBILE_MNO	No Cellular Service	Comm Error	2023-07-13T00:04:22 (UTC)	Mobile Network Operator
MOBILE_MNT	No Cellular Service	Comm Error	2023-07-13T00:04:22 (UTC)	Mobile network type
MOBILE_MPN	0	Comm Error	2023-07-13T00:04:22 (UTC)	Mobile phone number
MOBILE_SIGNAL_QUALITY	Not Connected	Comm Error	2023-07-13T00:04:22 (UTC)	Signal quality of mobile net work.
MOBILE_CSQ	0	Comm Error	2023-07-13T00:04:22 (UTC)	Received Signal Strength Indication

Time&Date

Set the current time and time zone of the device

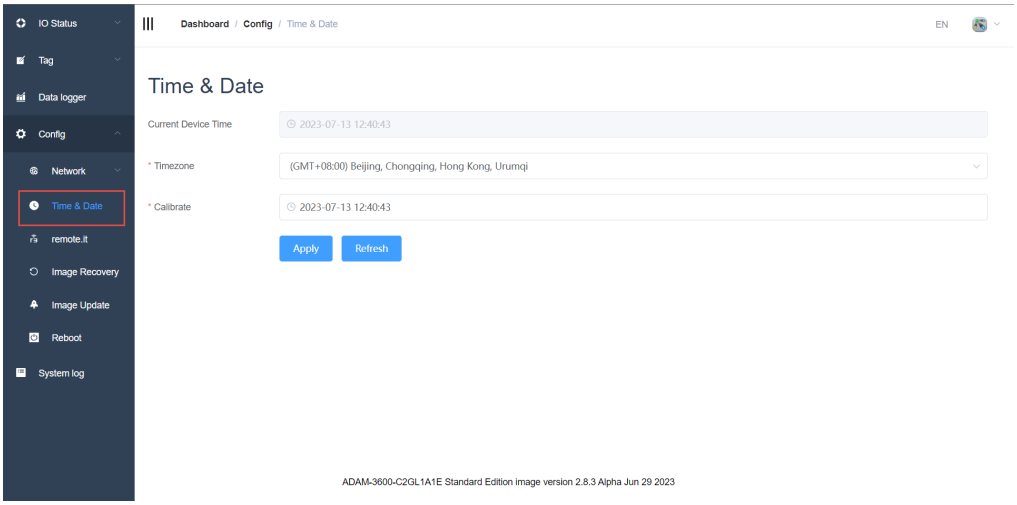
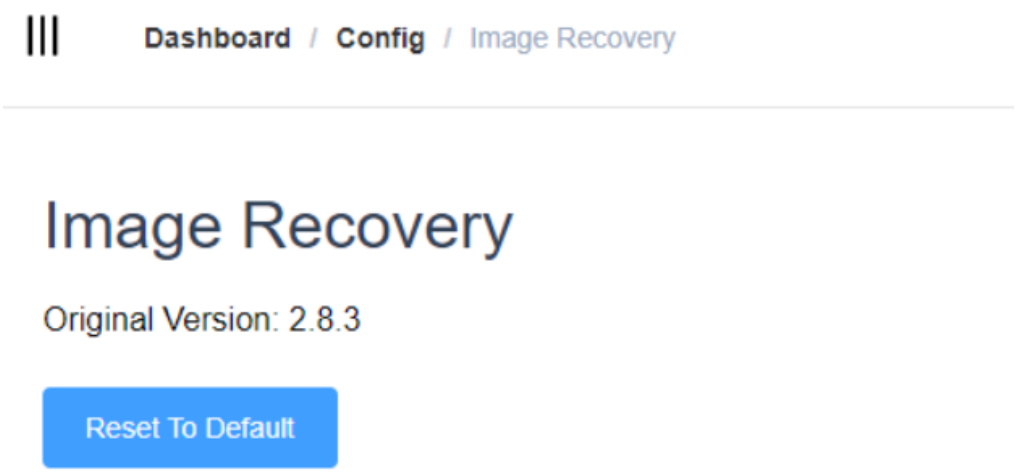


Image Recovery

IThe Image recovery function can help users restore the system version to the initial state of the currently used version



This function clears the configuration that the user has already made, so the permissions are high and a second confirmation is required.

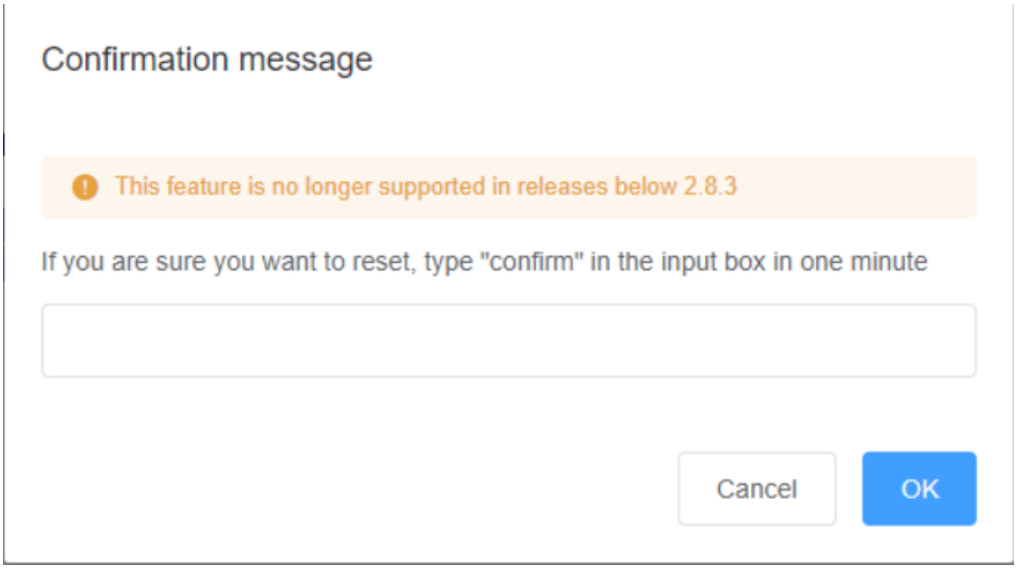
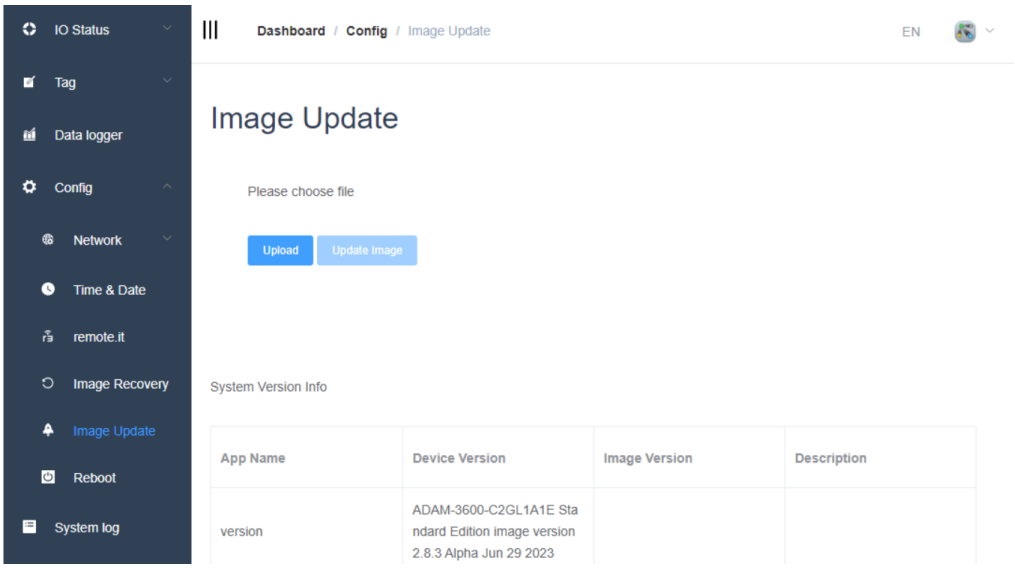


Image Update

The Image update page displays all system version and software version information of the current device, and can realize online firmware and software updates.



Information

The system version information of the current device is displayed as follows:

System Version Info

App Name	Device Version	Image Version	De
MLO			
u-boot.img	U-Boot 2015.07 for adv335x boar		
uImage	Linux-4.9.69-g9ce43c71ae		
ramdisk.gz			
am335x-adam3600.dtb			
System Volume Information			
ADAM-3600-mcu.bin	0 rev 01010194		
ADAM-3600-AI-aio.bin	0 rev 01010130		
ICDMANAGER-icdm.bin	01010148		

The software version information of the current device is displayed as follows:

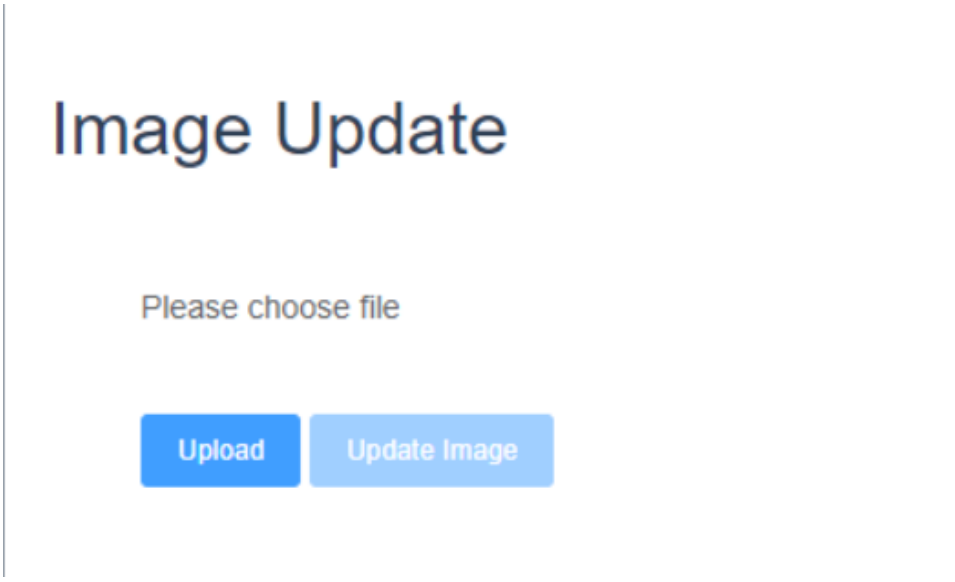
App & Lib Version Info

App Name	Device Version	Image Version
ActiveConnection	2.7.0 rev beeae91bb	
AdvAgentMain	2.7.0 rev beeae91bb	
AdvBurnInTest	2.7.0 rev beeae91bb	
AdvProgramMgr	2.7.0 rev beeae91bb	
AdvSystemSetting	2.7.0 rev beeae91bb	
AdvSystemTag	2.7.0 rev beeae91bb	
AdvUDBackup	2.7.0 rev beeae91bb	
AdvUserTag	2.7.0 rev beeae91bb	
AdvVersion	2.7.0 rev beeae91bb	
AdvWirelessCheckd	2.7.0 rev beeae91bb	
AutoDialup4G	2.7.0 rev beeae91bb	
BacnetDaemon	2.7.0 rev beeae91bb	
CalcTag	2.7.0 rev beeae91bb	
DNP3Daemon	2.7.0 rev beeae91bb	

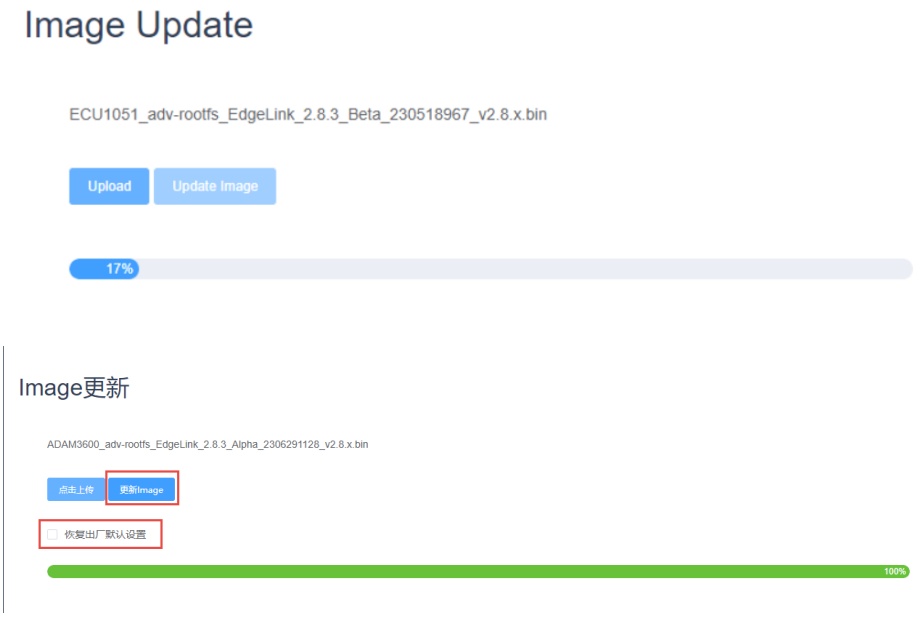
Image Update

> ! **Note**：You must first log in for this operation

1. Click Upload to select the bin file to be updated.



2. The process of uploading the file is shown below, and the whole process takes about a few minutes.



Before updating, you can choose whether to check ‘Restore factory default settings’, if checked, the original configuration will be cleared after the upgrade.

3. If the file is successfully uploaded, the ‘Update Image’ button will be displayed, as shown in the red box above. At the same time, the version number of each file in the uploaded package is listed, as shown in the following figure.

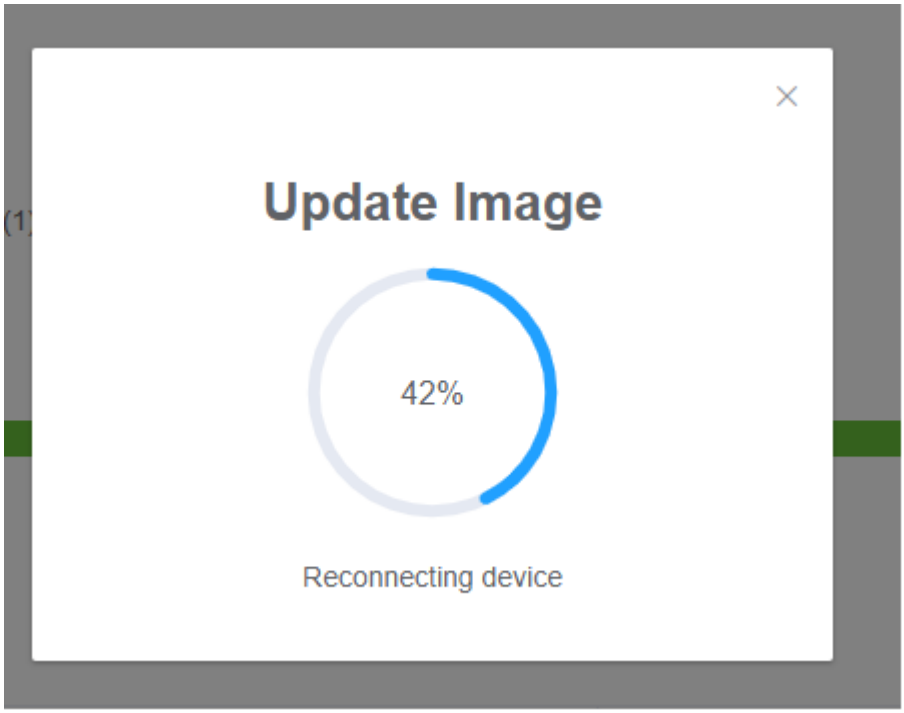
System Version Info

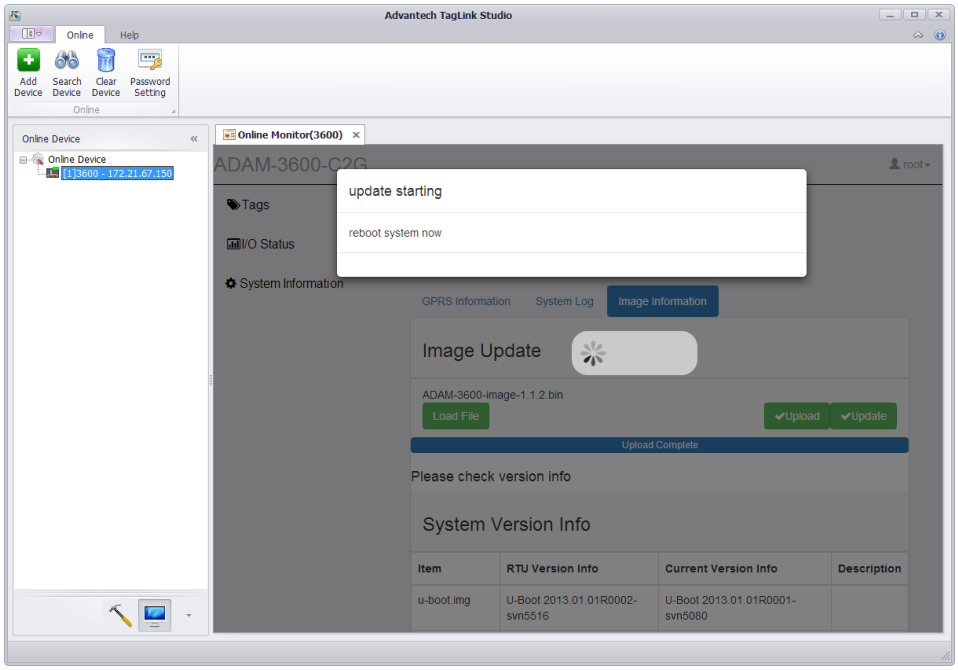
Item	RTU Version Info	Current Version Info	Description
u-boot.img	U-Boot 2013.01.01R0001-svn5080	U-Boot 2013.01.01R0001-svn5080	
uImage	Linux-3.12.10-rt15-ti2013.12.01	Linux-3.12.10-rt15-ti2013.12.01	
ramdisk.gz			
am335x-adam3600.dtb			
ADAM-3600-mcu.bin	0 rev 01010168	0 rev 01010169	
ADAM3600AI-aio.bin	0 rev 01010124	0 rev 01010124	
ADAM-3656-mcu.bin	2 rev 01010166	2 rev 01010169	
ICDMANAGER-icdm.bin	0xc0 rev 01010147	0xc0 rev 01010147	
rootfs.tar.gz	ADAM-3600-C2GL1AE image version 1.1.0 Release Aug 7 2015	ADAM-3600-C2GL1A1E image version 1.1.2 Release Sep 06 2015	

App & Lib Version Info

App Name	Device Version	Image Version
ActiveConnection	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvAgentMain	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvBurnInTest	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvProgramMgr	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvSystemSetting	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvSystemTag	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvUDBackup	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvUserTag	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvVersion	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AdvWirelessCheckd	2.7.0 rev beeae91bb	2.7.0 rev beeae9
AutoDialup4G	2.7.0 rev beeae91bb	2.7.0 rev beeae9
BacnetDaemon	2.7.0 rev beeae91bb	2.7.0 rev beeae9
CalcTag	2.7.0 rev beeae91bb	2.7.0 rev beeae9

4. Click Update to start the Image update, and the update process is shown in the following figure.

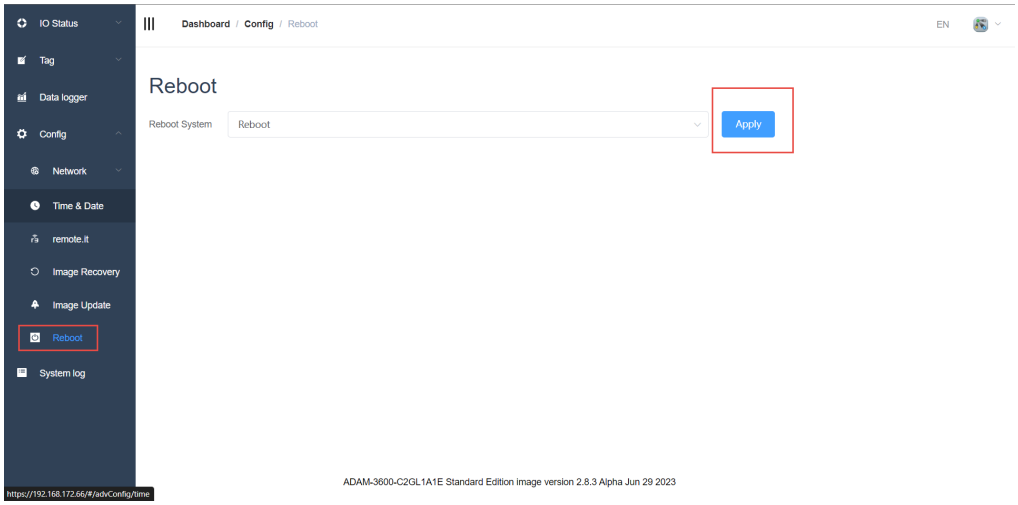




5. After the update is complete, the EdgeLink device will restart, and after restarting, it will jump to the login interface, and the user can log in before performing subsequent operations.

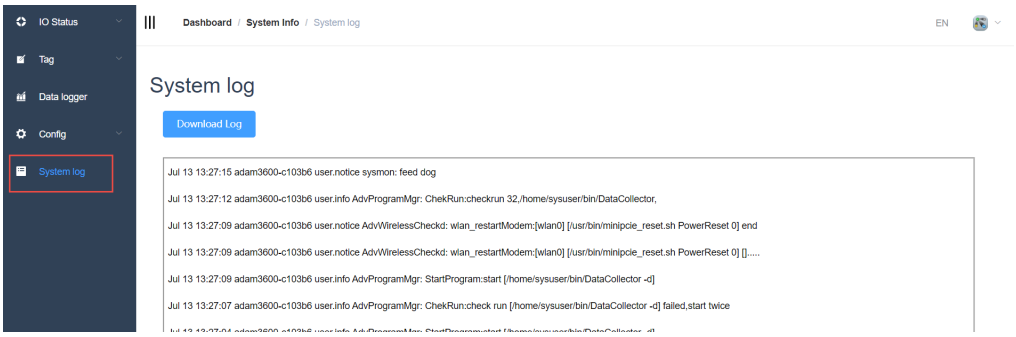
Reoobt

Restart the gateway online



System Log

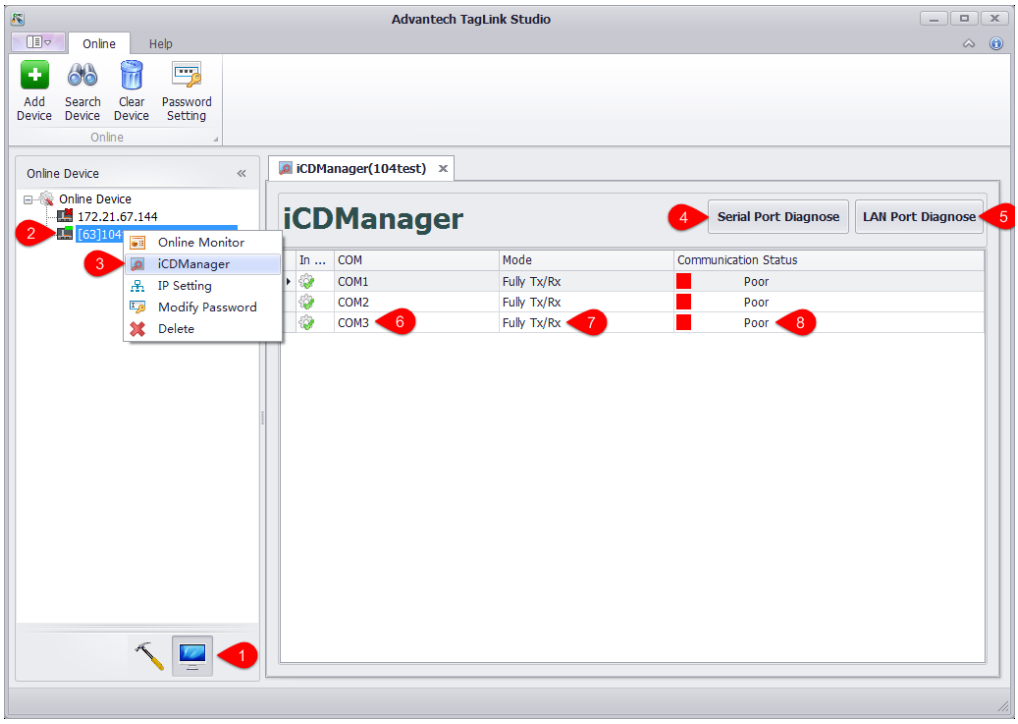
You can view the system logs of the device.



iCDManager

iCDManager is a communication monitoring unit which can diagnose both LAN port and serial port. For LAN port, iCDManager will acquire the network status information output by the network card to test its current status; for serial port, iCDManager will acquire the communication signals on physical layer of the serial port to obtain the related information, including its active status and the response time of the data package on serial port.

Main Interface of iCDManager



As shown in the figure above, right-click on the device name go to “iCDManager” page.

1. Click “Online” button.

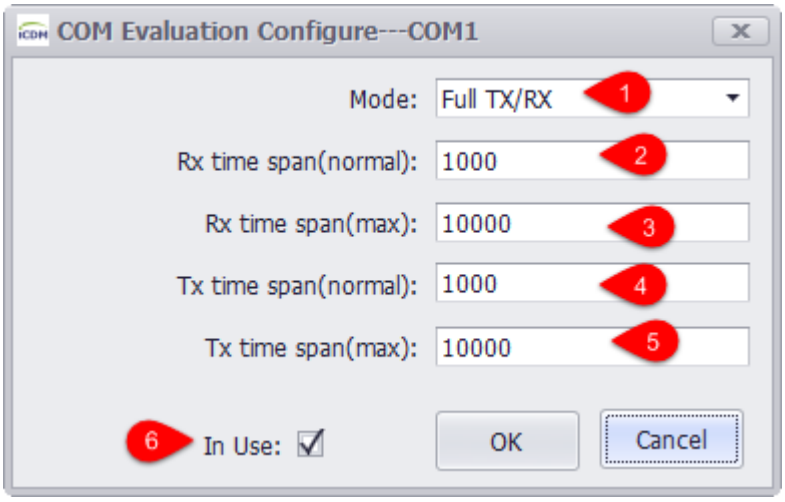
2. Select a device.
3. Right-click on the device name to open “iCDManager” page.
4. Click “Serial Port Diagnose” button to view the communication status of the serial port. The interface is shown as the above when it is opened for the first time.
5. Click “LAN Port Diagnose” button to view the communication status of the LAN port. Please refer to “Network Monitoring” for its interface.
6. Display the name of the serial port. Double-click it to pop up the parameter configuration window (refer to “Parameter Configurations of Serial Port”).
7. Show the monitoring mode (refer to “Parameter Configurations of Serial Port”).
8. Show the communication status: “Poor”, “Good” and “Excellent” (refer to “Monitoring Status Tips”).

Parameter Configurations of Serial Port

The time unit here is ms by default.

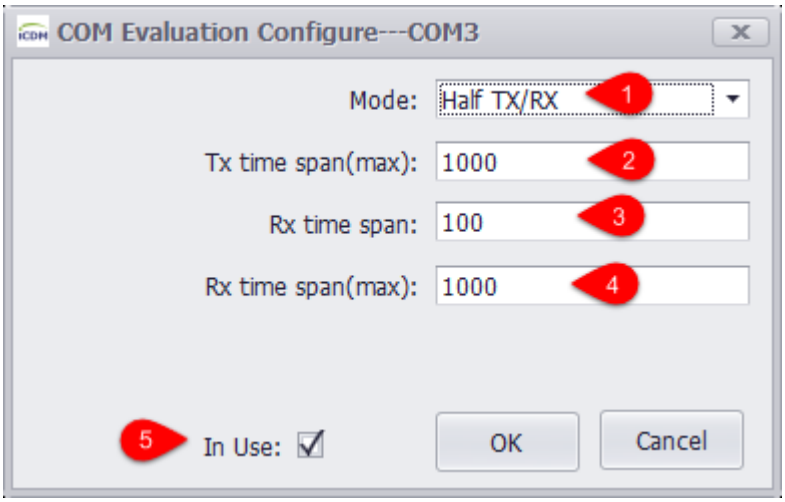
Full tx/rx

The parameters are described as follows:



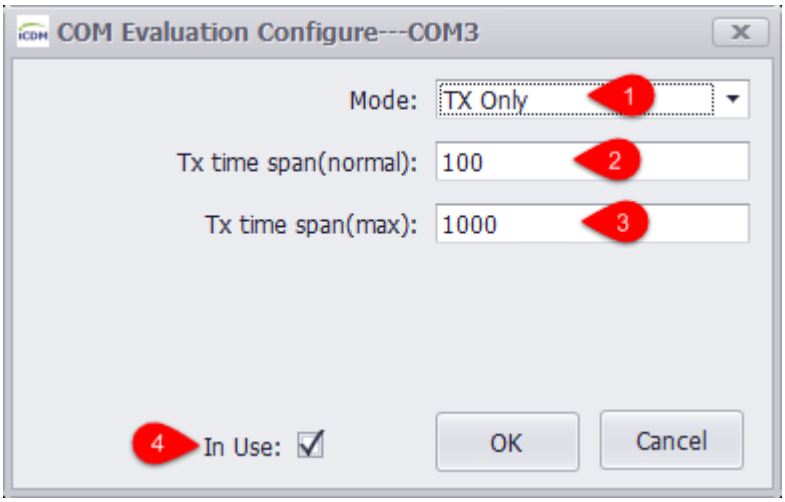
1. Here the monitoring mode is set to “Full tx/rx” which means full function monitoring mode.
2. The minimum time span for receiving line to monitor the signal level variation. If the actual time span is less than it, the monitoring result will be excellent.
3. The maximum time span for receiving line to monitor the signal level variation. If the actual time span is greater than it, the monitoring result will be poor.
4. The minimum time span for transmitting line to monitor the signal level variation. If the actual time span is less than it, the monitoring result will be excellent.
5. The maximum time span for transmitting line to monitor the signal level variation. If the actual time span is greater than it, the monitoring result will be poor.
6. Choose whether to display the information of this port.

Half tx/rx



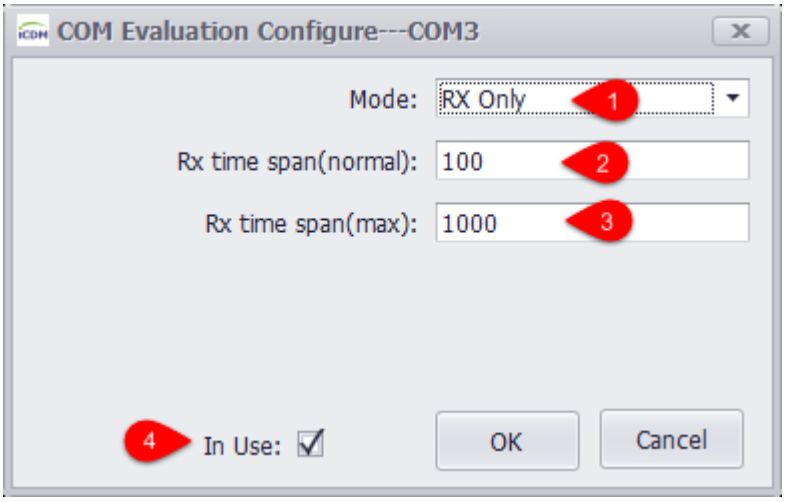
1. Here the monitoring mode is set to “Half tx/rx” which means heartbeat monitoring mode.
2. The maximum time span for transmitting line to monitor the signal level variation. If the actual time span is greater than it, the monitoring result will be poor; if the actual time span is less than it, the heartbeat packet is sent normally and the response time will be monitored.
3. The minimum time span for receiving line to monitor the signal level variation. If the difference between the transmitting time and the receiving time is less than it, the monitoring result will be excellent.
4. The maximum time span for receiving line to monitor the signal level variation. If the difference between the transmitting time and the receiving time is greater than it, the monitoring result will be poor.
5. Choose whether to display the information of this port.

Tx Only



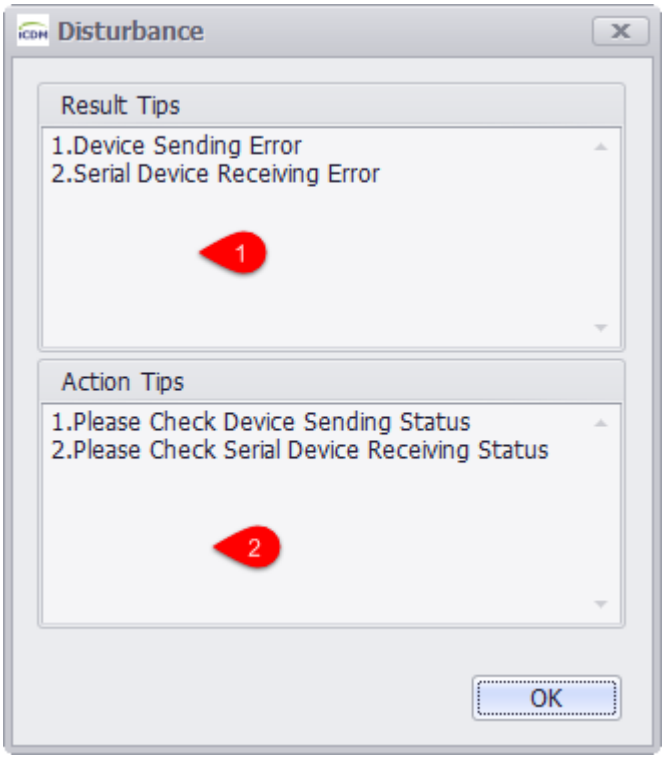
1. Here the monitoring mode is set to “Tx Only” which means only transmitting signals will be monitored.
2. The minimum time span for transmitting line to monitor the signal level variation. If the actual time span is less than it, the monitoring result will be excellent.
3. The minimum time span for receiving line to monitor the signal level variation. If the actual time span is less than it, the monitoring result will be poor.
4. Choose whether to display the information of this port.

Rx Only



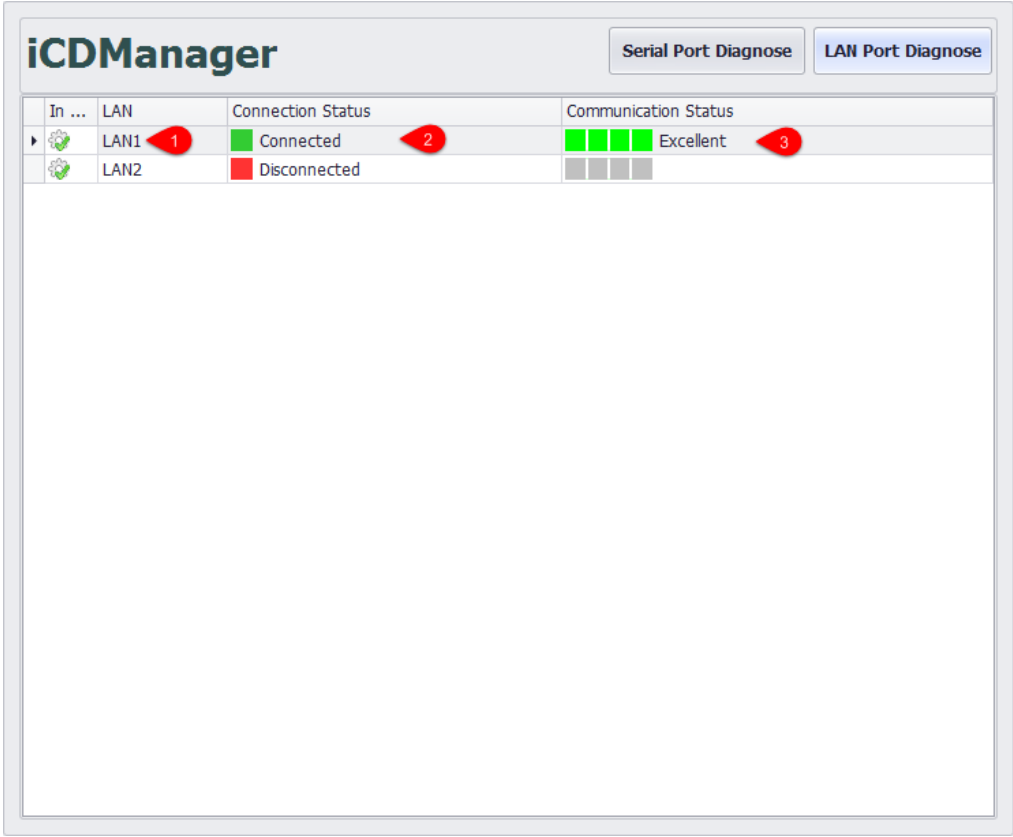
1. Here the monitoring mode is set to “Rx Only” which means only receiving signals will be monitored.
2. The minimum time span for receiving line to monitor the signal level variation. If the actual time span is less than it, the monitoring result will be poor.
3. The maximum time span for receiving line to monitor the signal level variation. If the actual time span is greater than it, the monitoring result will be poor.
4. Choose whether to display the information of this port.

Monitoring Status Tips



1. Result tips.
2. Action tips.

Network Monitoring



1. Network name.
2. Network connection status.
3. Network communication status.

PLC remote maintenance

The remote operation and maintenance described in this article refers to the process where customers configure remote PLCs by running PLC software on their control center computers.

Scenarios:

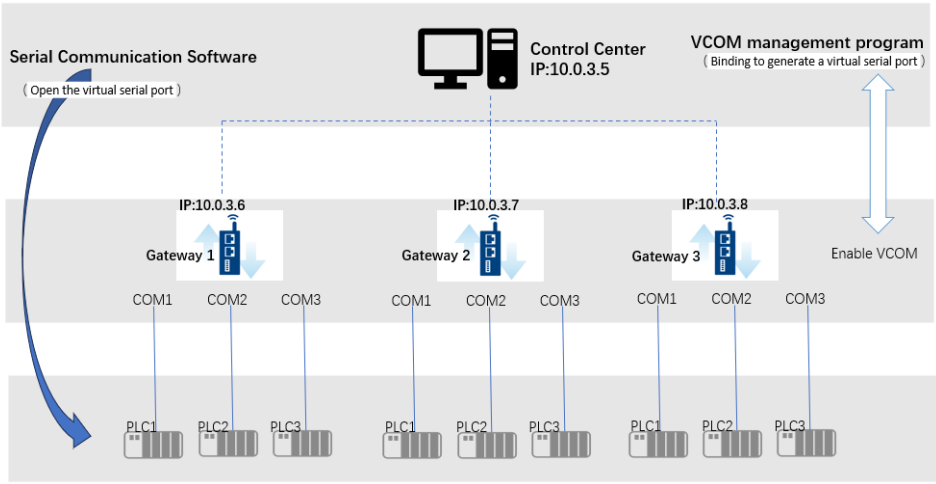
The PLC is a serial device, please refer to 4.1 Serial PLC Remote O&M

The PLC is a Ethernet device, please refer to 4.2 Ethernet PLC O&M

Serial PLC Remote Operation and Maintenance

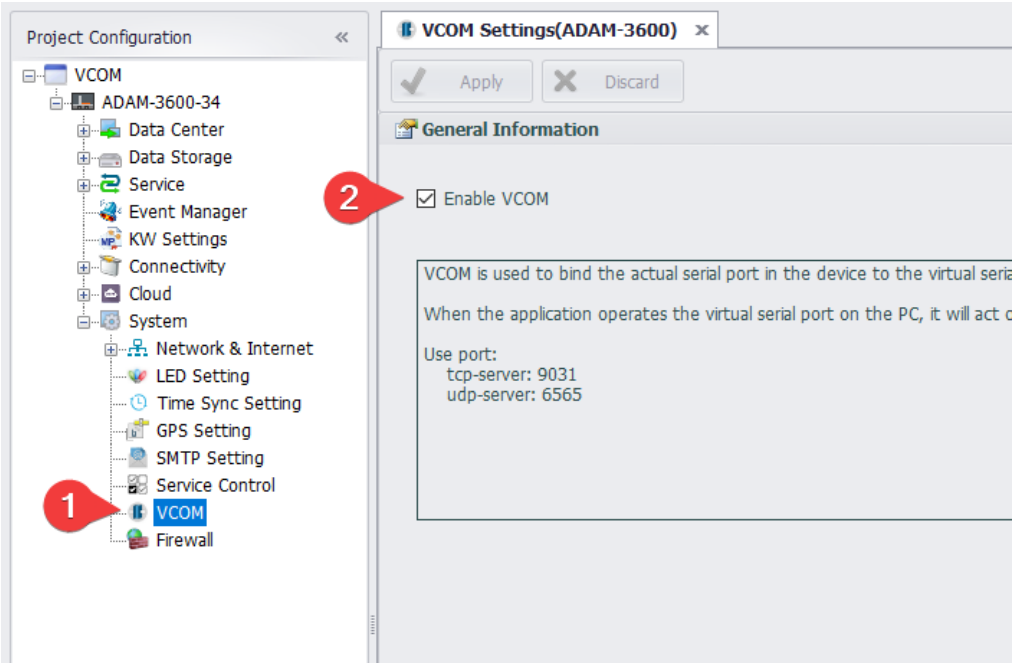
The general scenario involves a network connection (such as VPN) between the PC (control center) and the gateway, with serial devices (such as PLCs) connected below the gateway. Customers expect to use the serial communication software that comes with the serial devices to configure the serial devices on the PC (control center).

Architecture:



Operational Steps:

1. Enable the VCOM function on the gateway using EdgeLink Studio and download the configuration file to the gateway.



2. Install the VCOM management program on the PC (control center). The download link for the VCOM management program installation package is: https://www.advantech.tw/support/details/utility?id=1-24KJ5E7. You can download the installation package that starts with “SetupEdgeLinkVCOM”.

3. Virtualize the gateway’s serial port to the PC (control center) using the VCOM management program. For example, if COM1 of Gateway 1 is connected to PLC1 and you want to configure this PLC, bind COM1 of Gateway 1 to the VCOM management program. At this point, you can see the virtualized serial port and its port number in the VCOM management program.

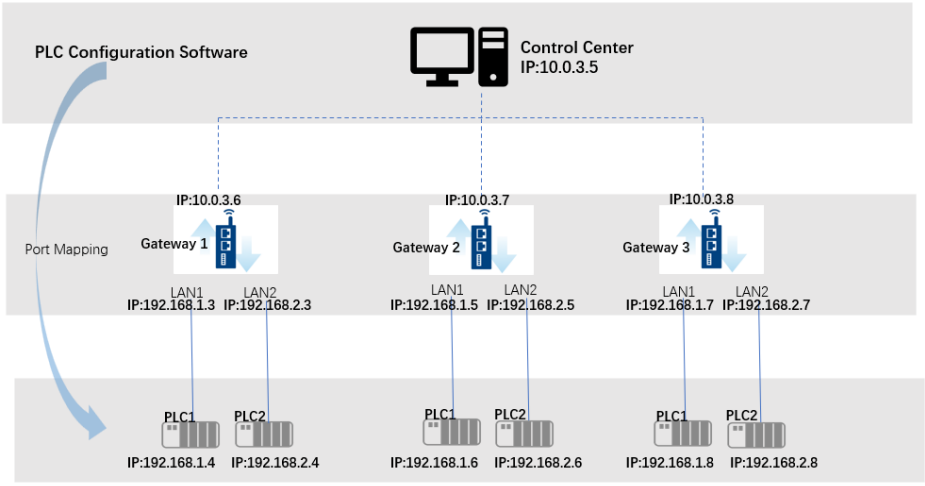
4. Open the virtual serial port through the serial communication software on the PC (control center) to configure the serial device.

For detailed instructions on configuring the VCOM management program, please refer to the 2.9.8 VCOM section.

Ethernet PLC Remote Operation and Maintenance

Scenario 1

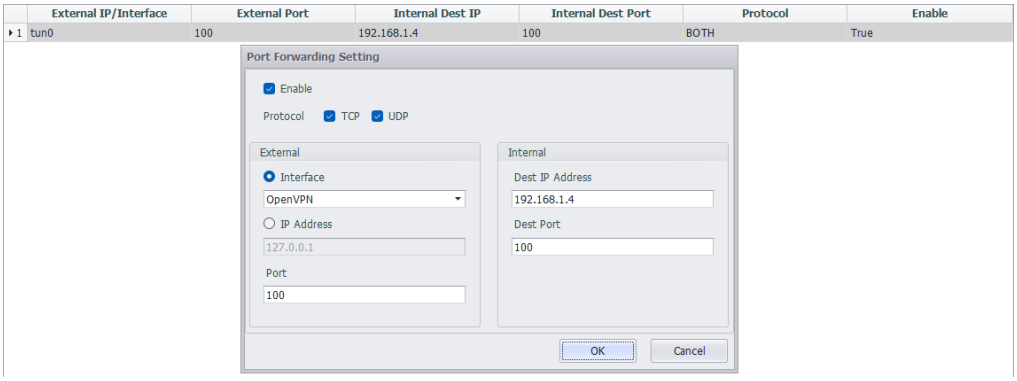
When a single Ethernet port of the gateway is connected to only one PLC, and the PLC configuration software transmits data through a fixed port, remote operation and maintenance can be directly achieved by using port forwarding.



For example, a PC (control center) establishes a network connection with the gateway via VPN. The gateway's LAN1 IP is: 192.168.1.3, and the IP of the PLC connected to LAN1 is: 192.168.1.4. The PLC communication software uses a communication port of: 100.

Operational Steps:

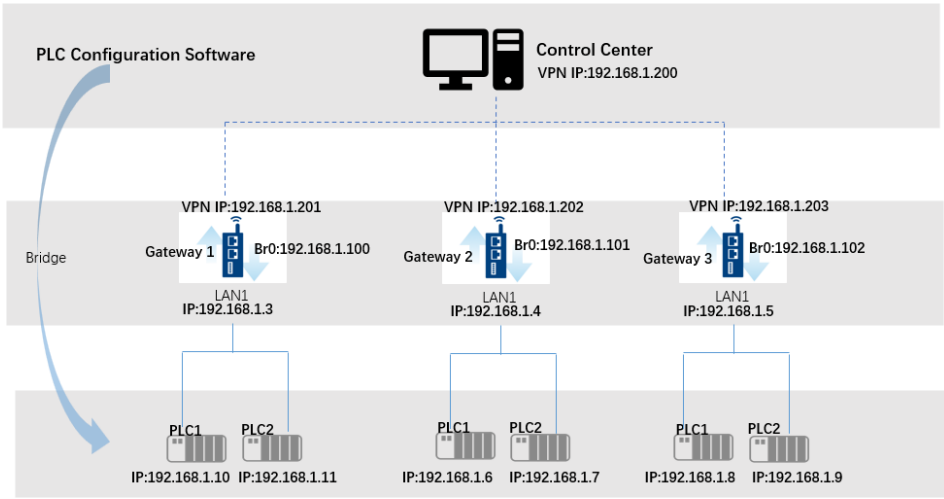
1. Configure the port forwarding on the gateway using EdgeLink Studio and download the project.



2. Open the PLC communication software at the control center to configure the PLC.(Connecting the communication software to 10.0.3.6 will enable the configuration to be pushed down to 192.168.1.4)

Scenario 2

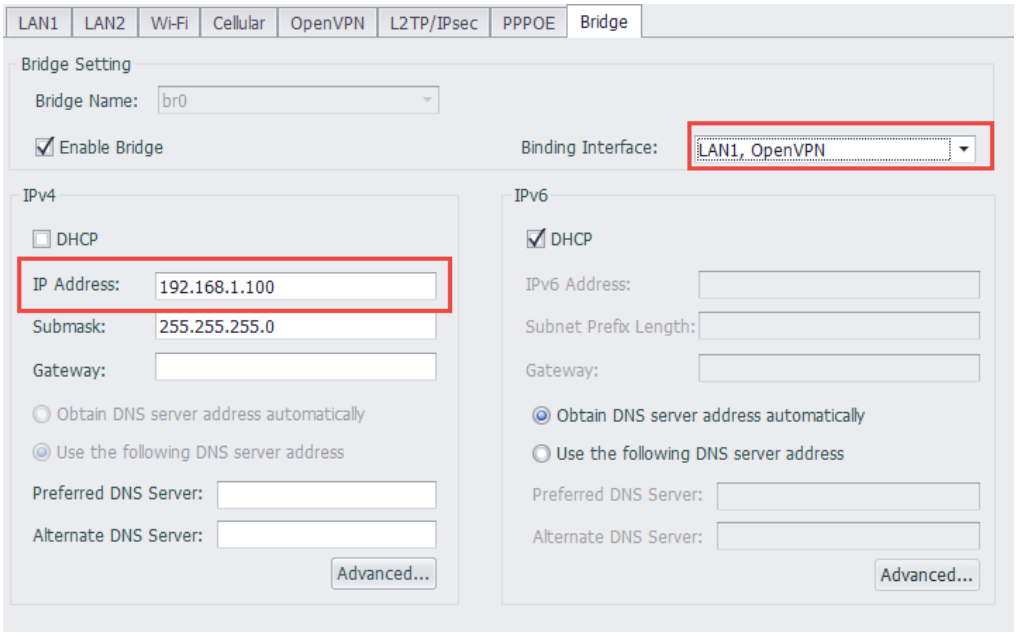
When a single Ethernet port of the gateway connects to multiple PLCs (if there are multiple gateways on site, please note: the IP addresses of the PLCs connected under each gateway must not be duplicated), remote operation and maintenance can be achieved using network bridging.(Please set the VPN to tap mode)



For example, a PC (control center) establishes a network connection with the gateway via VPN, and the VPN IP is set to be in the same subnet as the PLC. As shown in the figure, the PC (control center) VPN IP is: 192.168.1.200, the gateway VPN IP is: 192.168.1.201, the gateway's LAN1 IP is: 192.168.1.3, and the IP of the PLC connected to LAN1 is: 192.168.1.10.

Operational Steps:

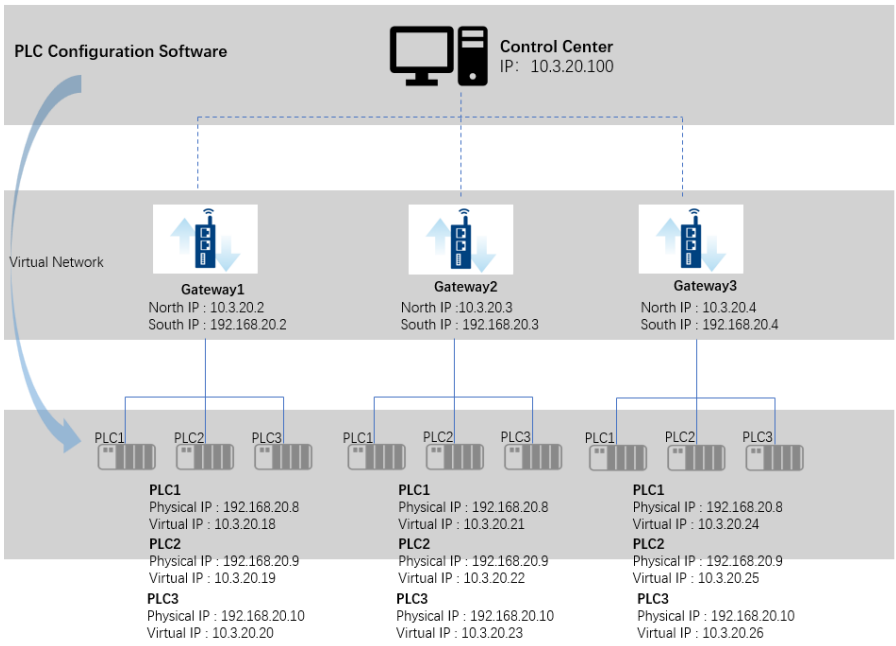
1. When deploying VPN, set the IP address to be in the same subnet as the PLC.
2. Use EdgeLink Studio to set up the VPN and LAN1 bridge together, and download it to the gateway. For example, set the br0 IP to: 192.168.1.100.



3. Open the PLC communication software at the control center to configure the PLC.(The communication software can directly connect to 192.168.1.10 for configuration)

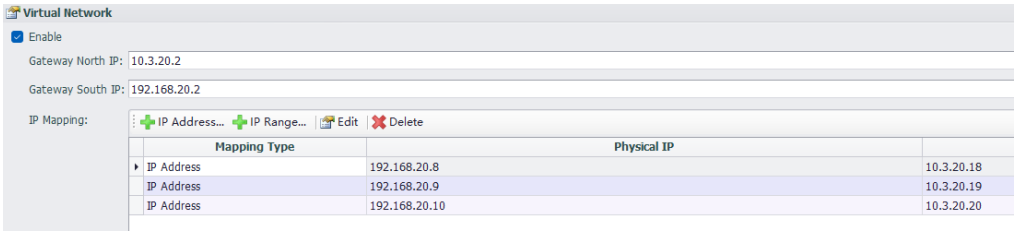
Scenario 3

When a single Ethernet port of the gateway is connected to multiple PLCs, and the IP addresses of the PLCs connected under multiple gateways are duplicated, virtual networking functionality is required to achieve remote operation and maintenance. (Scenarios 1 and 2 can also be achieved through virtual networking, but port forwarding and network bridging configurations are simpler and easier to get started with, so the methods for scenarios 1 and 2 are recommended.)

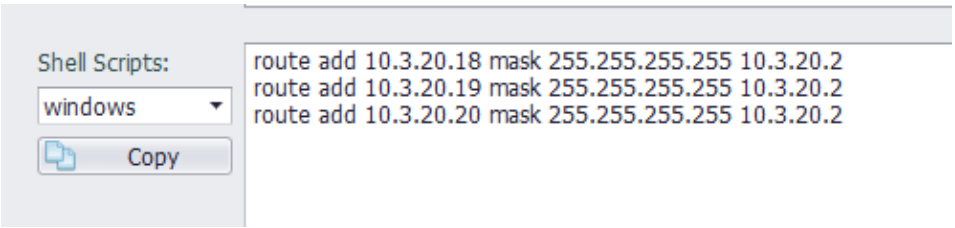


Operational Steps:

1. Set up virtual networking through EdgeLink Studio and download it to gateway 1 (other gateways should be configured according to the actual virtual networking).



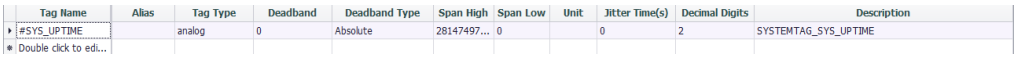
2. Configure the corresponding route at the control center. EdgeLink Studio provides a reference script, which can be copied and directly executed in the command line at the control center.



3. Open the PLC communication software at the control center to configure the PLC.(The communication software connects to 10.3.20.18 to configure PLC1 that is connected to Gateway 1)

For detailed configuration introduction of virtual networking, please refer to the 2.9.1.6 Virtual Network section.

Tag List Setting



Tag Name	Alias	Tag Type	Deadband	Deadband Type	Span High	Span Low	Unit	Jitter Time(s)	Decimal Digits	Description
#SYS_UPTIME		analog	0	Absolute	28147497...	0		0	2	SYSTEMTAG_SYS_UPTIME
Double click to edi...										

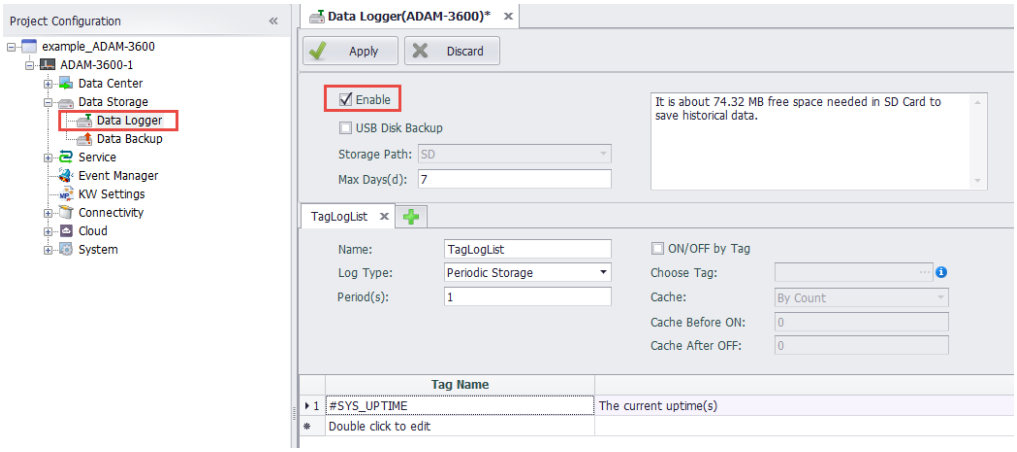
- **Tag Name**: Double-click this field to add or select a tag in the device.
- **Alias**: Set the name when uploading data. Use the tag name as the data name when the alias is empty.
- **Tag Type**: Displays the data type of the tag. This item is a read-only item and cannot be modified in this tag table. If you need to modify it, please modify the original tag attribute in the data center.
- **Deadband Type**: Used to configure the change detection method of tag values. There are two ways: absolute value and percentage. When the type is configured as an absolute value, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the *Deadband*, and if it is exceeded, the tag is considered to have changed; When the type is configured as a percentage, the difference between the current tag value of the tag and the last uploaded tag value is taken as an absolute value and compared with the last uploaded tag value. If the change exceeds the *Deadband*, the tag is considered to have changed.
- **Deadband**: Used to specify the Deadband value of the tag detection. The value change of the tag does

not trigger the tag value change within the threshold.

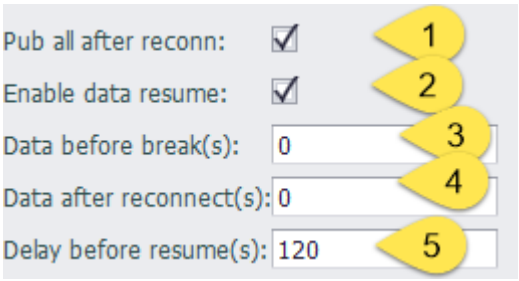
- **Unit**: Read-only item, when the Deadband type is percentage, a percent sign is displayed to distinguish it from the absolute value.
- **Jitter time**: The unit is second. When the detected tag value exceeds *Deadband*, verification of *jitter time* will start. When the tag value is detected as exceeding the *Deadband* within the specified *jitter time*, it will be finally judged as a little value change, and the changed value will be uploaded at this time, otherwise it will be judged as tag value jitter. Not uploaded.
- **Decimal Digits**: The number of digits after the decimal tag for specifying the analog tag value. The default is 2. When the actual tag value has only one integer value, you can set this field to 0 to save data traffic.
- **Description**: The description of the tag. This item is a read-only item and cannot be modified in this tag table. If you need to modify it, please modify the original tag attribute in the data center.

Data resume

- When an EdgeLink device is connected to an MQTT platform, the resumable upload function completes the data during the disconnection period
- **Prerequisites**: The tags that need to be resumably transferred must be configured to DataLogger for local storage, the device must have a memory card, you can refer to DataLogger description



Enable resumable transfer

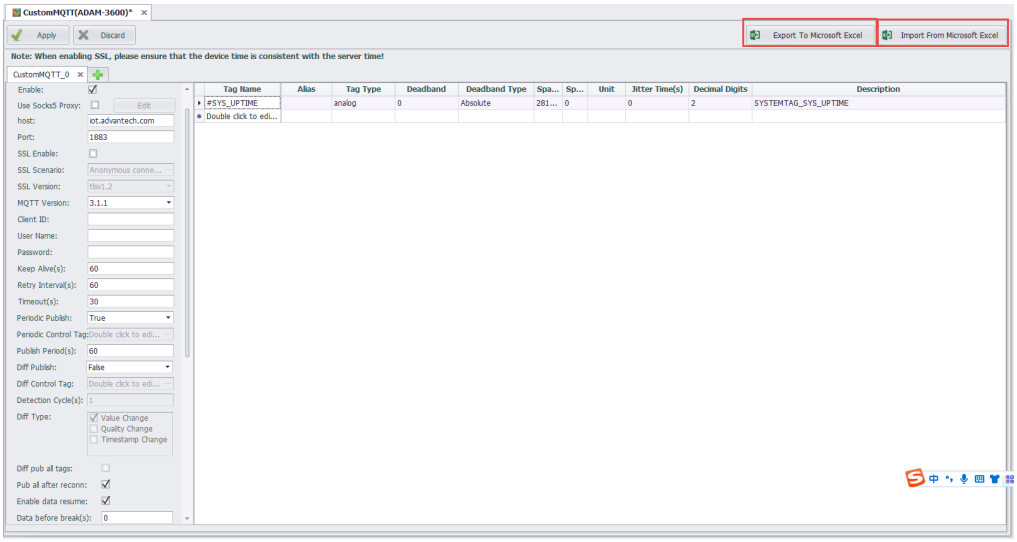


parameter	parameter description

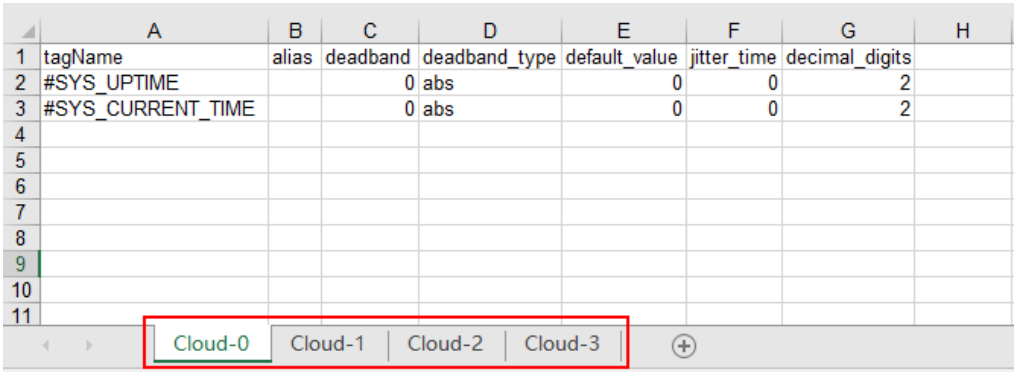
parameter	parameter description
`Pub all after reconn`	When EdgeLink establishes a connection with the cloud, does it upload the current values of all points once to the cloud, with enabling sending and disabling not sending? The default setting is enabling sending
`Enable data resume`	Enable switch for resume upload from break
`Data before break`	Default: 0, resume uploading data from the most recent n seconds before the disconnection
`Data after reconnect`	Default: 0, resume uploading data until the most recent n seconds after the reconnection
`Delay before resume`	Default: 120, resume uploading data after an interval of n seconds after the reconnection

Export/Import Tag List

- The cloud service configuration interface supports the import and export function of point list (edited according to the specified format, which is convenient for adding or deleting tags in batches)



- excel format



Overview

Libextext built-in multiple macro function that is used to the system time or tag value are formatted output, the user can use the macro function to prepare the required text template. This module can be used to output mail and short message content in event management, or for other applications that require forwarding text data, such as MQTT or HTTP forwarding.

Overview of macro functions

function	instructions	parameter	optional parameter
`$localtime(fmt)`	output local time	fmt:formatting	%F,%T,%H, ……
`$gmttime(fmt)`	output GMT time	fmt:formatting	%F,%T,%H, ……
`$ctime(fmt)`	output the time stamp	fmt:formatting	s,ms,sms
`$tagLocalTime(tag_name,fmt)`	output tag local time	tag_name:tag name fmt:formatting	%F,%T,%H, ……
`$tagGmtTime(tag_name,fmt)`	output tag GMT time	tag_name:tag name fmt:formatting	%F,%T,%H, ……
`$tagCTime(tag_name,fmt)`	output tag time stamp	tag_name:tag name fmt:formatting	s,ms,sms
`$tagName(tag_name)`	output tag name	tag_name:tag name	_
`$tagValue(tag_name,fmt)`	output tag value	tag_name:tag name fmt:formatting	%.1lf,%.2lf,%.3lf,%g
`$tagQuality(tag_name)`	output tag quality	tag_name:tag name	_
`$tagValueDescriptor(tag_name)`	output tag description	tag_name:tag name	_

Macro function is introduced in detail

System time function

`$localtime(fmt)` , `$gmttime(fmt)` and `$ctime(fmt)` The three macro function is used to the current system time formatted as text, its output format by `fmt` parameter specifies, supports the following parameters format.

parameter	instructions	formatting
%a	Short for day of the week	wed
%A	The day of the week in full	Wednesday
%b	Short for month	Nov
%B	The full name of the month	November
%c	Standard date time string	Wed Nov 11 13:59:53 2020
%C	The first two digits of the year	20
%d	The day of the month in decimal notation	20
%D	Month/day/year	11/11/20
%e	In the two-character field, The day of the month in decimal notation	20
%F	Year - Month - Date	2020-11-11
%g	The last two digits of the year, Use a week-based year	20
%G	Year, using a year based on the week	2020
%h	The abbreviated name of the month	Nov
%H	Twenty-four hours	14
%I	Twelve hours	02
%j	The day of the year in decimal notation	316
%m	A month in decimal notation	11
%M	The number of minutes in the ten hour system	12
%n	New line character	–
%p	Local AM or PM equivalent display	AM
%r	For 12 hours	02:05:53 PM
%R	Displays hours and minutes：hh:mm	14:06
%S	The number of seconds in decimal	39
%t	Horizontal tabs	–

parameter	instructions	formatting
%T	Displays minutes and seconds：hh:mm:ss	14:05:36
%u	The day of the week	5
%U	The week of the year, with Sunday as the first day	46
%V	The week of the year, using the week-based year	47
%w	A decimal representation of the day of the week	3
%W	Week of the year, Monday is the first day	45
%x	Standard date string	11/11/20
%X	Standard time series	14:04:07
%y	A decimal year without centuries	20
%Y	Ten years with century section	2020
%z	Time zone name	+0800
%Z	An acronym for a time zone name	CST
%%	percent	%

$localtime(fmt): Output local time

`fmt` :Time output format parameter item, the default output format parameter is: %F %T (year, month, day, hour, minute, second)

`result` : Output local time in format

`The sample` :

```
$localtime(%F %T) : 2020-11-10 17:07:15
$localtime(%T) : 17:07:15
```

$gmttime(fmt): Output GMT time

`fmt` :Time output format parameter item, the default output format parameter is: %F %T (year, month, day, hour, minute, second)

`result` : output GMT time in format

`The sample` :

```
$gmttime(%F %T):2020-11-10 09:07:15
$gmttime(%F):2020-11-10
```

$ctime(fmt): output the time stamp

`fmt`:Time output format parameter item, default output format parameter is sms (seconds and ms)

`result` : Output the timestamp by format

`The sample` :

```
$ctime(s):1604999235
$ctime(ms):291
$ctime(sms):1604999235291
```

The Tag function

$tagName(tag_name): Output tag name

`tag_name`：tag name

`result`：Output the tag name

`The sample`：

```
$tagName(tag_2):tag_2
```

$tagValue(tag_name，fmt): Output tag value

`tag_name`：tag name

`fmt`：Preserve valid bit parameters, default to 2 decimal digits (%.2lf)

`separator`：Parameters are separated by a comma (,)

`result`：Output the tag value. Failure returns :0

`The sample`：

```
$tagValue(tag_8,%.3lf):7.000
$tagValue(tag_9,%.9lf):8.000000
$tagValue(tag_10,%.g):9
$tagValue(tag_,%.2lf):0.00
```

$tagQuality(tag_name): output tag quality

`tag_name`：tag name

`result`：Output the tag quality. Fail to return :8080

`The sample`：

```
$tagQuality(tag_2):0
$tagQuality(tag_):8080
```

$tagValueDescriptor(tag_name): output tag description

`tag_name`：tag name

`result`：Output the tag description. Failure returns :0.00

`The sample`：

```
$tagValueDescriptor(test:D1)：111
$tagValueDescriptor(tag_)：0.00
```

$tagLocalTime(tag_name,fmt）：output tag local time

`tag_name`: tag name

`fmt`：Time output format parameter item, default output format %F %T(year, month, day, hour, minute, second)

`separator`：The arguments are separated by a comma (,)

`result`：Output the tag time according to the format,Failed to output:1970-01-01

08:00:00

`The sample`：

```
$tagLocalTime(tag_9,%F %T):2020-11-10 17:07:16
$tagLocalTime(tag_9,%F):2020-11-10
$tagLocalTime(tag_,%F)：1970-01-01 08:00:00
```

$tagGmtTime（tag_name，fmt）: output tag GMT time

`tag_name`：tag name

`fmt`：Time output format parameter item, default output format %F %T(year, month, day, hour, minute, second)

`separator`：The arguments are separated by a comma (,)

`result`：Output the tag time according to the format,Failed to output:1970-01-01 08:00:00

`The sample`：

```
$tagGmtTime(tag_9,%F %T):2020-11-10 09:07:16
$tagGmtTime(tag_9,%T):09:07:16
$tagGmtTime(tag_,%T): 1970-01-01 00:00:00
```

$tagCTime(tag_name，fmt): Output tag time stamp

`tag_name`：tag name

`fmt`：Time stamp output format parameter item, default time format sms (seconds and ms)

`separator`：The arguments are separated by a comma (,)

`result`：Output the tag stamp according to the format,Failed to output:0

`the sample`：

```
$tagCTime(tag_9,s):1604999236
$tagCTime(tag_9,ms):211
$tagCTime(tag_9,sms):1604999236211
$tagCTime(tag_,s):0
$tagCTime(tag_,sms):000
$tagCTime(tag_,sms):0000
```

Multi-tag custom template function

`$MulTagBegin(tag_1,tag_2...)`, `template` and `$MulTagEnd(separator)` are composed of three parts, corresponding to the beginning part, template part and end part respectively. Only when the input text successfully matches the beginning part and end part, can the template output defined by multiple tags be realized.

$MulTagBegin(tags) template $MulTagEnd(separator)

`tags`:Add tag name with a comma (,) as the tag divider

`the sample`：$MulTagBegin(tag_1,tag_2,……)

`template`:Templates to be output for each tag. Templates are user-defined

`the sample`：{" tagname ":$tagname (@)}, the @ character in the template will be

replaced by the tag name

`separator`:Template delimiter

`the sample`:$MultagEnd (,), with the comma (,) as the delimiter between the tag template

`Multi-tag custom template example`：

`input`：

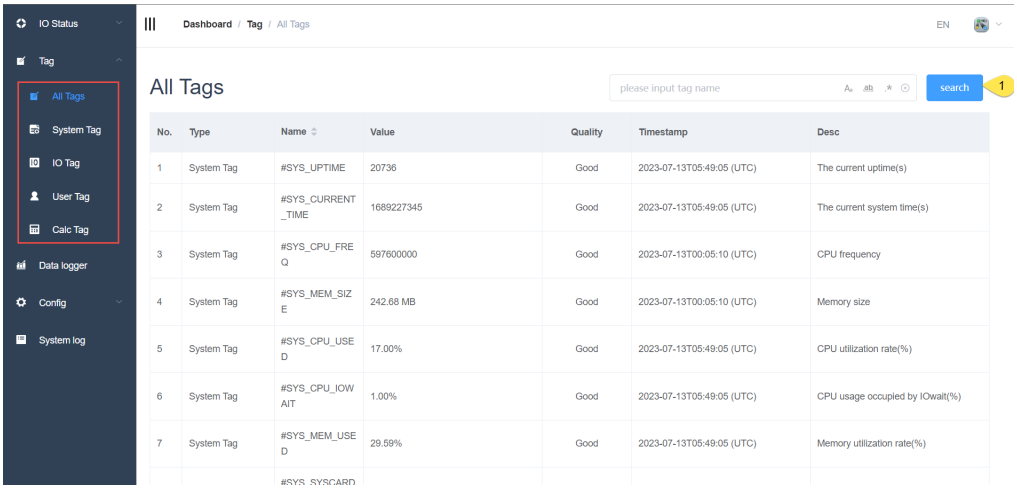
```
$MulTagBegin(tag_8,tag_2,tag_5)
{
$$gmttime(%F %T):$gmttime(%F %T),
$$tagName(@):$tagName(@)
}
$MulTagEnd(,)
```

`output`：

```
{
$gmttime(%F %T):2020-11-10 12:13:28,
$tagName(@):tag_8
}
,
{
$gmttime(%F %T):2020-11-10 12:13:28,
$tagName(@):tag_2
}
,
{
$gmttime(%F %T):2020-11-10 12:13:28,
$tagName(@):tag_5
}
```

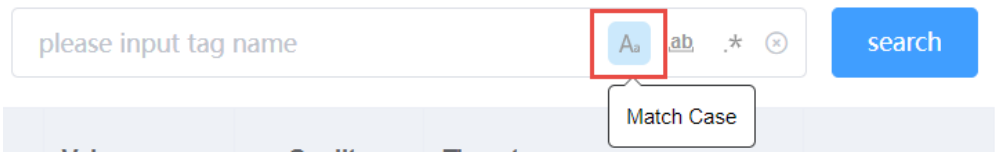
Tag Search

All pages of tags support searching by tag name

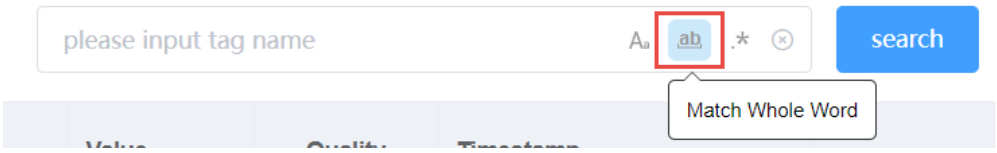


Type

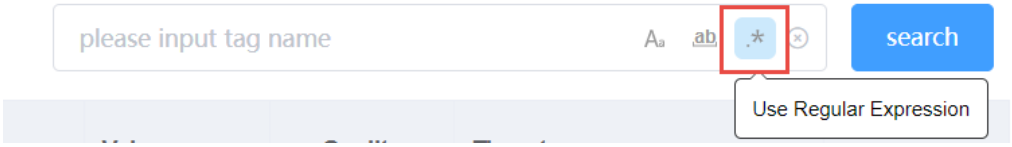
Type 1: Match Case



Type 2: Match Whole World



Type 3: Use Regular Expression



Search of IO Tag

In addition to searching by tag name, the IO Point page supports filtering based on ports and meters

button	Description
Confirm	After checking the port list, click the Confirm button to take effect
Reset	Click the reset button to uncheck all checks, that is, to revert to the state of no filtering