

AIG-101 Series User Manual

Version 2.0, April 2023

www.moxa.com/products

MOXA[®]

© 2023 Moxa Inc. All rights reserved.

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

© 2023 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc.
All other trademarks or registered marks in this manual belong to their respective manufacturers.

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	4
Overview	4
2. Getting Started	5
Connecting the Power	5
Connecting the Serial Devices	5
Connecting to a Network	5
Access to the Web Console	6
3. Web Console	8
Overview	8
System Overview	8
Network Overview	8
System Configuration	10
System Settings—General	10
System Settings—IP Address	11
System Settings—Cellular	12
System Settings—Serial	14
Moxa Device Extension—ioLogik	15
Moxa Device Extension—UPort	18
Southbound Protocol	20
Modbus Master	20
Tag Hub	33
Tag List	33
Tag Management	33
Tag Data Processing	35
Northbound Protocol	38
Azure IoT Device	38
AWS IoT Core	42
Generic MQTT Client	45
Modbus TCP Slave	49
Security	52
Service Enablement	52
HTTP/HTTPS	53
Firewall	53
Certificate Center	54
Account Management	54
Maintenance	57
Protocol Status	57
System Log	59
Event Log	60
General Operation—Reboot	62
General Operation - Config. Import/Export	63
General Operation—Firmware Upgrade	63
General Operation—Reset to Default	64
Device Management	64
Moxa DLM Service	64

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.

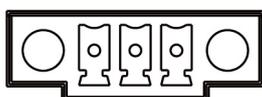
2. Getting Started

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:

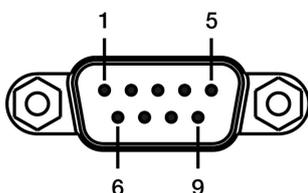


 V- V+

9-36 VDC

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:

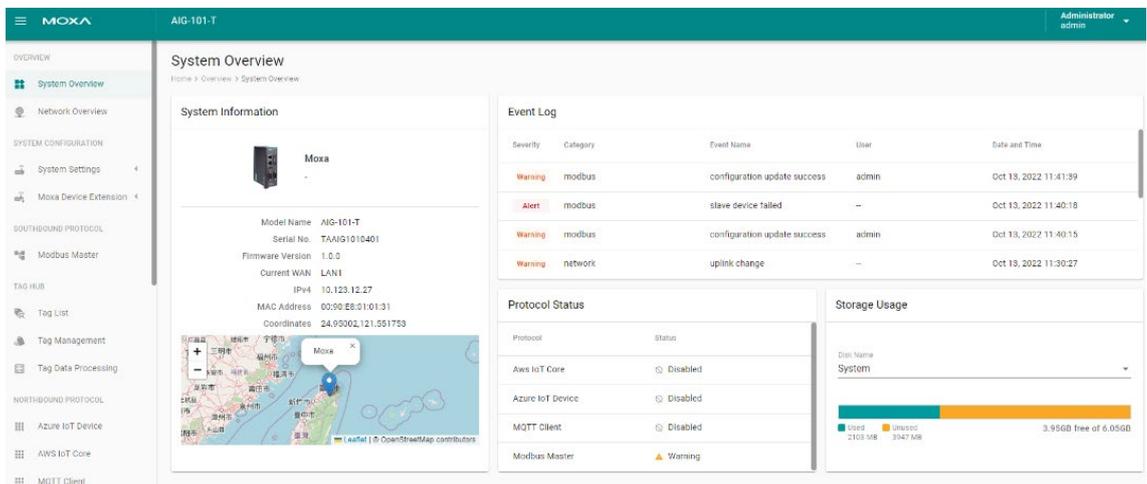
1. Ensure your host and AIG are in the same subnet (AIG default subnet mask: 255.255.255.0).
2. When you connect to LAN1, input <https://192.168.126.100:8443> in your web browser; when you connect to LAN2, input <https://192.168.127.100:8443> in your web browser.
3. Input default account and password

Default account: **admin**

Password: **admin@123**

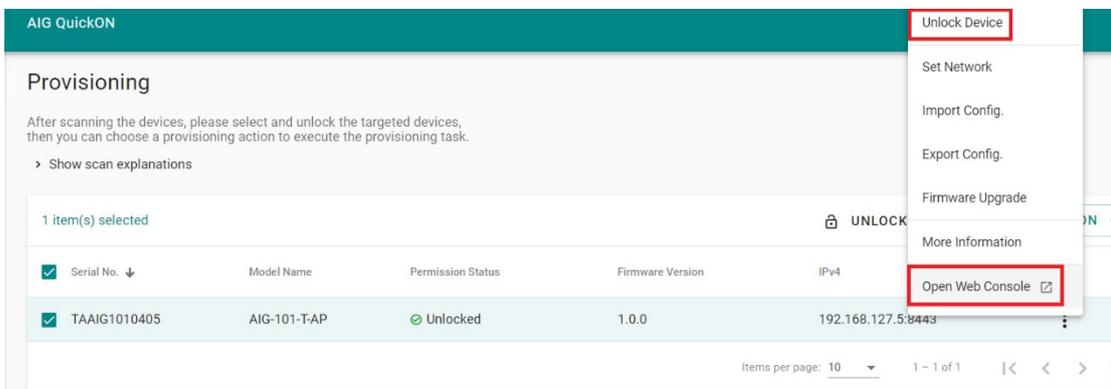
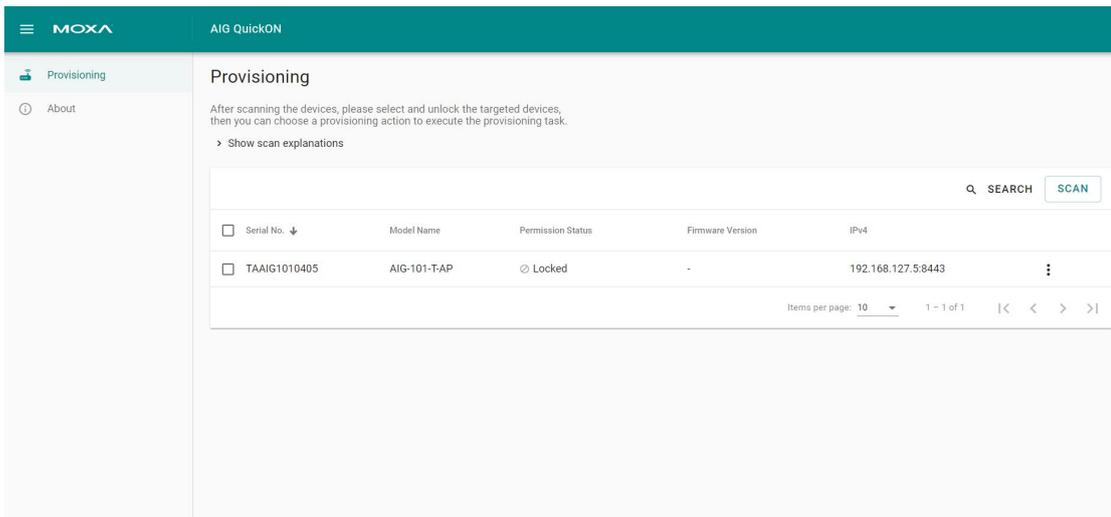


4. Login successful



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

1. Run the **AIG-QuickON-x.x.x-xxxxxxxxxxxx.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**.



3. 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.

The screenshot displays the 'System Overview' page in the Moxa web console. The left sidebar contains navigation options: OVERVIEW (System Overview, Network Overview), SYSTEM CONFIGURATION (System Settings, Moxa Device Extension), SOUTHBOUND PROTOCOL (Modbus Master), TAG HUB (Tag List, Tag Management, Tag Data Processing), NORTHBOUND PROTOCOL (Azure IoT Device, AWS IoT Core), and Administrator admin.

System Information:

- Model Name: AIG-101-T
- Serial No.: TAAIG1010401
- Firmware Version: 1.0.0
- Current WAN: LAN1
- IPv4: 10.123.12.27
- MAC Address: 00-90-E8-01-01-31
- Coordinates: 24.95002, 121.551753

Event Log:

Severity	Category	Event Name	User	Date and Time
Warning	modbus	function failed	--	Sep 11, 2022 20:40:28
Warning	system	system load 5 min >= 1	--	Sep 11, 2022 02:06:24
Warning	system	system load 5 min >= 1	--	Sep 08, 2022 19:06:29
Warning	modbus	function failed	--	Sep 08, 2022 18:31:45

Protocol Status:

Protocol	Status
Aws IoT Core	Disable
Azure IoT Device	Disable
MQTT Client	OK
Modbus Master	Warning

Storage Usage:

Disk Name	Used	Unused	Total
System	1392 MB	4658 MB	6.05GB

Network Overview

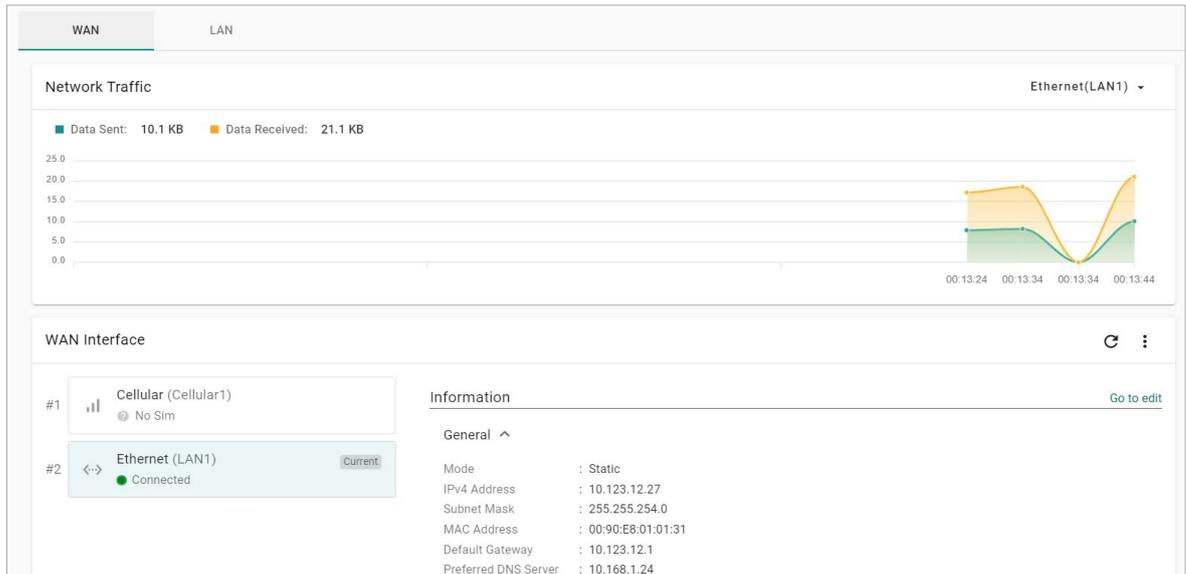
This dashboard displays information on the WAN and LAN interfaces and the network traffic passing through the interfaces.

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

The screenshot shows the 'Network Overview' page. It features a 'Network Status' section with a diagram illustrating the connection path: Moxa Device (represented by a Wi-Fi icon) is connected to the Network (represented by a network icon), which is then connected to the Internet (represented by a globe icon). A green checkmark and the text 'Connected to the Internet' are displayed below the diagram.

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

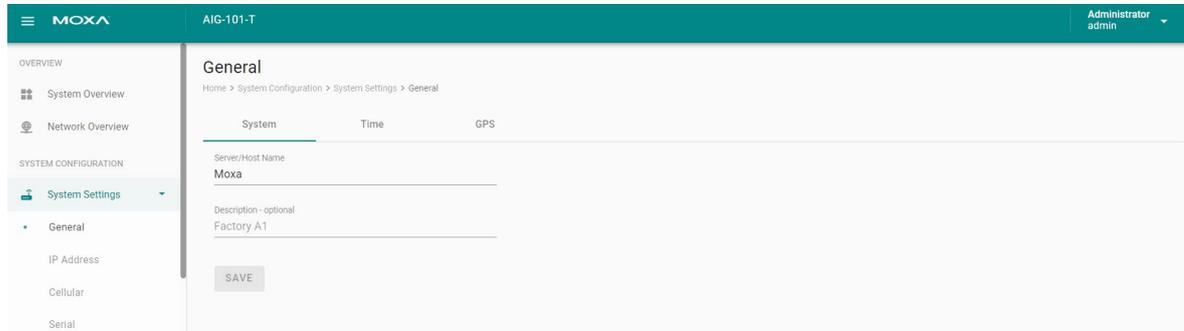
Information on the LAN interfaces is organized under the **LAN** tab and includes information on the usage of the interfaces and the traffic passing through them.



System Configuration

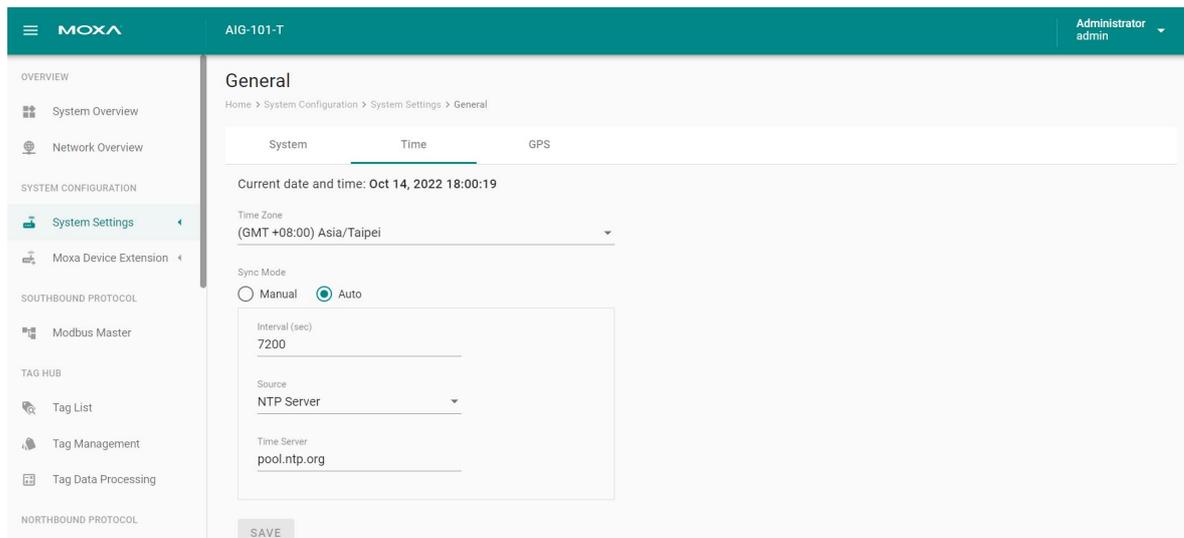
System Settings—General

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."

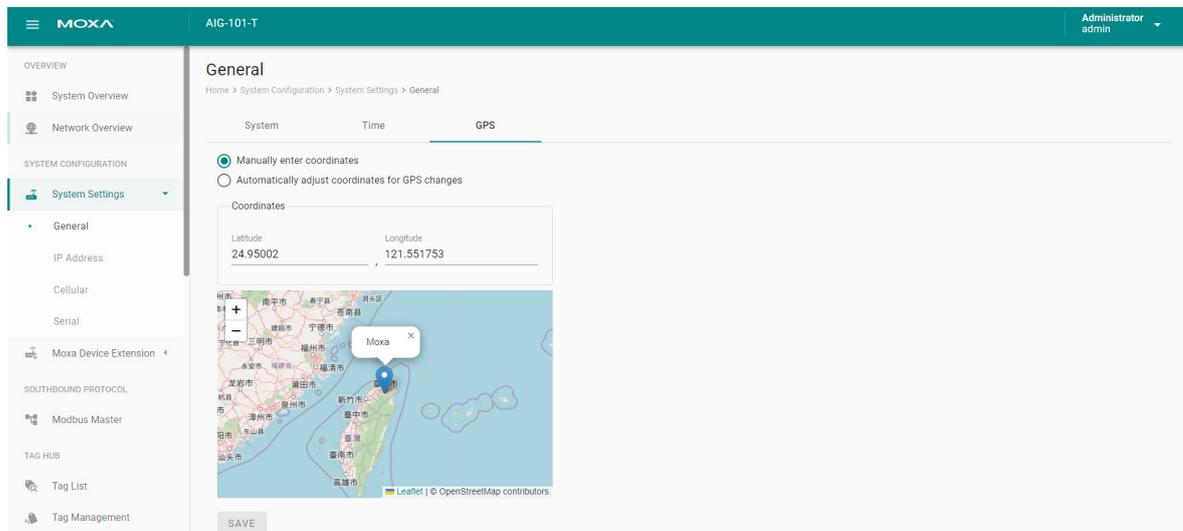
Go to **System Settings > General > Time** to select a time zone. Choose between the Manual or Auto option to update the system time.



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.

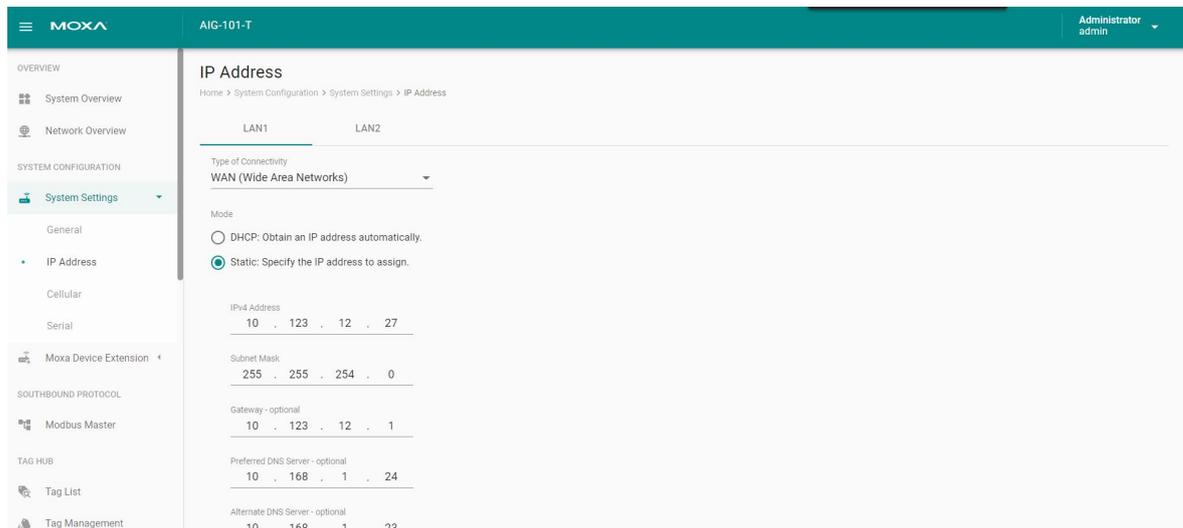


System Settings—IP Address

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

To configure the network, do the following:

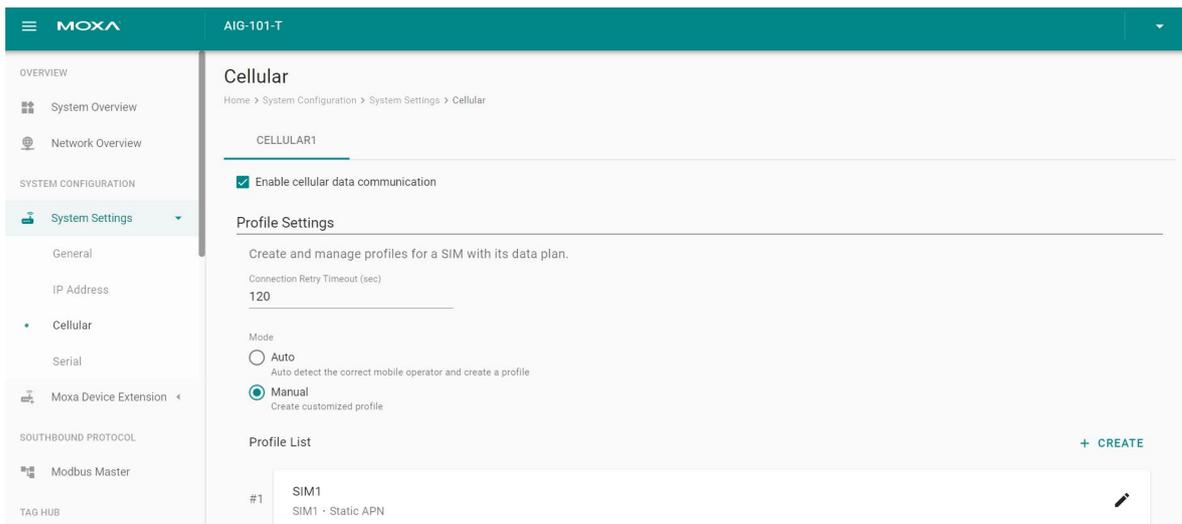
1. Choose **LAN1** or **LAN2** for configuration.
2. Select the **WAN (Wide Area Networks)** or **LAN (Local Area Networks)**.
3. Select **DHCP** or **Static** mode.
4. Configure **IP address, Subnet mask, Gateway, and DNS**.



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. 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.



You can select **Auto** mode to create a customized profile automatically.

You also can create customized cellular profiles by choosing the **Manual** option in the **Profile Settings** section. A list of all the profiles in the system is displayed. **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.

Create New Profile

Profile Name

SIM

SIM1

Pin Code - optional

Carrier

NTT

PDP CID

1

APN Type

Static

APN

CANCEL DONE

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.

Enable check-alive

Target Host	Ping Interval (sec)
8.8.8.8	60

Reboots the device when pings to the target host fail continuously for a specified time interval.

Reboot Timer (min)

20

INFO: The Reboot Timer should be higher than ((total connection retry timeout) * (number of profiles)) to avoid the device from being rebooted before all the profiles are used.

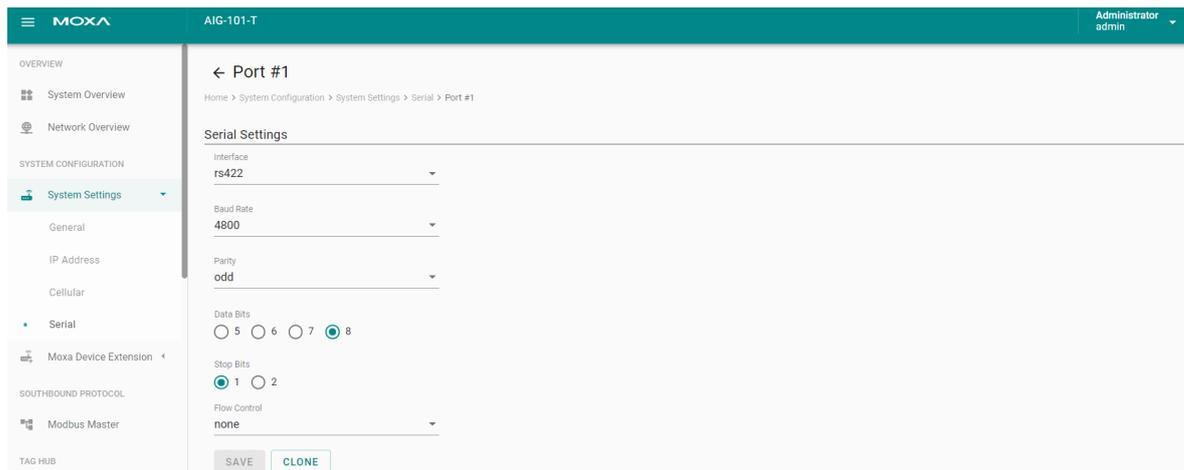
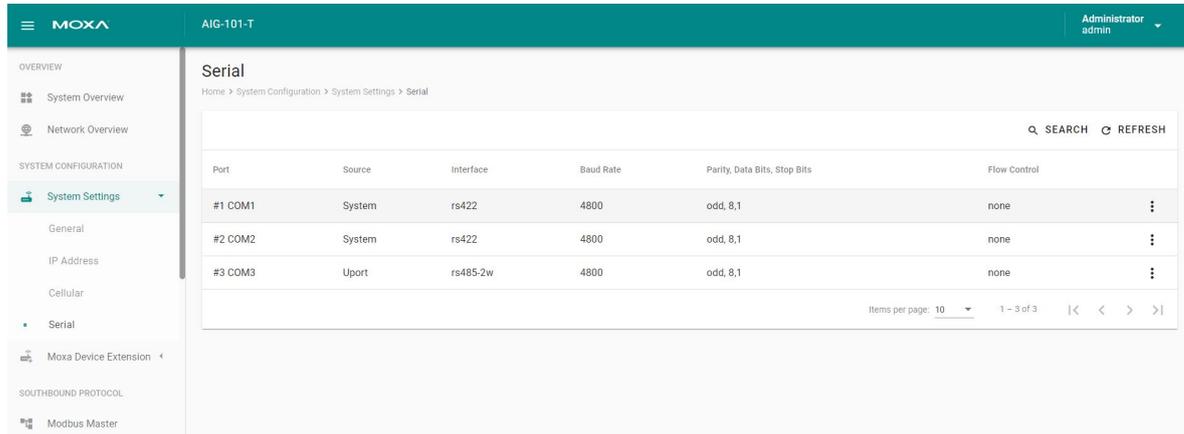
Go to **Network Overview > WAN** if you want to check the cellular network's connection status afterwards.

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

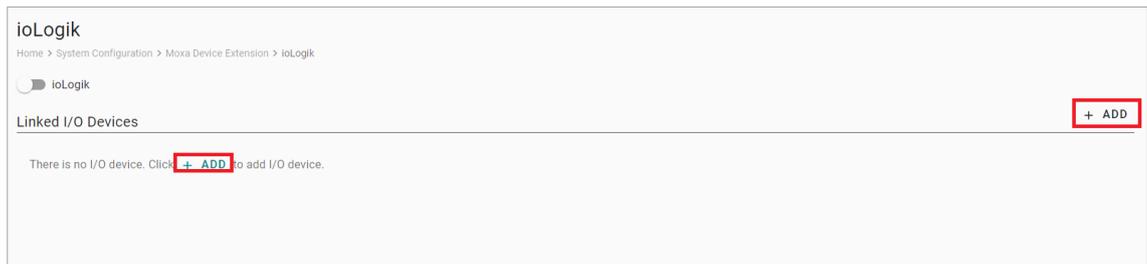
Moxa Device Extension—ioLogik

The device can easily extend I/O interfaces by connecting to ioLogiks. The maximum of connected ioLogik is up to **2** devices. Here are the supported models:

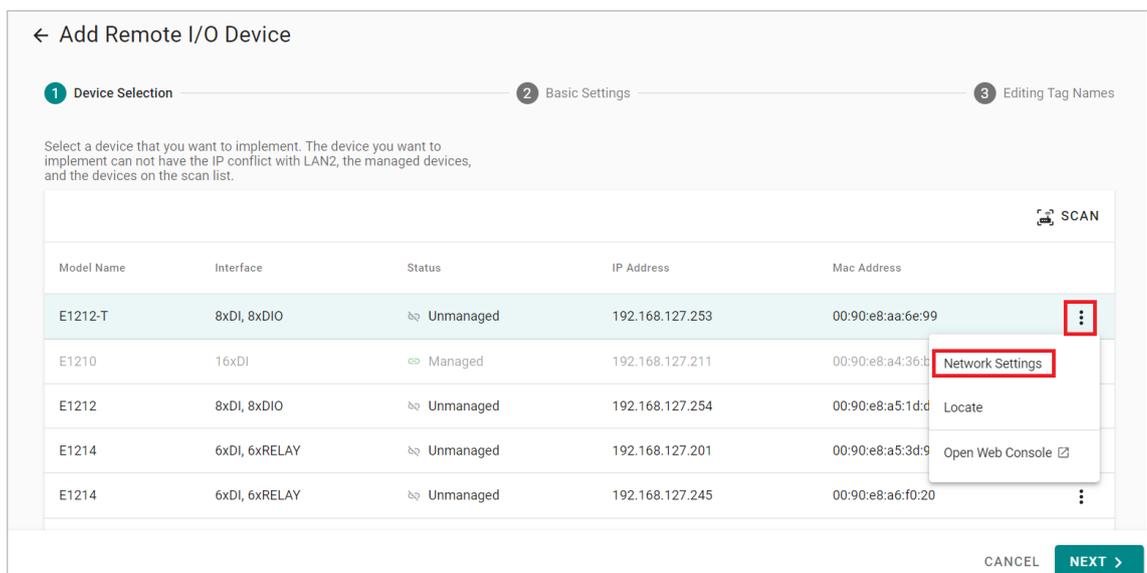
1. ioLogik E1210, ioLogik E1210-T
2. ioLogik E1212, ioLogik E1212-T
3. ioLogik E1214, ioLogik E1214-T

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**.



Edit Network Settings

INFO: The device you want to manage should be in LAN2 and the IP address should be unique within the managed devices. The device will reboot after you change the network settings.

LAN2 IP Address : 192.168.127.100
 LAN2 Subnet Mask: 255.255.255.0

ioLogik

IP Address

192 . 168 . 127 . 253

Subnet Mask

255 . 255 . 255 . 0

CANCEL DONE

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Editing Tag Names

Select a device that you want to implement. The device you want to implement can not have the IP conflict with LAN2, the managed devices, and the devices on the scan list.

It takes time for the machine to be searched again after changing the network settings. Please click the scan button to refresh the list after 10-20 seconds.

SCAN

Model Name	Interface	Status	IP Address	Mac Address	
E1212-T	8xDI, 8xDIO	Unmanaged	192.168.127.253	00:90:e8:aa:6e:99	⋮
E1210	16xDI	Managed	192.168.127.211	00:90:e8:a4:36:b8	⋮
E1212	8xDI, 8xDIO	Unmanaged	192.168.127.254	00:90:e8:a5:1d:de	⋮

CANCEL NEXT >

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

Please enter the password of Remote I/O device to complete authentication.

Click "CONFIRM" directly if Remote I/O hasn't set the password.

Password

.....

CONFIRM

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

Device Name
my_first_io

Poll Interval (Sec)
1

Model Name : E1210
Interface : 16xDI
Firmware Version : V3.2
IP Address : 192.168.127.127
Subnet Mask : 255.255.255.0
Mac Address : 00:90:e8:a4:36:e1

7. (Optional) Edit Alias Name.

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

Tag Information

Device	Tag Name	Tag Type	Read/Write
Device_Status	Device_Status	INT32	Read

Channel	Mode	Alias Name	Tag	
DI-0	DI	DI-000000	DI-000000_DL_Status	⋮
DI-1	DI	DI-01111111	DI-01111111_DL_Status	⋮
DI-2	DI	DI-02345888	DI-02345888_DL_Status	⋮

Edit Alias Name

8. Click **DONE**.

ioLogik

Home > System Configuration > Moxa Device Extension > ioLogik

ioLogik

Linked I/O Devices + ADD

my_first_io
Connected

MANAGE

Model Name: E1210
Interface: 16xDI
Firmware Version: V3.2
IP Address: 192.168.127.127
Subnet Mask: 255.255.255.0
MAC Address: 00:90:e8:a4:36:e1
Poll Interval (sec): 1
View Tag Information



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**.

Tag List
Home > Tag Hub > Tag List

+ Add a filter

Provider	Source	Name		
modbus_serial_master	ddd	status	int32	Read
modbus_tcp_master	test	status	int32	Read
remoteio	my_first_io	DI-08_DL_Status	boolean	Read
remoteio	my_first_io	DI-14_DL_Status	boolean	Read
remoteio	my_first_io	DI-13_DL_Status	boolean	Read
remoteio	my_first_io	DI-12_DL_Status	boolean	Read
remoteio	my_first_io	DI-11_DL_Status	boolean	Read
remoteio	my_first_io	DI-10_DL_Status	boolean	Read
remoteio	my_first_io	DI-09_DL_Status	boolean	Read
remoteio	my_first_io	DI-15_DL_Status	boolean	Read

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

ioLogik
Home > System Configuration > Moxa Device Extension > ioLogik

ioLogik

Linked I/O Devices + ADD

my_first_io

● Connected

Model Name: E1210
Interface: 16xDI
Firmware Version: V3.2
IP Address: 192.168.127.127
Subnet Mask: 255.255.255.0
MAC Address: 00:90:e8:a4:36:e1
Poll Interval (sec): 1
[View Tag Information](#)

MANAGE

- Edit Poll Interval
- Device Authentication
- Open Web Console
- Remove Device

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*

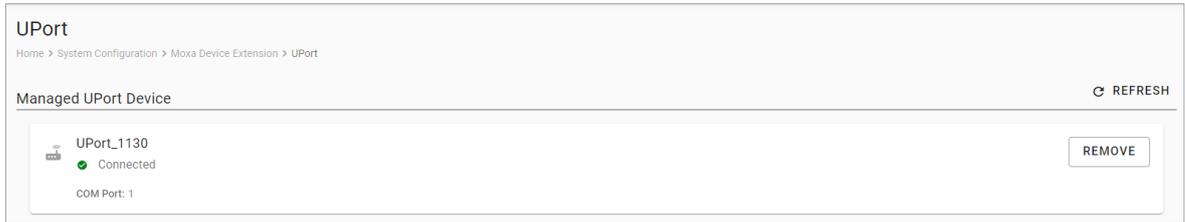


NOTE

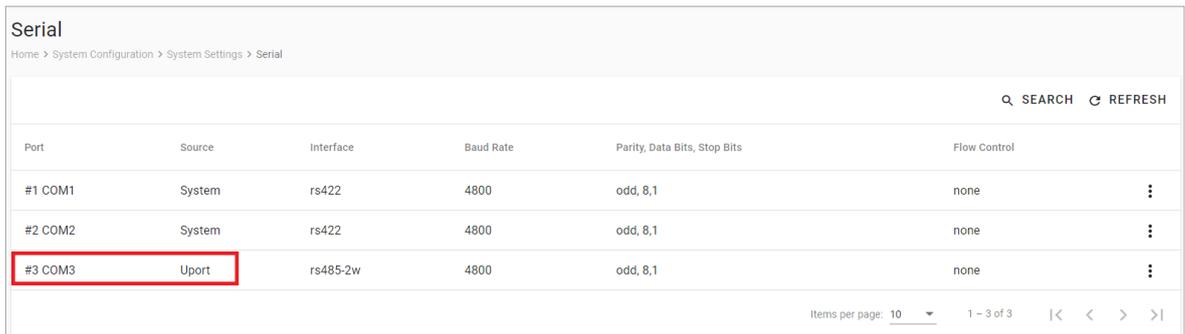
*Note that external power is needed for the UPort 1250I.

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:

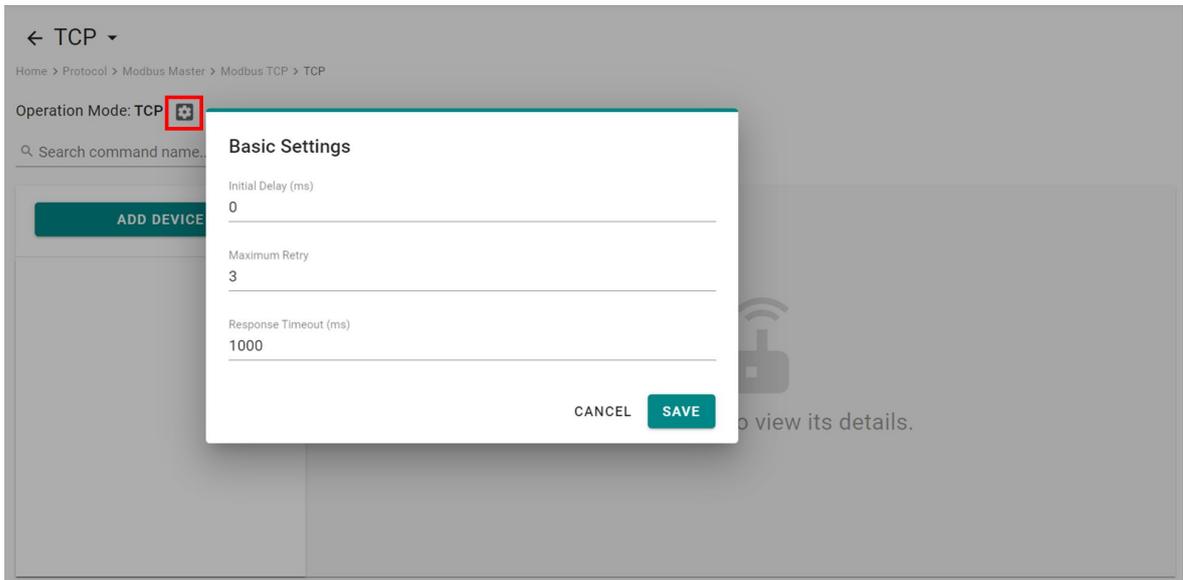
1. Click **TCP** under Modbus TCP or **COMx** under Modbus RTU/ASCII.
2. Click **ADD DEVICE** and go to the 3-step wizard page.
3. Input **device name, slave ID, IP Address,** and **TCP port,** then press **NEXT.**
4. Click **+ ADD COMMAND** to add Modbus commands to collect the data, then press **NEXT.**
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.

The screenshot shows the 'Modbus Master' configuration page. At the top, there is a breadcrumb trail: 'Home > Protocol > Modbus Master'. Below this, a summary card for 'Modbus Master' (Version: 1.4.1) is shown with a 'MANAGE' button and status indicators for 'Device Event: Enable' and 'Command Event: Enable'. The page is divided into two main sections: 'Modbus TCP' and 'Modbus RTU/ASCII'. Under 'Modbus TCP', there is a 'TCP' button labeled 'Not configured'. Under 'Modbus RTU/ASCII', there are two buttons: 'COM1 (RTU)' labeled '1 Device, 1 Command' and 'COM2 (RTU)' labeled 'Not configured'. At the bottom right, there are 'DISCARD' and 'APPLY' buttons.

Modbus TCP

Basic Settings

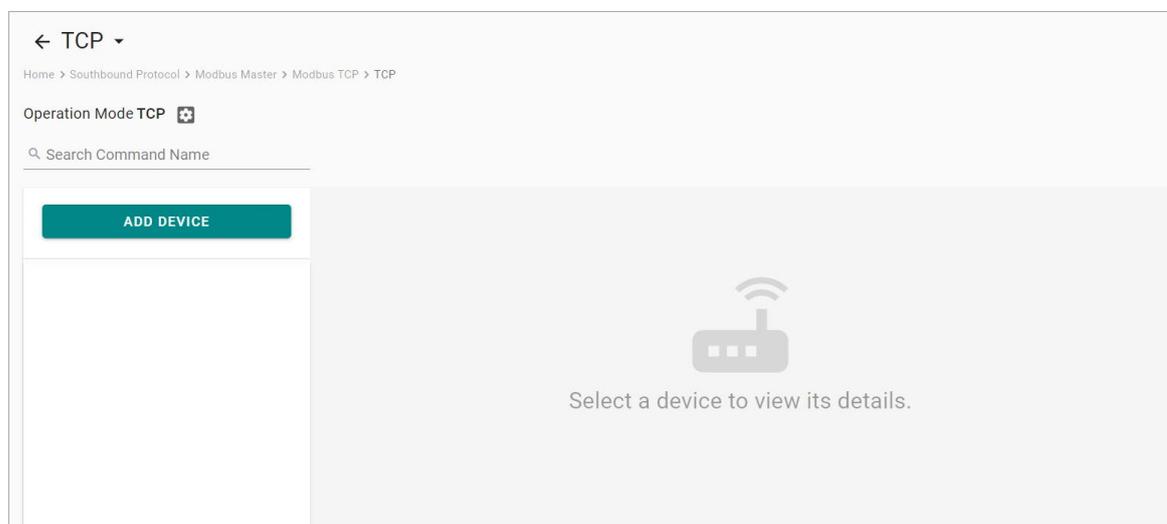
When you access the Modbus TCP setting page, you will first need to configure the basic settings.



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: 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 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 on hand, select **Import Configuration** mode. Importing a configuration file will help you reduce configuration time.

← Create New Device

1 Basic Settings — 2 Command Optional — 3 Confirm

Mode

Manual Import Configuration

Info: You can import configuration file that include command settings. Click "BROWSE" button to select your configuration file.

Command Configuration

BROWSE...

< BACK CANCEL NEXT >

Step 3. Confirm

Review whether the information of the settings is correct.

← Create New Device

1 Basic Settings — 2 Command Optional — 3 Confirm

Confirm the device settings and click DONE to save your changes. After the device is created in the system, you can edit your device settings at any time.

Device Name: SE_Meter
Slave ID: 1
Slave IP: 192.168.127.50
Slave Port: 502
Status: Enable
Number of Commands: 1

< BACK CANCEL DONE

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.

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP 🔄

🔍 Search command name...

ADD DEVICE

SE_Meter

🟢 Enable

Slave IP: 192.168.127.100
Slave Port: 502
Slave ID: 1

+ ADD COMMAND IMPORT EXPORT

No.	Command Name	Function	Address, Quantity	Trigger	Poll Interval (ms)	Enable
1	Voltage	3	Read 0, 10	Cyclic	1000	Enable ⋮

Items per page: 10 ▾ 1 - 1 of 1 |< < > >|

Editing GO TO APPLY SETTINGS

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP 🔄

🔍 Search command name...

ADD DEVICE

SE_Meter

🟢 Enable

Slave IP: 192.168.127.100
Slave Port: 502
Slave ID: 1

+ ADD COMMAND IMPORT EXPORT

Trigger	Poll Interval (ms)	Enable
Cyclic	1000	Enable ⋮

Items per page: 10 ▾ 1 - 1 of 1 |< < > >|

Import Command Configuration

You can import configuration file that include command settings to replace original command settings. Click 'BROWSE' button to select your configuration file.

Command Configuration

BROWSE...

CANCEL DONE

Editing GO TO APPLY SETTINGS

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

Modbus Master

Home > Protocol > Modbus Master

Modbus Master
Version: 1.4.1
Device Event: Enable
Command Event: Enable

MANAGE ▾

Modbus TCP

TCP
1 Device, 1 Command

Modbus RTU/ASCII

COM1 (RTU)
1 Device, 1 Command

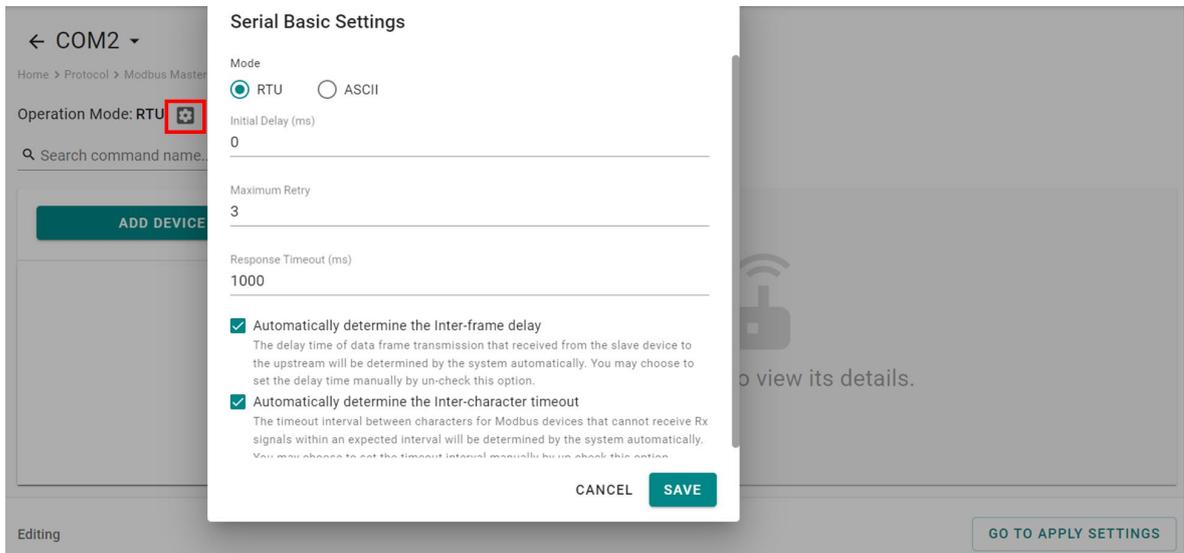
COM2 (RTU)
Not configured

Editing APPLY DISCARD

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

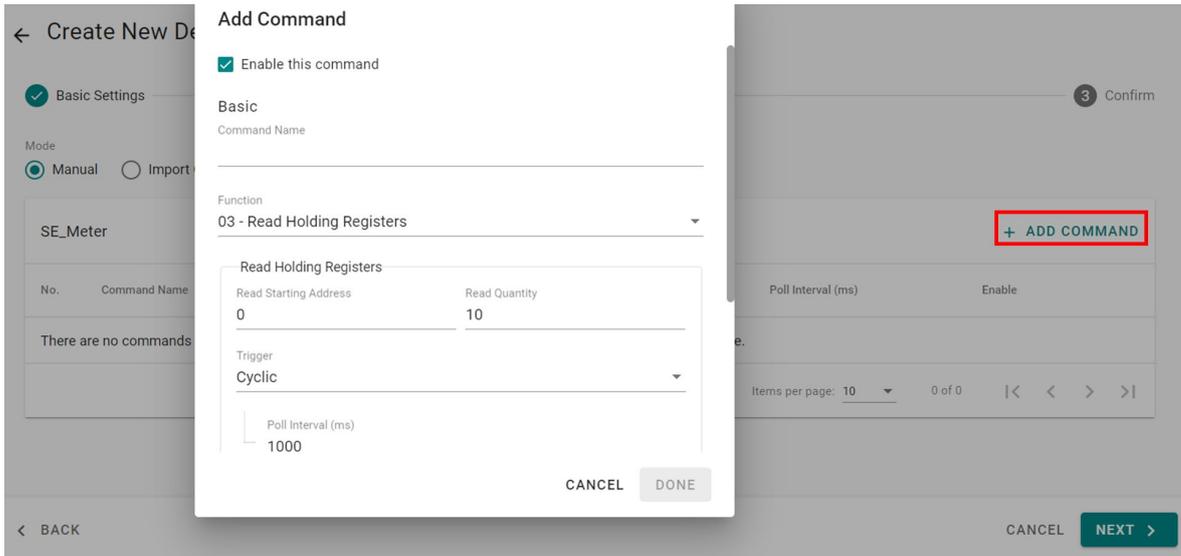
Fill in the basic parameters for the Modbus RTU/ASCII device.

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.

← Create New Device

✓ Basic Settings

2 Command Optional

3 Confirm

Mode

Manual
 Import Configuration

Info: You can import configuration file that include command settings. Click "BROWSE" button to select your configuration file.

Command Configuration

BROWSE...

← BACK
CANCEL
NEXT >

Step 3. Confirm

Review whether the information of the settings is correct.

← Create New Device

✓ Basic Settings ✓ Command Optional 3 Confirm

Confirm the device settings and click DONE to save your changes. After the device is created in the system, you can edit your device settings at any time.

Device Name: SE_Meter1
Slave ID: 1
Status: Enable
Number of Commands: 1

← BACK CANCEL DONE

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.

← COM2 ▾

Home > Protocol > Modbus Master > Modbus RTU/ASCII > COM2

Operation Mode: RTU +

🔍 Search command name...

ADD DEVICE

SE_Meter + ADD COMMAND IMPORT EXPORT

No.	Command Name	Function	Address, Quantity	Trigger	Poll Interval (ms)	Enable
1	Voltage	3	Read 0, 10	Cyclic	1000	Enable

Items per page: 10 1 - 1 of 1 |< < > >|

Editing GO TO APPLY SETTINGS

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

The screenshot shows the 'Modbus Master' configuration page. At the top, there is a breadcrumb trail: 'Home > Protocol > Modbus Master'. Below this, a card displays 'Modbus Master' with a star icon, 'Version: 1.4.1', and 'Device Event: Enable' and 'Command Event: Enable'. A 'MANAGE' dropdown menu is located in the top right of this card. The page is divided into sections: 'Modbus TCP' with a 'TCP' card showing '1 Device, 1 Command'; and 'Modbus RTU/ASCII' with 'COM1 (RTU)' (1 Device, 1 Command) and 'COM2 (RTU)' (Not configured) cards. At the bottom, there is an 'Editing' status and two buttons: 'DISCARD' and 'APPLY', with the 'APPLY' button highlighted by a red box.

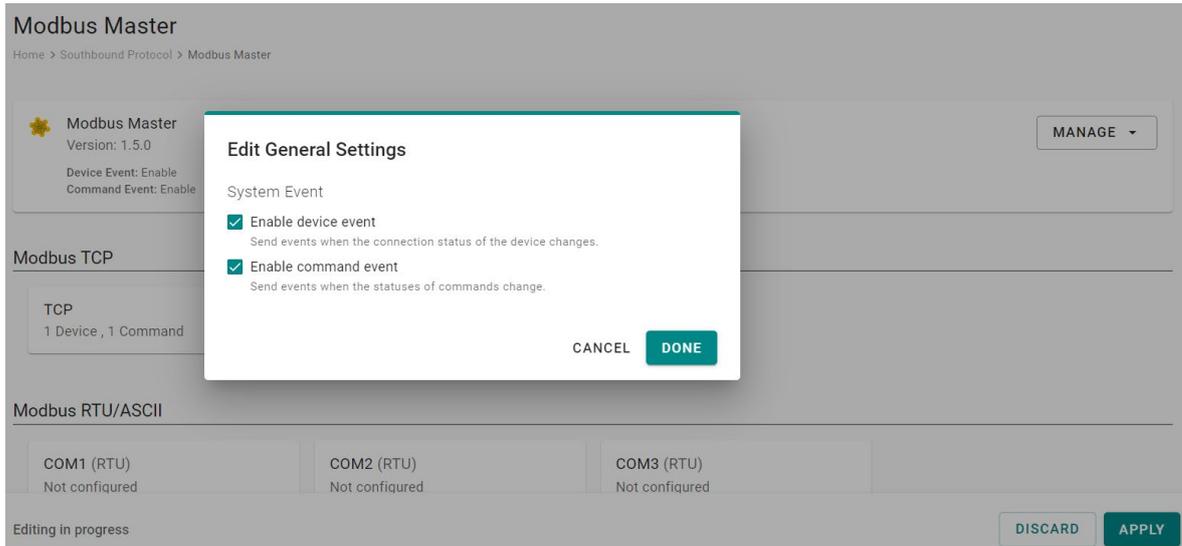
Manage

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

This screenshot shows the same 'Modbus Master' configuration page as above, but with the 'MANAGE' dropdown menu open. The menu options are 'Edit General Settings', 'Import Configuration', and 'Export Configuration'. The entire 'MANAGE' dropdown menu is highlighted with a red box. The 'APPLY' button at the bottom right is also highlighted with a red box.

Edit General Settings

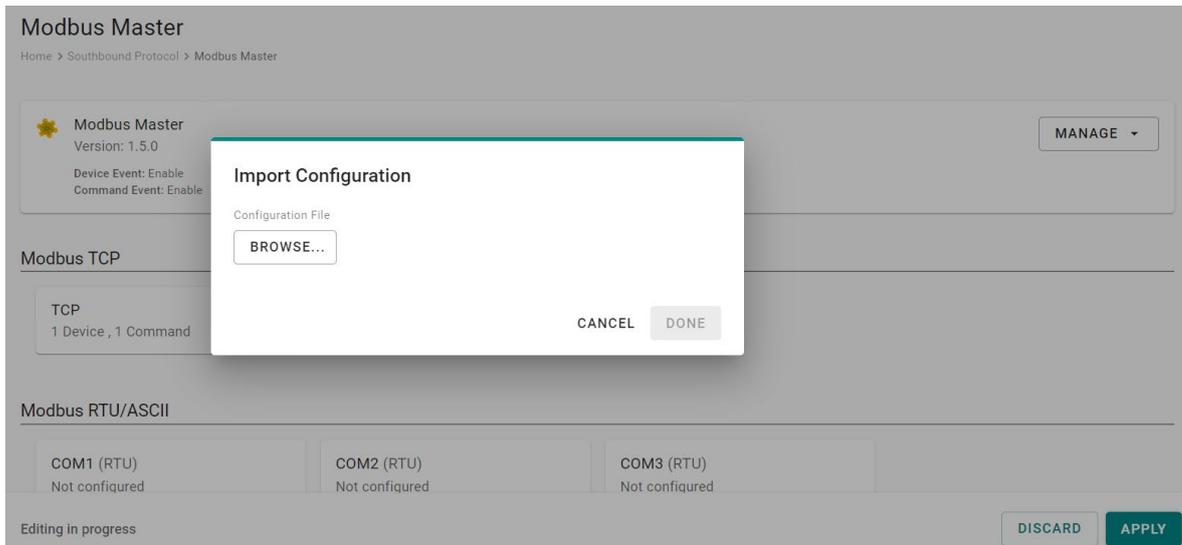
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



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-interfaces																									
id	master	tcp	initialDelay	retryCount	responseTimeout																				
1	1	1	0	3	1000																				
ser-masters																									
id	name																								
1	modbus_serial_master																								
master-ser-interfaces																									
id	serMasterPort	valueFormat	initialDelay	retryCount	responseTime	frameInterval	charInterval																		
1	1	0	0	0	3	1000	0	0																	
2	1	1	0	0	3	1000	0	0																	
remote-devs																									
id	remoteMasterSerMasterTcpName	enable	slaveId	slaveIp	slaveTcpPort																				
1	1	1	1232	1	1.0.0.0	502																			
2	2	1	SE_Meter	1	1.0.0.0	502																			
3	3	1	GE_Meter	1	1.1.1.1	502																			
mcmds																									
id	name	enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollInterval	swap	fpFunc	fpTou	fpData	scalingFu	intercept	interceptC	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	0	1	Voltage_t1	int16	r	20
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	0	1	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.

Provider	Source	Name	Type	Access
modbus_serial_master	ddd	device_info_t2	int16	Read
modbus_serial_master	ddd	status	int32	Read
modbus_serial_master	ddd	Power2	int16	Read
modbus_serial_master	ddd	Power1	int16	Read
modbus_serial_master	ddd	device_info_t27	int16	Read
modbus_serial_master	ddd	device_info_t26	int16	Read
modbus_serial_master	ddd	device_info_t25	int16	Read

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**.

Provider	Source	Name	Type	Value	Access	Last Update
No tags are being monitored. Click + EDIT TAGS to add the first tag to monitor.						

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

Edit Tags

Select the tags you want to display in the list.

83 Item(s) selected CLEAR SEARCH

<input checked="" type="checkbox"/>	Provider	Source	Name	Type	Access
<input checked="" type="checkbox"/>	modbus_serial_master	ddd	device_info_t2	int16	Read
<input checked="" type="checkbox"/>	modbus_serial_master	ddd	status	int32	Read
<input checked="" type="checkbox"/>	modbus_serial_master	ddd	Power2	int16	Read
<input checked="" type="checkbox"/>	modbus_serial_master	ddd	Power1	int16	Read
<input checked="" type="checkbox"/>	modbus_serial_master	ddd	device_info_t27	int16	Read

Items per page: 5 1 - 5 of 83 < > |

CANCEL **SAVE**

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

Tag Management

Home > Tag Hub > Tag Management

Add tags and monitor them here. You can also set values for writable tags by clicking " : ". The values take effect within a few seconds.

Monitoring tags ... SEARCH + EDIT TAGS

Provider	Source	Name	Type	Value	Access	Last Update	
modbus_serial_master	ddd	device_info_t2	int16	-	Read	-	⋮
modbus_serial_master	ddd	status	int32	-2147483648	Read	Sep 14, 2022, 11:38:19	⋮
modbus_serial_master	ddd	Power2	int16	-	Read	-	⋮
modbus_serial_master	ddd	Power1	int16	-	Read	-	⋮

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 Management

Home > Tag Hub > Tag Management

Add tags and monitor them here by clicking " : ". The values take effect within a few seconds.

Monitoring tags ... SEARCH + EDIT TAGS

Provider	Source	Name	Type	Value	Access	Last Update	
modbus_serial_master	123	DO	boolean		Write	-	⋮

Items per page: 10 1 - 1 of 1 < > |

CANCEL **SAVE**

CANCEL **NEXT >**

Write value

Provider: modbus_serial_master

Source: 123

Name: DO

Type: boolean

Value *

INFO: The value will take effect in a few seconds.

CANCEL **SAVE**

Tag Data Processing

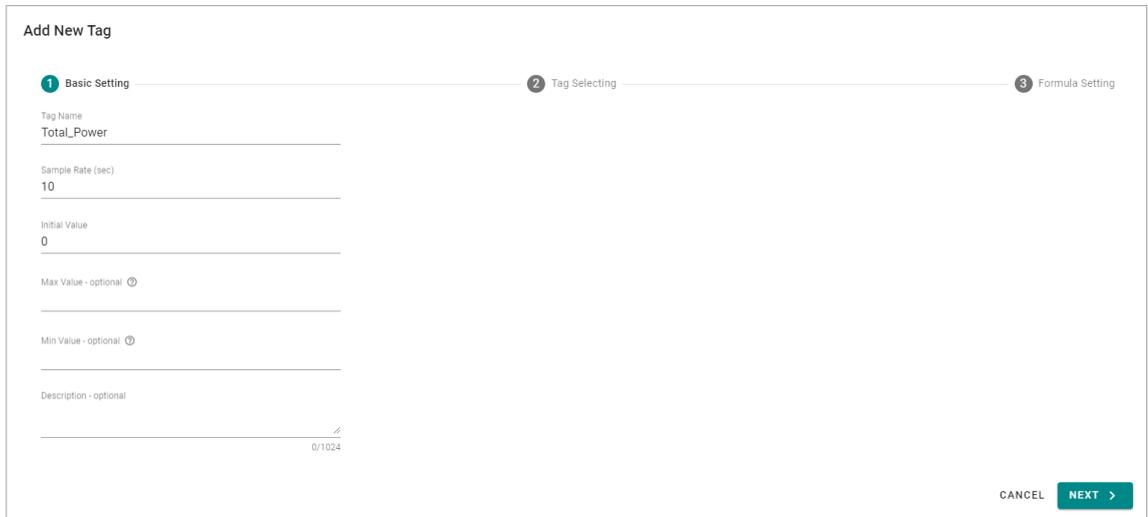
The device has a built-in intuitive no-code solution that can preprocess data before sending it to the northbound system. This feature helps eliminate the programming effort in data processing.

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

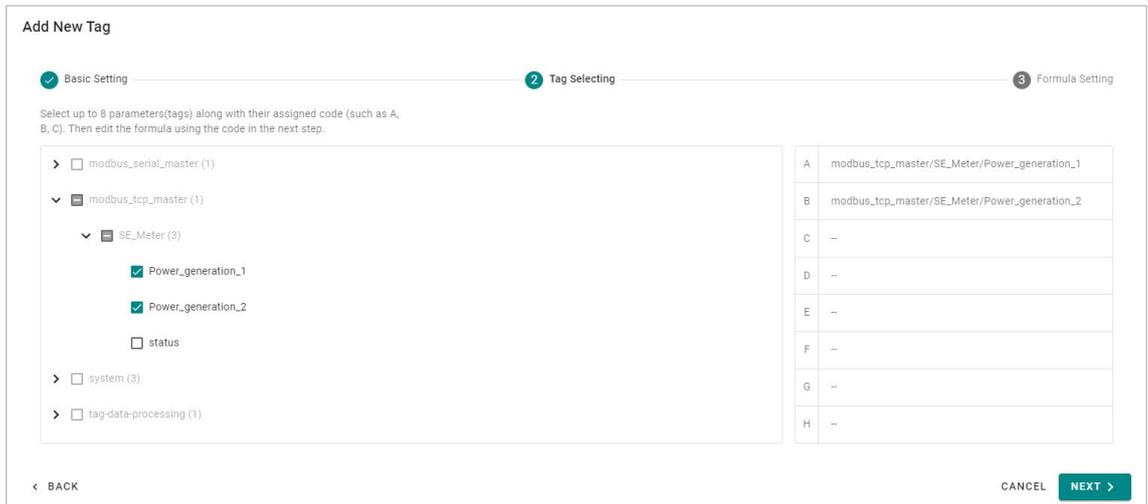
1. Click **+ ADD TAG**.



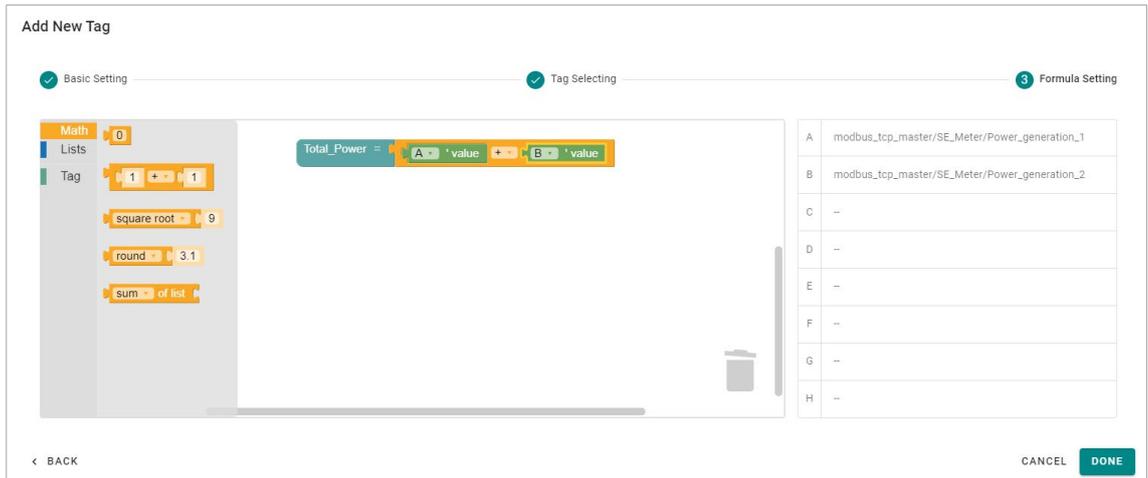
2. Specify **Tag Name**, **Sample Rate**, and other parameters for the new tag, then click **NEXT**.



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



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



5. Click **DONE** and you will see the new tag in the list.

Tag Data Processing

Home > Tag Hub > Tag Data Processing

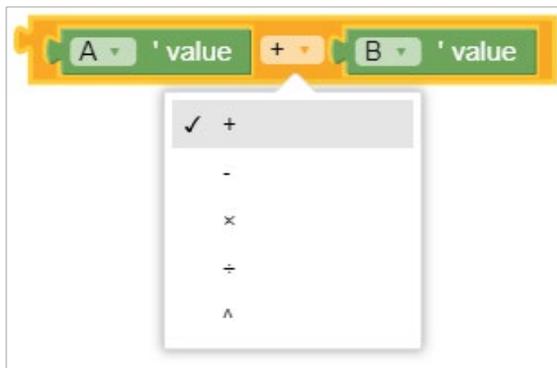
+ ADD TAG

No.	Tag Name	Sample Rate (sec)	Initial Value	Max Value	Min Value	Description
1	Total_Power	10	0	--	--	--

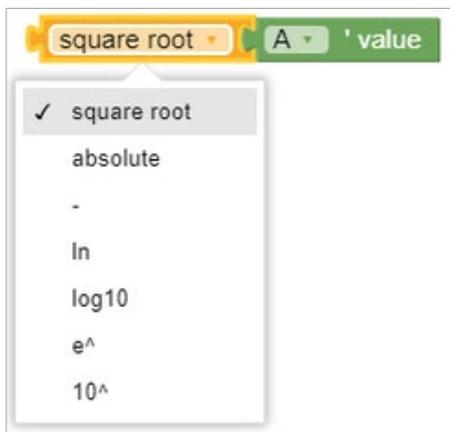
Items per page: 10 | 1 - 1 of 1 | < >

The supported formulas are:

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



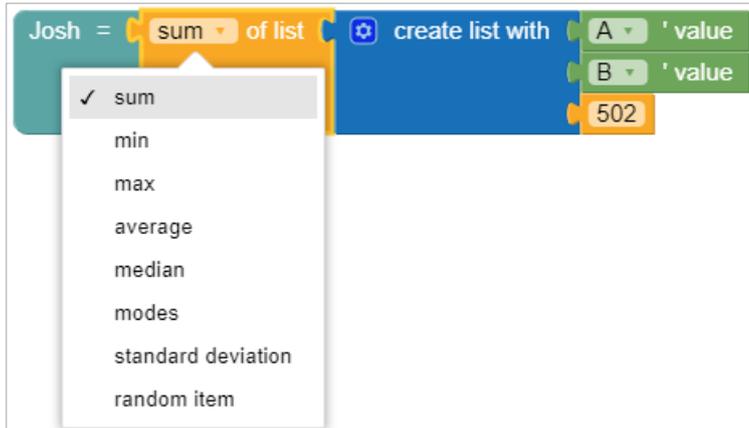
2. square root, absolute, negative(-), natural logarithm(ln), 10 logarithm(log10), power by Euler's number(e^), power by 10(10^).



3. round, round up, round down.



4. 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 connection.
2. Enter **Connection String**.
3. Select a **Connection Protocol**.
4. Select an **Authentication Type**.
5. (Optional) Upload X.509 Certificate and Private Key.
6. 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=Vq2qbpo07l/PUFt0s

Connection Protocol
mqtt (Port: 8883)

Authentication Type

Symmetric Key X.509 Certificate

Trusted Root CA - optional

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. Enter the **Polling Interval** in seconds.

The screenshot shows the 'Create New Telemetry Message' dialog with the 'Basic Settings' step selected. The progress bar at the top indicates four steps: 1. Basic Settings (active), 2. Message Tags, 3. Custom Payload Optional, and 4. Properties Optional. The 'Enable Telemetry Message' checkbox is checked. The 'Output Topic' field contains the text 'Test'. The 'Polling Interval (sec)' field is set to '0'. The 'Send Threshold' is set to 'By size 4096 bytes or every 60 seconds'. At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

4. Set up a threshold by file size (bytes) or time interval (seconds),
5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).

The screenshot shows the 'Create New Telemetry Message' dialog with the 'Message Tags' step selected. The progress bar at the top indicates four steps: 1. Basic Settings, 2. Message Tags (active), 3. Custom Payload Optional, and 4. Properties Optional. The 'Select Tags' section contains an info message: 'Info: Select one or more tag providers and select tags to map data.' Below this, the 'Providers' dropdown is set to 'modbus_serial_master, modbus_tcp_master'. A search modal is open, showing a list of tags with checkboxes: 'Power2' (checked), 'Power1' (checked), 'device_info_t27' (unchecked), and 'device_info_t26' (unchecked). At the bottom of the modal, it says 'Total: 41, Selected: 2' and has a 'DONE' button. At the bottom right of the main dialog, there are 'CANCEL' and 'NEXT >' buttons.

- (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/>).

Create New Telemetry Message

Basic Settings Message Tags **3 Custom Payload** Optional 4 Properties Optional

Enable JQ filter
INFO: If the default payload format doesn't meet your requirement, edit the format using the JQ filter.

Basic Editing Advanced Editing

Tag Pre-merge Format

Message Result

```
1 {
2   "tags": {
3     "modbus_serial_master": {
4       "123": {
5         "DO": {
6           "values": [
7             {
8               "updateTimeStamp": "2020-02-14T05:53:23Z",
9               "value": true
10            }
11          ]
12        }
13      }
14    }
15  }
16 }
```

< BACK CANCEL **NEXT** >

- Click **NEXT**.

- (Optional) Enter Property Key and Value.

Create New Telemetry Message

Basic Settings Message Tags Custom Payload Optional **4 Properties** Optional

Property Key Property Value

+ Add another

< BACK CANCEL **SAVE**

- Click **SAVE**.

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.

Azure IoT Device

Telemetry Message **Store and Forward**

You can store telemetry data in the local storage to prevent data loss when a device goes offline. Enable the feature and define the store and forward policy below.

Enable Store and Forward

Storage Settings

INFO: You may lose part of the stored data if you reduce the Maximum Storage Cache or a Time to Live settings.

Target Disk Status
System (3.59 GB free of 6.05 GB)

Maximum Storage Cache (MB) ⓘ
10

Storage Full Policy ⓘ
 Drop Oldest Drop Newest

Advanced Storage Limitation

Enable Time to Live
Time to live (TTL) is the time (sec) until the cached messages expire.

Time to Live (sec)
7200



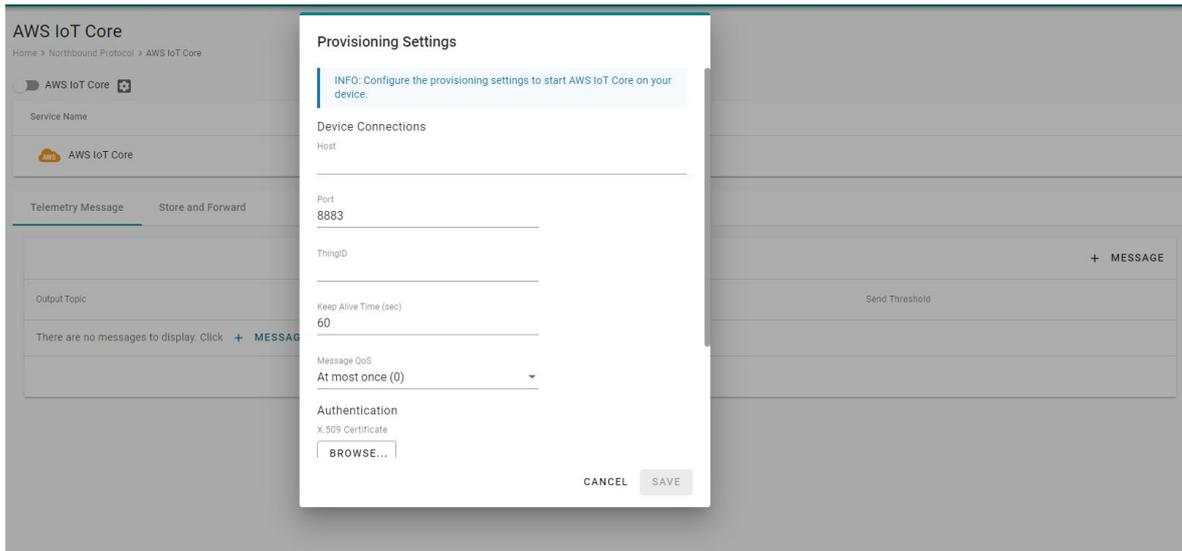
NOTE

If you want to use the direct method to write tags from the cloud, refer to <https://docs.moxa.online/tpe/openapi/taghub/#tag/access>.

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:

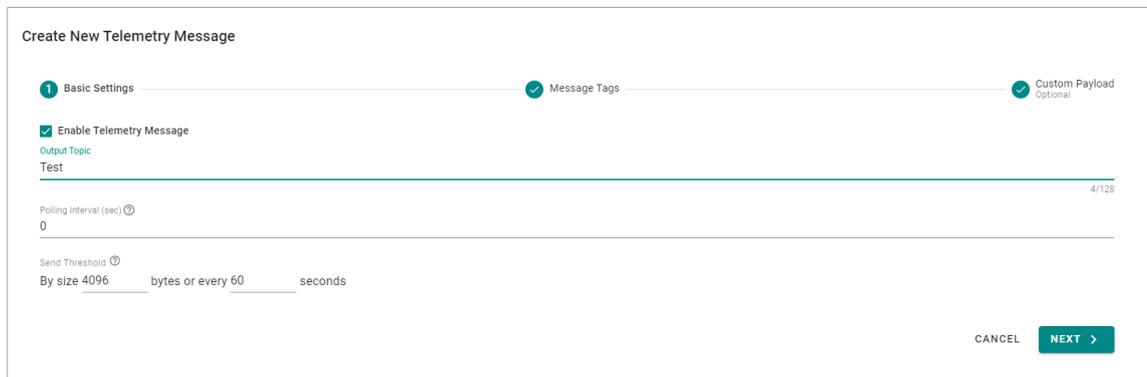
1. Click  to set connection.
2. Enter **Host (Endpoint)**. **Port** (default: 8883).
3. Enter **ThingID**.
4. Input **Keep Alive Time** (sec)
5. Select a way of message **QoS**.
6. Upload X.509 Certificate, Private Key, and (optional) Trusted Root CA.
7. Click **SAVE**.



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. Enter the **Polling Interval** in seconds.
4. Set up a threshold by file size (bytes) or time interval (seconds),
5. Click **NEXT**.



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

Create New Telemetry Message

1 Basic Settings

2 Message Tags

3 Custom Payload Optional

Select Tags

INFO: Select one or more tag providers and select tags to map data.

Providers
events, modbus_serial_master, modbus_tcp_master

Selected Tags
123_t2 (+10 others)

< BACK

CANCEL NEXT >

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/>).

Create New Telemetry Message

1 Basic Settings

2 Message Tags

3 Custom Payload Optional

Enable JQ filter
INFO: If the default payload format doesn't meet your requirement, edit the format using the JQ filter.

Basic Editing Advanced Editing

Tag Pre-merge Format

Message Result

```
1- {
2-   "tags": {
3-     "modbus_tcp_master": {
4-       "SE_meter": {
5-         "123_t2": {
6-           "values": [
7-             {
8-               "updateTimeStamp": "2020-02-14T05:53:23Z",
9-               "value": 11
10-            }
11-           ]
12-         },
13-         "123_t10": {
14-           "values": [
15-             {
16-               "updateTimeStamp": "2020-02-14T05:53:23Z",
17-               "value": 11
18-            }
19-           ]
20-         },
21-         "123_t2": {
22-           "values": [
```

< BACK

CANCEL SAVE

8. Click **SAVE**.

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.

Stores telemetry data in the local storage to prevent data loss when a device goes offline. You can enable this feature by defining policies in the following section.

Enable Store and Forward

Storage Setting

INFO: You may lose part of the stored data if you reduce the maximum Disk Size or Time to Live settings.

Target Disk
System (3.59GB free of 6.05GB)

Maximum Storage Cache (MB) [?]
10

Storage Full Policy [?]
 Drop Oldest Drop Newest

Advanced Storage Limitation

Enable Time to Live
Time to live (TTL) is the time (sec) until the cached messages expire.

Time to Live (sec)
7200

SAVE



NOTE

If you want to use the direct method to write tags from the cloud, refer to <https://docs.moxa.online/tpe/openapi/taghub/#tag/access>.

Generic MQTT Client

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

Note that you need to create a connection first and 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).

Connect to New MQTT Broker

General SSL/TLS Will and Testament

Server _____ Port 8883

MQTT Version
 3.1.1 3.1

Client ID _____

Username
admin

Password
.....

Keep Alive Time (sec)
60

Clean Session
 Don't persist messages on the broker when disconnected.

CANCEL SAVE

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**.

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

The screenshot shows a dialog box titled "Connect to New MQTT Broker" with three tabs: "General", "SSL/TLS", and "Will and Testament". The "SSL/TLS" tab is active. Under the "SSL/TLS" heading, there is a checked checkbox for "Enable SSL/TLS". Below this, there is a "TLS Version" section with three radio buttons: "1.2" (selected), "1.1", and "1.0". There are three "BROWSE..." buttons for "Client Certificate - optional", "Client Key - optional", and "Trusted Root CA - optional". At the bottom, there is an unchecked checkbox for "Ignore Server Certificate". "CANCEL" and "SAVE" buttons are at the bottom right.

- (Optional) Enable Will flag.
- (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:

- Click **+ MESSAGE**.
- Specify an **output topic**.

The screenshot shows a dialog box titled "Create New Telemetry Message" with three steps: "1 Basic Settings", "2 Message Tags", and "3 Custom Payload Optional". The "Basic Settings" step is active. There is a checked checkbox for "Enable Telemetry Message". Below it is an "Output Topic" field. There is a "Polling Interval (sec)" field with a value of "0". There is a "Send Threshold" field with a value of "4096" bytes or every "60" seconds. "CANCEL" and "NEXT >" buttons are at the bottom right.

- Enter a time for the **polling interval**.
- Set up a **threshold by size** or a **certain interval**.
- Click **NEXT**.

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

Create New Telemetry Message

Basic Settings Message Tags Custom Payload Optional

Select Tags

INFO: Select one or more tag providers and select tags to map data.

Providers
— None —

Selected Tags
— None — 0 Tags

< BACK CANCEL NEXT >

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

Create New Telemetry Message

Basic Settings Message Tags Custom Payload Optional

Enable JQ filter
INFO: If the default payload format doesn't meet your requirement, edit the format using the JQ filter.

Basic Editing Advanced Editing

Tag Pre-merge Format

Message Result

```
1 {
2   "tags": {
3     "events": {
4       "device setting": {
5         "configuration update failed": {
6           "values": [
7             {
8               "updateTimeStamp": "2020-02-14T05:53:23Z",
9               "value": "event message"
10            }
11          ]
12        },
13        "configuration update success": {
14          "values": [
15            {
16              "updateTimeStamp": "2020-02-14T05:53:23Z",
17              "value": "event message"
18            }
19          ]
20        },
21        "time sync failed": {
22          "values": [
```

< BACK CANCEL SAVE

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 the jq website (<https://stedolan.github.io/jq/manual/>).

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.

ADD CONNECTION

test.mosquitto.org
Connected

Telemetry Message | **Store and Forward** | Remote API Invocation

Stores telemetry data in the local storage to prevent data loss when device goes offline. You can enable this feature by defining policies here.

Enable Store and Forward

Storage Setting

INFO: You may lose part of stored data stored if you reduce the maximum Disk Size or Time to Live settings.

Target Disk
System (3.59GB free of 6.05 GB)

Maximum Storage Cache (MB) ⓘ
10

Storage Full Policy ⓘ
 Drop Oldest Drop Newest

Advanced Storage Limitation

Enable Time to Live
Time to live (TTL) is the time (sec) until the cache messages expire.

Time to Live (sec)
7200

SAVE

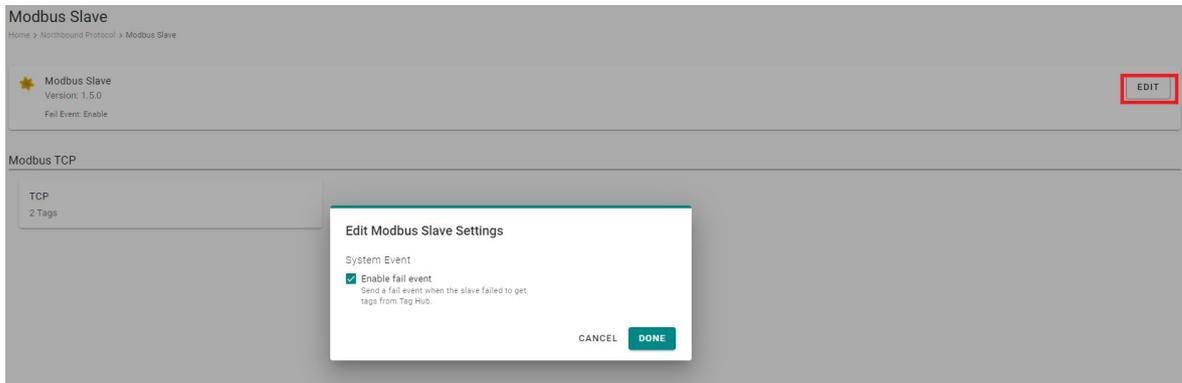


NOTE

If you want to use the direct method to write tags from the cloud, refer to <https://docs.moxa.online/tpe/openapi/taghub/#tag/access>.

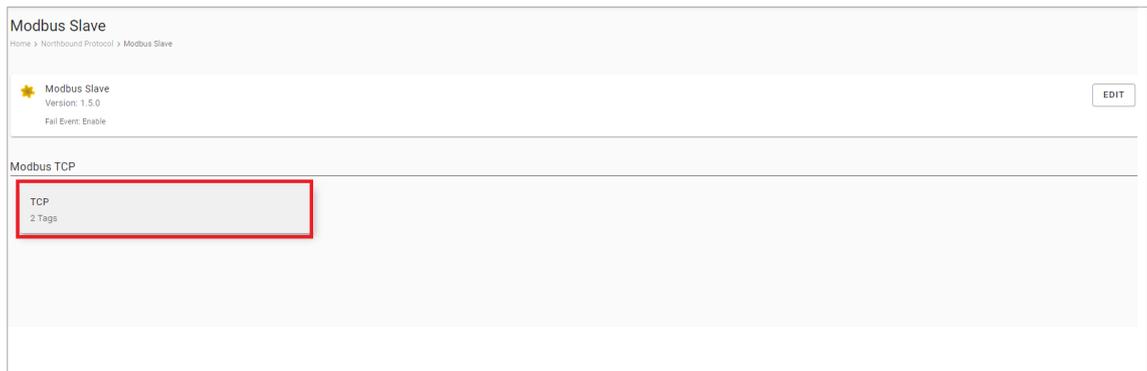
Modbus TCP Slave

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.

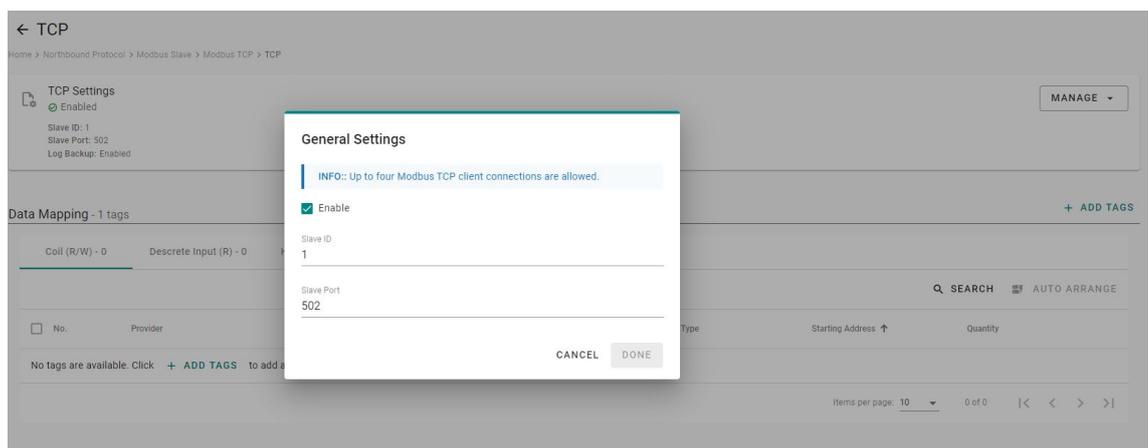


To create a Modbus TCP server (slave), following the steps below:

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

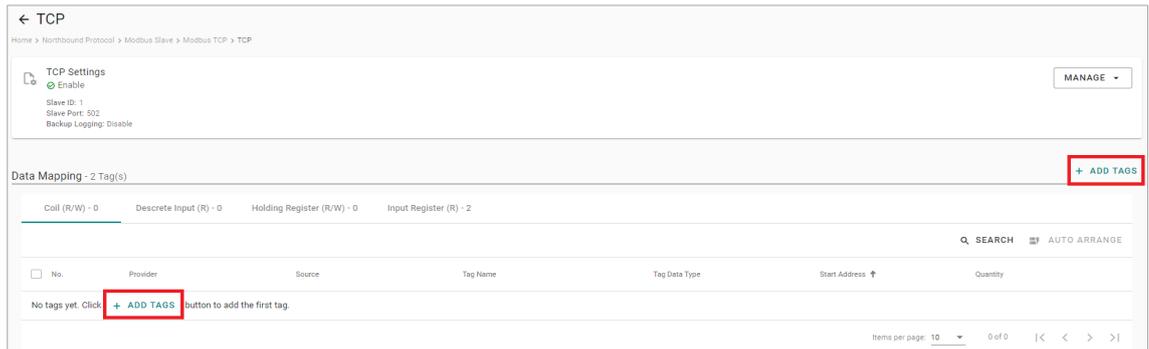


2. Click **MANAGE > General Settings**.



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

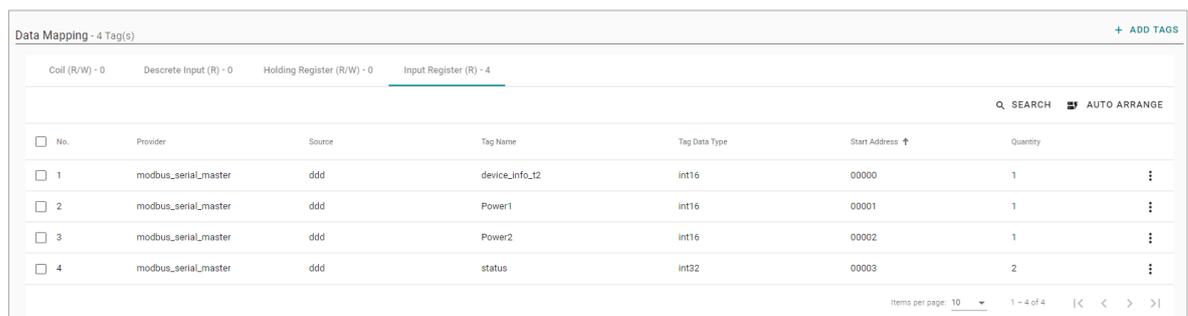
3. Click **+ADD TAGS** to select tags (e.g., Modbus Master).



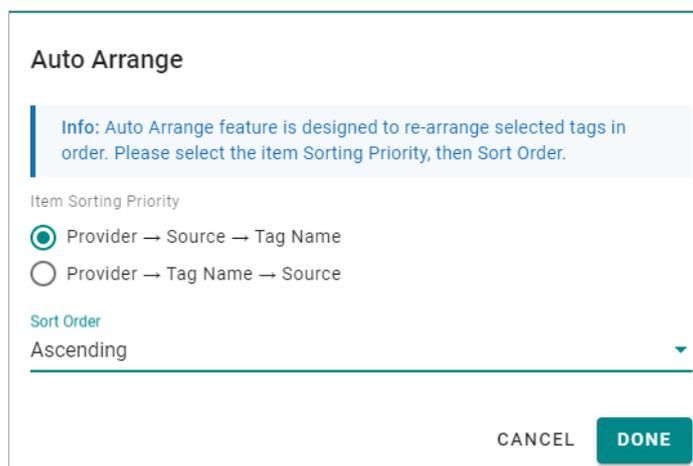
4. Click **DONE** to finish settings.

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**.

Edit Backup Logging Settings

Info: When the SD card is removed or function disabled, related parameter settings will not be functioning.

Enable backup logging

Folder Name
Modbus TCP Slave

Maximum Storage (MB) ⓘ
1024

Log Interval (sec)
30

CANCEL **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.

Service Enablement

Home > Security > Service Enablement

Users can enable/disable the system service by toggling the buttons below.

System		^
Event Log	<input checked="" type="checkbox"/>	
HTTP Service	<input type="checkbox"/>	
HTTPS Service	<input checked="" type="checkbox"/>	
Internet Check Alive Service ?	<input type="checkbox"/>	
Login Policy	<input checked="" type="checkbox"/>	
NAT Service ?	<input type="checkbox"/>	
NTP Service	<input checked="" type="checkbox"/>	
SD Card	<input checked="" type="checkbox"/>	
System Log	<input checked="" type="checkbox"/>	

Network		^
Cellular1	<input checked="" type="checkbox"/>	
LAN1	<input checked="" type="checkbox"/>	
LAN2	<input checked="" type="checkbox"/>	

Provision Service		^
AIG QuickON	<input checked="" type="checkbox"/>	

HTTP/HTTPS

To ensure secure access to the web console of the device, we strongly recommend you to **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.

HTTP/HTTPS

Home > Security > HTTP/HTTPS

HTTP Service

Enable HTTP Service

HTTPS Service

Enable HTTPS Service

Port Number
8443

Import TLS/SSL Certificate

Certificate
 default.crt

Private Key
 default.key

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.

Firewall

Home > Security > Firewall

Inbound

System SEARCH

Action	Priority ↑	Rule Name	Gateway Port	Protocol	Source IP	Destination IP
Deny	1	default deny all	--	Any	Any	Localhost
Allow	1	https service	8443	TCP	Any	Localhost
Allow	1	discovery service	40404	UDP	Any	Localhost
Allow	6	app(remoteio) filter port	6012	UDP	Any	Localhost

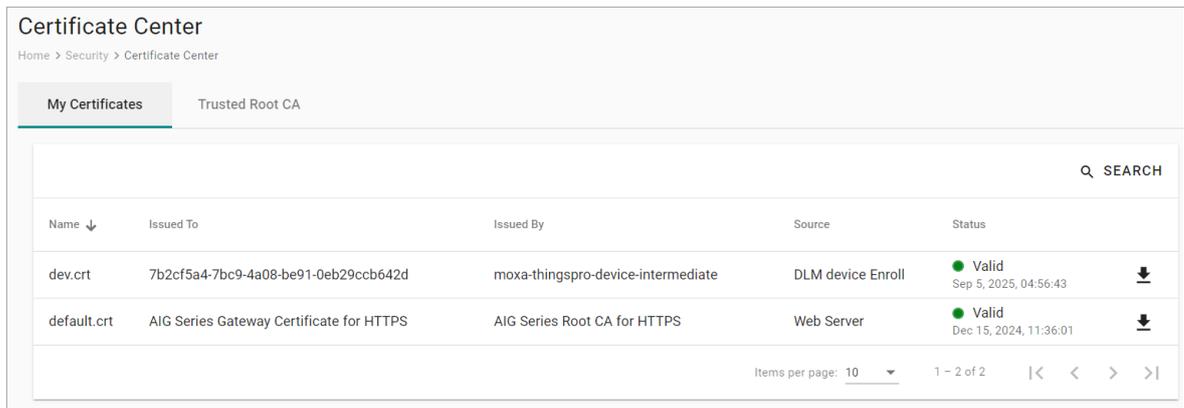
Items per page: 10 1 - 4 of 4 |< < > >|

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



The screenshot shows the 'Certificate Center' interface. It has a breadcrumb trail: Home > Security > Certificate Center. There are two tabs: 'My Certificates' (selected) and 'Trusted Root CA'. A search bar is located at the top right. Below is a table with columns: Name, Issued To, Issued By, Source, and Status. Two certificates are listed: 'dev.crt' and 'default.crt'. The 'dev.crt' certificate is issued to '7b2cf5a4-7bc9-4a08-be91-0eb29ccb642d' by 'moxa-thingspro-device-intermediate' and is 'Valid' as of 'Sep 5, 2025, 04:56:43'. The 'default.crt' certificate is an 'AIG Series Gateway Certificate for HTTPS' issued by 'AIG Series Root CA for HTTPS' and is 'Valid' as of 'Dec 15, 2024, 11:36:01'. Both certificates have a download icon. At the bottom, it shows 'Items per page: 10' and '1 - 2 of 2'.

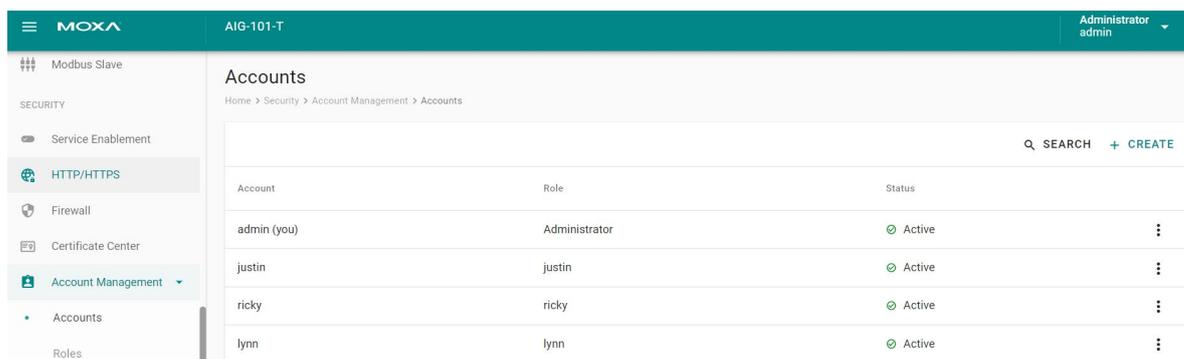
Name ↓	Issued To	Issued By	Source	Status
dev.crt	7b2cf5a4-7bc9-4a08-be91-0eb29ccb642d	moxa-thingspro-device-intermediate	DLM device Enroll	Valid Sep 5, 2025, 04:56:43
default.crt	AIG Series Gateway Certificate for HTTPS	AIG Series Root CA for HTTPS	Web Server	Valid Dec 15, 2024, 11:36:01

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.



The screenshot shows the 'Accounts' management interface. The top header includes the MOXA logo, the device ID 'AIG-101-T', and the user 'Administrator admin'. A left sidebar contains a 'SECURITY' menu with options: Service Enablement, HTTP/HTTPS, Firewall, Certificate Center, Account Management (selected), Accounts, and Roles. The main content area shows a table of accounts with columns: Account, Role, and Status. There are four accounts listed: 'admin (you)' with role 'Administrator', 'justin', 'ricky', and 'lynn', all with 'Active' status. Search and Create buttons are at the top right.

Account	Role	Status
admin (you)	Administrator	Active
justin	justin	Active
ricky	ricky	Active
lynn	lynn	Active

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
<div style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center;">Create New Account</p> <p>Account Josh 4/16</p> <p>Role Administrator</p> <p style="color: red;">Password </p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p style="color: red; font-weight: bold;">! Contains at least 8 characters</p> <p style="font-size: small; color: green;">✓ Contains at least 1 number</p> </div> <p>Confirm Password </p> <p>Email - optional</p> <p style="text-align: right;">CANCEL SAVE</p> </div>	<div style="border: 1px solid #ccc; padding: 10px;"> <p style="text-align: center;">Create New Account</p> <p>Account Josh 4/16</p> <p>Role Administrator</p> <p>Password </p> <p style="color: green;">Confirm Password </p> <p>Email - optional</p> <p style="text-align: right;">CANCEL SAVE</p> </div>

Managing Existing User Accounts

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

Accounts			
Home > Security > Account Management > Accounts			
			Q SEARCH + CREATE
Account	Role	Status	
admin (you)	Administrator	Active	
justin	justin	Active	Edit
ricky	ricky	Active	Change Password

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.

Role Name	Accounts	Actions
Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	1 account	⋮
justin --	1 account	⋮
ricky --	1 account	⋮
lynn --	1 account	⋮
albert --	1 account	⋮

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

Create New Role

justin 6 / 30

Description - optional 0 / 100

Access Permissions

You must grant at least one privilege to this role.

- AWS IoT Core
- Azure IoT Device
- Moxa Service
- Modbus Master
- Modbus Slave
- MQTT Client
- Maintenance
- System Configuration
- Security
- Tag Hub

CANCEL SAVE

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

Roles		
Home > Security > Account Management > Roles		
		SEARCH + CREATE
Role Name		
Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	1 account	⋮
justin --	1 account	⋮

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**.

The screenshot shows the 'Protocol Status' page. It is divided into two sections: 'Northbound Protocols' and 'Southbound Protocols'. Under 'Northbound Protocols', there are three cards: 'AWS IoT Core' with a 'Disable' icon and a 'CHECK' button; 'Azure IoT Device' with a green 'OK' status and a 'CHECK' button; and 'MQTT Client' with a green 'OK' status and a 'CHECK' button. Under 'Southbound Protocols', there is one card: 'Modbus Master' with a yellow warning icon and a 'CHECK' button with a dropdown arrow.

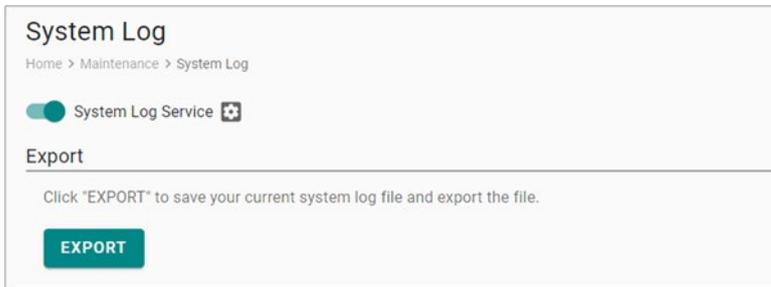
2. Click **START**.

The screenshot shows the 'Azure IoT Device' diagnostic page. At the top, there is a back arrow and the title 'Azure IoT Device'. Below the title, there is a breadcrumb 'Home > Maintenance > Protocol Status > Azure IoT Device' and a description: 'Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to Azure IoT Device'. A table follows with columns: 'Service Name', 'Connection Status', and 'Last Upload Status'. The table contains one row for 'Azure IoT Device' with status 'Connected' (green checkmark) and 'Success' (green checkmark). Below the table, there is an 'Advanced Diagnostic' section with a black background and two buttons: 'START' (in a blue box) and 'EXPORT' (with a download icon).

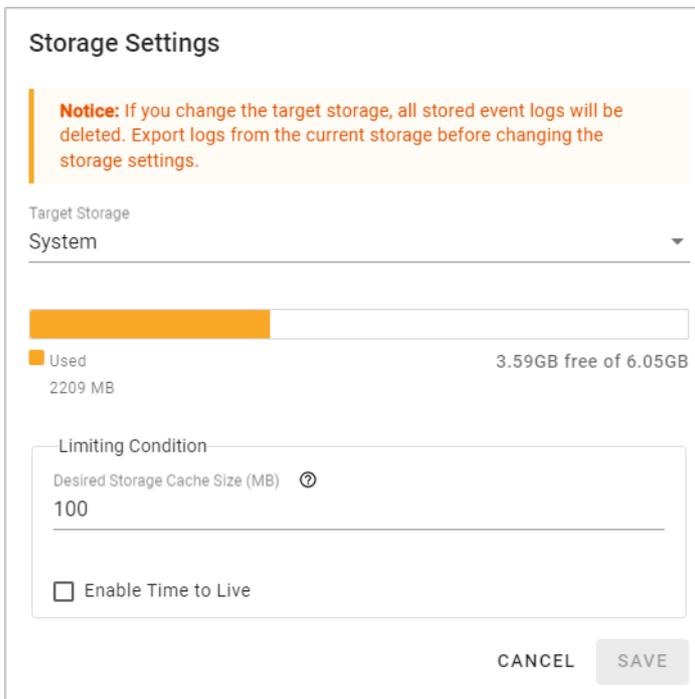
System Log

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.



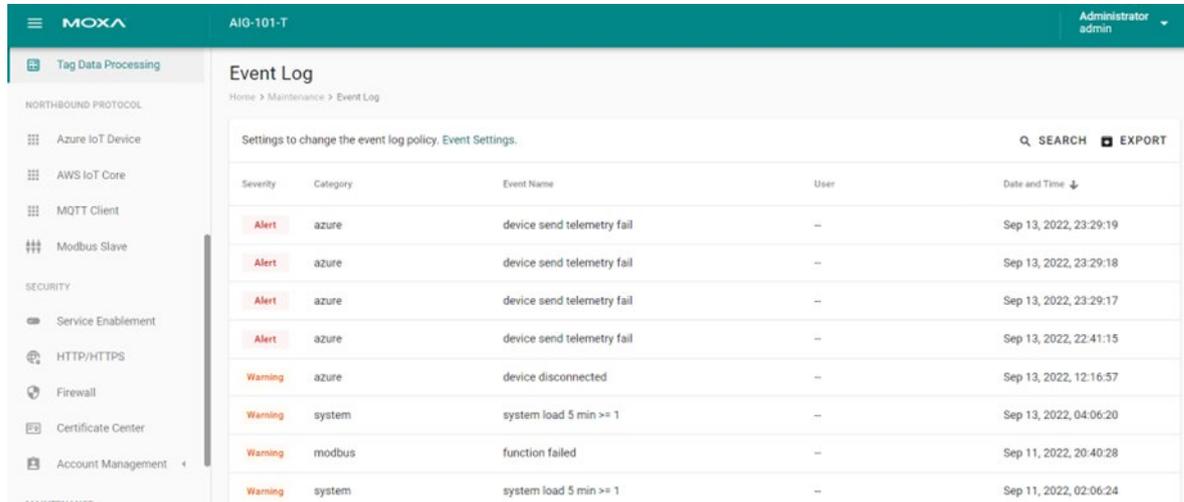
Click  to specify the location to store the event logs. To optimize the use of storage space on your AIG, you can check the Enable **Time to Live** option and specify the maximum storage space for the system logs. Click **SAVE** to confirm your settings.



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.

← Event Settings

Home > Maintenance > Event Log > event settings

Event Log Service

Event Index

Log data only for the selected events will persist into the storage.

All events Severity: Alert Severity: Warning Severity: Info

aws

- device connected
- device connection failed
- device disconnected
- device send telemetry

azure

1 - 73 of 73, Selected: 44

SAVE

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.

Storage Settings

Notice: If you change the target storage, all stored event logs will be deleted. Export logs from the current storage before changing the storage settings.

Target Storage

System

Used 2209 MB 3.59GB free of 6.05GB

Limiting Condition

Desired Storage Cache Size (MB)

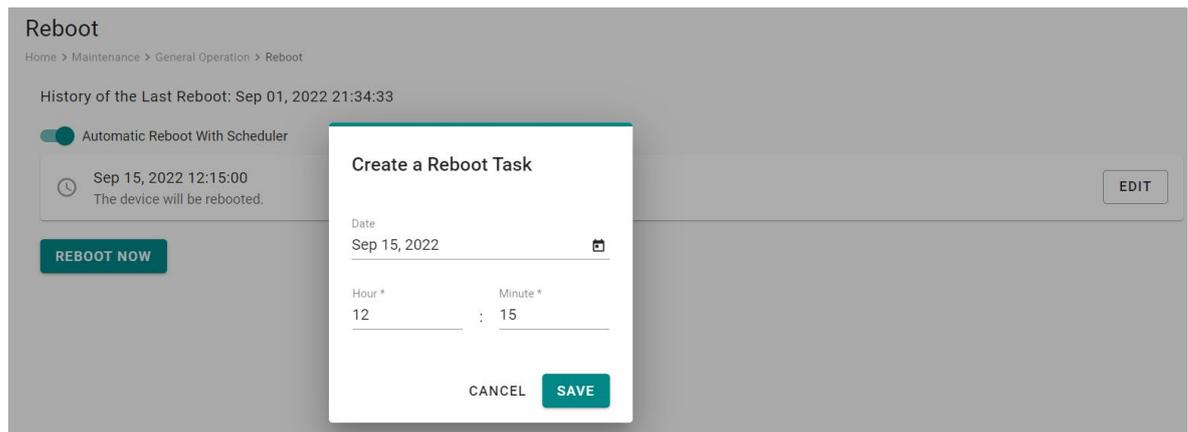
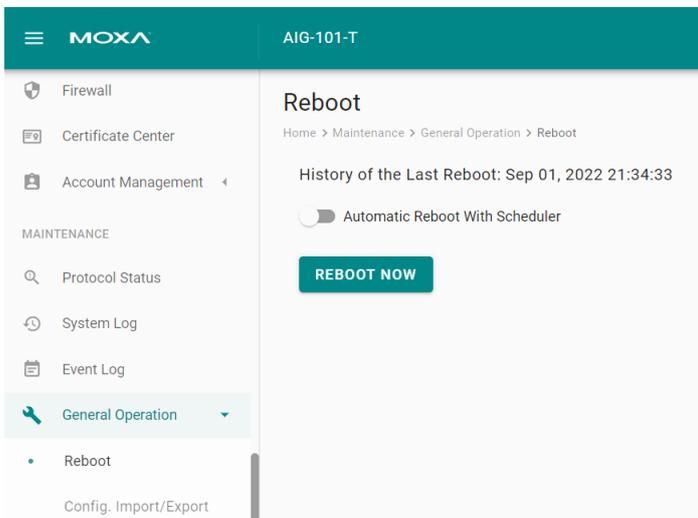
100

Enable Time to Live

CANCEL SAVE

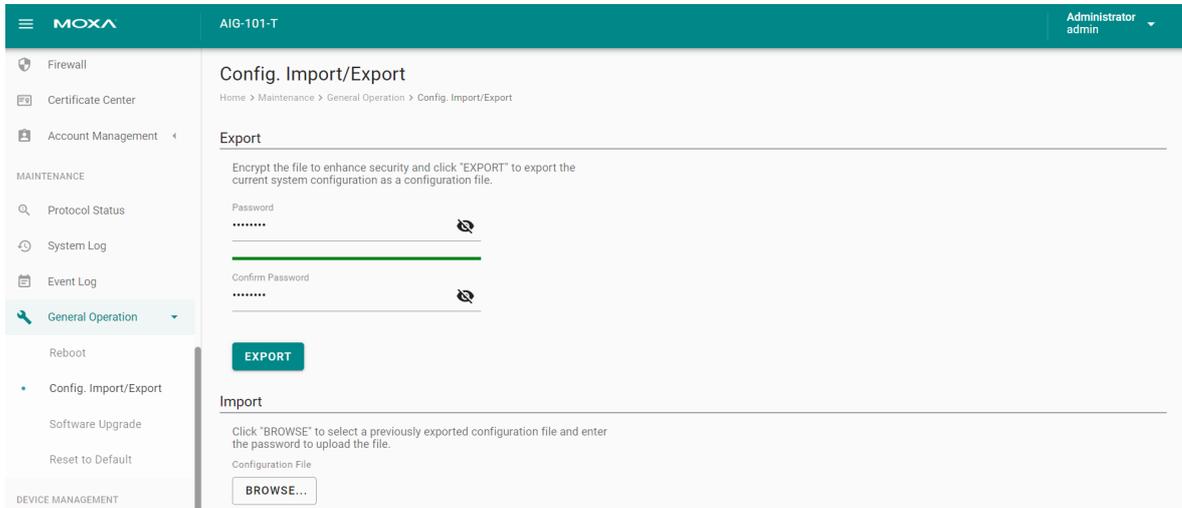
General Operation—Reboot

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.



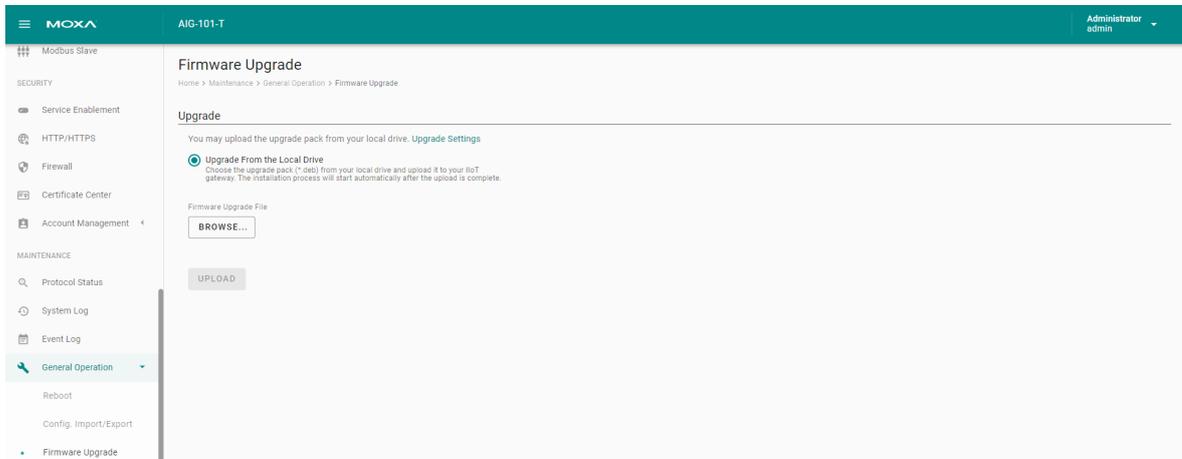
General Operation - Config. Import/Export

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

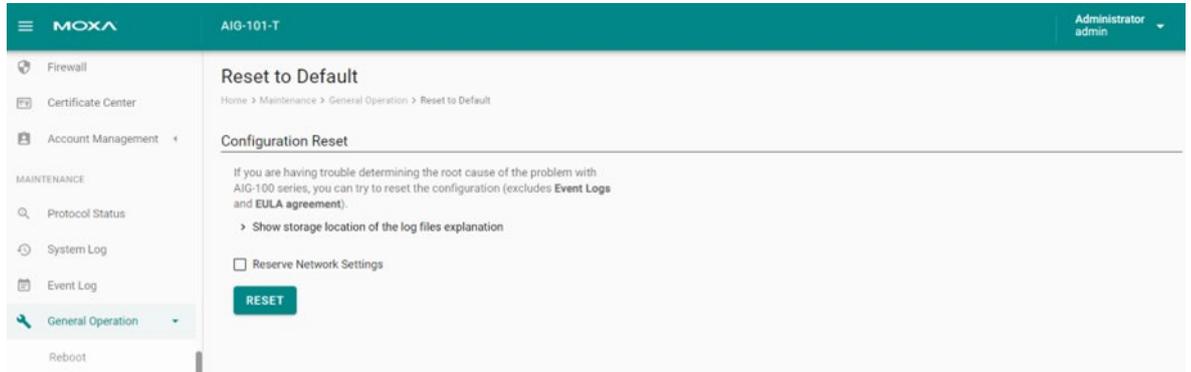
Go to **General Operation > Firmware Upgrade** to upgrade this device with Moxa's software packages. Click **BROWSER** and select the software package file in *.deb file format on your computer, then click **UPLOAD**.



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).

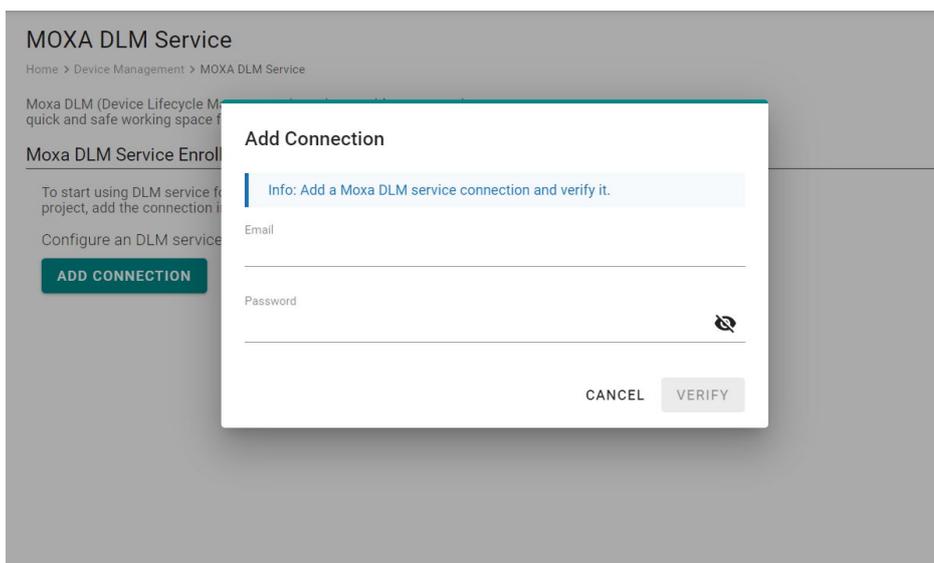
Device Management

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 the **Moxa DLM Service** to register the product to go 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.

MOXA DLM Service
Home > Device Management > MOXA DLM Service

Moxa DLM (Device Lifecycle Management) service provides a convenient, quick and safe working space for you to manage AIG Series.

Moxa DLM Service Enrollment

To start using DLM service for the device and connect to the DLM service project, add the connection in the device and select a project to enroll.

Configure an DLM service connection

Moxa DLM service connection

Verified

Email: joshua.lin@moxa.com

Password:

EDIT

Enrollment setting

Project Name
AIG-101 Demo

ENROLL

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

MOXA DLM Service
Home > Device Management > MOXA DLM Service

Moxa DLM (Device Lifecycle Management) service provides a convenient, quick and safe working space for you to manage AIG Series.

Moxa DLM Service Enrollment

To start using DLM service for the device and connect to the DLM service project, add the connection in the device and select a project to enroll.

Configure an DLM service connection

Moxa DLM service connection

Verified

Email: joshua.lin@moxa.com

Password:

EDIT

Enrollment setting

Project Name
AIG-101 Demo

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.

MOXA DLM Service

Home > Device Management > MOXA DLM Service

Moxa DLM service

Project Name	Status
AIG-101 Demo	<input type="radio"/> Disconnect

Moxa DLM Service Certificate

Moxa DLM service certificate is a leaf X.509 certificate which issued by Moxa DLM service and allow device to connect with.

dev.crt

Verified

Issued By: moxa-thingspro-device-intermediate
Expires: Oct 30, 2025 07:24:22
Organization: Moxa Inc.

Model Name: AIG-101-T
MAC Address: 0090E8010131
Serial Number: TAAIG1010401

5. Log in to the Moxa DLM Service. You will see the AIG online and you can manage it.

All Devices

Home > Projects > All Devices

Connected Status:online × REFRESH

<input type="checkbox"/>	Serial Number	Model Name	Host Name	Connection Status	Labels
<input type="checkbox"/>	TAAIG1010401	AIG-101-T	Moxa	Online Connected on Oct 13, 2022 11:31:46	-

Items per page: 10 1 - 1 of 1