AIG-101 Series User Manual

Version 2.1, November 2023

www.moxa.com/products

AIG-101 Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

Overview

The AIG-101 is an entry IIoT gateway that connects Modbus RTU/ASCII/TCP to the Azure, AWS, and MQTT cloud platforms. To integrate existing Modbus devices onto the cloud platform, use the AIG-101 as a Modbus master to collect data and transmit the data to the cloud. The MQTT standard with supported cloud solutions on the AIG-101 leverages advanced security, configuration, and diagnostics for troubleshooting to deliver scalable and extensible solutions that are suitable for remote monitoring applications such as energy management and assets management.

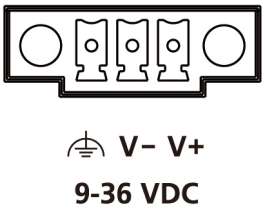
2. Getting Started

Connecting the Power

The unit can be powered by connecting a power source to the terminal block:

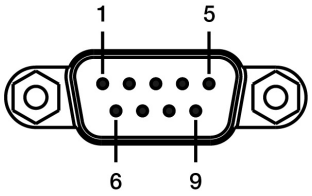
1. Loosen or remove the screws on the terminal block.
2. Turn off the power source and then connect a 9–36 VDC power line to the terminal block.
3. Tighten the connections, using the screws on the terminal block.
4. Turn on the power source.

Note that the unit does not have an on/off switch. It automatically turns on when it receives power. It takes a couple of seconds for the system to boot up. Once the system is ready, the SYS LED will light up. Power terminal block pin assignments are shown below:



Connecting the Serial Devices

The AIG device supports connecting to Modbus serial devices. The serial port uses the DB9 male connector. It can be configured by software for the RS-232, RS-422, or RS-485 mode. The pin assignment of the port is shown below:



Pin	RS-232	RS-422	RS-485
1	DCD	TxD-(A)	–
2	RxD	TxD+(B)	–
3	TxD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	–	–	–

Connecting to a Network

Connect one end of the Ethernet cable to the AIG's 10/100M Ethernet port and the other end of the cable to the Ethernet network. The AIG will show a valid connection to the Ethernet by LAN1/LAN2 maintaining solid green color.

Access to the Web Console

Access to the web console to configure the AIG by just inputting the default IP address (default LAN1: 192.168.126.100; default LAN2: 192.168.127.100) or use AIG QuickON to scan the AIG in the network.

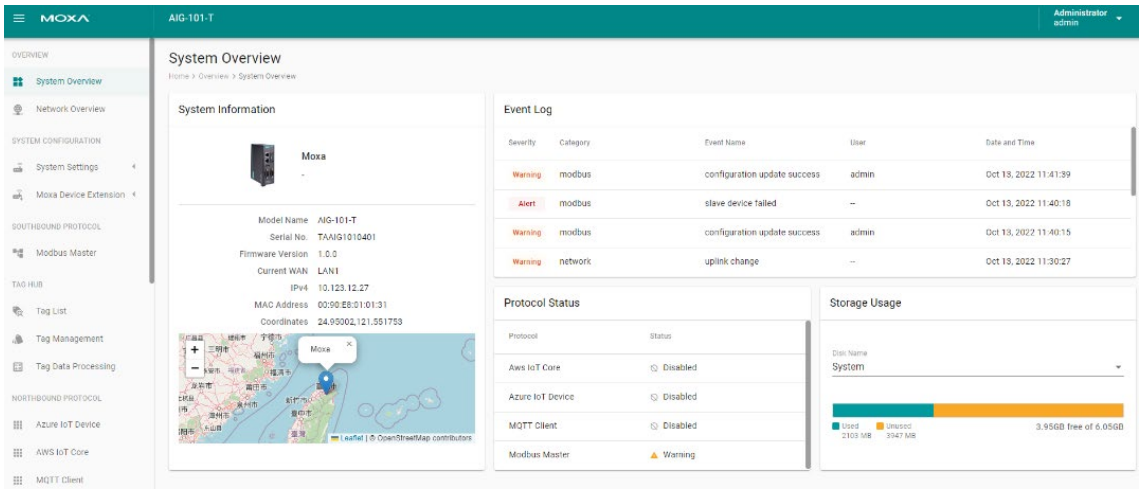
When you use default IP to access, do the following:

1. Ensure your host and AIG are in the same subnet (AIG default subnet mask: 255.255.255.0).
2. When you connect to LAN1, input https://192.168.126.100:8443 in your web browser; when you connect to LAN2, input https://192.168.127.100:8443 in your web browser.
3. Input default account and password

   Default account: **admin**

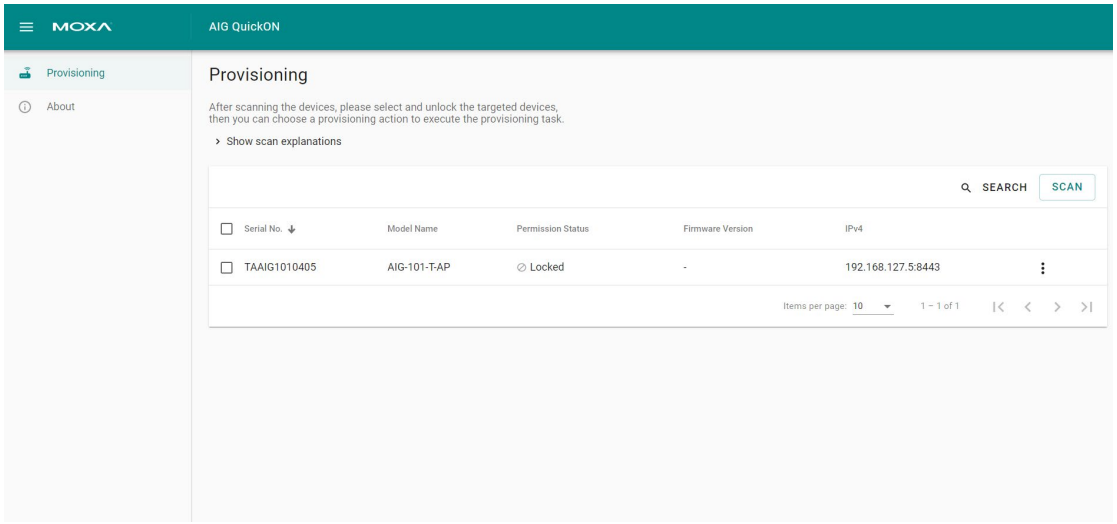
   Password: **admin@123**

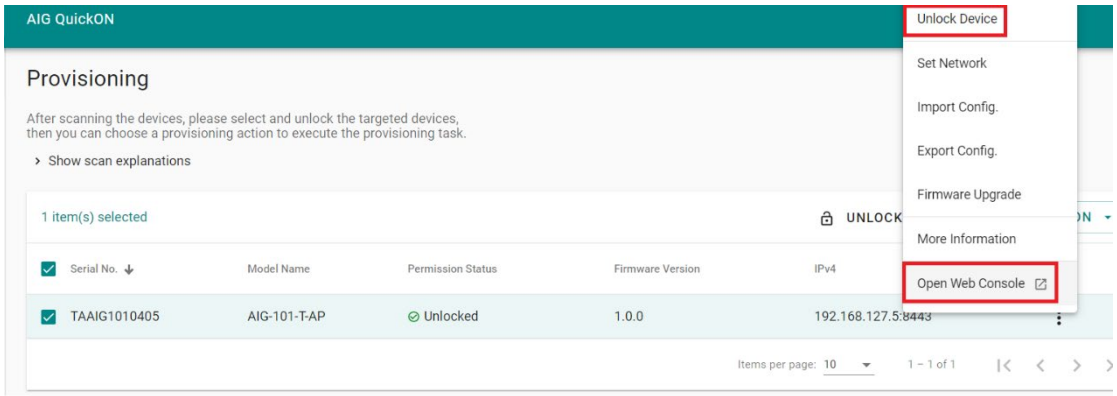
4. Login successful



To access the AIG using the AIG QuickON tool, do the following:

1. Run the **AIG-QuickON-x.x.x-xxxxxxxxxxx.exe** to install the tool.
2. At the **Welcome** screen, click **Next** to continue.
3. At the **Select Destination Location** window, click **Next** to continue.
   You can change the destination directory by first clicking on **Browse...**
4. At the **Select Additional Tasks** window, click **Next** to continue.
5. Click **Install** to copy the software files.
   A progress bar will appear. The procedure should take only a couple of seconds to complete. A message will show to indicate that the AIG QuickON has been successfully installed.
6. Go to **Start** > **Program** > **AIG QuickON** folder > **AIG QuickON** and run the tool to automatically scan for AIG devices.
7. If a device is locked, click **Unlock Device** and use the login Account and Password. (Default Account: **admin**, Password: **admin@123**).
8. To access the device, click **Open Web Console**.





Overview

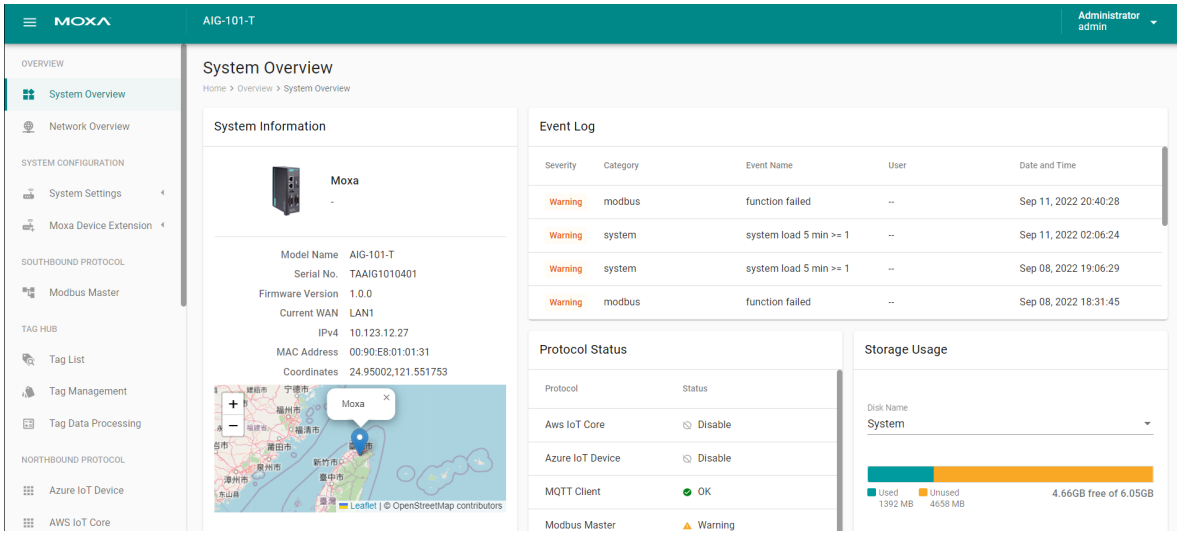
System Overview

This page gives you an overview of the gateway's status.

System information provides basic information such as model name, serial No., and firmware version.

Event logs and protocols status provide useful information for troubleshooting purposes.

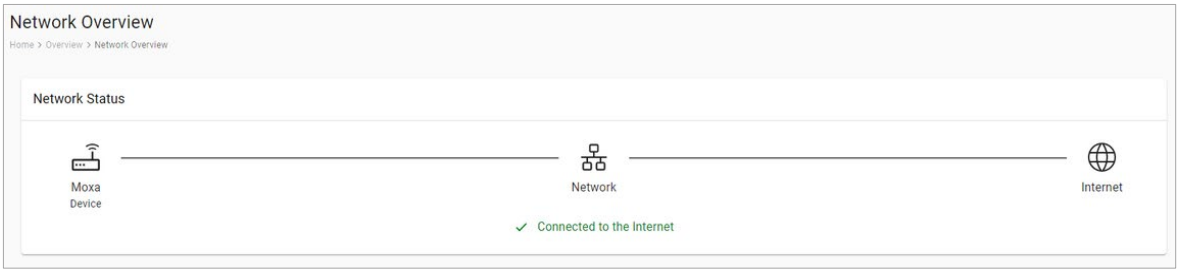
Storage usage provides the remaining storage for the system or SD card.



Network Overview

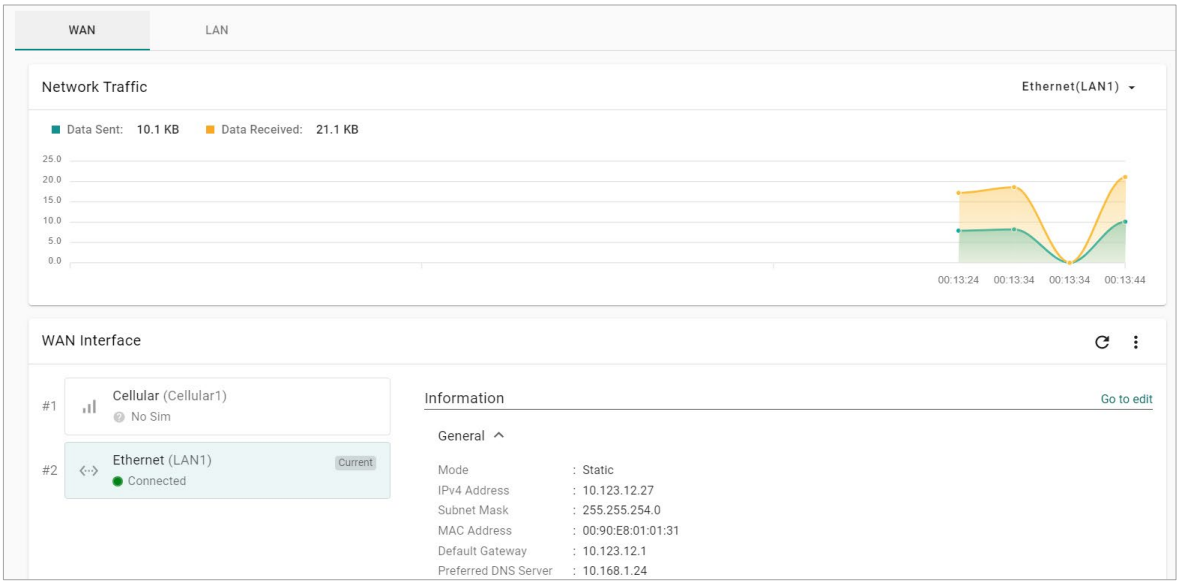
This dashboard displays information on the WAN and LAN interfaces and the network traffic passing through the interfaces.

Network Status shows whether the gateway can connect to the Internet.



WAN

WAN displays information of the data sent and received through the WAN interfaces. You can select the interface that you want to monitor. In addition, other details on the usage of the WAN interfaces are displayed on the page. The information is refreshed every 10 seconds.



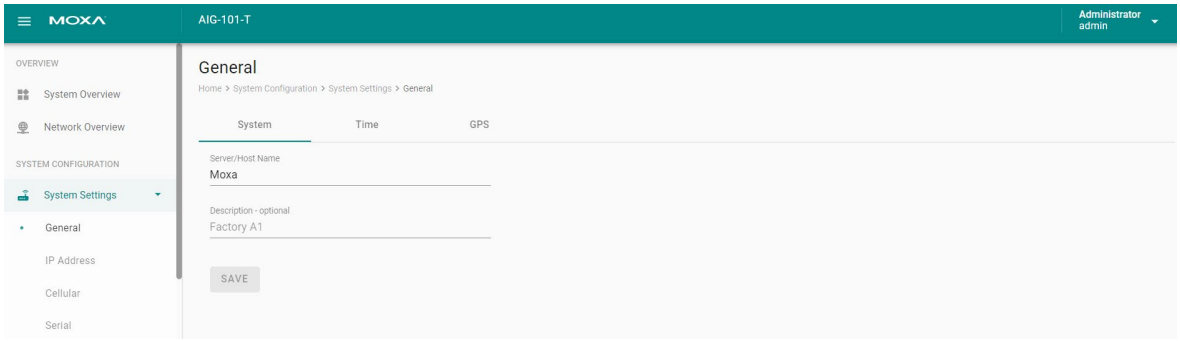
LAN

Information on the LAN interfaces is organized under the **LAN** tab and includes information on the usage of the interfaces and the traffic passing through them.

System Configuration

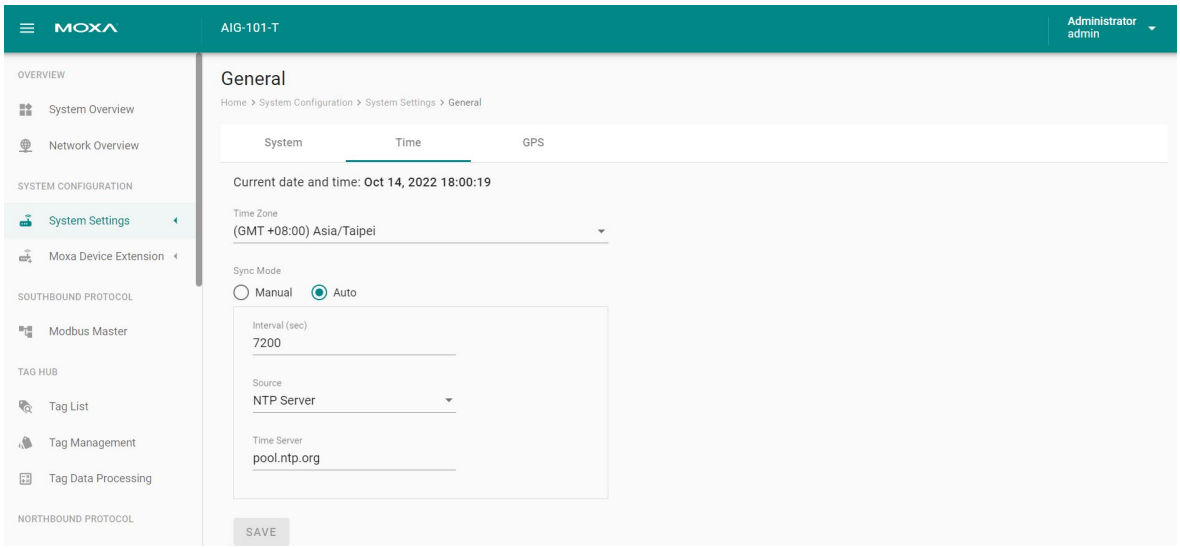
System Settings—General

Go to **System Settings > General > System** to specify a new server/host name and enter a description for the device.



Parameter	Value	Description
Server/Host Name	Alphanumeric string	You can enter a name to identify the unit, such as one that is based on the function.
Description - optional	Alphanumeric string	You can enter a description to help identify the unit location, such as "Cabinet A001."

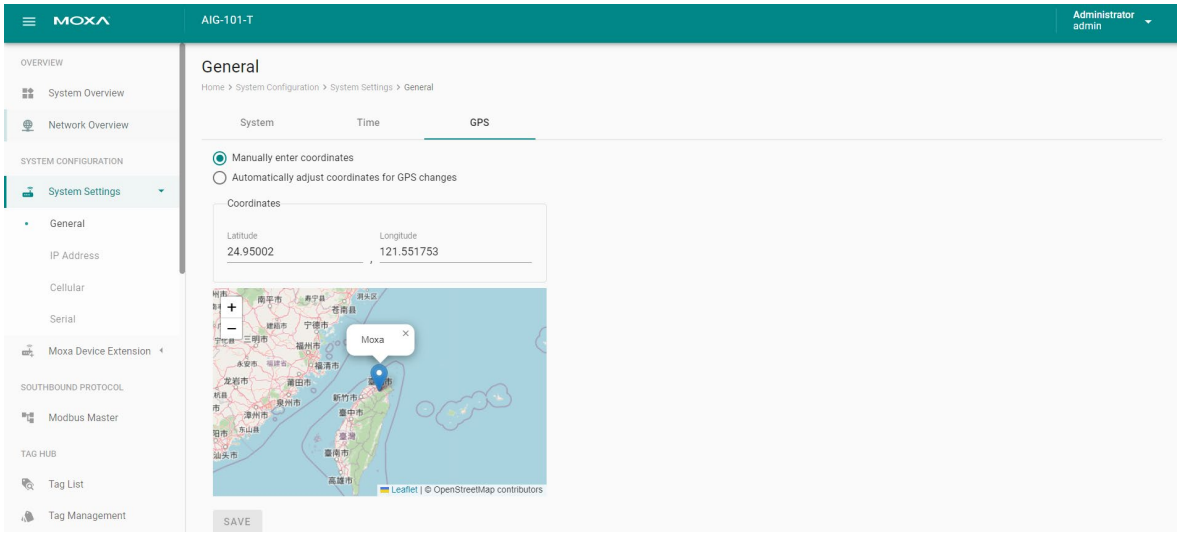
Go to **System Settings > General > Time** to select a time zone. Choose between the Manual or Auto option to update the system time.



Parameter	Value	Description
Time Zone	User's selectable time zone	The field allows you to select a different time zone.
Sync Mode	Manual Auto	Manual: input the time parameters by yourself Auto: it will automatically sync with time source. NTP and GPS can be selected. NOTE: When the Auto mode is selected, in general, it takes 2 to 4 minutes. If the satellite search is slower, it could take up to 12 minutes (worst-case scenario)
Interval (sec)	60 to 2592000	How long to sync the time source
Source	NTP Server GPS	How to sync the time clock
Time Sever	IP or Domain address (e.g., 192.168.1.1 or pool.ntp.org)	This field is required to specify your time server's IP or domain name if you choose the NTP server as the source

Go to **System Settings > General > GPS** to view the GPS location of the device on a map. There are two options:

1. Input latitude and longitude in **manual**.
2. check the **Automatically adjust coordinates for GPS changes** option if you want the system to automatically update the device coordinates.

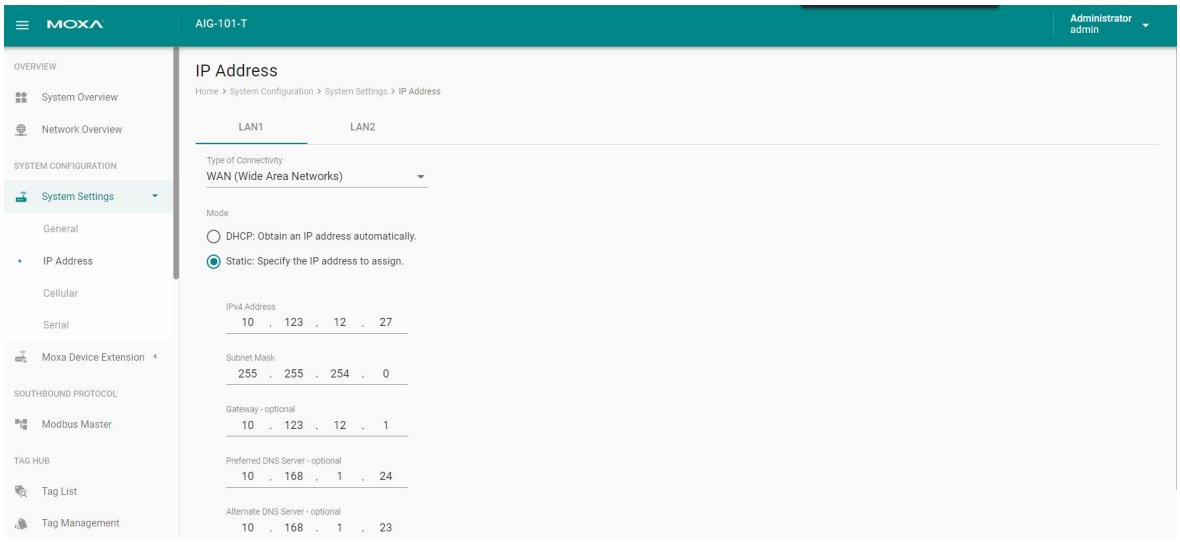


System Settings—IP Address

Go to **System Settings > IP Address** to view and configure LAN1 and LAN2 network settings.

To configure the network, do the following:

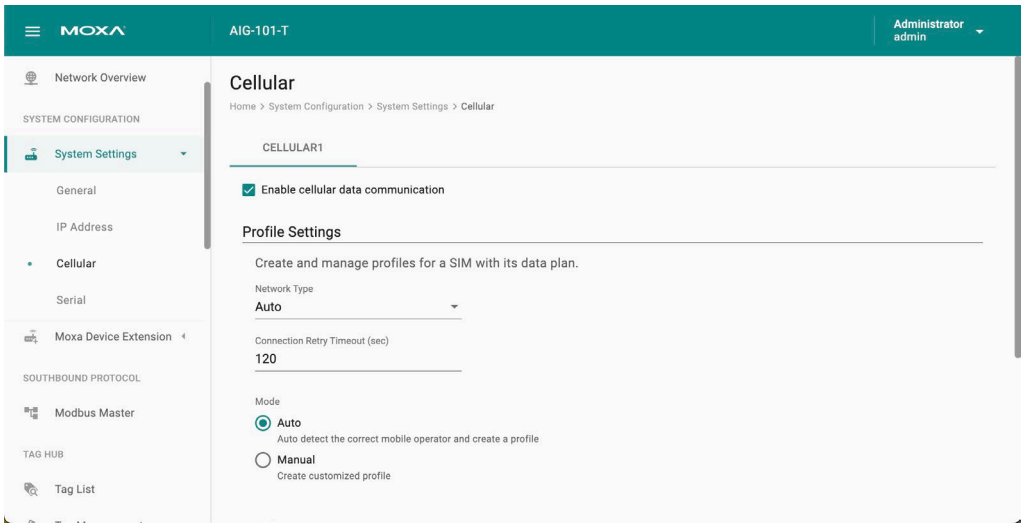
1. Choose **LAN1** or **LAN2** for configuration.
2. Select the **WAN (Wide Area Networks)** or **LAN (Local Area Networks)**.
3. Select **DHCP** or **Static** mode.
4. Configure **IP address, Subnet mask, Gateway,** and **DNS**.



Parameter	Value	Description
Types of connectivity	WAN LAN (Note: PS: LAN2 only supports LAN)	WAN: Wide Area Networks LAN: Local Area Networks
Mode	DHCP Static	DHCP: Gets the IP address automatically. Static: Specify the IP address
IPv4 Address	LAN1 default: 192.168.126.100 LAN2 default: 192.168.127.100(or other 32-bit number)	The IP (Internet Protocol) address identifies the server on the TCP/IP network
Subnet Mask	Default: 255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
Gateway—optional	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server —optional	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
Alternate DNS Server— optional	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

System Settings—Cellular

Go to **System Settings > Cellular** to view the current cellular settings. Here you can enable or disable cellular connectivity on your device, create profiles, manage **Profile Settings**, and enable or disable the connection **Check-alive** function to optimize the cellular connection.



First, you must select a network type Auto, 3G, or 4G.

NOTE

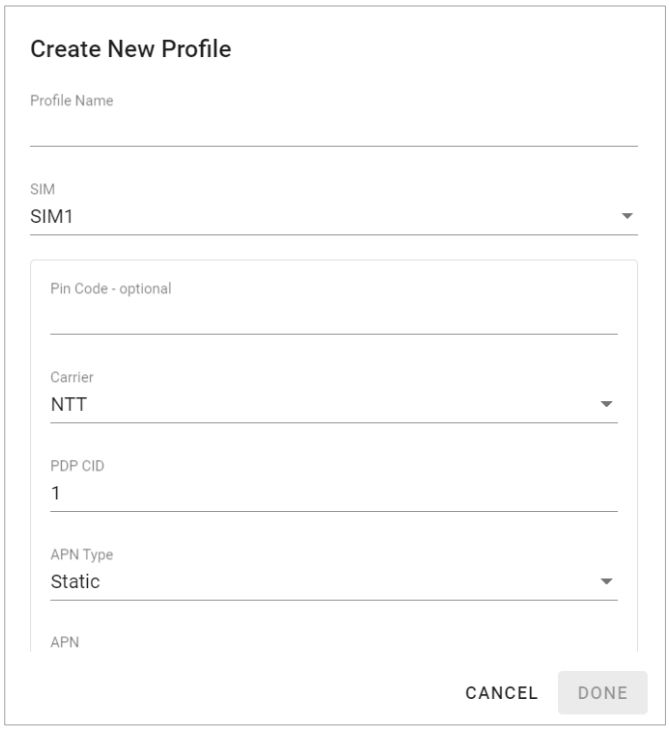
If you are not sure about the type of network, select Auto (default)

To connect a mobile operator, you can either select **Auto** mode to create a customized profile automatically, or **Manual** mode to create customized cellular profiles. **Create**, **Edit**, or **Delete** cellular profiles here.

To create a new cellular connection profile, do the following:

1. Click **+ CREATE**.
2. Specify a unique **Profile Name**.
3. Specify the target **SIM** card.
4. Enter the **PIN Code** if your SIM card requires it. **NOTE:** Three wrong attempts will lock the SIM card.

5. Choose a **Carrier**. (**NOTE:** This option is displayed only if the cellular module supports carrier switching.)
6. Refer to instructions from your cellular carrier to select **Static** or **Dynamic** APN and configure the corresponding settings.

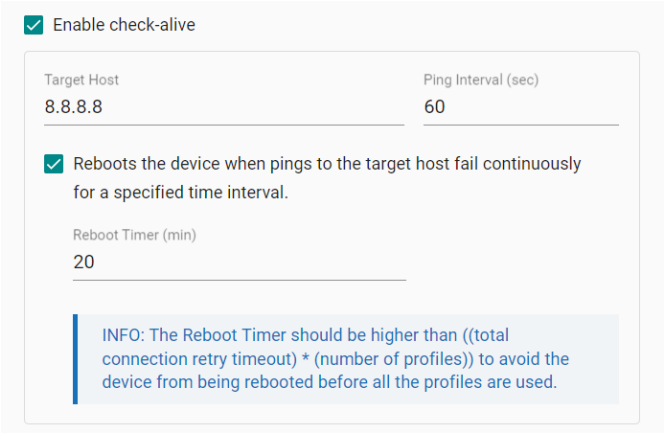


7. Click **DONE**.
8. On the **Cellular** setting page, click **SAVE**.

When you click **SAVE** on the Cellular section, the module restarts to apply the changes. The settings will take effect after the cellular module is successfully initialized.

The **Check-alive** function will help you maintain the connection between your device and the carrier service by pinging a specific host on the Internet at periodic intervals.

In some circumstances, a system reboot might bring an unstable or malfunctioning device back to a normal state. To enable automatic system reboot, select the **Reboot the unit when ping to the target host failed continuously for a certain amount of time** option and specify a reboot interval.



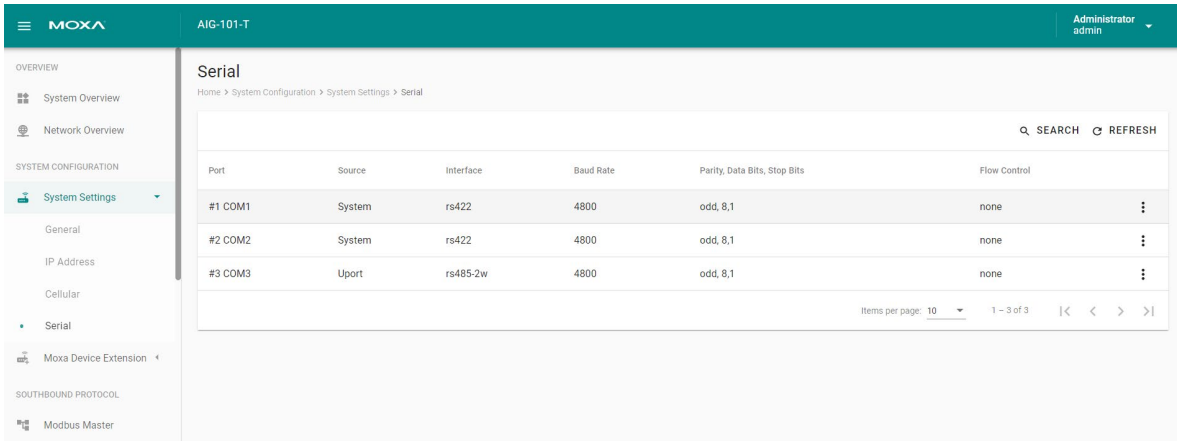
Go to **Network Overview > WAN** if you want to check the cellular network's connection status afterwards.

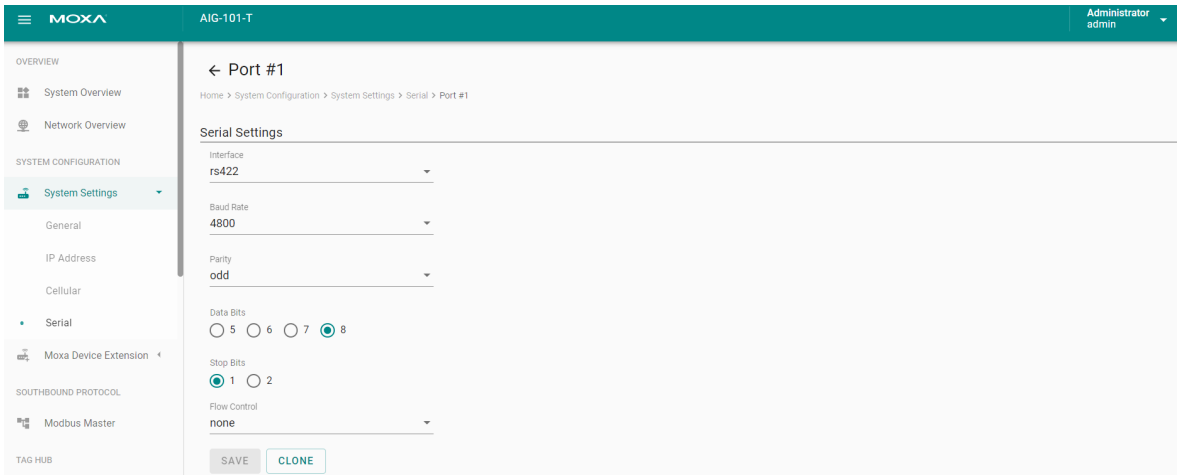
System Settings—Serial

Go to **System Settings > Serial** to view and configure serial parameters. (Once you connect the UPort 1100/1200 Series into the gateway, the extended serial ports will be shown here.)

To configure serial setting, do the following:

1. **Click** the COM port.
2. **Configure** the baudrate, parity, data bits, and stop bits when enabling Modbus RTU/ASCII mode. (Incorrect settings will cause communication failures.)
3. Click **Save** for the settings to take effect.





Parameter	Value	Description
Interface	rs232 rs422 rs485-2w rs-485 4w	
Baud Rate	300 to 921600	
Parity	none, odd, even, space, mark	
Data Bits	5, 6, 7, 8	
Stop Bits	1, 2	
Flow Control	none hardware	Hardware: flow control by RTS/CTS signal

Moxa Device Extension—ioLogik

The AIG device can easily extend I/O interfaces by connecting to ioLogik devices. Here are the supported models:

- ioLogik E1210, ioLogik E1210-T
- ioLogik E1212, ioLogik E1212-T
- ioLogik E1214, ioLogik E1214-T
- ioLogik E1211, ioLogikE1211-T
- ioLogik E1213, ioLogikE1213-T
- ioLogik E1240, ioLogikE1240-T
- ioLogik E1241, ioLogikE1241-T
- ioLogik E1242, ioLogikE1242-T

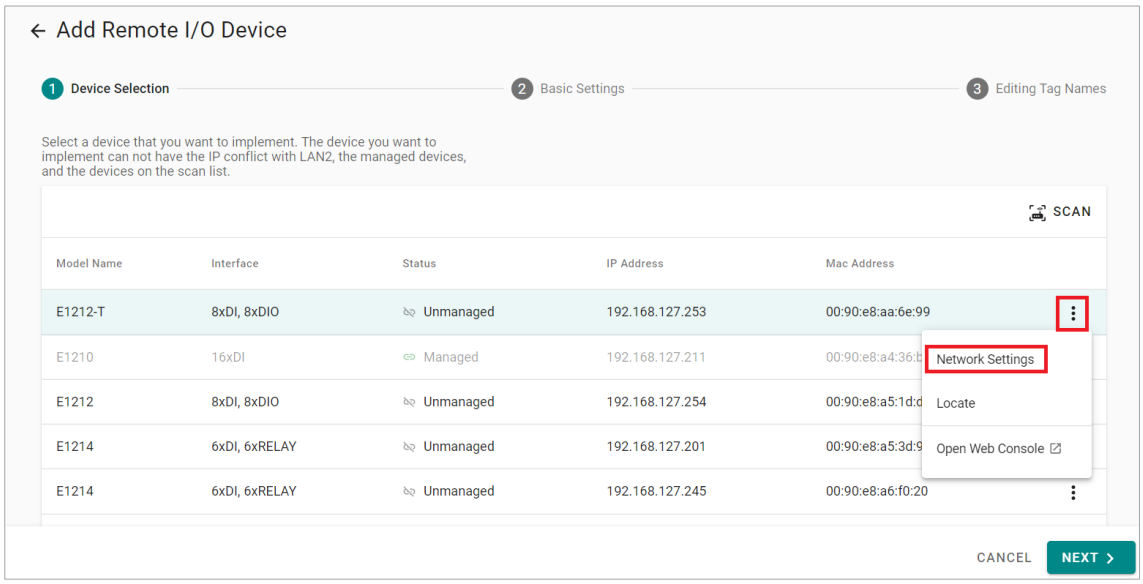
NOTE

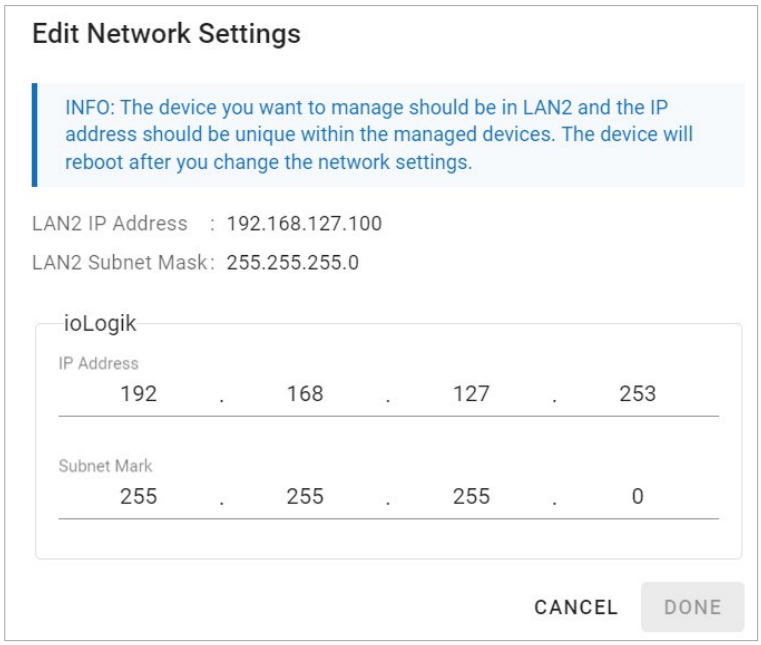
A maximum of 4 ioLogik devices can be connected to the AIG.

Before configuration the ioLogik, connect it to **LAN2** of this device, and then go to **Moxa Device Extension > ioLogik**. To extend I/O interfaces, do the following:

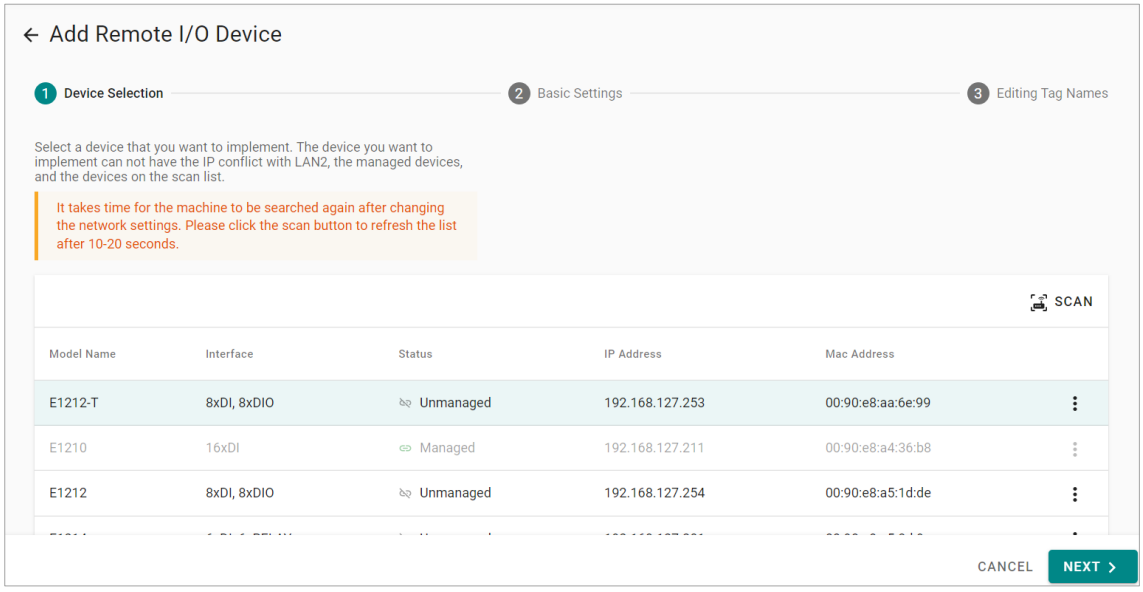
1. Click **+ ADD** and go to the wizard setting page.

2. Click the ⋮ icon to click **Network Settings,** input **Password "moxa",** change network settings, and click **DONE**.

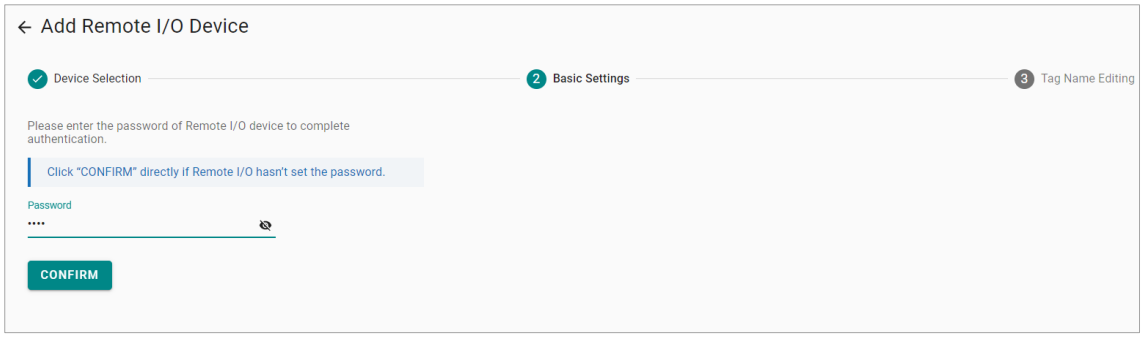




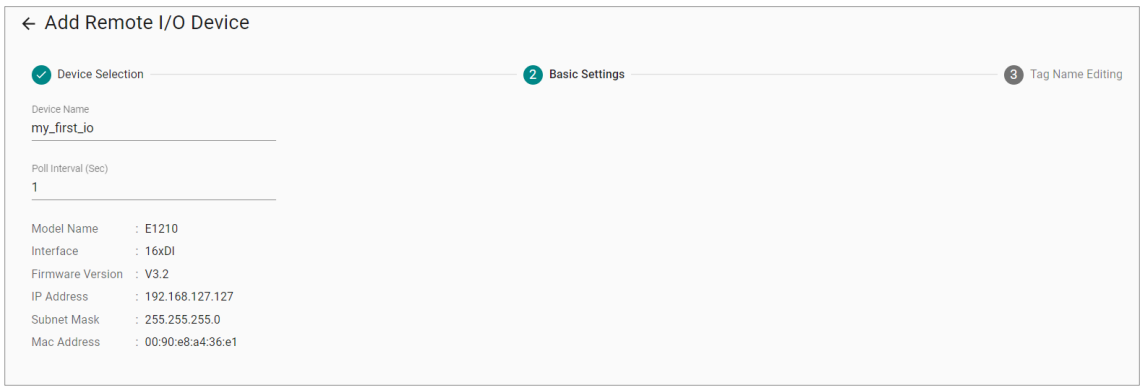
3. Click **SCAN** if the ioLogik has not been detected* yet.
4. **Choose the model** you want to configure, then click **NEXT**.



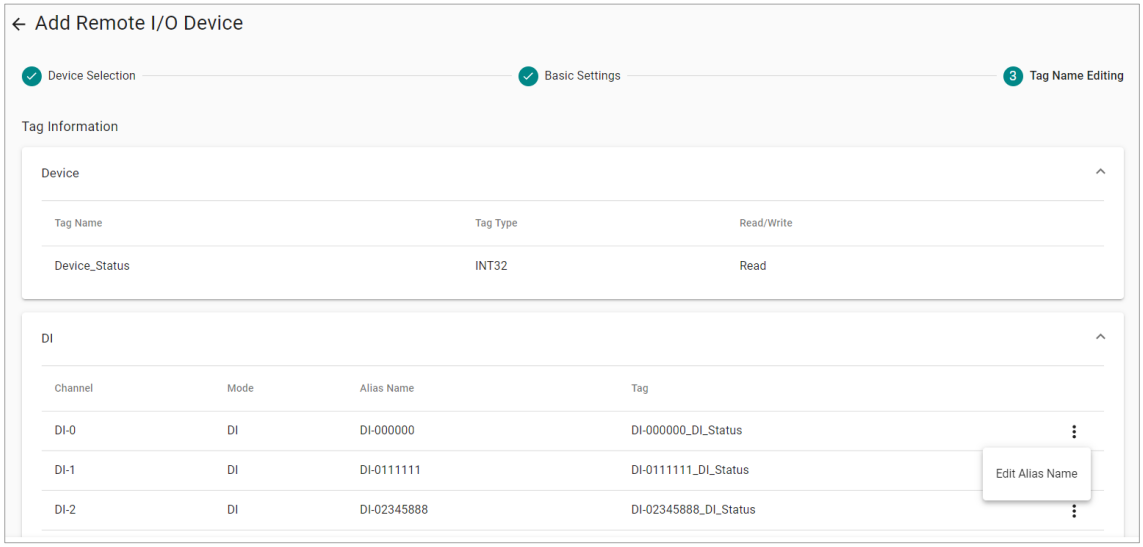
5. Input the **password "moxa"** for security policy, then click **CONFIRM**.



6. Specify **Device Name** and **Poll Interval**, then click **NEXT**.



7. (Optional) Edit Alias Name.

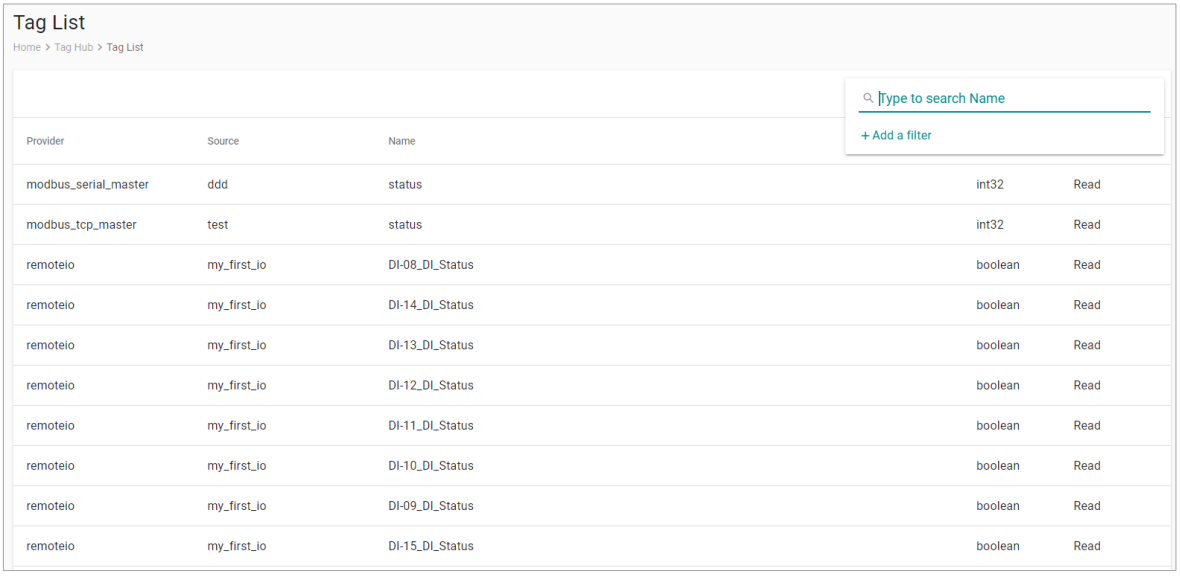


8. Click **DONE**.

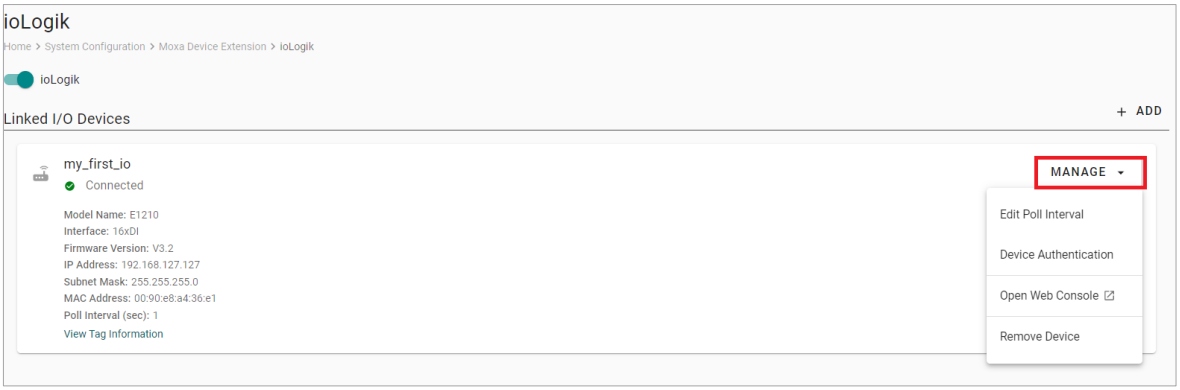
NOTE

*Ensure that both devices are under the same subnet mask.

Once you manage the ioLogik, meaning that all the I/O data has been sent to tag hub, you can check the corresponding tags in the **Tag List.**



If you want to do other settings, such as edit the poll interval, open the web console, and remove the device, click **MANAGE**.



NOTE

The maximum number of ioLogik units supported is 4. The performance of tag acquisition, processing, and transmission depends on overall system usage, including Modbus, cloud services, and tag processing.

Moxa Device Extension—UPort

The device easily extends serial ports by connecting the UPort 1100/1200 Series to a USB interface on the front panel. These UPort models are supported:

1. UPort 1100
2. UPort 1130, UPort 1130I
3. UPort 1150, UPort 1150I
4. UPort 1250, UPort 1250I*

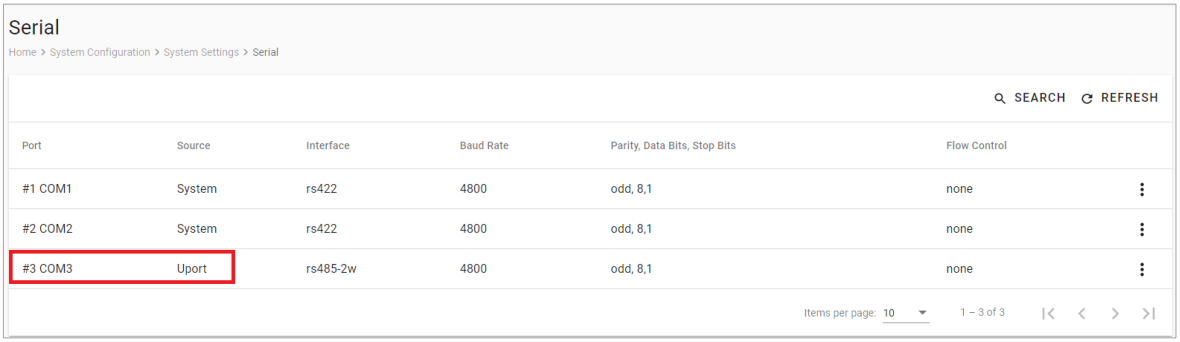
NOTE

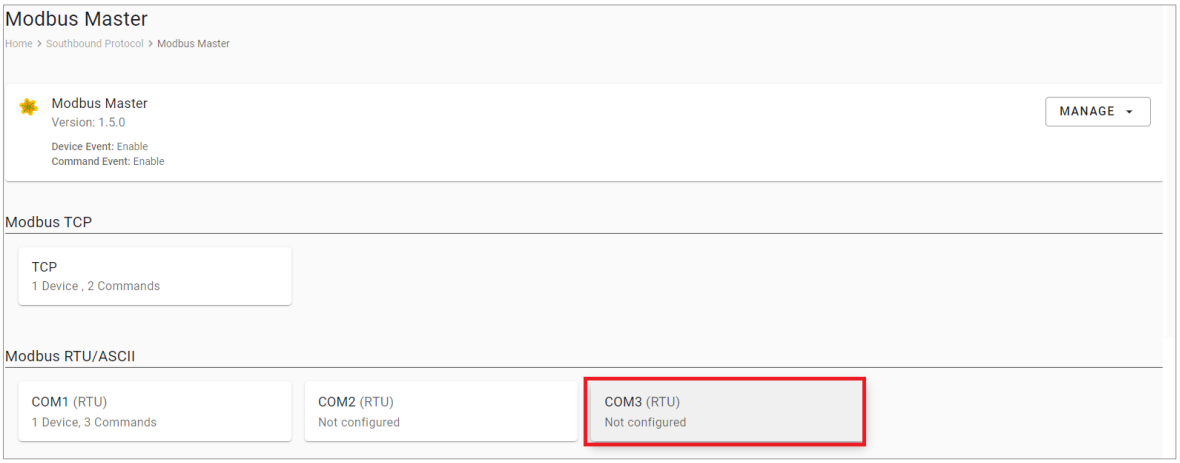
*Note that external power is needed for the UPort 1250I.

After connecting the UPort to this device, go to **Moxa Device Extension > UPort** to view whether the UPort has been detected.

- Once this UPort has been detected, it will show the UPort model name and status in the list.
- If this UPort is not detected, unplug and plug in the UPort, then click **REFRESH**.

When the UPort has been detected, you can go to **System Settings > Serial** to see the new COM port shown as below. The user experience is just like the native COM ports. You can change the serial parameters and configure Modbus settings on the COM port.





If we want to change to another UPort, do the following:

1. Backup Modbus configuration file that is based on UPort's COM port.
2. Unplug **UPort** from the device.
3. Click **REMOVE**.
4. **Plug** in another new UPort.
5. Press **REFRESH**, then the new UPort should be detected.

NOTE

The configuration of serial parameters and Modbus settings on the COM could be deleted. Ensure to do the configuration backup before replacing it with a new one.

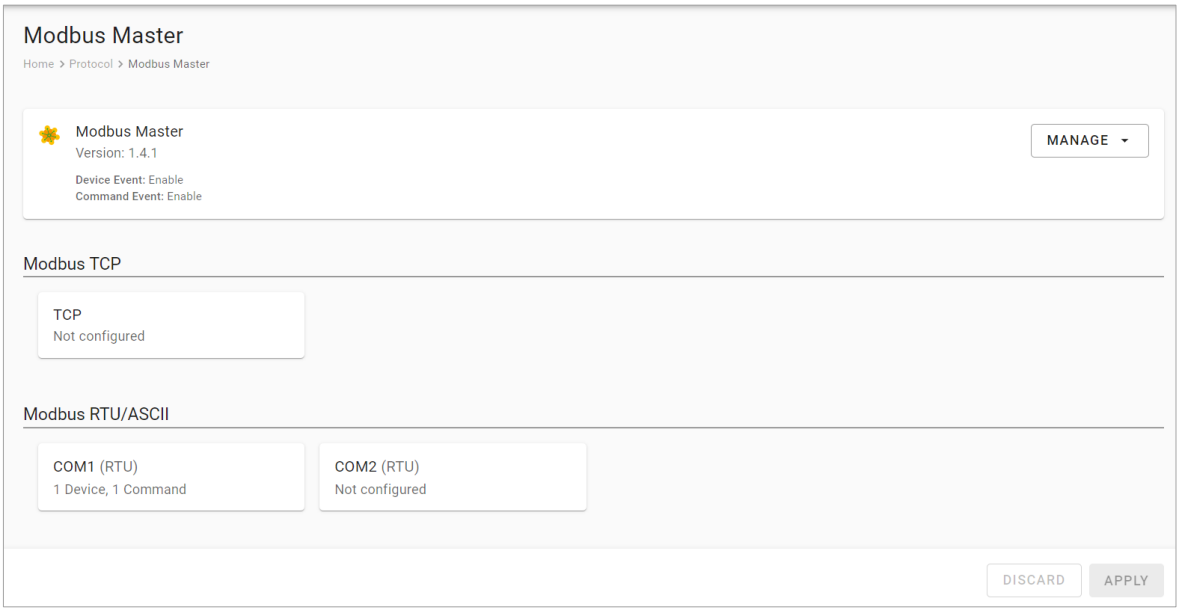
Southbound Protocol

Modbus Master

Go to **Modbus Master** to configure Modbus commands to collect the data from Modbus TCP, Modbus RTU, Modbus ASCII devices.

To create a new Modbus Master to collect data, do the following:

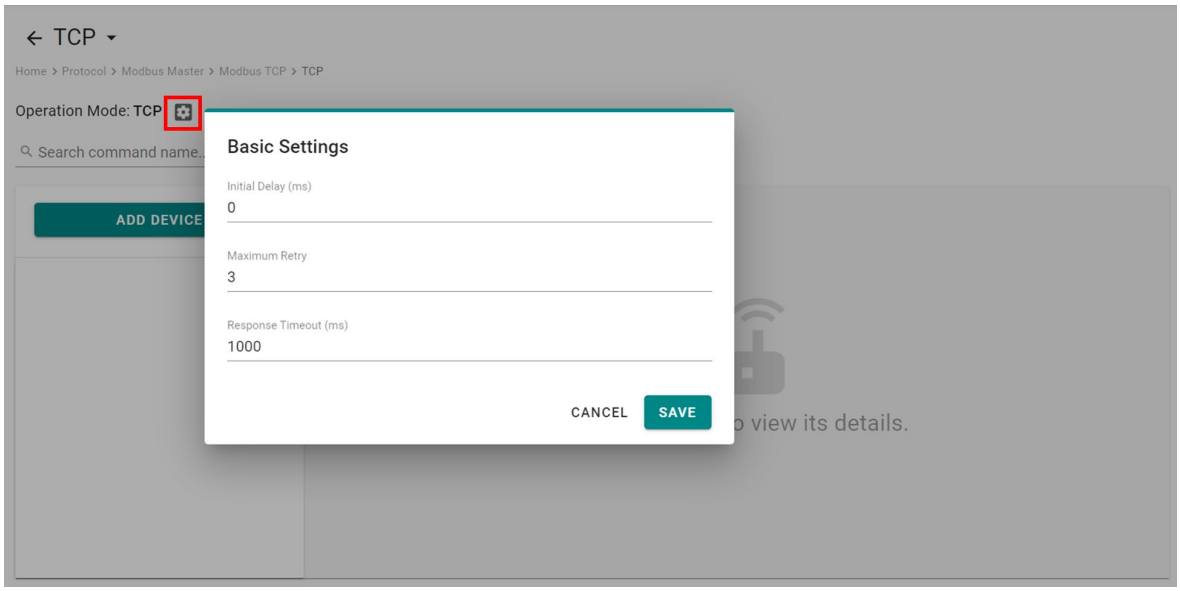
1. Click **TCP** under Modbus TCP or **COMx** under Modbus RTU/ASCII.
2. Click **ADD DEVICE** and go to the 3-step wizard page.
3. Input **device name**, **slave ID, IP Address,** and **TCP port**, then press **NEXT.**
4. Click **+ ADD COMMAND** to add Modbus commands to collect the data, then press **NEXT.**
5. Click **DONE** if you have confirmed the settings are correct.
6. Click **GO TO APPLY SETTINGS** and **APPLY** for the settings to take effect.



Modbus TCP

Basic Settings

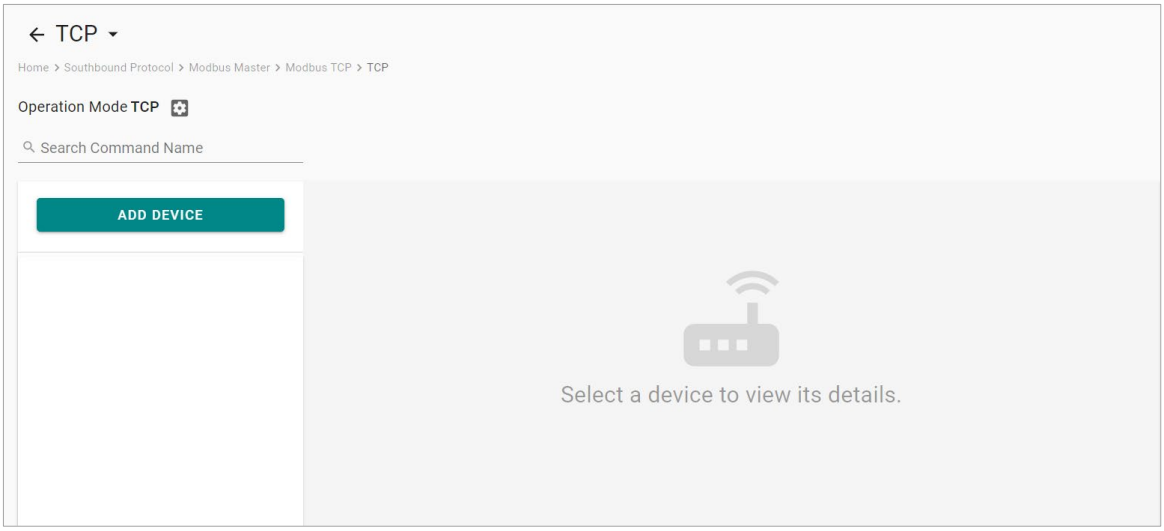
When you access the Modbus TCP setting page, you will first need to configure the basic settings.



Parameter	Value	Default	Description
Initial Delay (ms)	0 to 30000	0	Some Modbus slaves may take more time to boot up than other devices. In some environments, this may cause the entire system to suffer from repeated exceptions during the initial bootup. After booting up, you can force the AIG to wait some time before sending the first request by setting a value for this parameter.
Maximum Retry	0 to 5	3	Configure how many times AIG will retry to communicate with the Modbus slave when the Modbus command times out.
Response Timeout (ms)	10 to 120000	1000	You can configure a Modbus master to wait a certain amount of time for a slave's response. If no response is received within the configured time, the AIG will disregard the request and continue operation.

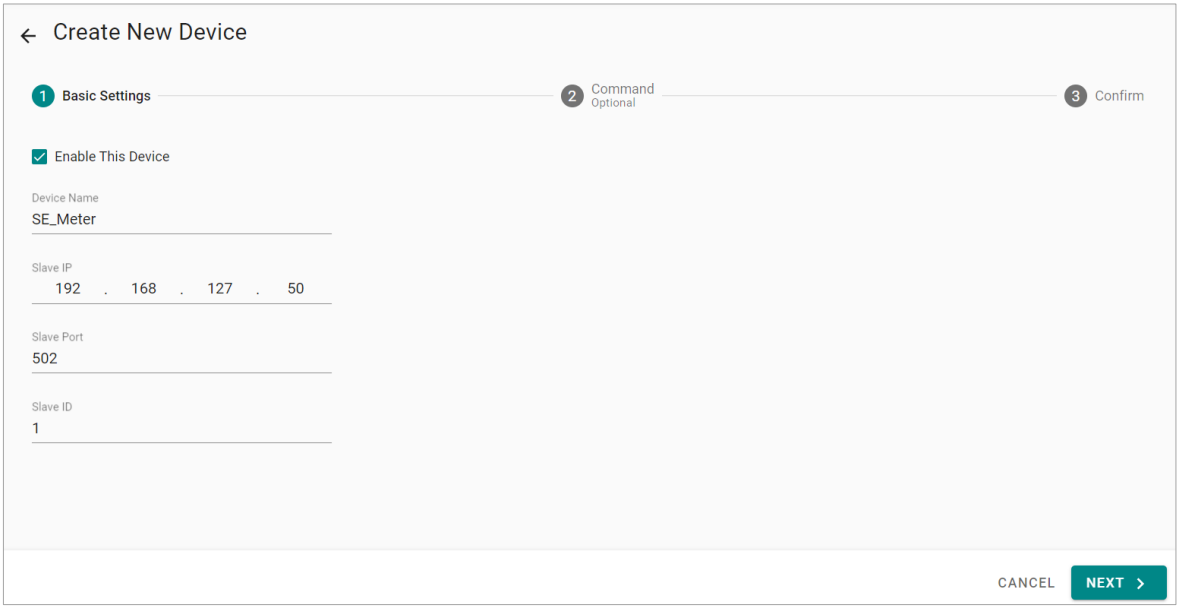
Modbus Device Settings

After configuring the basic settings, configure related parameters to retrieve data from the Modbus device. In the beginning, press **ADD DEVICE** and go to the wizard to guide you through the configuration step by step.



Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.

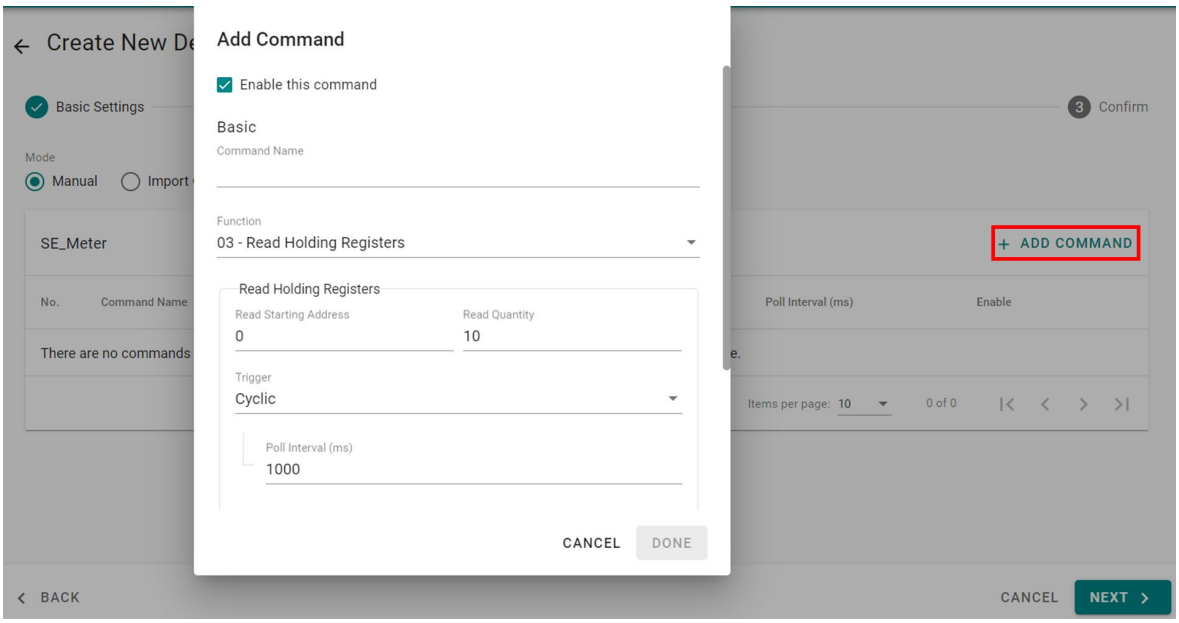


Parameter	Value	Default	Description
Device Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name your Modbus device
IP Address	0.0.0.0 to 255.255.255.255	–	The IP address of a remote slave device.
Slave Port	1 to 65535	502	The TCP port number of a remote slave device.
Slave ID	1 to 255	–	The slave ID of a remote slave device.

Step 2. Command

When you configure the device for the first time, select **Manual** mode and press **ADD COMMAND.**

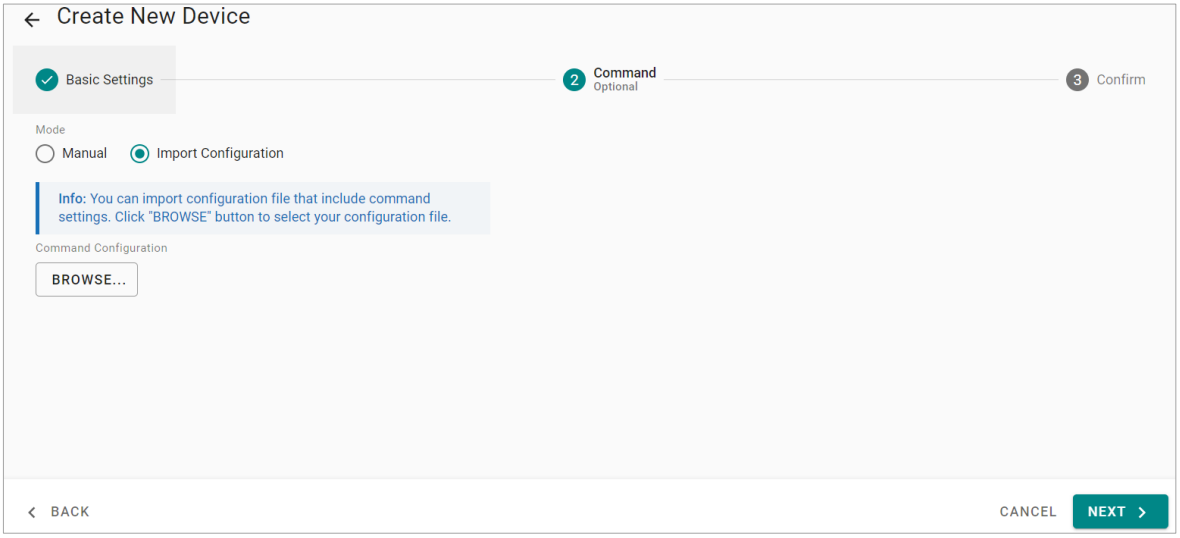
The command settings will pop up.



Parameter	Value	Default	Description
Command Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name the command
Function	01 – Read Coils 02 – Read Discrete Inputs 03 – Read Holding Registers 04 – Read Inputs Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 23 – Read/Write Multiple Registers	03 – Read Holding Registers	How to collect data from the Modbus device
Read Starting Address	0 to 65535	0	Modbus registers the address for the collected data
Read quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how much data to read
Write start address	0 to 65535	0	Modbus registers the address for the written data
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends all requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	**None:** not to swap **Byte:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C **Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. **Byte and Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.

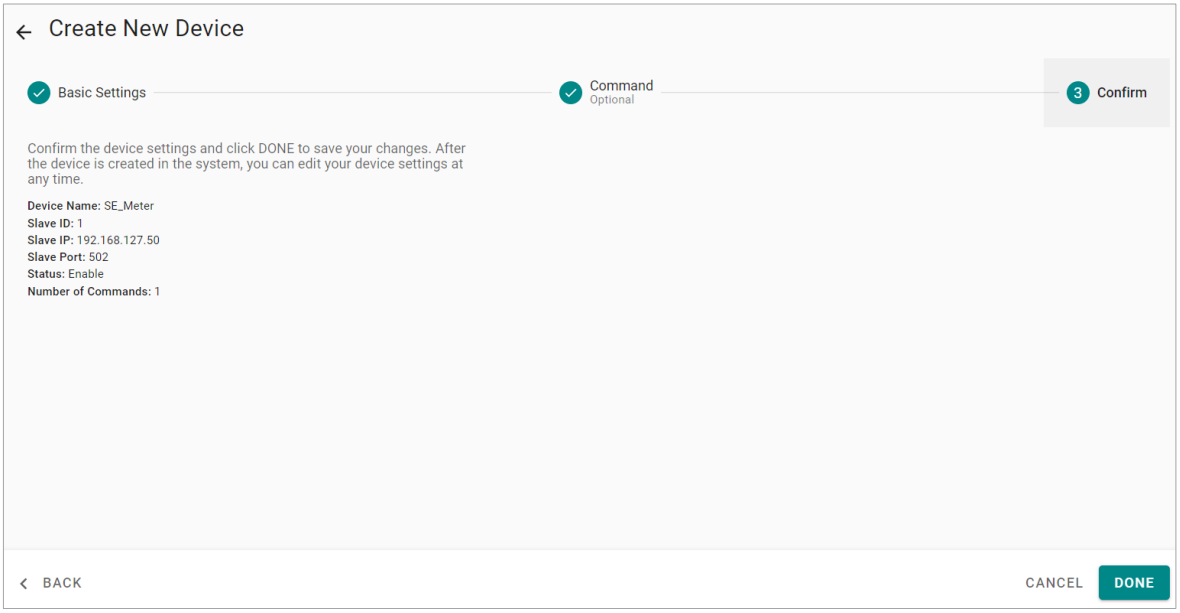
Parameter	Value	Default	Description
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in tag hub.

If you already have a Modbus command file, select **Import Configuration** mode. Importing a configuration file will help you reduce configuration time.



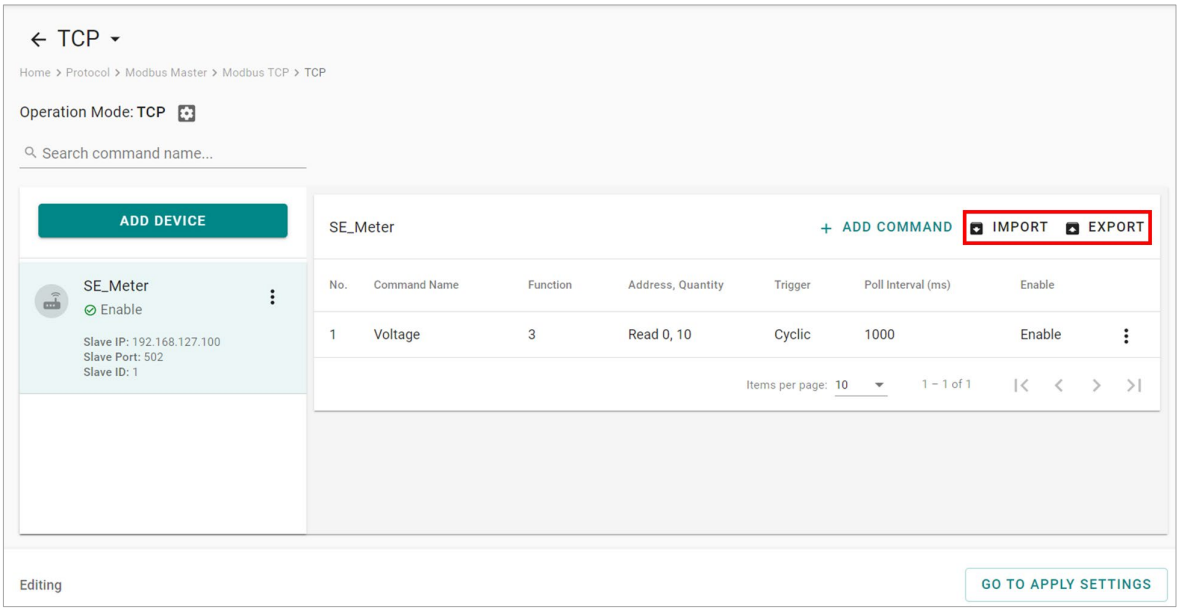
Step 3. Confirm

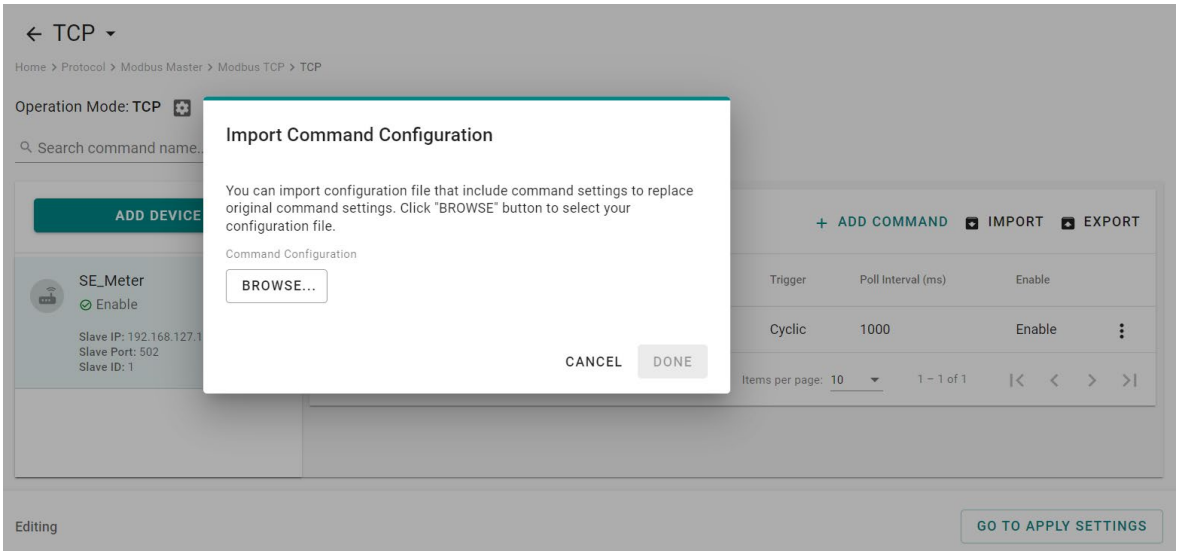
Review whether the information of the settings is correct.



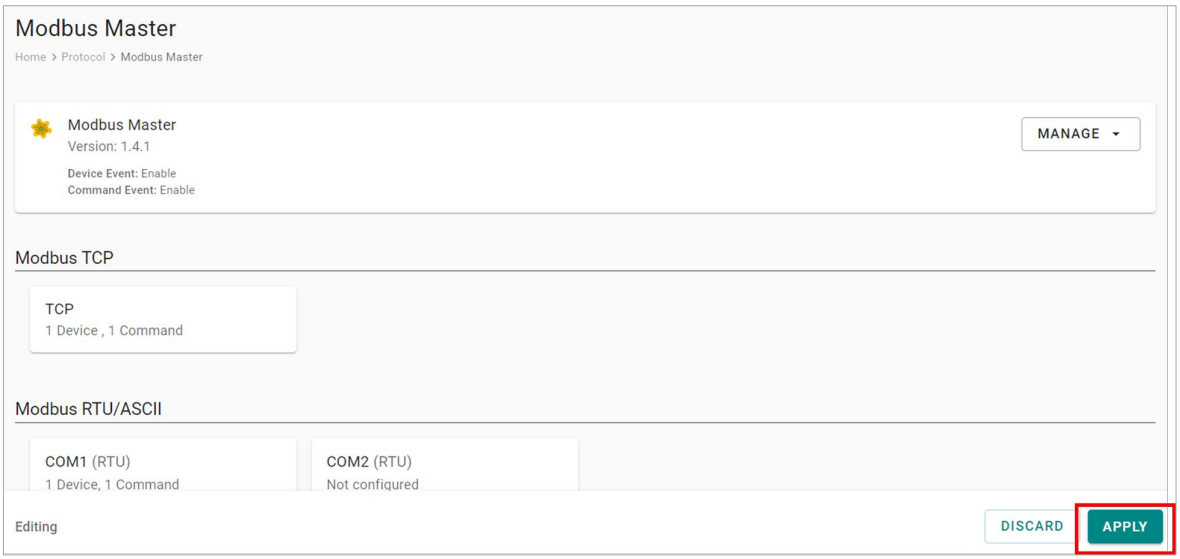
Then, you will see the setting results.

The product provides an easier way for installation and maintenance. You can **EXPORT** all the Modbus commands into a file for backup purposes, or you can **IMPORT** a file (golden sample) to reduce configuration time.





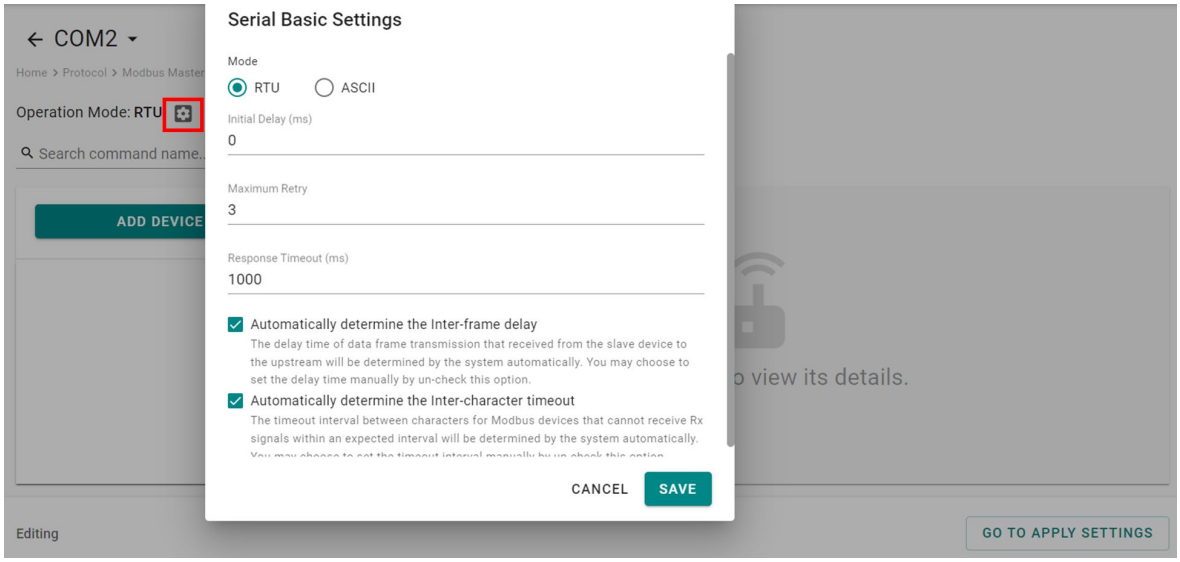
After finishing all the settings, press **GO TO APPLY SETTINGS** and click **APPLY** for the settings take effect.



Modbus RTU/ASCII

Basic Settings

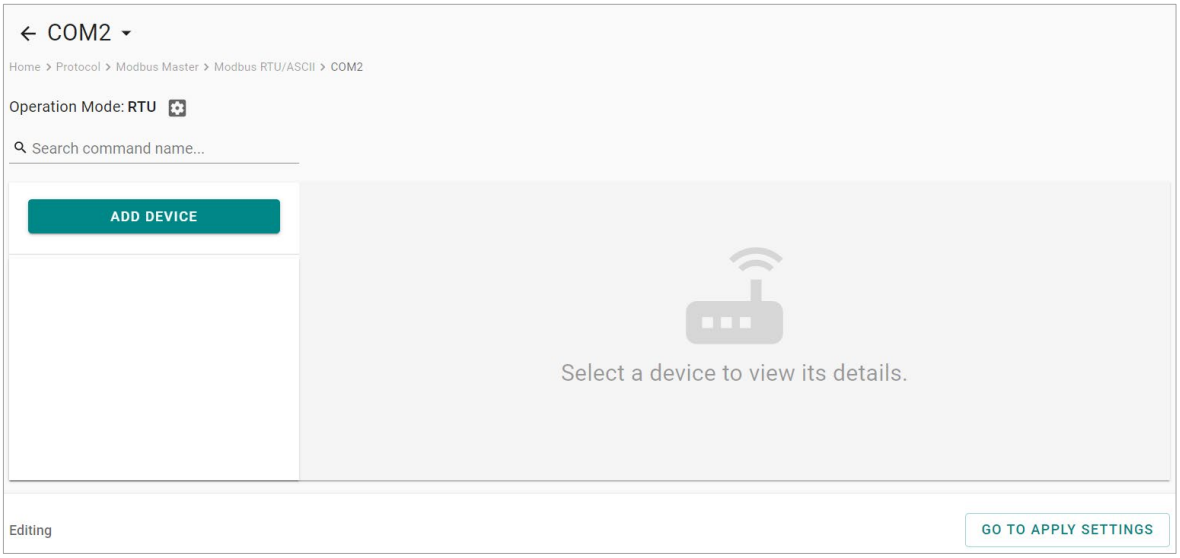
When you access the Modbus RTU/ASCII setting page, you will first need to configure basic settings.



Parameter	Value	Default	Description
Mode	RTU/ASCII	RTU	
Initial Delay (ms)	0 to 30000	0	Some Modbus slaves may take more time to boot up than other devices. In some environments, this may cause the entire system to suffer from repeated exceptions during the initial bootup. After booting up, you can force the AIG to wait some time before sending the first request by setting a value for this parameter.
Maximum Retry	0 to 5	3	Use this to configure how many times AIG will retry to communicate with the Modbus slave when the Modbus command times out.
Response Timeout (ms)	10 to 120000	1000	You can configure a Modbus master to wait a certain amount of time for a slave's response. If no response is received within the configured time, the AIG will disregard the request and continue operation.
Automatically determine the inter-frame delay (ms)	Check uncheck: 10 to 500	check	Inter-frame delay is the time between the response and the next request. This is to ensure a legacy Modbus slave device can handle packets in a short time. **Check:** The AIG will automatically determine the time interval. **Uncheck:** You can input a time interval.
Automatically determines the intercharacter timeout (ms)	Check uncheck: 10 to 500	check	Use this function to determine the timeout interval between characters for receiving Modbus responses. If AIG can't receive Rx signals within an expected time interval, all received data will be discarded. **Check:** The AIG will automatically determine the time out. **Uncheck:** You can input a specific timeout value.

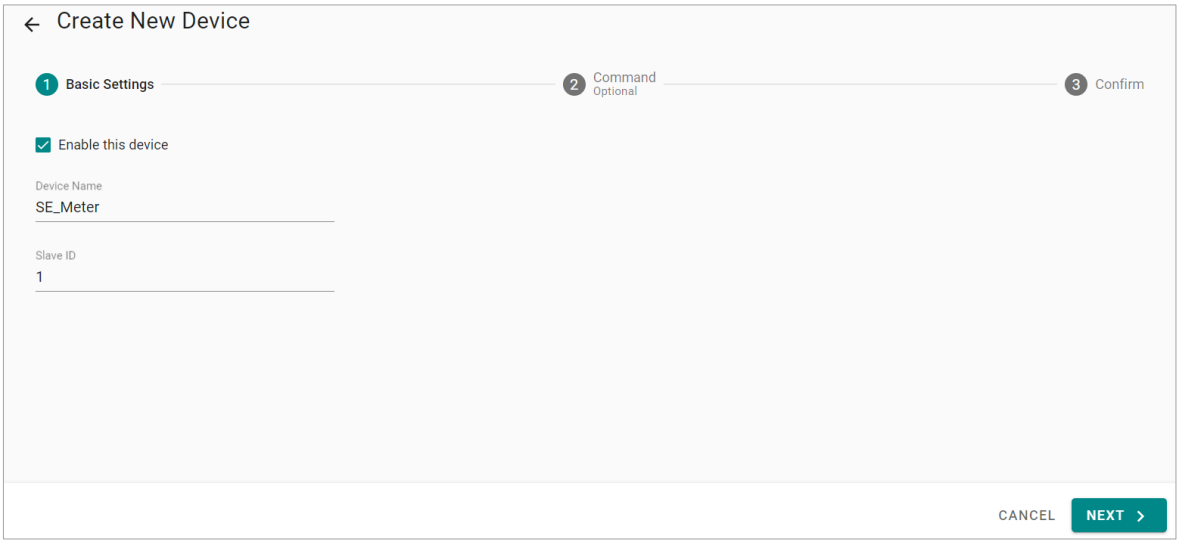
Modbus Device Settings

After basic settings, you must configure related parameters to retrieve data from the Modbus device. In the beginning, press **ADD DEVICE** and go to the wizard that guides you through the configuration step by step.



Step 1. Basic Settings

Fill in the basic parameters for the Modbus RTU/ASCII device.

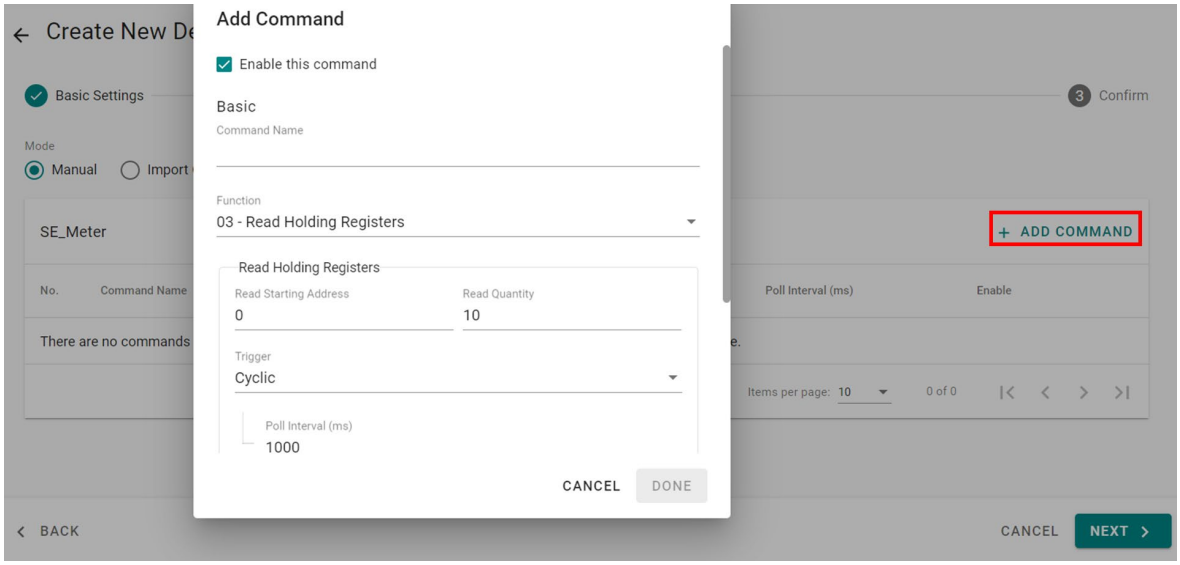


Parameter	Value	Default	Description
Device Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name your Modbus device
Slave ID	1 to 255	–	The slave ID of a remote slave device.

Step 2. Command

If you are configuring the device for the first time, select the **Manual** and press **ADD COMMAND.**

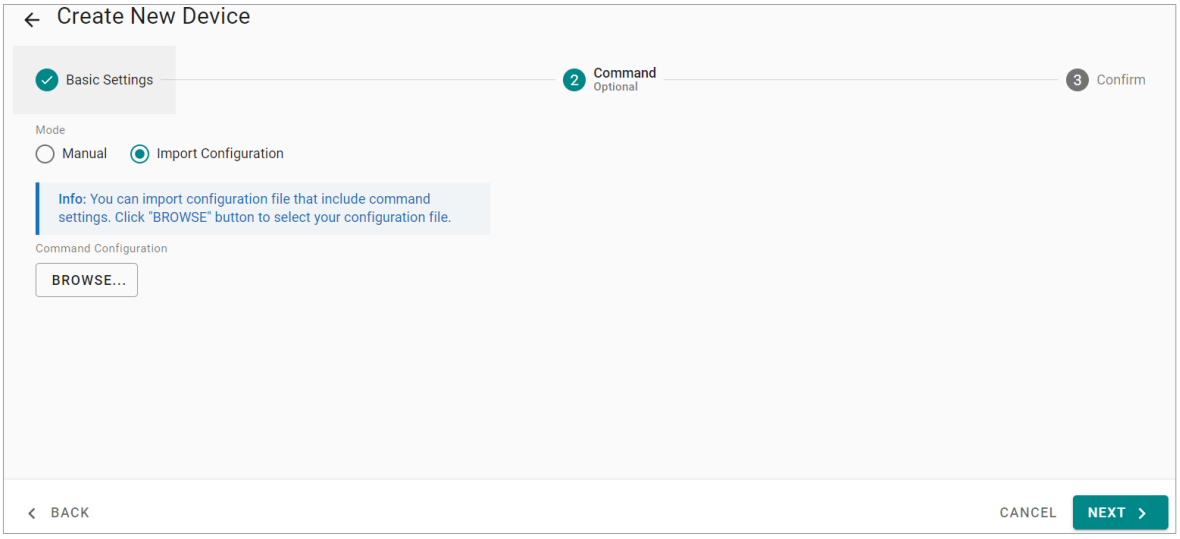
The command settings will pop up.



Parameter	Value	Default	Description
Command Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name the command
Function	01 – Read Coils 02 – Read Discrete Inputs 03 – Read Holding Registers 04 – Read Inputs Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 23 – Read/Write Multiple Registers	03 – Read Holding Registers	How to collect data from the Modbus device
Read Starting Address	0 to 65535	0	Modbus registers the address for the collected data
Read quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how much data to read
Write starting address	0 to 65535	0	Modbus registers the address for the written data

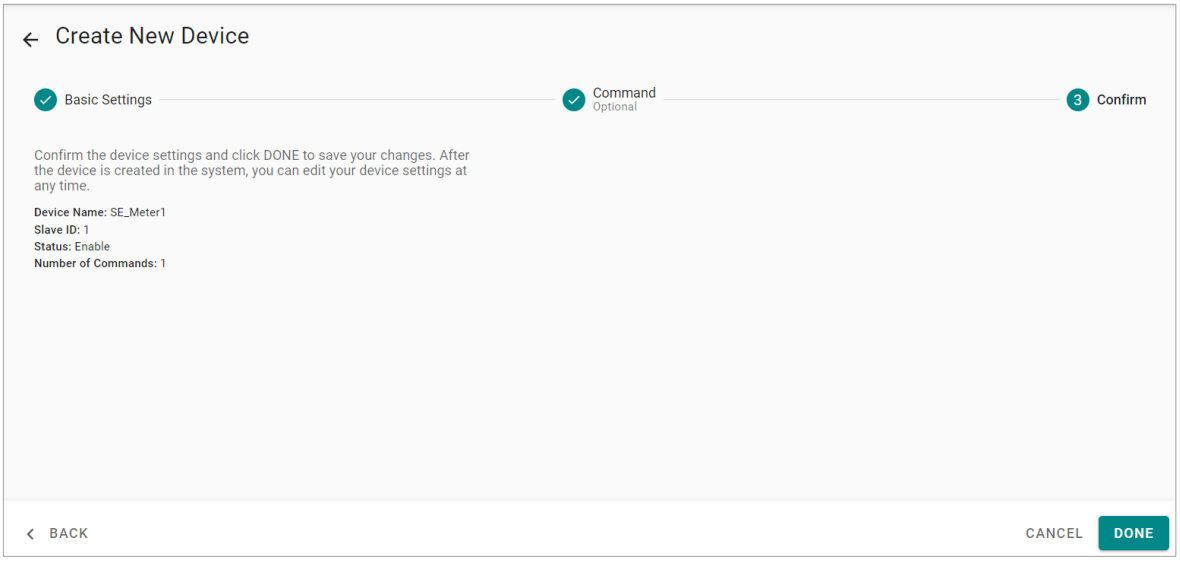
Parameter	Value	Default	Description
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	**None:** not to swap **Byte:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C **Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. **Byte and Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in the tag hub.

If you already have a Modbus command file on hand, select the **Import Configuration** mode. Importing a configuration file will help you reduce configuration time.



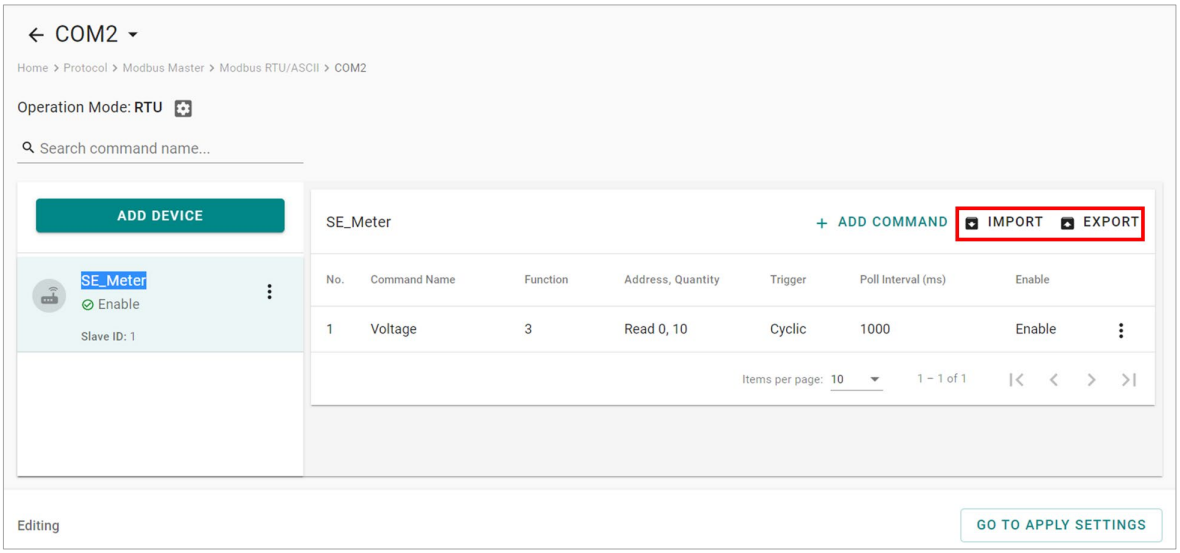
Step 3. Confirm

Review whether the information of the settings is correct.

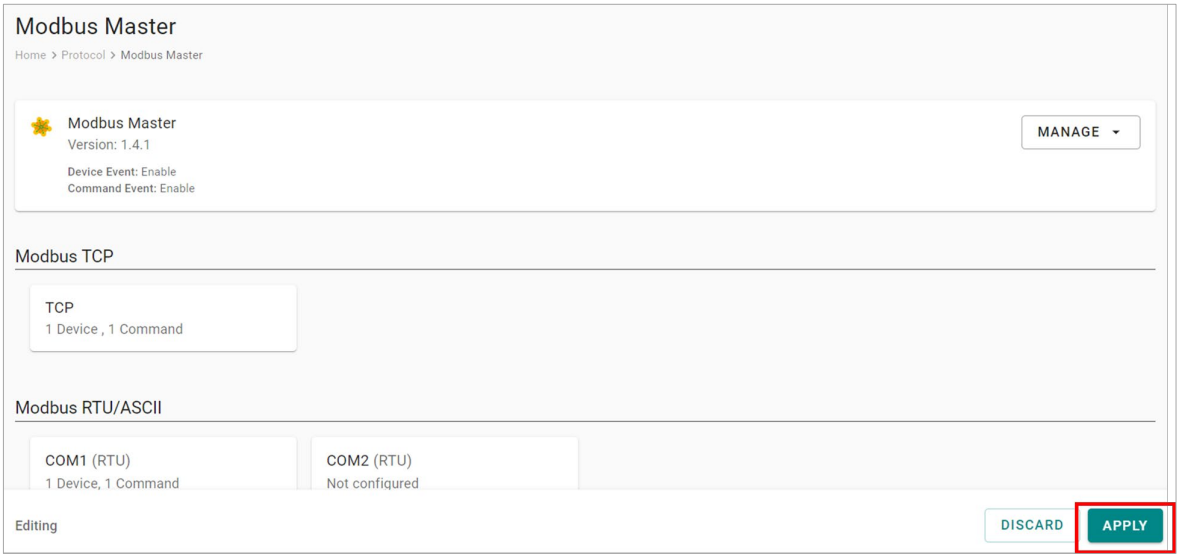


Then, you will see the setting results.

Moreover, the product provides an easier way for installation and maintenance. You can **EXPORT** all the Modbus commands into a file for backup purposes; or you can **IMPORT** a file (golden sample) to reduce configuration time.

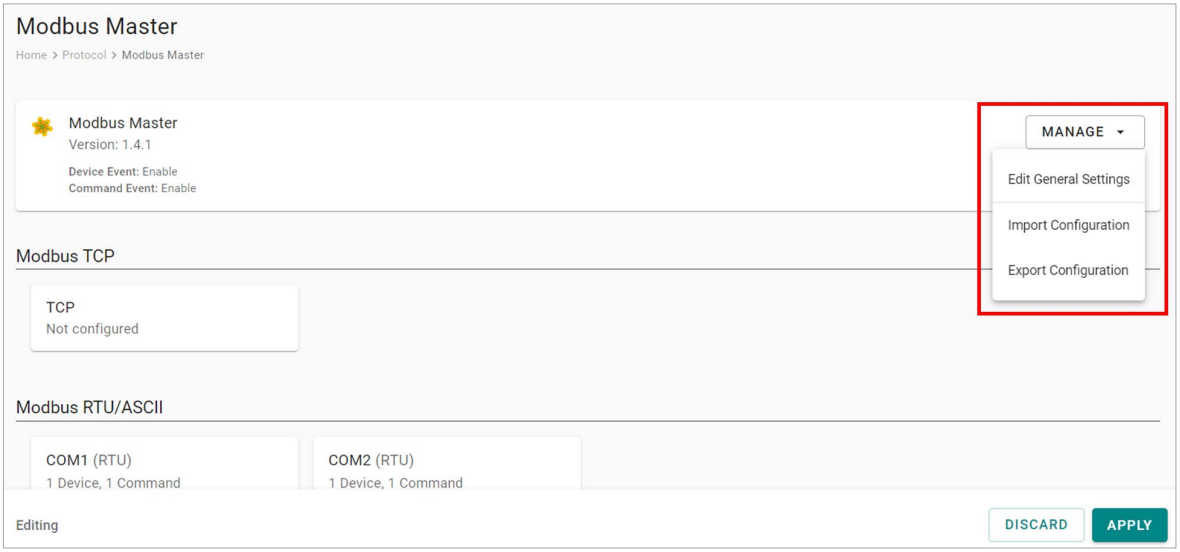


After finishing all the settings, press **GO TO APPLY SETTINGS** and click **APPLY** for the settings to take effect.



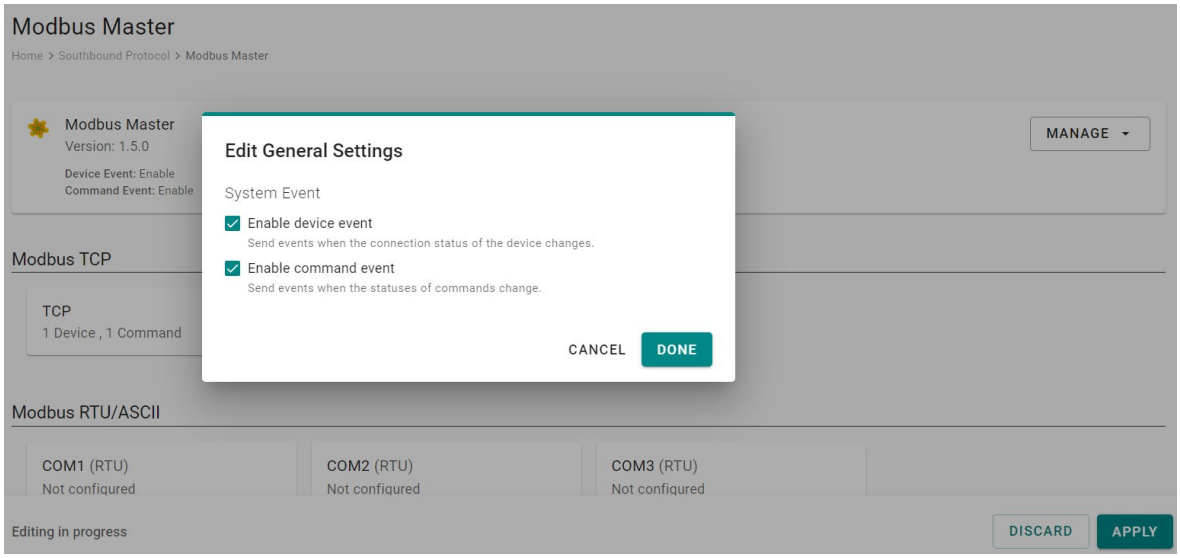
Manage

The AIG provides advanced features that help you save installation time and maintenance effort.



Edit General Settings

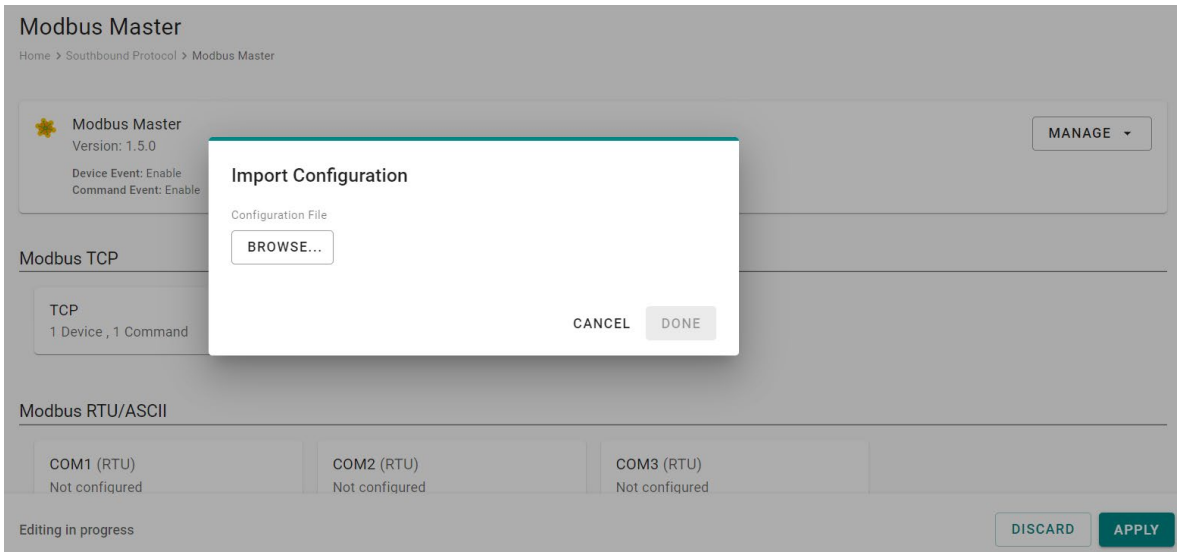
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	**Check:** If the Modbus communication fails, such as the TCP connection gets disconnected, the Modbus response timeout, the value of the status tag in the tag hub, will change to 1. **Uncheck:** Disable the function
Enable command event	Check uncheck	Check	**Check:** If the Modbus command fails, e.g., Modbus exception code is received, the Modbus response timeout, the value of the status tag in the tag hub, will change to 1. **Uncheck:** Disable the function

Import/Export Configuration

You can Import/Export all **of the Modbus Master settings,** which will be stored in XML format.



An example of an exported file that can be viewed/edited by EXCEL.

[master-tcp-ifaces]

@master	tcpMaste	initialDel	retryCour	responseTout
1	1	0	3	1000

[ser-masters]

@serMas	configId	name
1	1	modbus_serial_master

[master-ser-ifaces]

@master	serMaster	portValue	format	initialDel	retryCour	response	frameInte	charInterval
1	1	0	0	0	3	1000	0	0
2	1	1	0	0	3	1000	0	0

[remote-devs]

@remote	masterSer	masterTcp	name	enable	slaveId	slaveIpad	slaveTcpPort
1	1		1232	1	1	0.0.0.0	502
2	2		SE_Meter	1	1	0.0.0.0	502
3		1	GE_Meter	1	1	11.1.1.1	502

[mcmds]

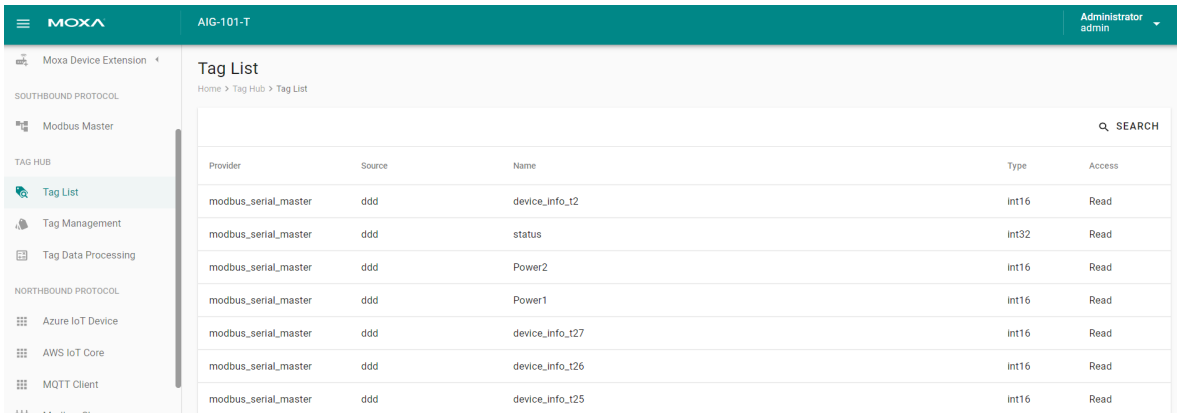
@remote	name	enable	mode	func	readAddr	readQuar	writeAddr	writeQua	pollInterv	swap	fpFunc	fpTout	fpData	scalingFu	intercept	intercept	pointSou	pointSou	pointTarg	pointTarg	tagName	dataType	dataUnit	access	dataSize
1	231	1	0	3	0	10	0	1	1000	0	0	3600		0	1	0	0	1	0	1	231	raw		r	20
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600		0	1	0	0	1	0	1	Voltage_t1	int16		r	
																					Voltage_t2	int16		r	
																					Voltage_t3	int16		r	
																					Voltage_t4	int16		r	
																					Voltage_t5	int16		r	
																					Voltage_t6	int16		r	
																					Voltage_t7	int16		r	
																					Voltage_t8	int16		r	

Tag Hub

Tag List

If you want to confirm what tags have been created in a tag hub, go to **Tag List** to view all the tags.

Since it shows all the tags in all the devices, use **SEARCH** to review easily.

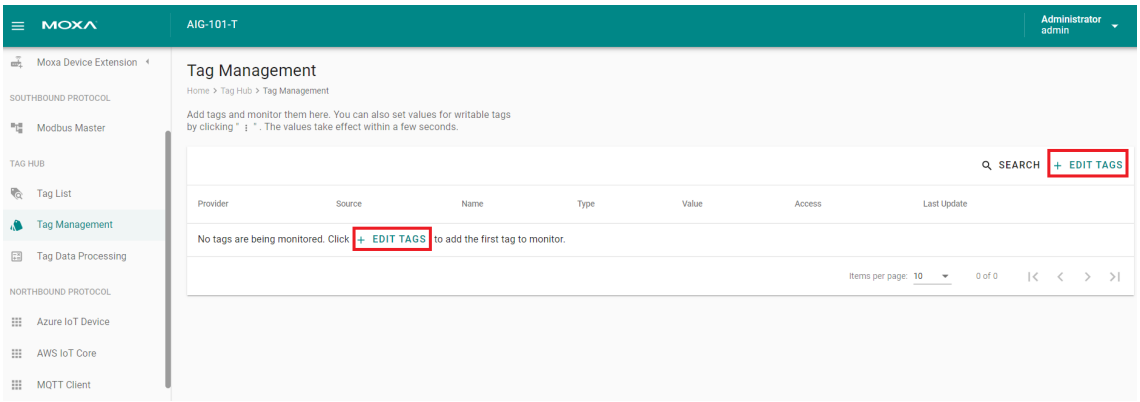


Tag Management

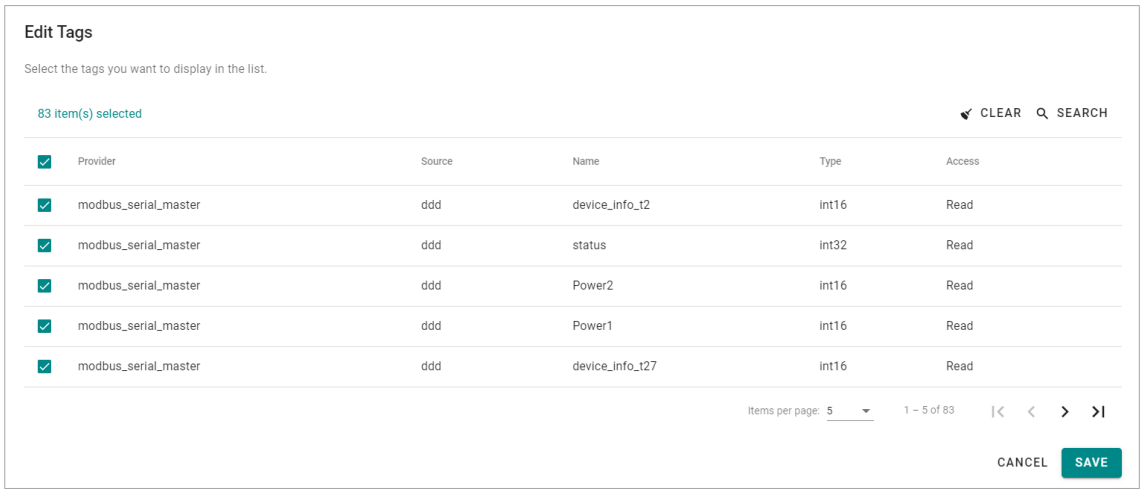
Go to **Tag Management,** where you can create and monitor the real-time tag value for troubleshooting purposes.

To see the tag's real-time value, do the following steps:

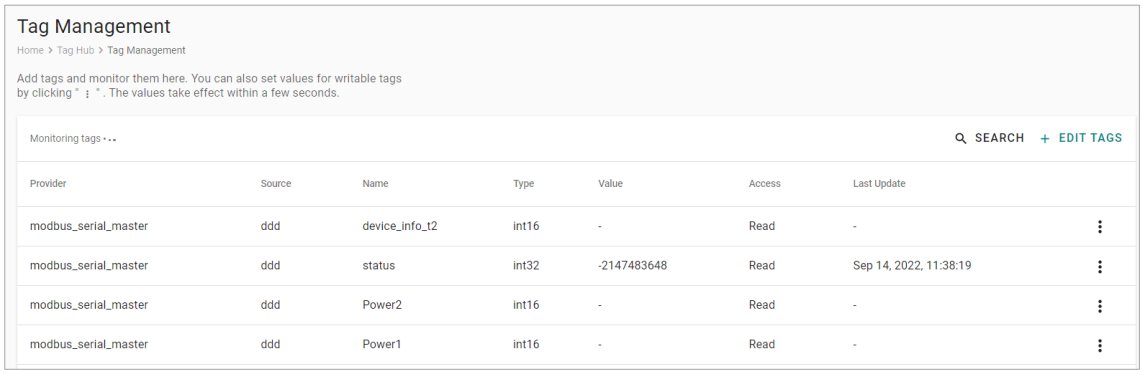
1. Click **+ EDIT TAGS**.



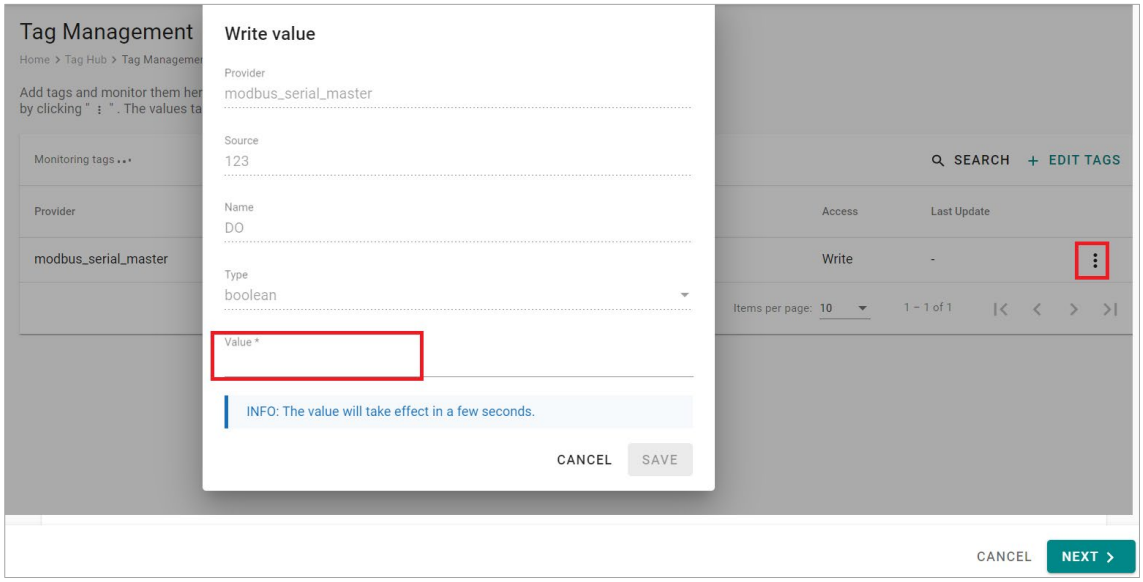
2. Select the **tags** to monitor in the list.



3. (Optional) use **SEARCH** to find the tags quickly.



4. Click **SAVE**.
5. (Optional) press the icon to deactivate the monitoring tags.
6. (Optional) press the icon to write value for test purposes.

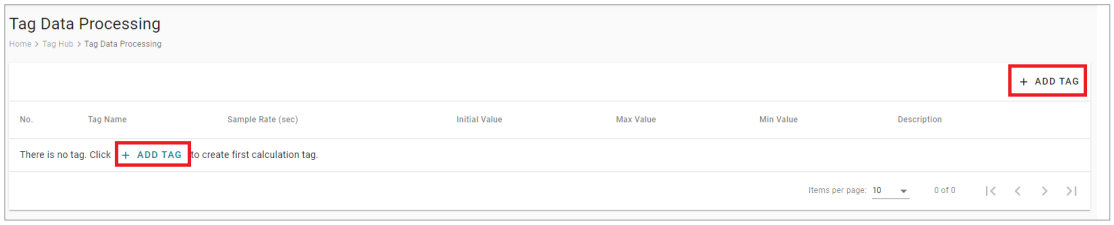


Tag Data Processing

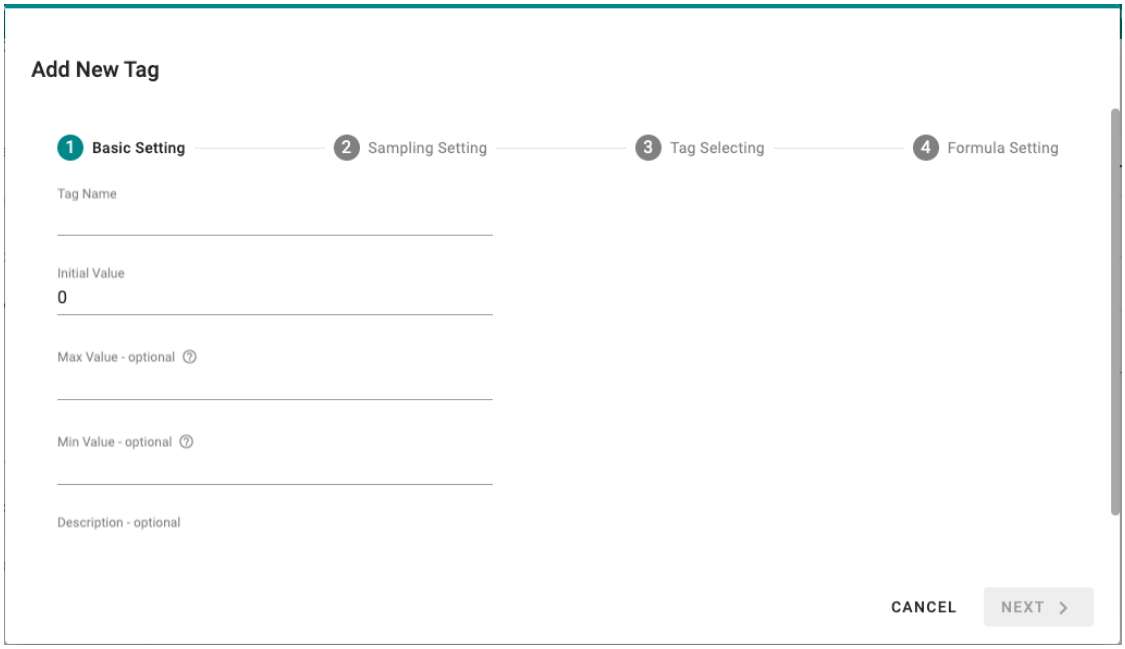
The device has a built-in intuitive no-code solution that can preprocess data before sending it to the northbound system. This feature helps eliminate the programming effort in data processing.

Go to **Tag Data Processing**, and do the following steps:

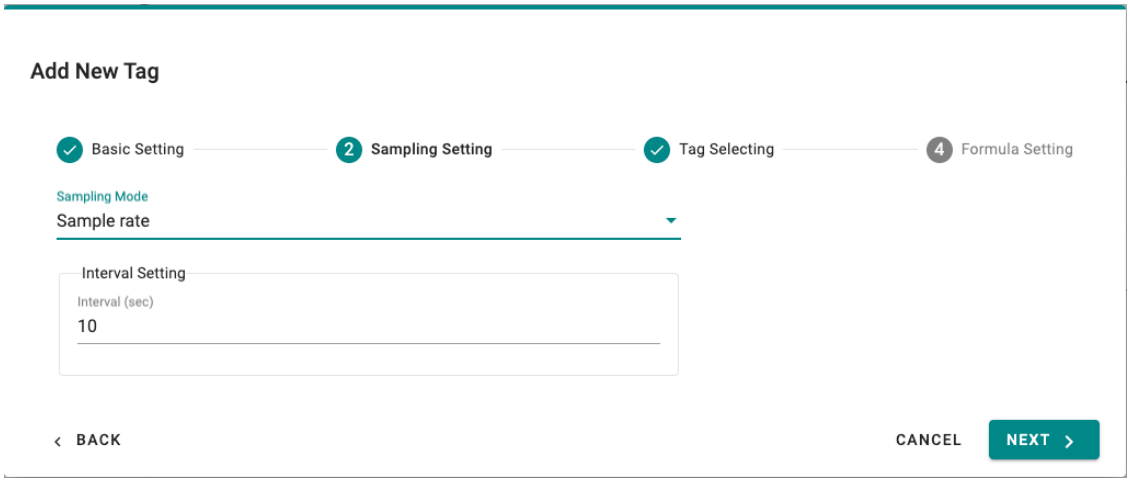
1. Click **+ ADD TAG**.



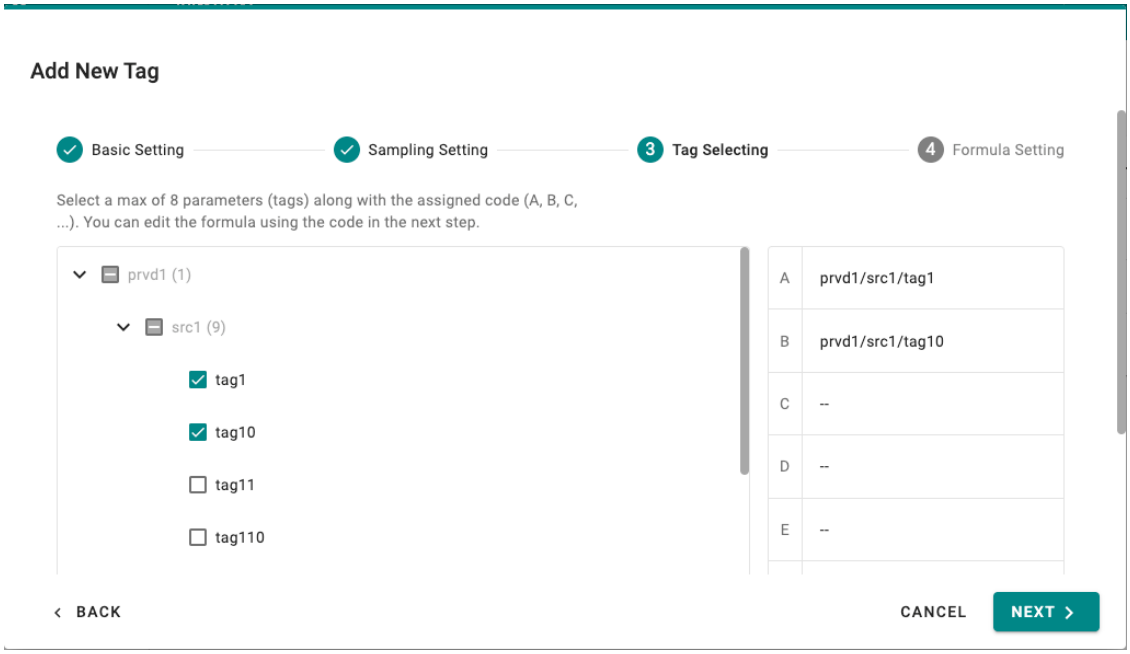
2. Specify **Tag Name, Sample Rate**, and other parameters for the new tag, then click **NEXT**.



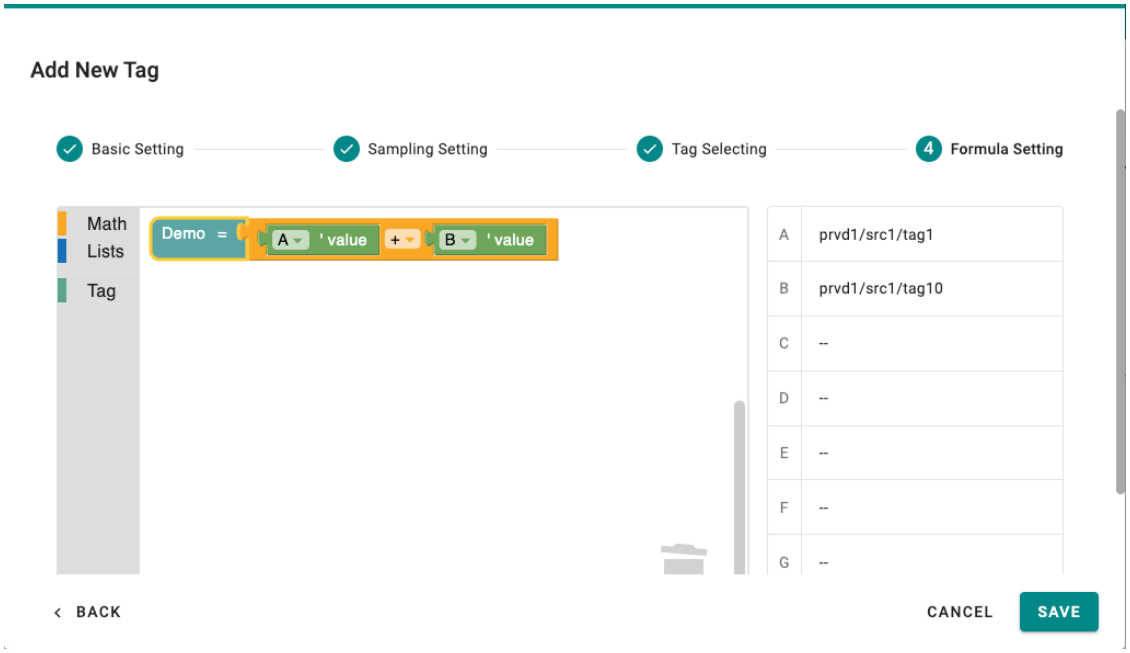
3. Select a sampling mode and click **NEXT**.



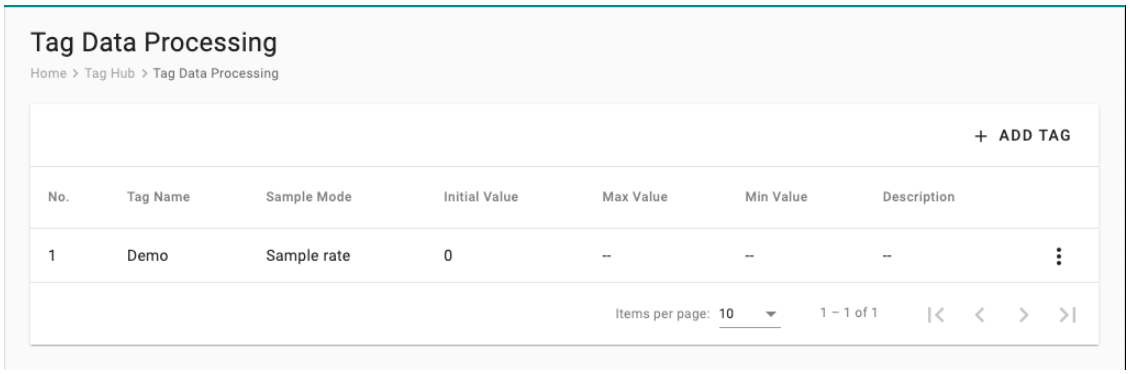
4. Select the tags from system or Modbus that you want to process, then click **NEXT**.



5. Drag and drop the formula and tags from **Math** and **Tag**.

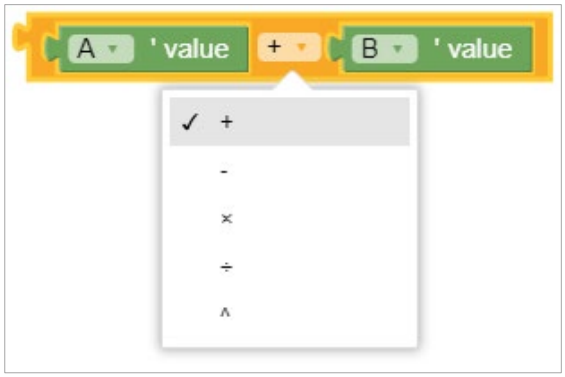


6. Click **SAVE** and you will see the new tag in the list.

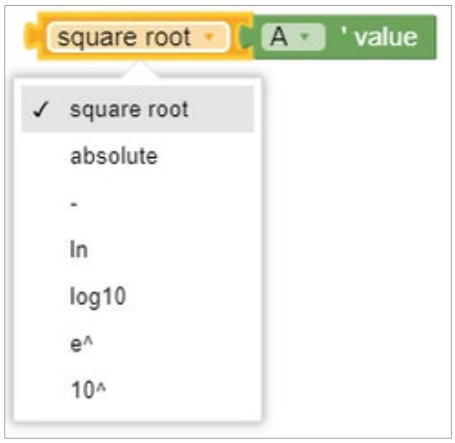


The supported formulas are:

- **addition(+), subtraction(-), multiplication(x), division(/), and power(^)**

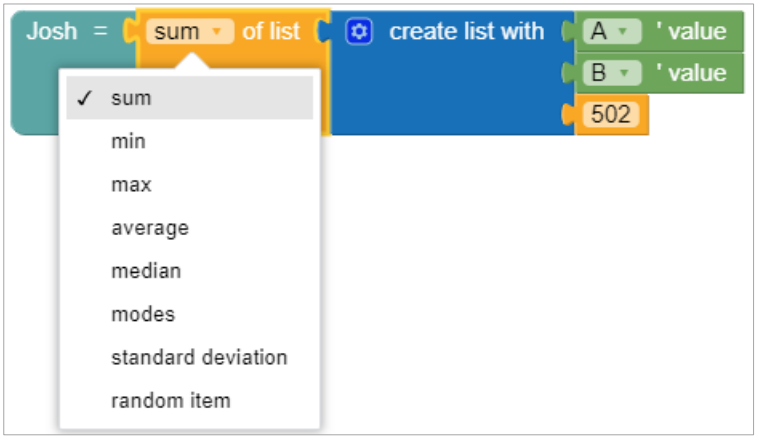


- **square root, absolute, negative(-), natural logarithm(ln), 10 logarithm(log10), power by Euler's number(e^), power by 10(10^)**



- **round, round up, round down**

- **sum, minimum, maximum, average, median, modes, standard deviation, random items**



Northbound Protocol

Azure IoT Device

Go to **Azure IoT Device**. You can enable or disable the Azure IoT Device.

Note that you will need to register an Azure account to manage the Azure IoT Device service for your IIoT application.

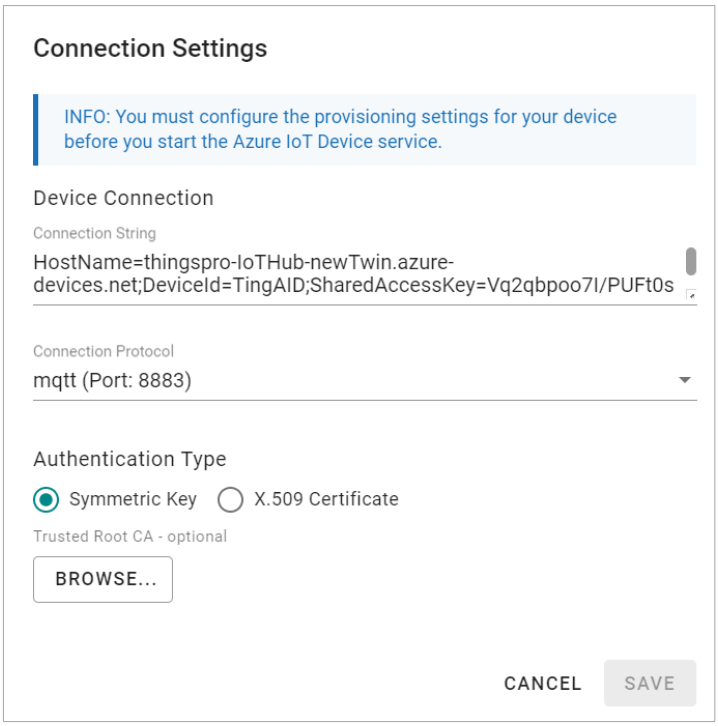
To create the Azure IoT Device connectivity, follow the steps below:

1. Click  to set up the connection.
2. Enter **Connection String.**
3. Select a **Connection Protocol.**
4. Select an **Authentication Type.**

   When using the X.509 authentication type, you only need to enter the HostName (FQDN) in the **Connection String**. TPE will automatically complete the connection string based on the following format:

   `HostName={iothub name}.azure-devices.net;DeviceId={device ID};x509=true`

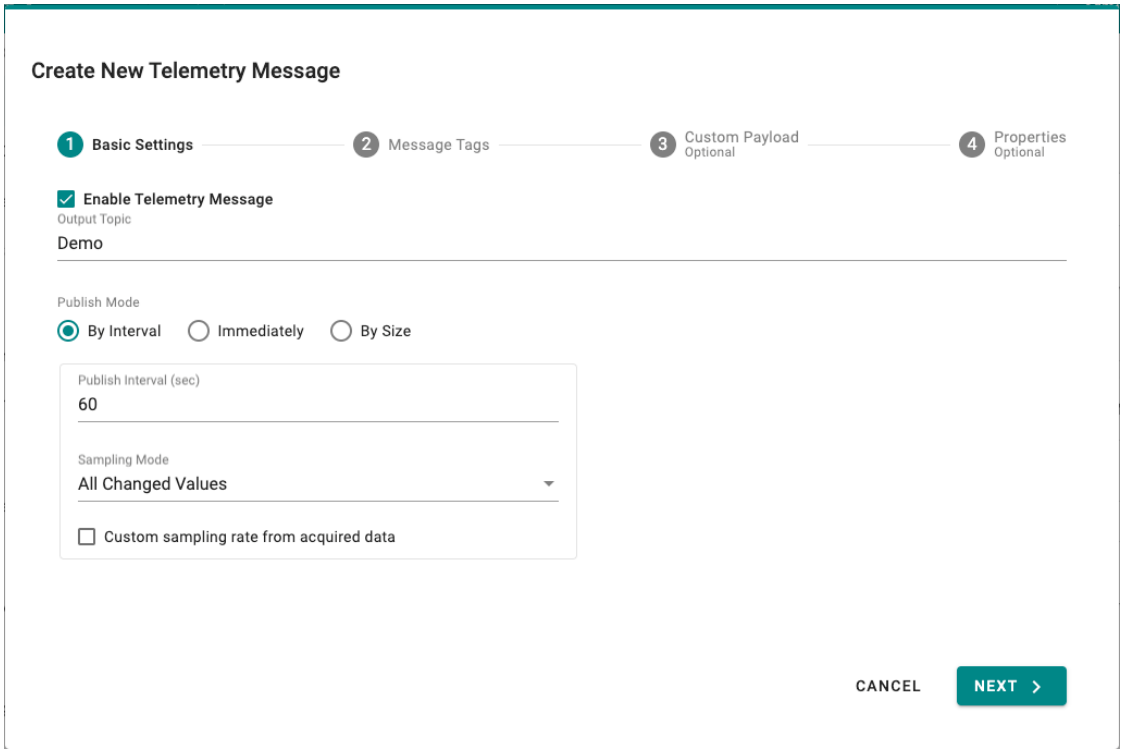
   `{iothub name:` The connection string parameter that you provide
   `{device ID}`: Abstracted from the cn of the subject in X.509 certificate.
5. (optional) Upload X.509 Certificate and Private Key.
6. (optional) Upload a trusted root CA to connect to a transparent gateway (e.g., Azure IoT Edge).
7. Click **SUBMIT**.


Connection Settings
INFO: You must configure the provisioning settings for your device before you start the Azure IoT Device service.
Device Connection
Connection String
HostName=thingspro-IoTHub-newTwin.azure-devices.net;DeviceId=TingAID;SharedAccessKey=Vq2qbpoo7l/PUFt0s
Connection Protocol
mqtt (Port: 8883)
Authentication Type
Symmetric Key
X.509 Certificate
Trusted Root CA - optional
BROWSE...
CANCEL
SAVE

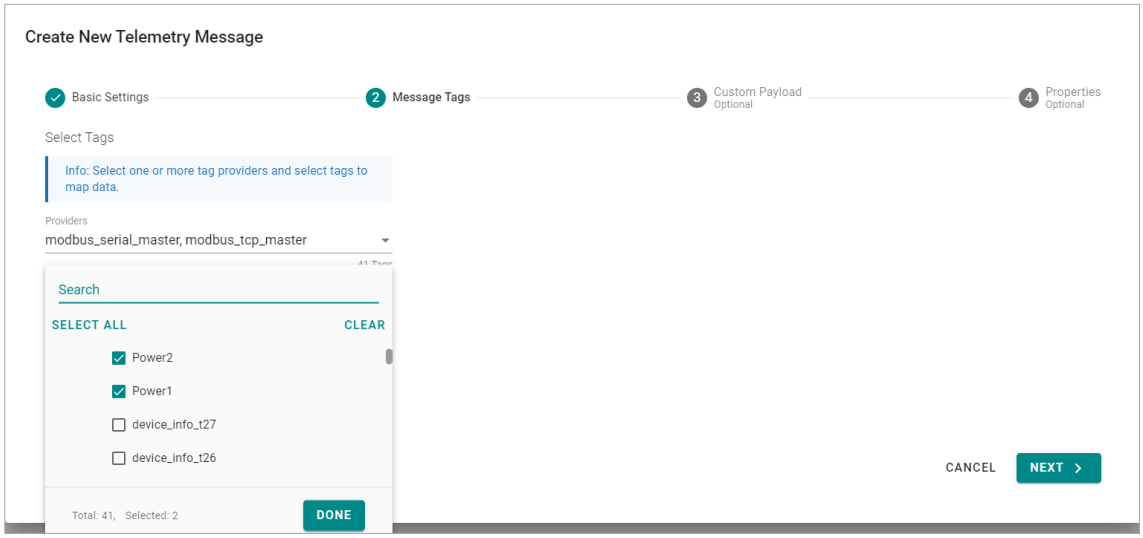
Telemetry Message

The simplest message type for sending IoT device data to your IIoT applications is a telemetry message. To create a telemetry message, do the following:

1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.

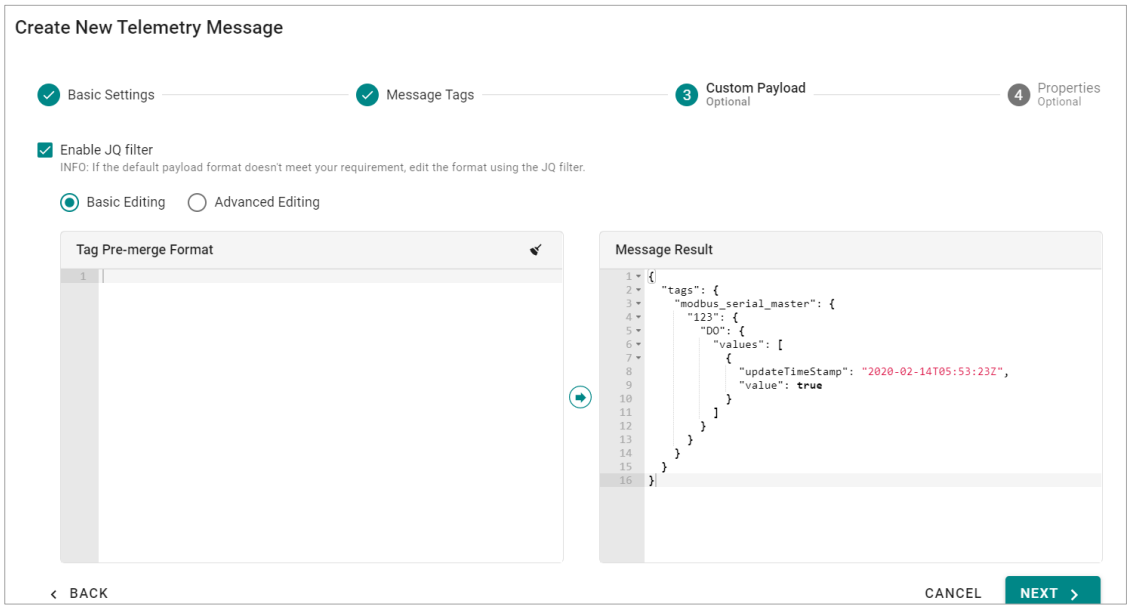


5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).

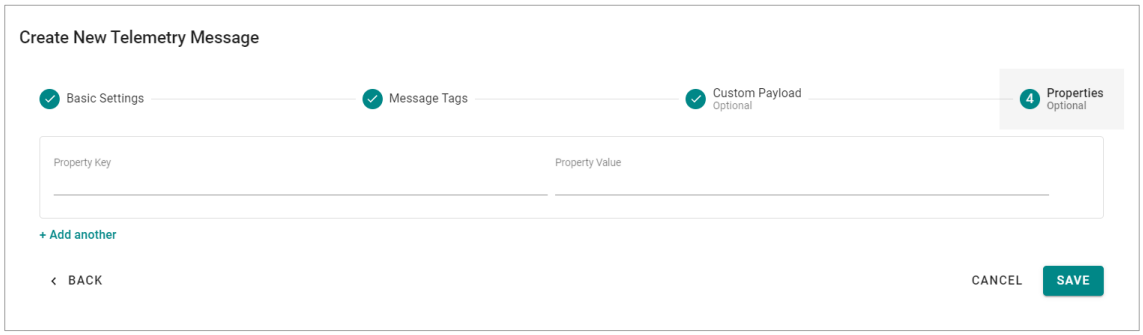


7. (Optional) Enable custom payload by using the jq filter.

   The device-to-cloud (D2C) message policy allows you to transform default payload to your desired payload schema via the jq filter. For additional information, refer to the jq website (https://stedolan.github.io/jq/manual/).



8. Click **NEXT**.
9. (Optional) Enter Property Key and Value.



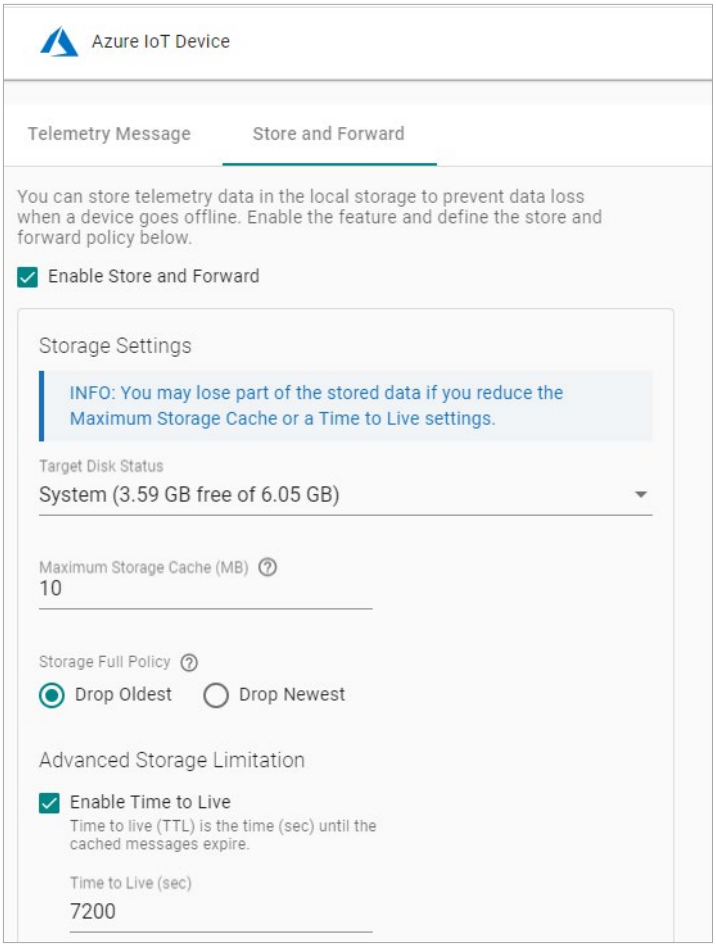
10. Click **SAVE**.

NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.

Store and Forward

D2C messages can be cached in a specified location and sent to the cloud later. This feature helps you keep the acquired data temporarily in a queue when the network between your IIoT Gateway and the cloud is disconnected. It will transmit the data to its destination once the network reconnects. To enable the function, click **Store and Forward** and select **Enable Store and Forward**. Select a target disk and a maximum storage cache, a retention policy, and a TTL (Time to Live) value for the messages.



NOTE

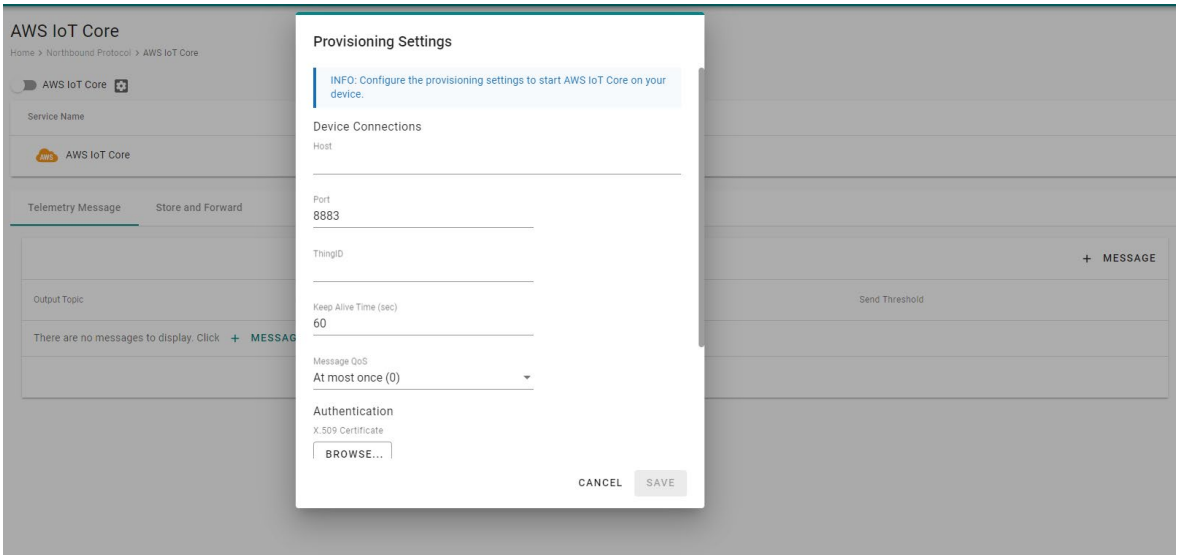
If you want to use the direct method to write tags from the cloud, refer to

https://tpe-tiger.github.io/AIG101/V1.1.0/taghub/#

AWS IoT Core

Go to **AWS IoT Core** and enable or disable the AWS IoT Core. To create the AWS IoT Core connectivity, follow the steps below:

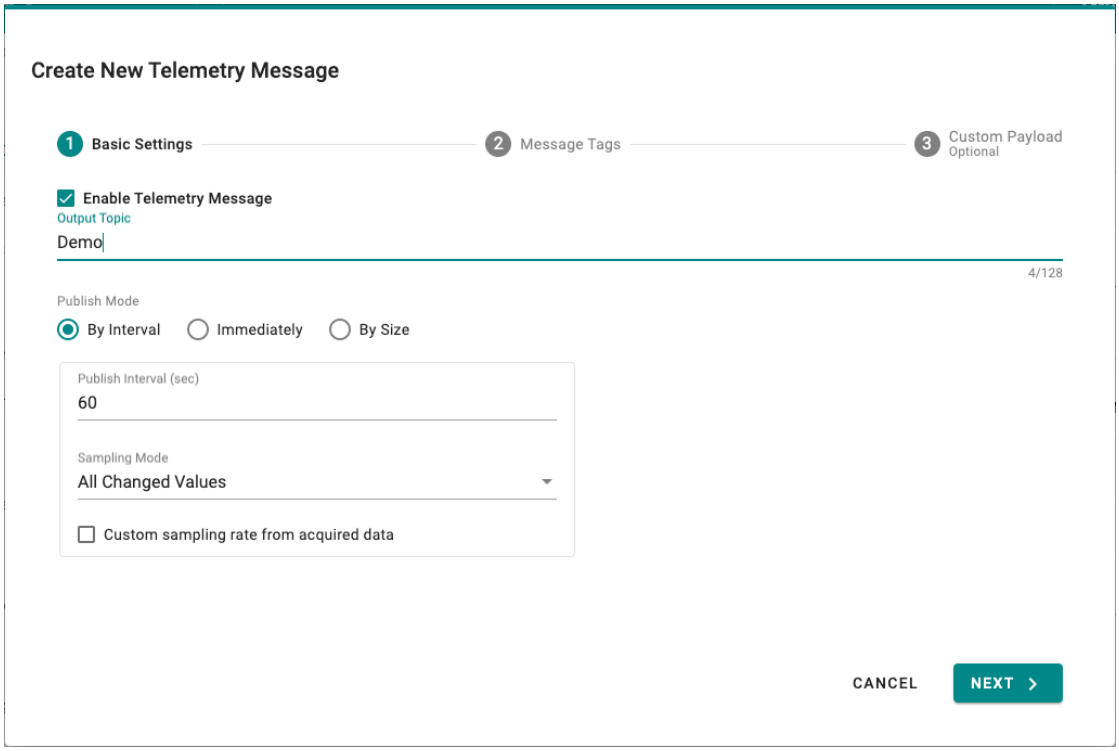
1. Click  to set connection.
2. Enter **Host (Endpoint)**. **Port** (default: 8883).
3. Enter **ThingID**.
4. Input **Keep Alive Time** (sec)
5. Select a way of message **QoS**.
6. Upload X.509 Certificate, Private Key, and (optional) Trusted Root CA.
7. Click **SAVE**.



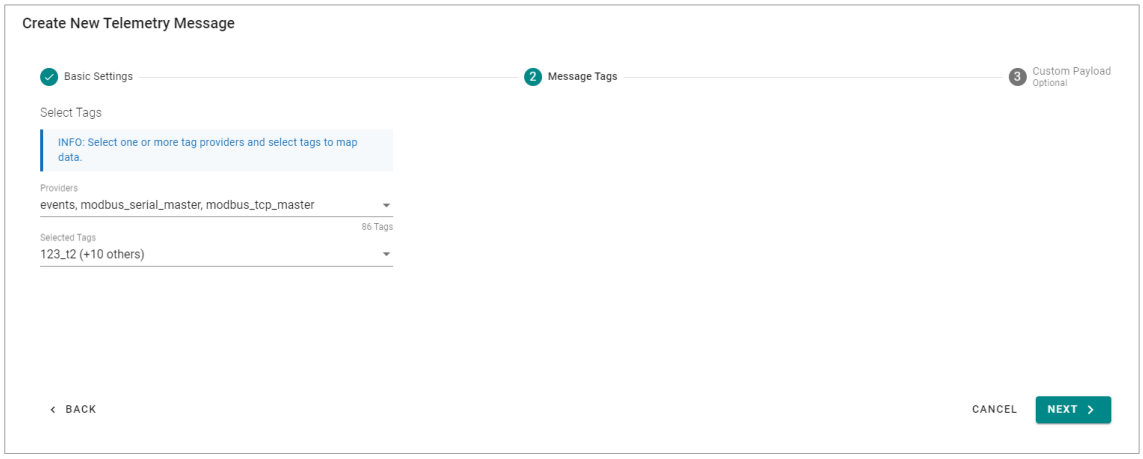
Telemetry Message

The simplest message type for sending IoT device data to your IIoT applications is a telemetry message. To create a telemetry message, do the following:

1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.

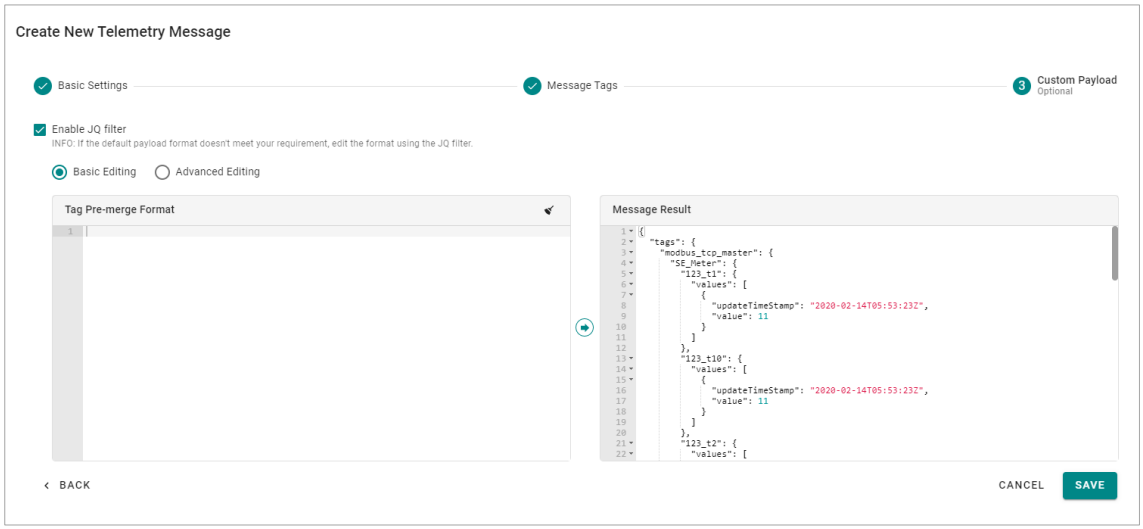


6. Select tags (e.g., Modbus Master).



7. (Optional) Enable custom payload by using the jq filter.

   The device-to-cloud (D2C) message policy allows you to transform default payload to your desired payload schema via the jq filter. For additional information, refer to the jq website (https://stedolan.github.io/jq/manual/).



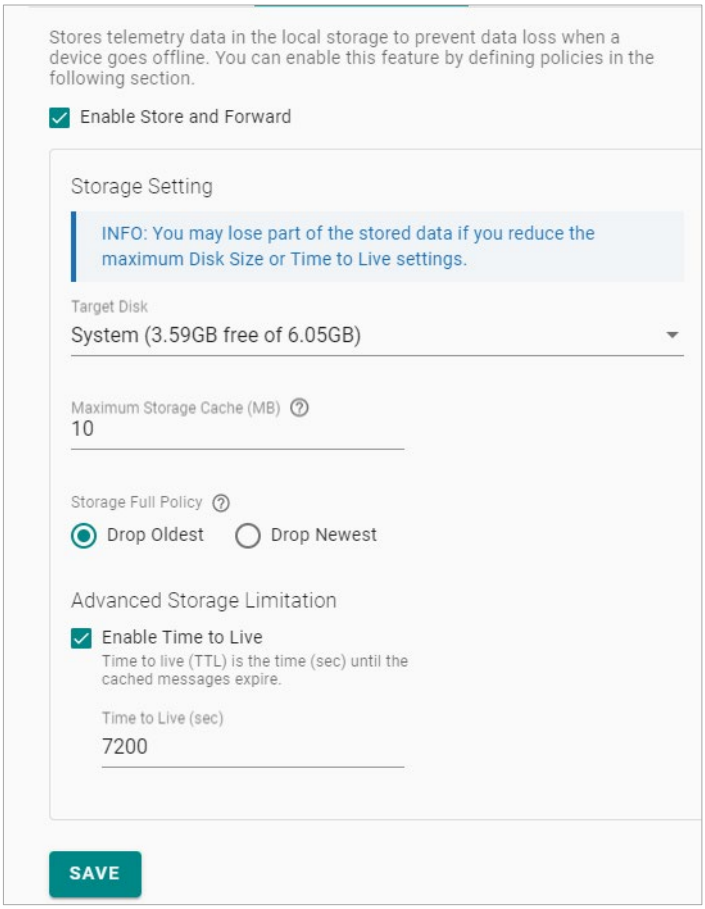
8. Click **SAVE.**

NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.

Store and Forward

D2C messages can be cached in a specified location and sent to the cloud later. This feature helps you keep the acquired data temporarily in a queue when the network between your IIoT Gateway and the cloud is disconnected. It will transmit the data to its destination once the network reconnects. To enable the function, click **Store and Forward** and select **Enable Store and Forward**. Select a target disk and a maximum storage cache, a retention policy, and a TTL (Time to Live) value for the messages.



NOTE

If you want to use the direct method to write tags from the cloud, refer to https://tpe-tiger.github.io/AIG101/V1.1.0/taghub/#

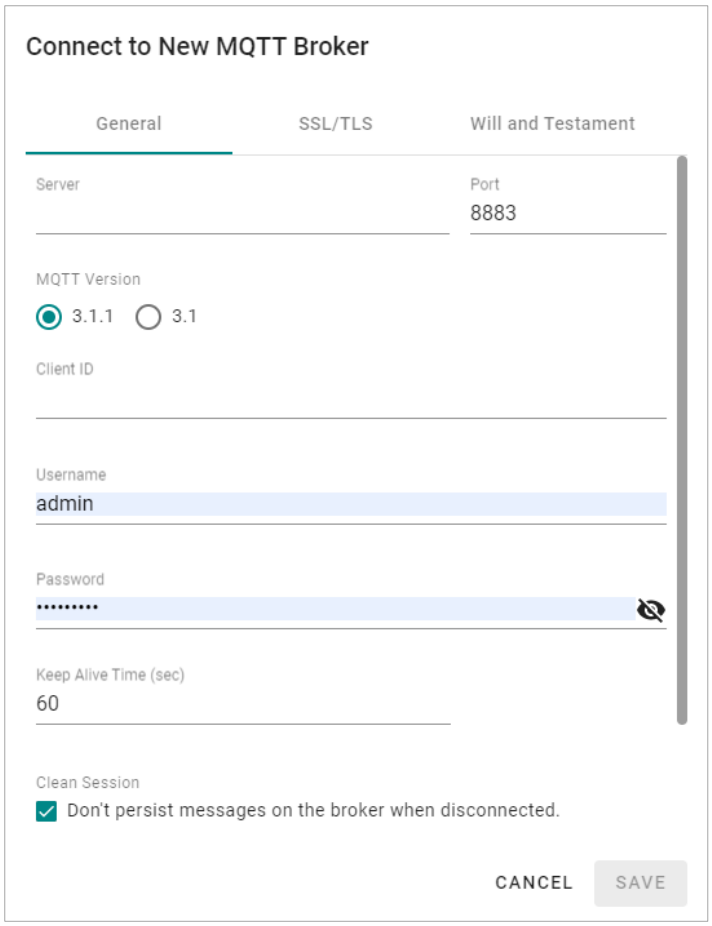
Generic MQTT Client

Go to **MQTT Client**, and you can add multiple connections to MQTT Broker.

> **NOTE**
>
> You must create a connection first and then select D2C telemetry messages to an MQTT broker.

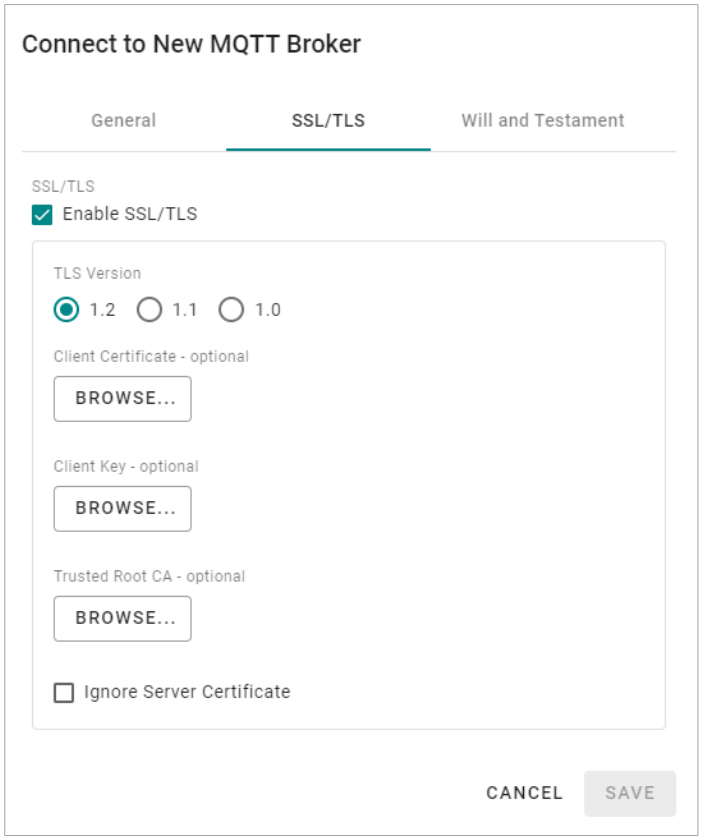
To create an MQTT Client, follow the steps below:

1. Click **ADD CONNECTION**.
2. Specify a **Server** (default port: 8883).



3. Select an **MQTT Version**.
4. (Optional) If the broker requires, enter **Client ID**, **Username**, and **Password**.
5. (Optional) Enable persistent session.
6. Select a type of **QoS** and **retain function on/off**.

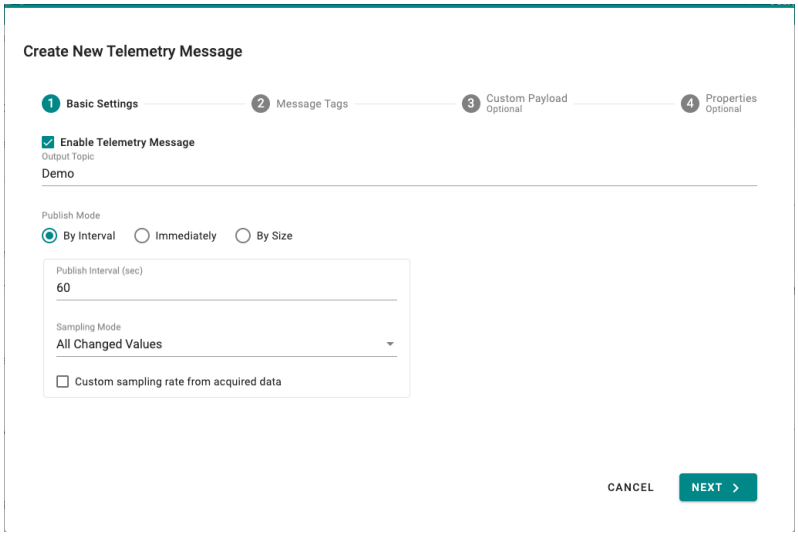
7. (Optional) Enable SSL/TLS, and upload Client Certificate, Client Key, Trusted Root CA.



8. (Optional) Enable Will flag.
9. (Optional) Select type of QoS and retain function for Will flag.

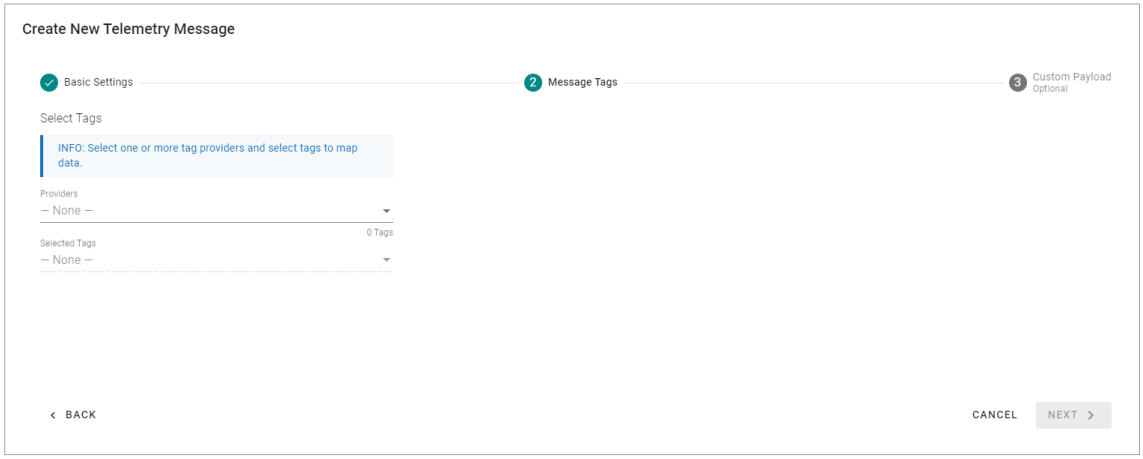
Once an MQTT Broker has been created, create a new telemetry message by following the steps below:

1. Click **+ MESSAGE**.
2. Specify an **output topic.**

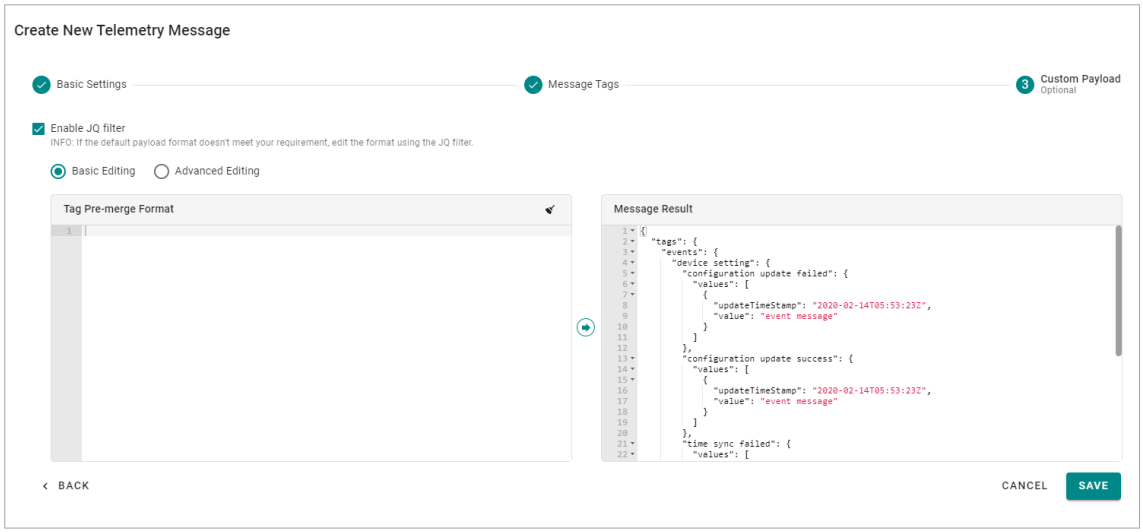


3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.

6. **Select tags** from providers (e.g., Modbus Master).



7. (Optional) Enable custom payload by using the jq filter.



8. Click **SAVE**.

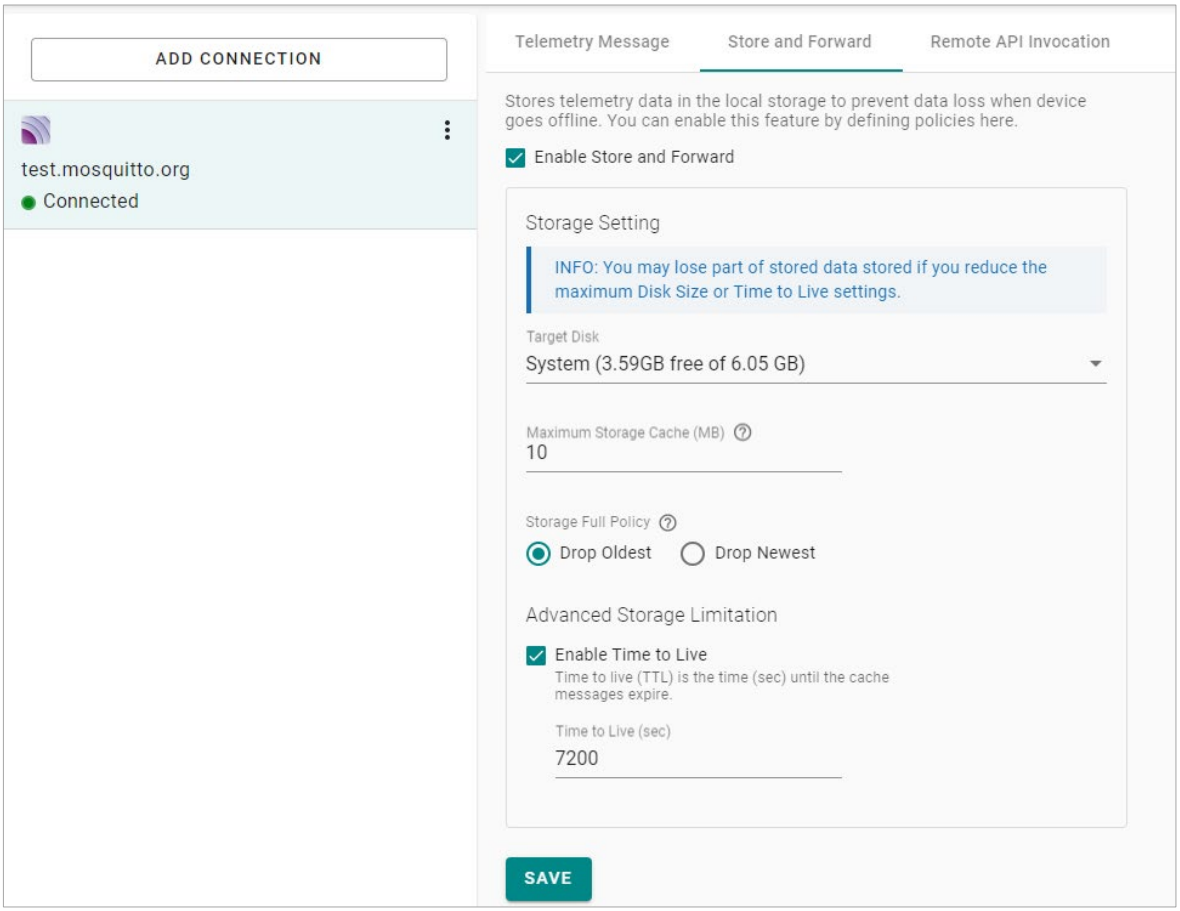
The device-to-cloud (D2C) message policy allows you to transform the default payload to your desired payload schema via the jq filter. For additional information, refer to: https://stedolan.github.io/jq/manual/.

NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.

Store and Forward

D2C messages can be cached in a specified location and sent to the cloud later. This feature helps you keep the acquired data temporarily in a queue when the network between your IIoT Gateway and the cloud is disconnected. It will transmit the data to its destination once the network reconnects. To enable the function, click **Store and Forward** and select **Enable Store and Forward**. Select a target disk and a maximum storage cache, a retention policy, and a TTL (Time to Live) value for the messages.

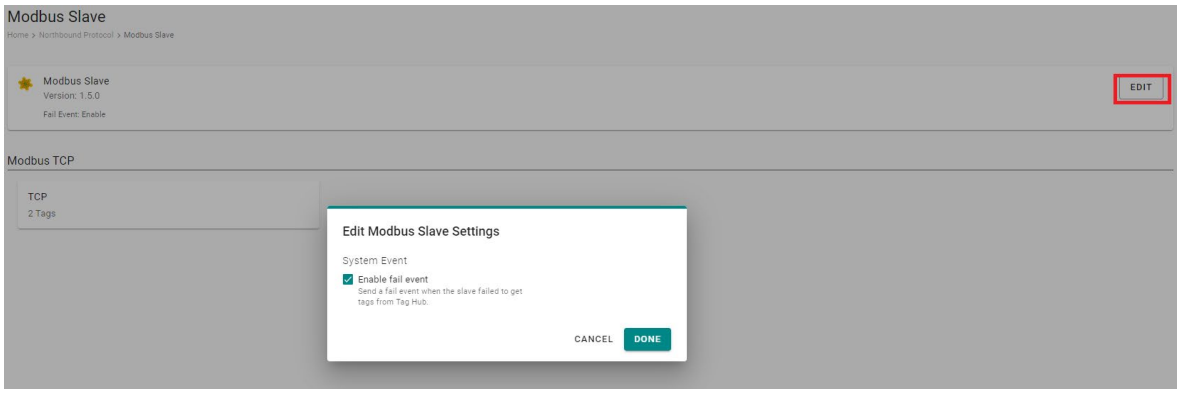


NOTE

If you want to use the direct method to write tags from the cloud, refer to https://tpe-tiger.github.io/AIG101/V1.1.0/taghub/#

Modbus TCP Slave

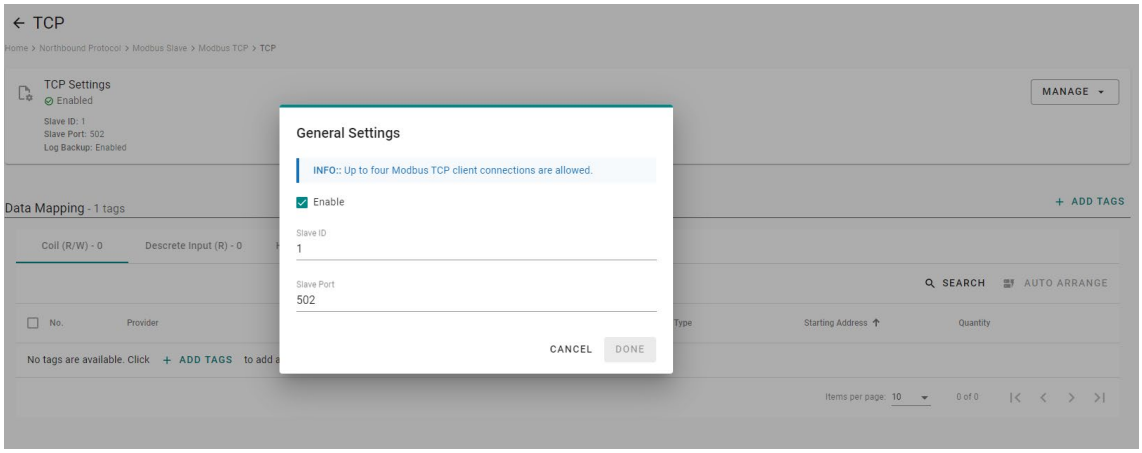
Go to **Modbus Slave** and enable Modbus TCP server to communicate with SCADA as a Modbus TCP client. Click **EDIT** for Modbus Slave advanced settings. If you want to create an event under the event log for when the Modbus TCP connection might get disconnected, you can enable the fail event function.



To create a Modbus TCP server (slave), following the steps below:

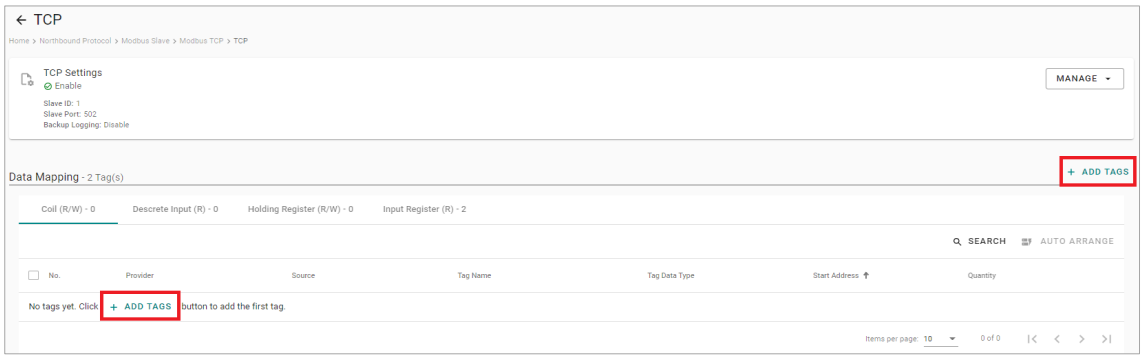
1. Click **TCP** under Modbus TCP.

2. Click **MANAGE > General Settings.**



Check **Enable this slave**, input **Slave ID** and **Slave Port**, then click **DONE.**

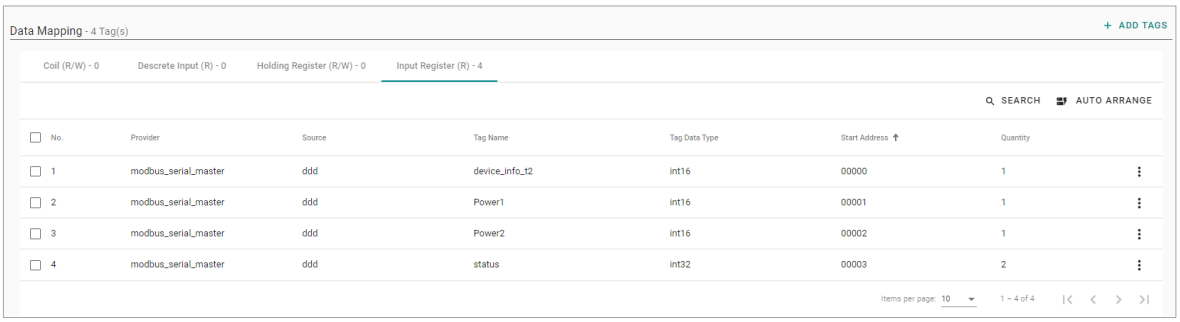
3. Click **+ADD TAGS** to select tags (e.g., Modbus Master).



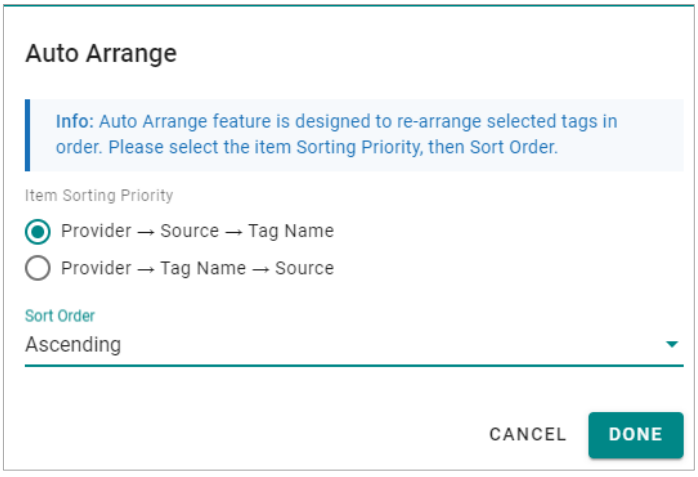
4. Click **DONE** to finish settings.

Under Data Mapping, you can view all the selected tags, which will be divided into Coil, Discrete Input, Holding Register, and Input Register. The rule is based on the tag's attribute stored in the tab hub. For example, if the tag type is Boolean and Tag Access permissions are Read, the tag will be mapped to Discrete Input in Modbus TCP server (slave).

	Tag Type	**Tag Access Permissions**
Coil	Boolean	Read/Write
Discrete Input	Boolean	Read
Holding Register	Non-boolean	Read/Write
Input Register	Non-boolean	Read



If you want to rearrange the Modbus table, click **AUTO ARRANGE**. You can select different sorting priorities and sort order types.

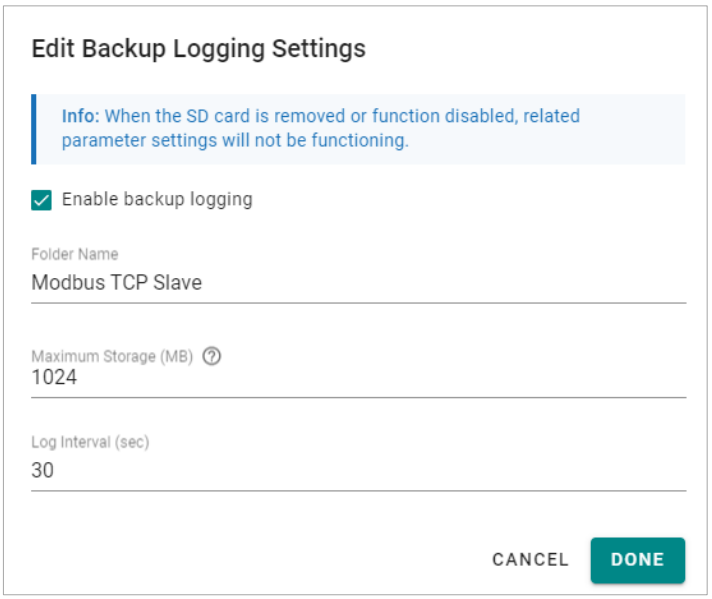


Backup Logging

If you want to enable the data logger function, go to **MANAGE > Backup Logging > Edit Settings** to enable the feature. The data logs will be stored in the SD card, meaning you have to ensure the SD card has been installed before enabling this function. (Note: the SD card capacity should be over 1 GB at least.)

The configuration steps:

1. **Enable** backup logging.
2. Specify **folder name, maximum storage, and log interval**.
3. Click **DONE.**



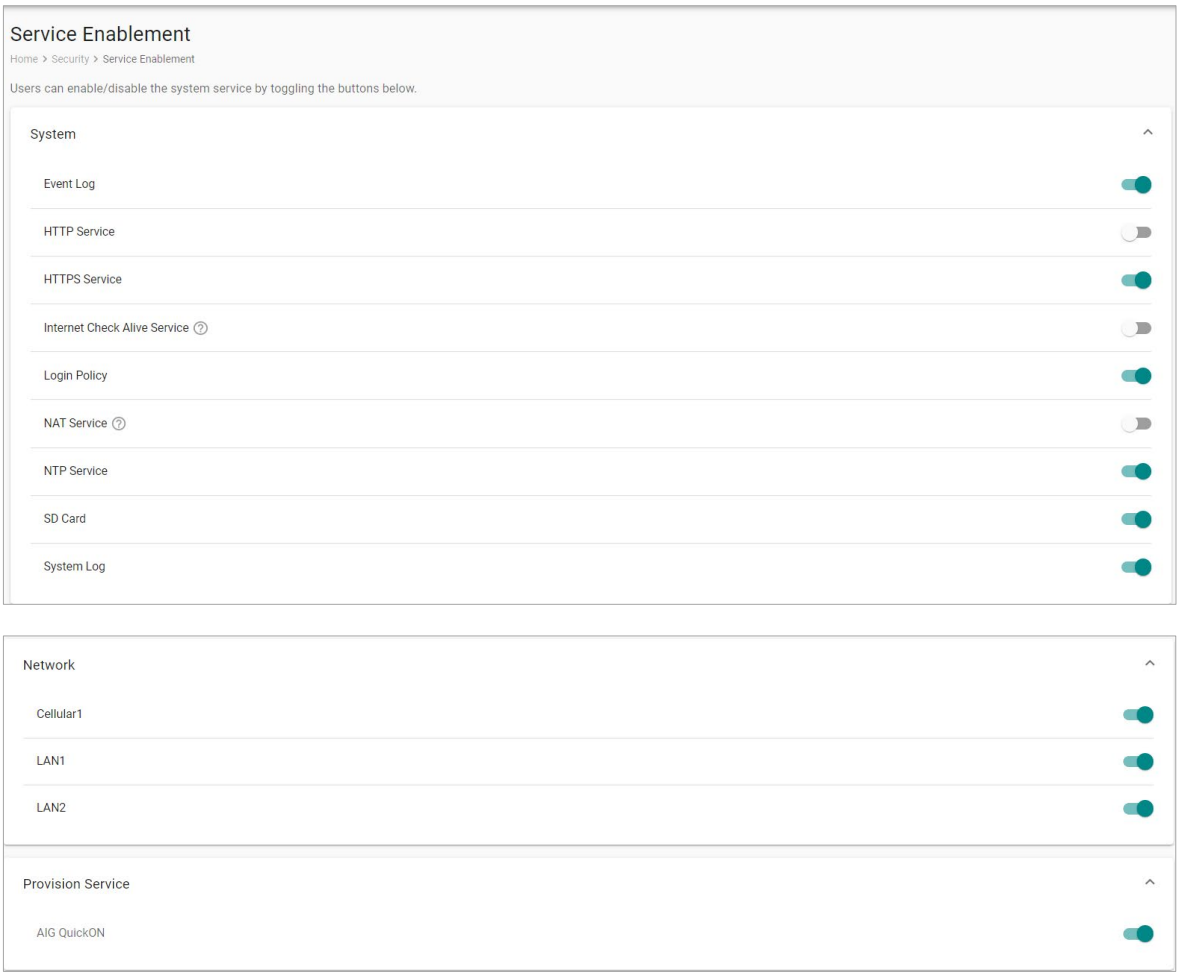
NOTE

When you replace the SD card, reboot your device to make sure the function is working properly.

Security

Service Enablement

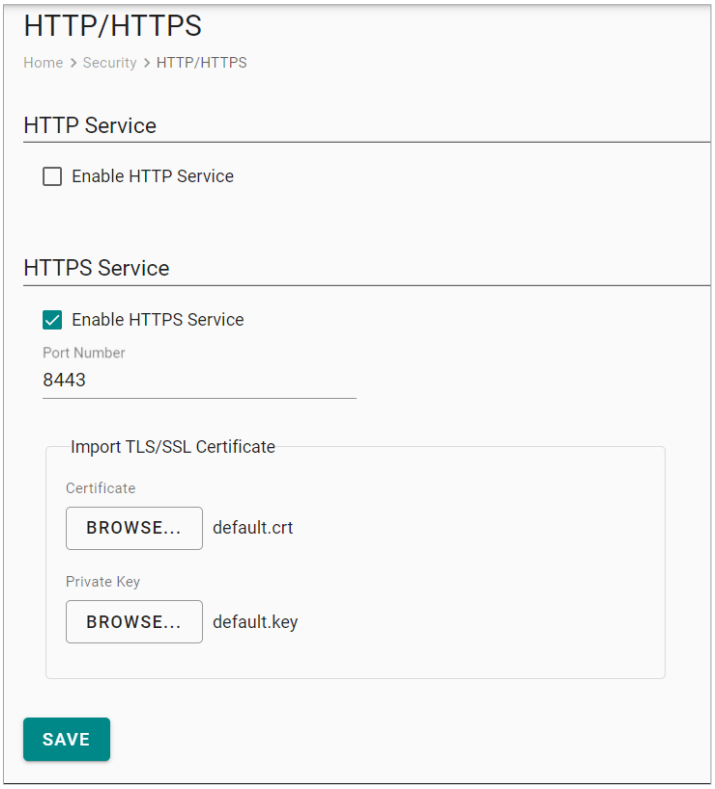
For security reasons, disable all unused services. Go to **Security > Service Enablement** to disable or enable the system service by just toggling the buttons.



HTTP/HTTPS

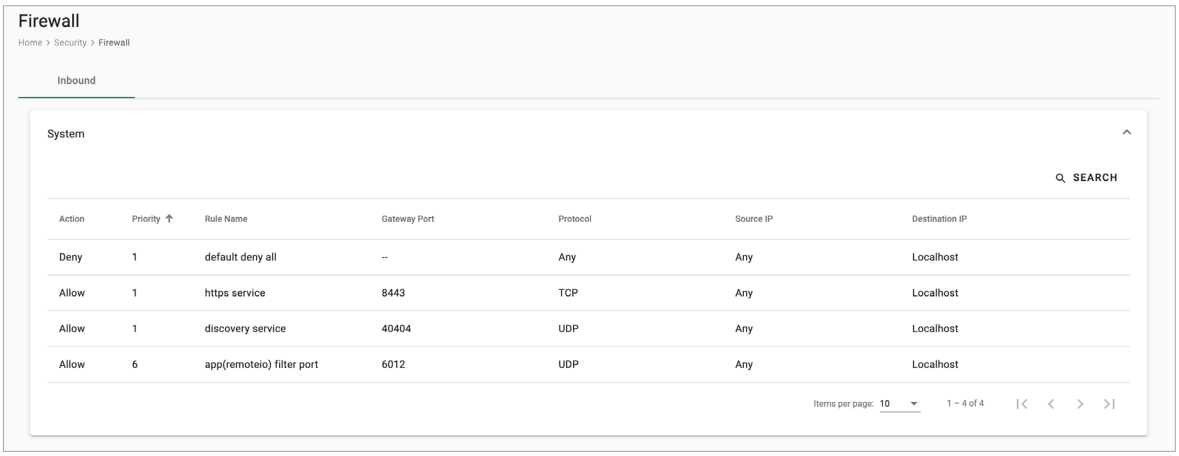
To ensure secure access to the web console of the device, we strongly recommend you **disable HTTP** and **enable HTTPS**. To do this, go to **Security > HTTP/HTTPS.**

To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority. If there are no imported certificates, the AIG Series can generate the "AIG Series Root CA for HTTPS" certificate instead.



Firewall

If we want to see the ports, protocols, and services that are used to communicate between the AIG Series and other devices, go to **Security > Firewall** to view all the information.

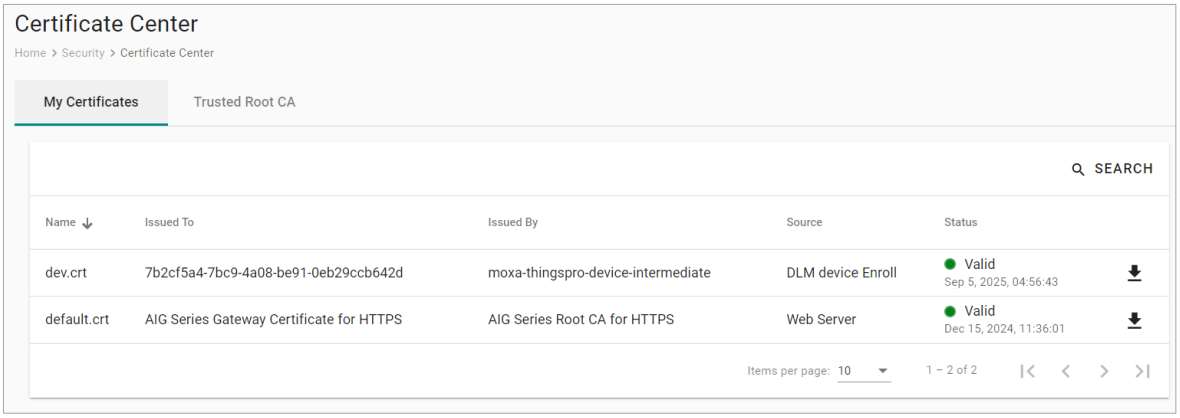


Certificate Center

If we want to check what certificates have been used on the devices, go to **Security > Certificate Center** to view all of them. On this page, you can search, view the status, and download the certificate for backup purpose.

rootCA.cer is used to sign the HTTP SSL X.509 certificate, default.crt. You can download this root CA and import it to your client devices to enable trust for the HTTPS connection between clients and the AIG. To import to Google Chrome, you can refer to the below link:

https://docs.moxa.online/tpe/users-manual/security/certificate_center/#import-rootcacer-to-google-chrome



OpenVPN Client

OpenVPN allows you to create secure connections over the internet. It provides encryption and authentication to ensure confidentiality and integrity of your data. OpenVPN uses a client-server architecture where the server acts as the VPN endpoint and the client connects to the server to establish a secure connection.

To enable the function, go to **Security > OpenVPN Client** and do the following:

1. Download the OpenVPN profile template.
2. Revise the profile by inputting the necessary information provided by your VPN service provider.

   This information includes:

   a. Remote server IP: This is the address of the VPN server you want to connect to.

   b. Port number: The port through which the VPN connection will be established. The default is usually 1194.

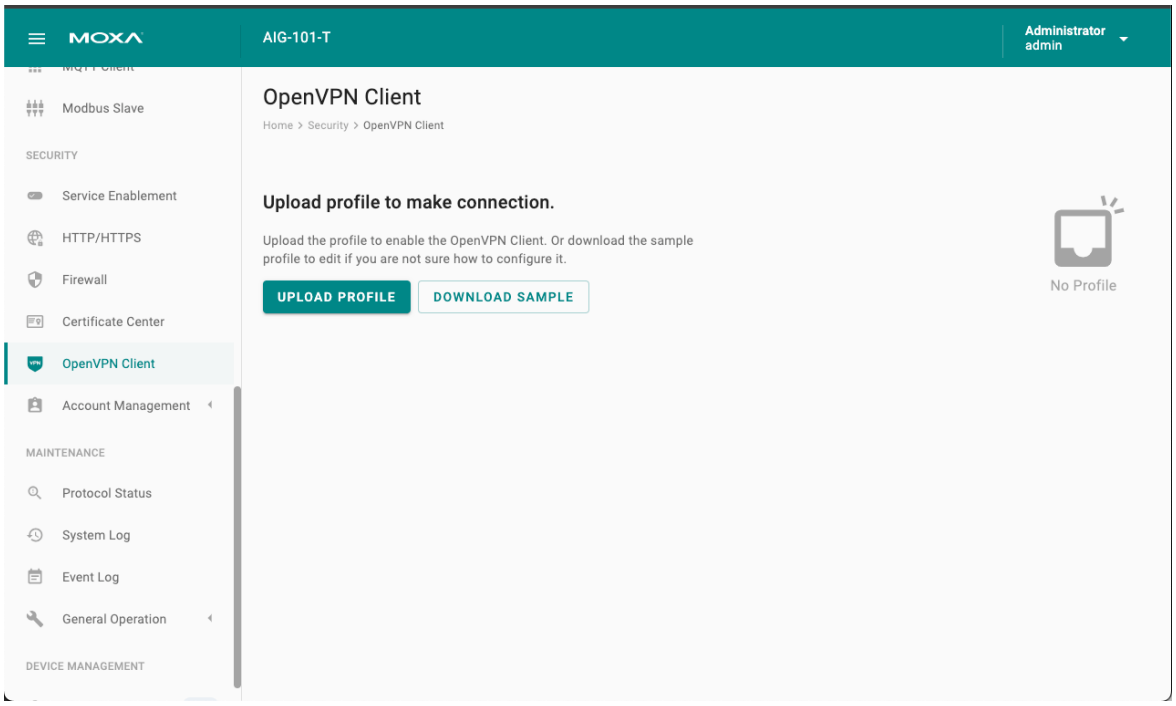
   c. Protocol: The protocol to be used for the VPN connection, such as UDP or TCP.

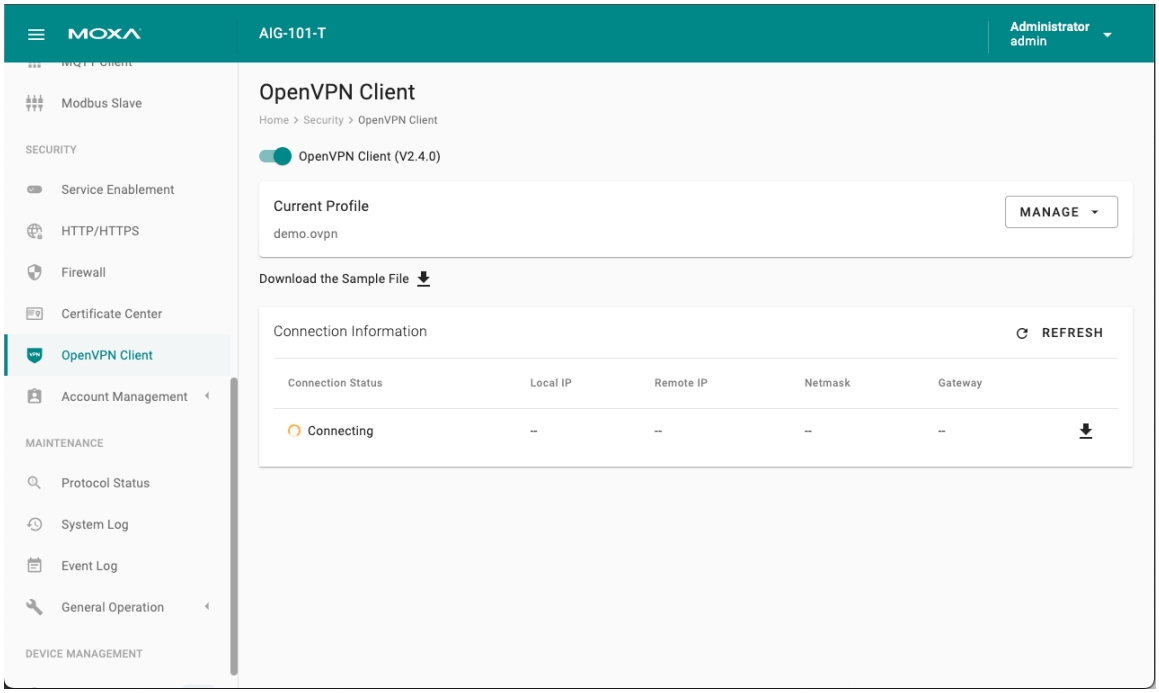
   d. Authentication method: The method used to authenticate your connection.

   e. Encryption settings: The encryption algorithm to be used for securing the VPN connection.
2. Import the OpenVPN profile.

   You should see it listed in the OpenVPN client.
3. Click the button to enable OpenVPN client to connect.

If the connection is successful, you will be connected to the VPN network, and your internet traffic will be encrypted and routed through the VPN server.


MOXA
AIG-101-T
Administrator
admin
Modbus Slave
SECURITY
Service Enablement
HTTP/HTTPS
Firewall
Certificate Center
OpenVPN Client
Account Management
MAINTENANCE
Protocol Status
System Log
Event Log
General Operation
DEVICE MANAGEMENT
OpenVPN Client
Home > Security > OpenVPN Client
Upload profile to make connection.
Upload the profile to enable the OpenVPN Client. Or download the sample profile to edit if you are not sure how to configure it.
UPLOAD PROFILE
DOWNLOAD SAMPLE
No Profile

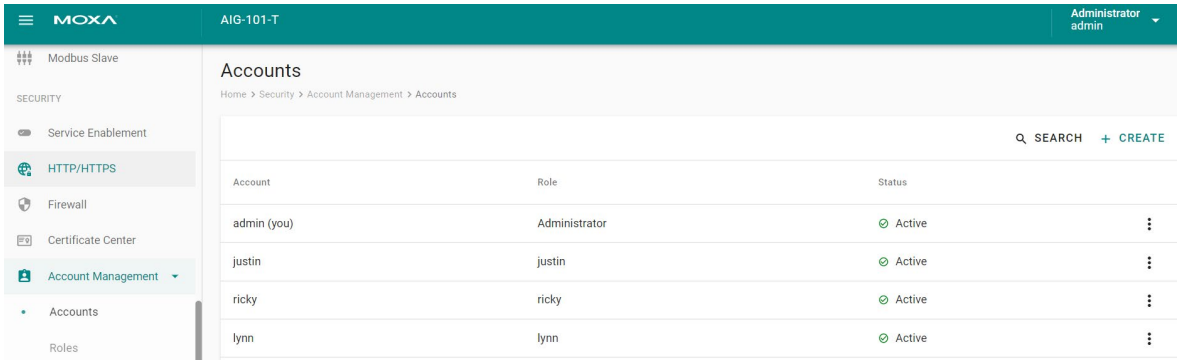

MOXA
AIG-101-T
Administrator
admin
Modbus Slave
SECURITY
Service Enablement
HTTP/HTTPS
Firewall
Certificate Center
OpenVPN Client
Account Management
MAINTENANCE
Protocol Status
System Log
Event Log
General Operation
DEVICE MANAGEMENT
OpenVPN Client
Home > Security > OpenVPN Client
OpenVPN Client (V2.4.0)
Current Profile
demo.ovpn
MANAGE
Download the Sample File
Connection Information
REFRESH
Connection Status
Local IP
Remote IP
Netmask
Gateway
Connecting
--
--
--
--

Account Management

You can maintain user accounts and assign a role with specific permissions to each account. These functions allow you to track and control who accesses this device.

Accounts

You can **View**, **Create**, **Edit**, **Deactivate**, and **Delete** user accounts. In the main menu, go to **Security > Account Management > Accounts** to manage user accounts.

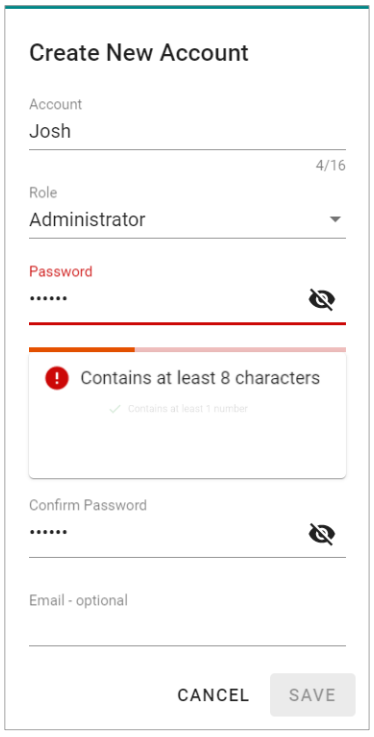
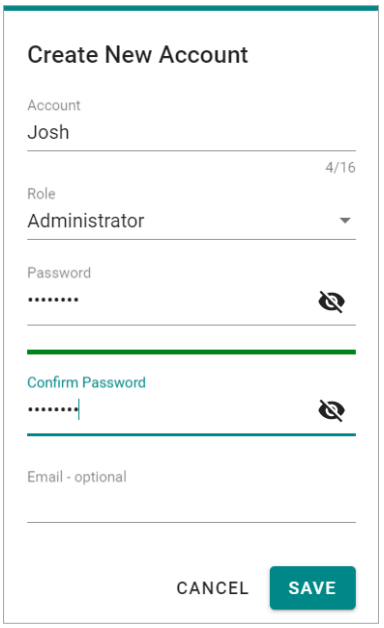


Creating a New User Account

Click on **+ CREATE** to create a new user account. In the dialogue box that is displayed, fill up the fields and click **SAVE**.

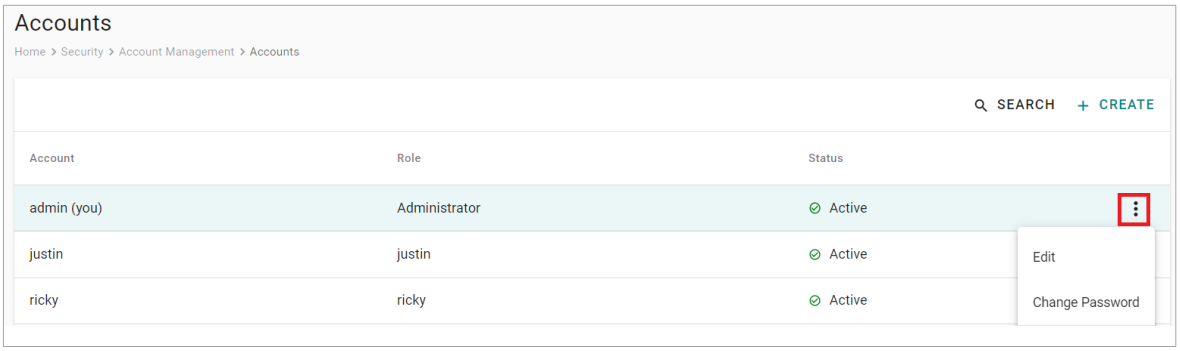
NOTE

We recommend that you specify a strong password that is at least eight characters long, consisting of at least one number and at least one special character.

Password Policy	Valid Password
	

Managing Existing User Accounts

To manage an account, click on the pop-up menu icon for the account.



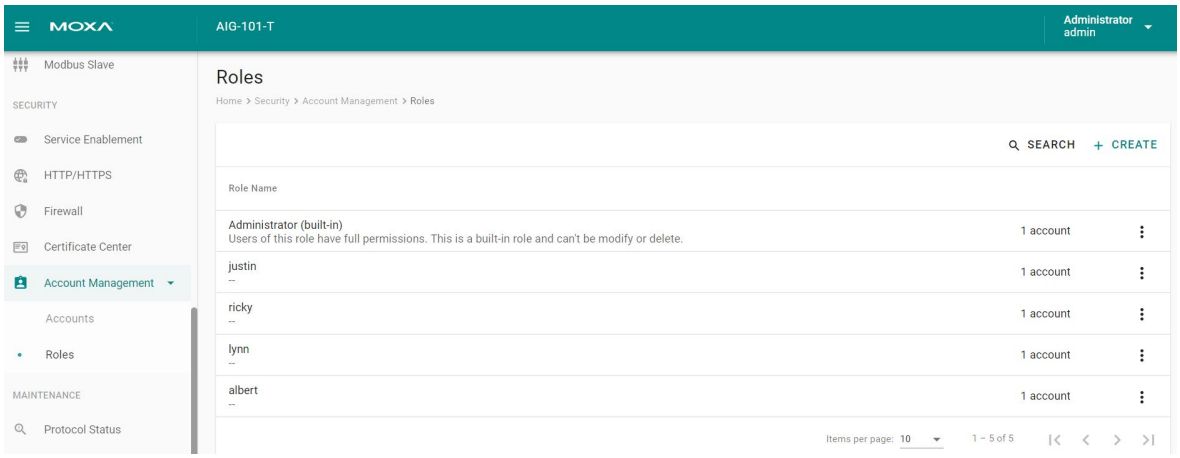
Function	Description
Edit	Change the role, email, or password of an existing account.
Deactivate	Does not allow the user to log in to this device.
Delete	Delete the user account. **NOTE:** This operation is irreversible.

NOTE

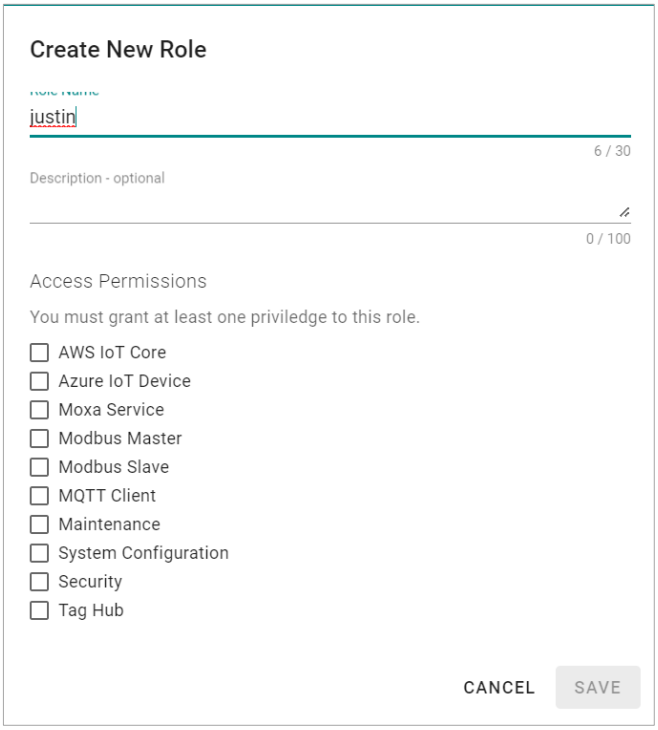
You cannot **Deactivate** or **Delete** the last remaining account with an Administrator role. This is to prevent an unauthorized account from fully managing this system. When the system detects only one active account when the Administrator role is selected, all items in the pop-up menu will be grayed out.

User Roles

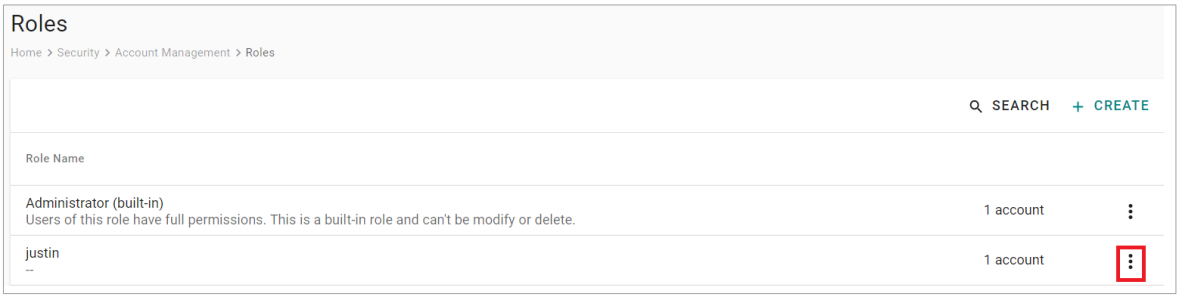
You can **View**, **Create**, **Edit**, and **Delete** user roles in ThingsPro Edge. In the main menu, go to **Security > User Management > Roles** to manage the user roles.



Click **+ CREATE** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions. When you are done, click on the button **"SAVE"** to create the role in the system.



You can **edit** the settings or **delete** an existing role by clicking on the pop-up menu icon next to the role.



Maintenance

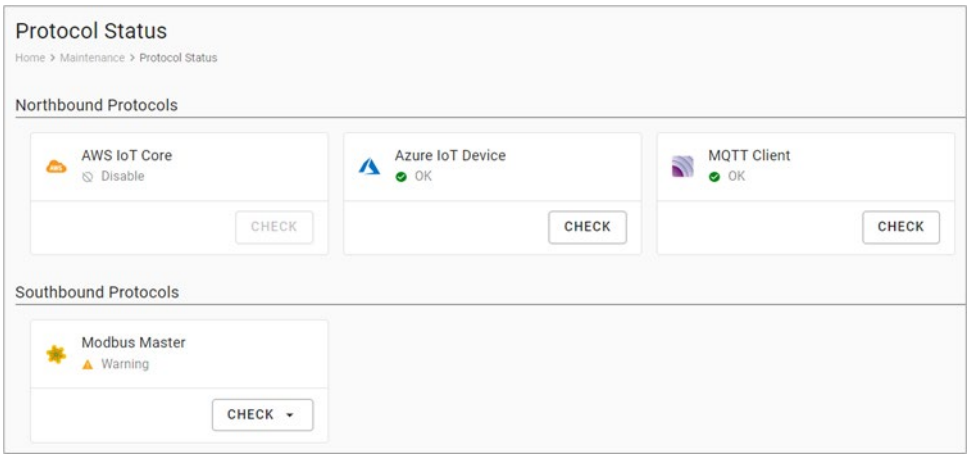
Protocol Status

In case of A communication issue, go to **Maintenance > Protocol Status Check**. The device provides comprehensive troubleshooting tools to help you identify the issue easily.

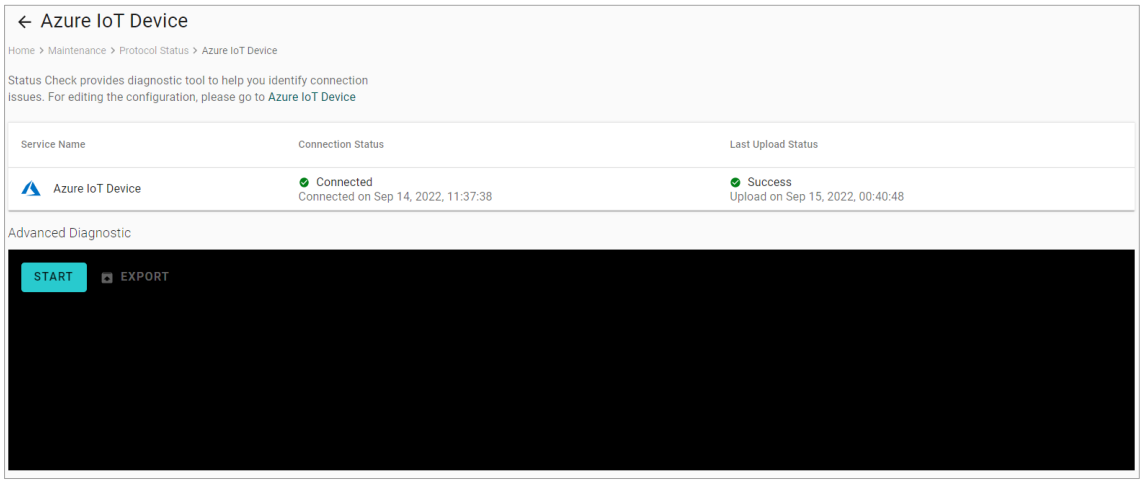
When you access the page, you can see an overview of the status for Northbound Protocols and Southbound Protocols.

For AWS, Azure, MQTT Client troubleshooting, do the following:

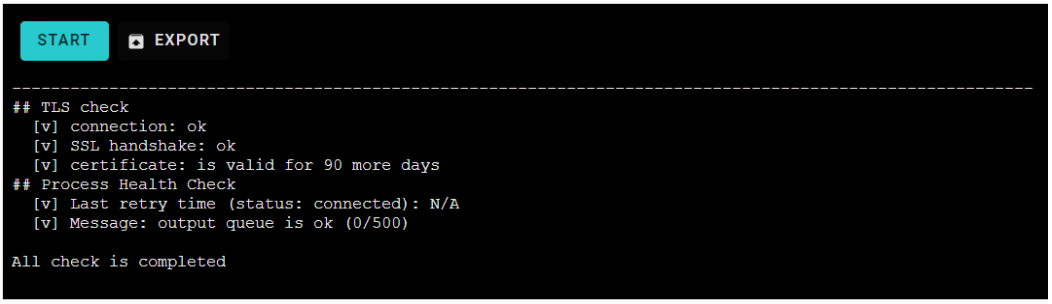
1. Click **CHECK**.



2. Click **START.**



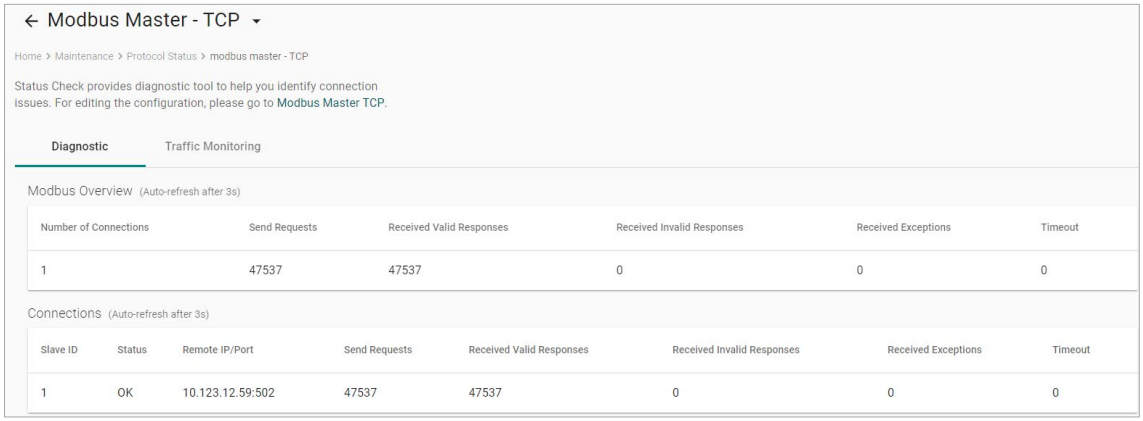
3. View the logs to identify the issue.



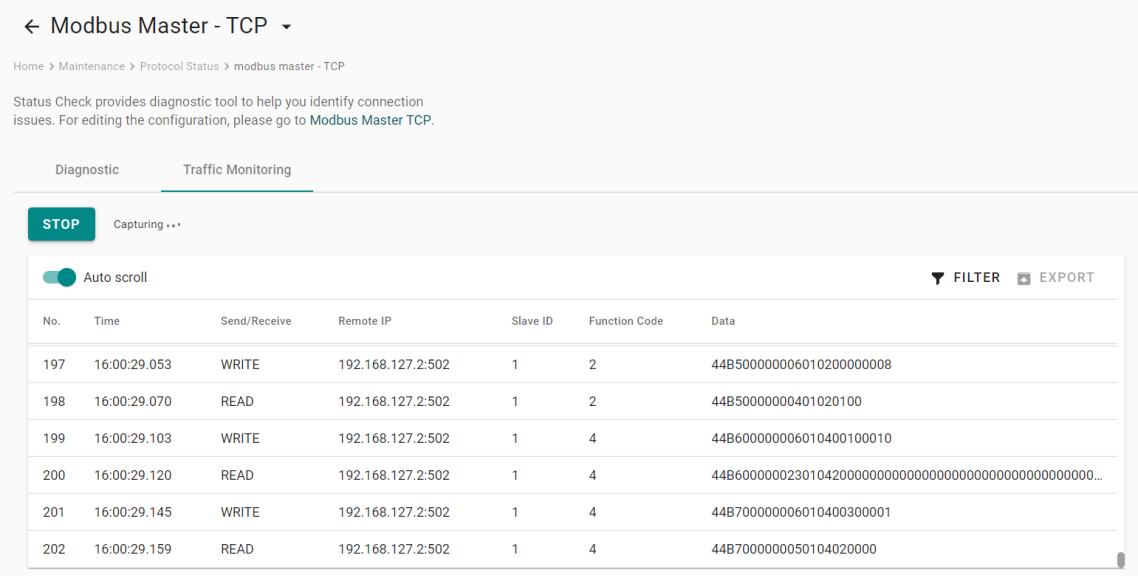
4. (Optional) **Export** the logs.

The steps below take Modbus TCP as an example:

1. Click **CHECK**.
2. Choose **TCP** or **COMx**.
3. View the diagnostic information.



4. Click the Traffic Monitoring tab to capture the traffic logs.

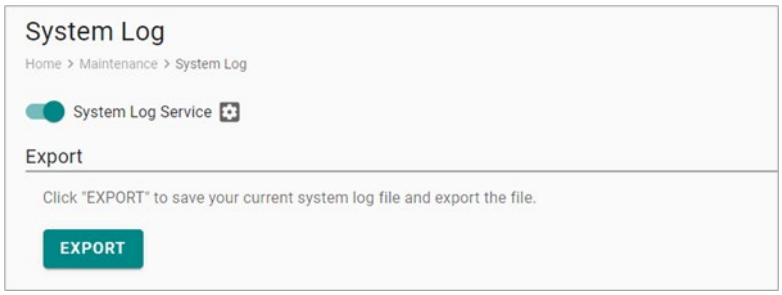


5. (Optional) **Export** the traffic logs to send to experienced engineer for further analysis.

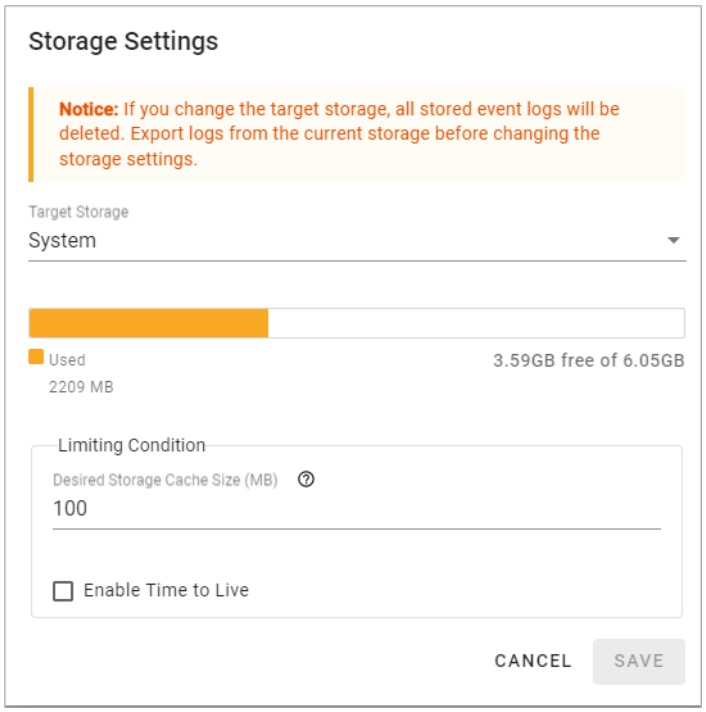
System Log

The main purpose of system log is to help Moxa engineers with troubleshooting. When you encounter an issue that you are not able to solve by yourself, export the log file and send it to Moxa TS for analysis.

Go to **System Log** to export the system log file and specify the location to save the system logs.



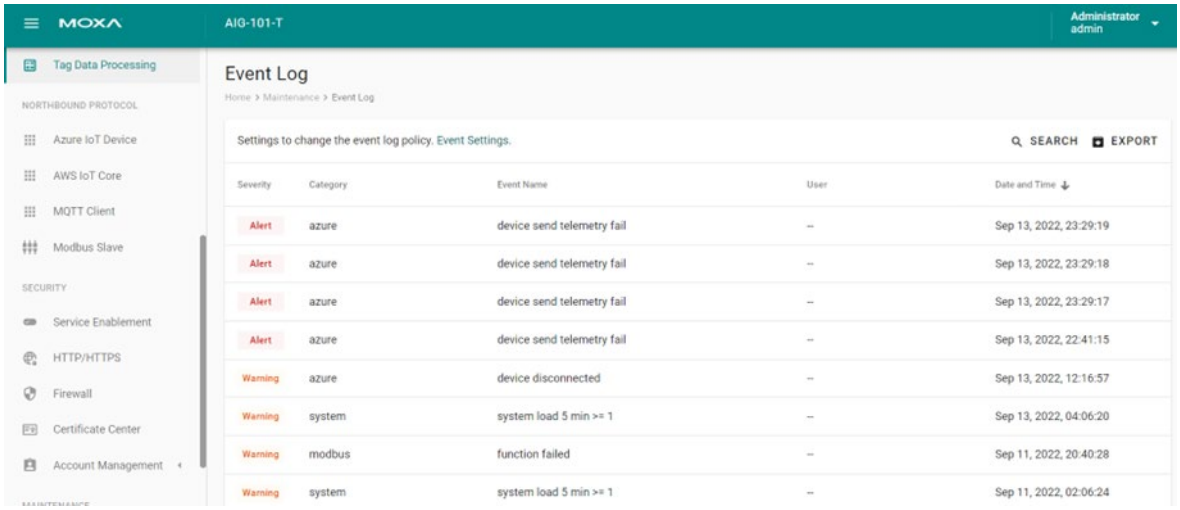
Click  to specify the location to store the event logs. To optimize the use of storage space on your AIG, you can check the Enable **Time to Live** option and specify the maximum storage space for the system logs. Click **SAVE** to confirm your settings.



Event Log

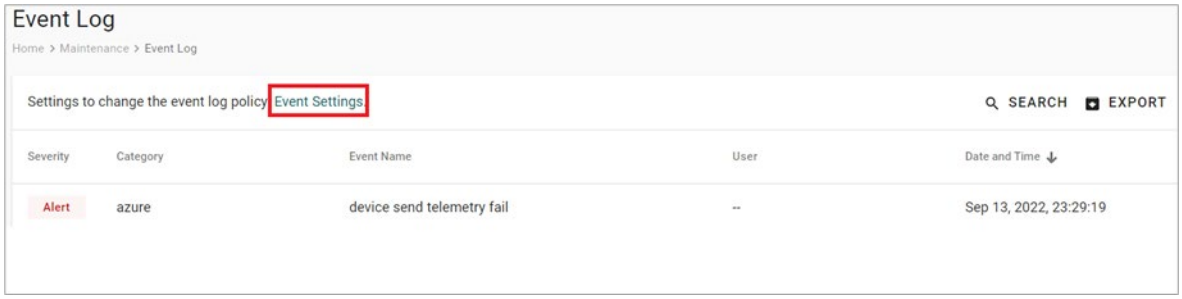
When you face issues, you can check the event logs for recorded events that help you to narrow down the problems. If there are a large number of event logs, you can export the log to read easily.

Go to **Event Logs** to view all event logs categorized by **Severity**, **Event Name**, and **Category**. You can use the **SEARCH** function to filter the Event logs to find a specific event. The Event Logs can be exported as a *.zip file and downloaded on to your computer.

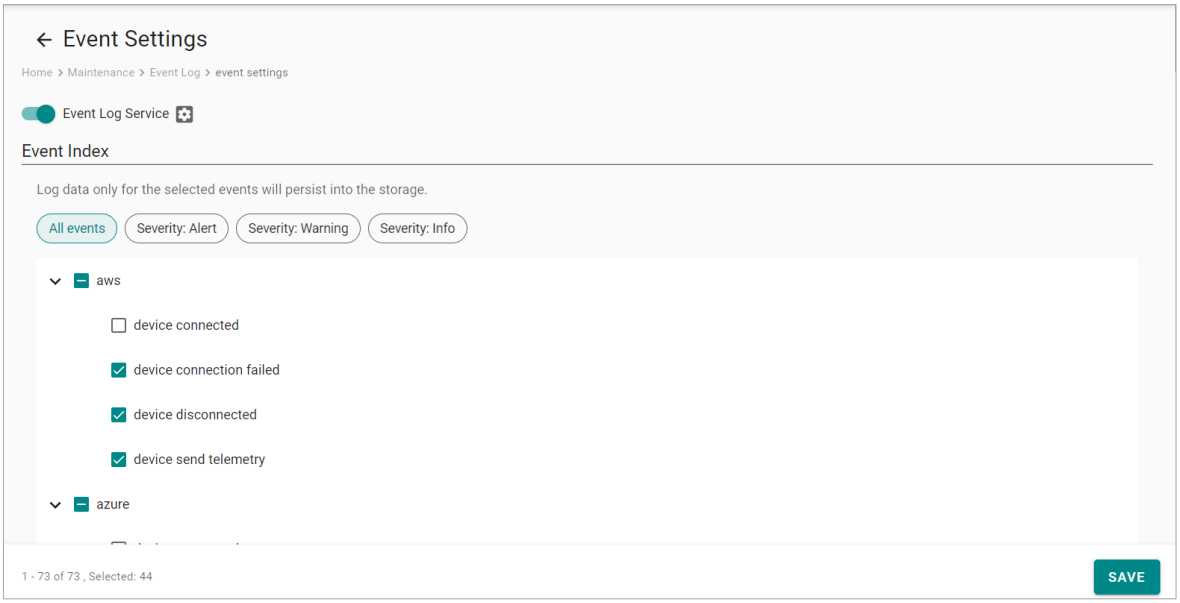


Configuring Event Log Settings

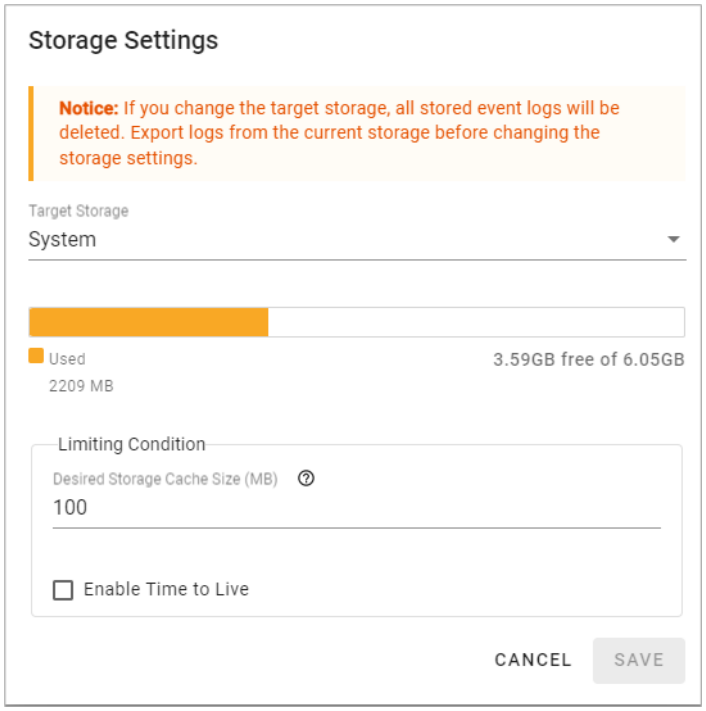
Choose the type of events to be stored, specify where to keep the logs, and the maximum storage size to use. Click the **Event Settings** to access these settings.



You can select the type of events to be stored by clicking on the different levels of Severity: **Alert**, **Warning**, or **Info**. You can also select the individual event that you want to keep.

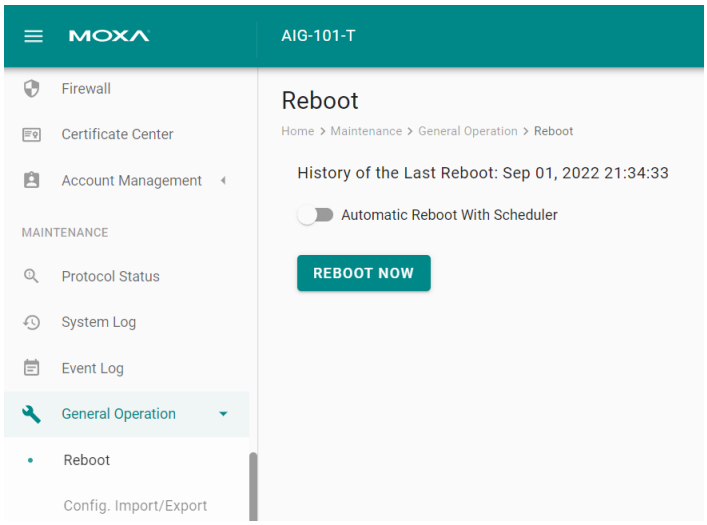


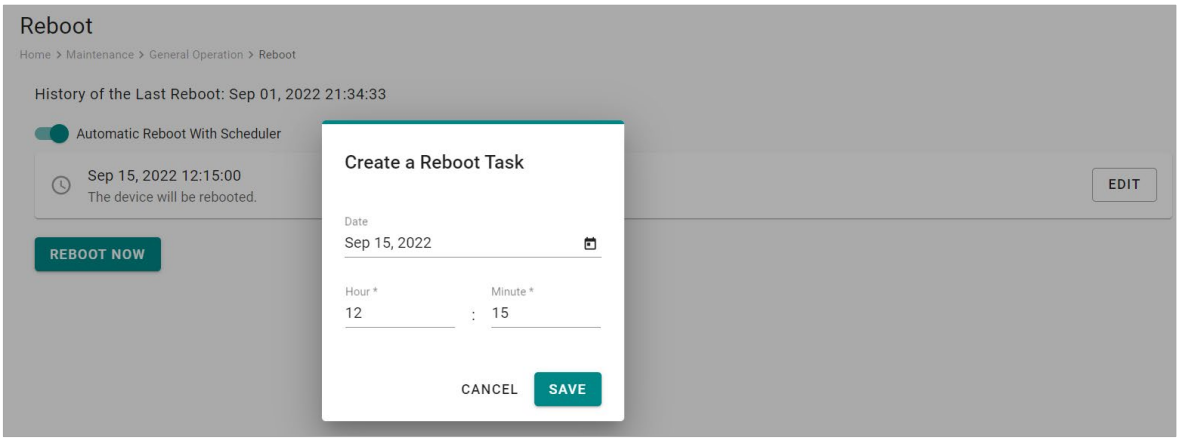
Click  to specify the location to store the event logs. To optimize the use of storage space on your AIG, you can check the Enable **Time to Live** option and specify the maximum storage space for the system logs. Click **SAVE** to confirm your settings.



General Operation—Reboot

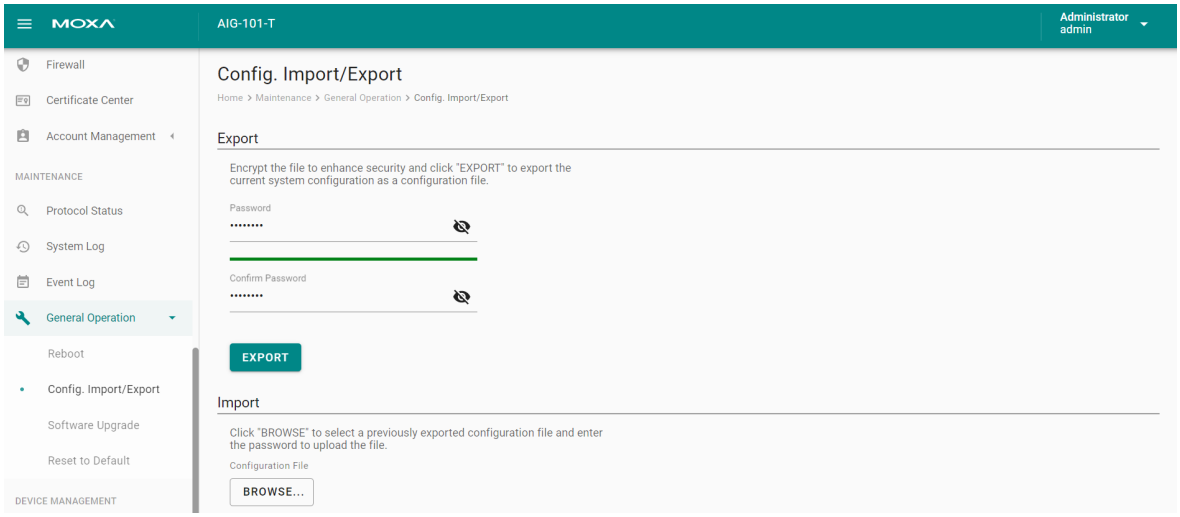
If you want to reboot the device, go to **General Operation > Reboot** and click **REBOOT NOW**. If you want to arrange a specific time to reboot, you can enable **Automatic Reboot With Scheduler** and enter the date, hour, and minutes.





General Operation - Config. Import/Export

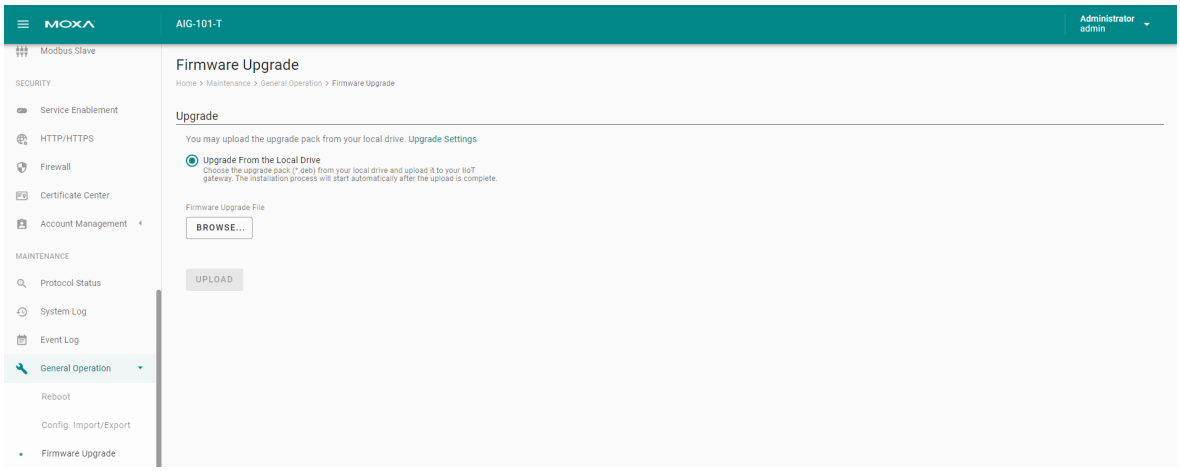
Go to **General Operation > Config. Import/Export,** where you can import or export the gateway configuration file with a given password. The exported configuration file will be compressed to the **tar.gz** format and downloaded on your computer.



General Operation—Firmware Upgrade

Go to **General Operation > Firmware Upgrade** to upgrade this device with Moxa's software packages.

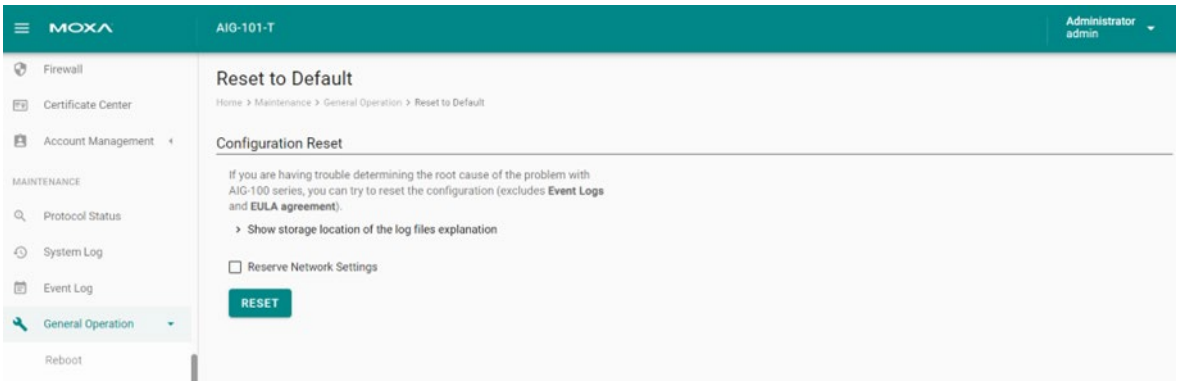
Click **BROWSER** and select the software package file in *.deb file format on your computer, then click **UPLOAD.**



General Operation—Reset to Default

If you want to clear all the settings to configuration default, there are two ways:

1. Go to **General Operation > Reset to Default** >press **RESET**. If you want to keep the network settings, enable **Reserve Network Settings** before clicking **RESET**.



2. Press and hold the Reset button on the device till the SYS LED blinks (approximately seven seconds).

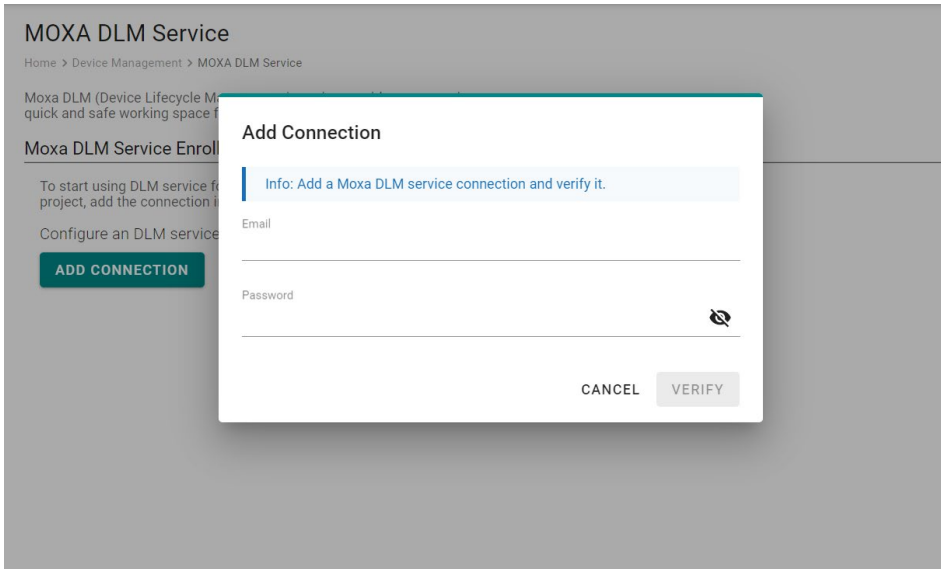
Device Management

Moxa DLM Service

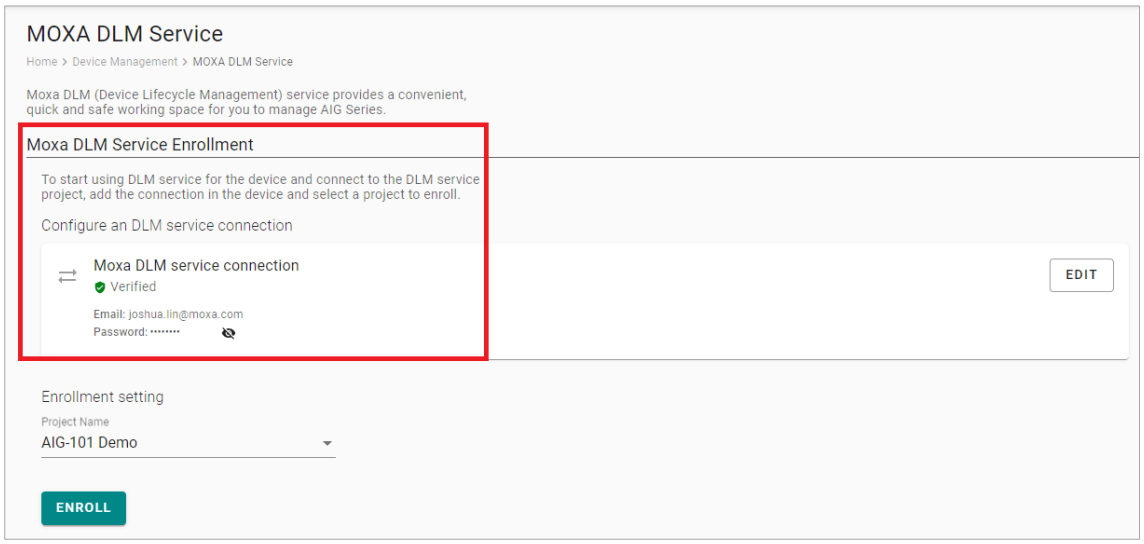
Moxa DLM (device lifecycle management) service is used for management of the AIG Series. Imagine sitting in your office and using this service to remotely manage a large number of devices distributed around the world. You can monitor the device's health status, upgrade firmware, import/export configuration, and remotely log into the device's web console. If you want to apply for this service, contact the product manager, Joshua Lin, at joshua.lin@moxa.com.

Once you get the service, go to **Moxa DLM Service** to register the product online. Follow these steps:

1. Input DLM **email** and **password**, and press **VERIFY**.



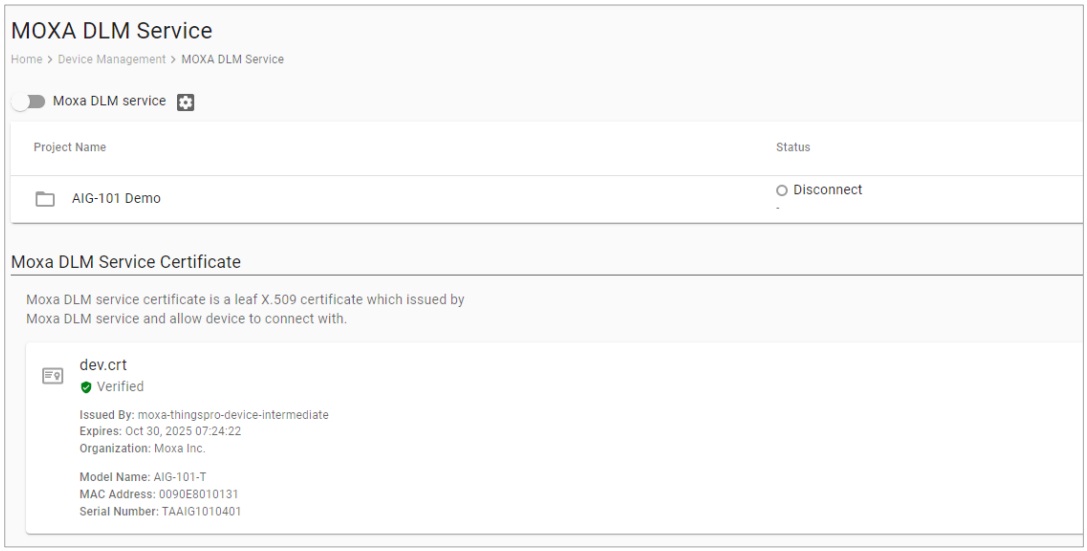
2. If the input information is correct, you will see the connection has been verified.



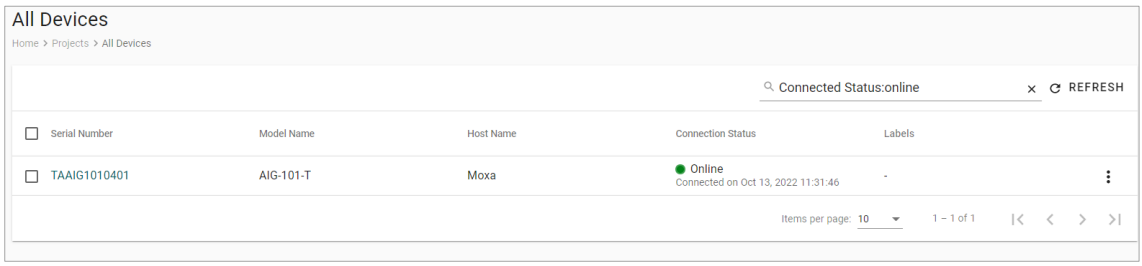
3. Choose the **Project** and Press **ENROLL** to enroll.

4. Once the enrollment is successful, you will see the following information.

> **NOTE**
>
> Ensure the Moxa DLM service is enabled at the top left corner.



5. Log in to the Moxa DLM Service to check if the AIG device is online.



Publish Mode

Publish Mode	Parameters	Value	Description
By Interval	Publish Intervals (sec)	0 - 86400	The frequency to upload the data to the cloud.
	Sampling Mode	All Values Latest Values All Changed Values Latest Changed Values	All Values: All values recorded within a specified interval will be sent to the cloud. Latest Values: Only the most recent value will be sent to the cloud. All Changed Values: All values that have changed within the configured interval will be sent to the cloud. Latest Changed Values: Only the most recent value that has changed will be sent to the cloud.
	Custom Sampling rate from acquired data (sec)	0 - 86400	The frequency to synchronize the tag value with tag hub.
Immediately	Sampling Mode	Enable/disable	Enable: Only publish the changed values to the cloud immediately. Disable: Publish all data to the cloud immediately once one of data item changes in the topic.
	Minimal Publish Interval (sec)	0 – 60	To avoid transmitting a large amount of data to the cloud in a short period, it is possible to set a time interval that ensures a delay between each data transmission.
By Size	Publish Size (bytes)	0 -262144	Once the data size reaches the specified threshold, the data will be transmitted to the cloud.
	Sampling Mode	All Values All Changed Values	All Values: All values recorded within the specified size will be sent to the cloud. All Changed Values: All values that have changed within the configured size will be sent to the cloud.
	Custom Sampling rate from acquired data (sec)	0 - 86400	The frequency to synchronize the tag value with tag hub.
	Idle Timer (sec)	0 – 86400	To avoid situations where the data takes a long time to reach the desired size, a threshold value can be set to ensure that the data is sent out as soon as it reaches the specified timer setting.