

AIG-301 Series User Manual

Version 2.1, November 2024

www.moxa.com/products

MOXA[®]

© 2024 Moxa Inc. All rights reserved.

AIG-301 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

© 2024 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 Serial Devices	5
Connecting to a Network	5
Access to the Web Console	6
3. Web Console	7
Dashboard	7
System Dashboard	7
Network Dashboard	7
System Configuration	9
System Settings—General	9
System Settings—IP Address	10
System Settings—Cellular	11
System Settings—HTTP/HTTPS	13
System Settings—Serial	14
System Settings—I/O	15
System Settings—DHCP Server	16
System Settings—Wi-Fi	17
Protocol	18
Modbus Master	18
Modbus TCP Slave	31
OPC UA Server	37
Edge Computing	41
Function Management	41
Tag Management	42
Cloud Connectivity	44
Azure IoT Edge	44
Azure IoT Device	49
AWS IoT Core	53
Generic MQTT Client	57
Sparkplug	61
Moxa DLM Service	68
Security	70
Certificate Center	70
Firewall	70
OpenVPN Client	74
Account Management	75
Maintenance	78
Protocol Status	78
General Operation	80
Diagnostic	84
A. Appendix	87
Publish Mode	87
B. Additional Documentation	88
Software Downloads	88
Technical Documentation	88
OpenAPI Documentation	88

1. Introduction

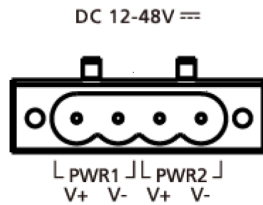
Overview

The AIG-301 Series advanced IIoT gateways are designed for Industrial IoT applications, especially for distributed and unmanned sites in harsh operating environments. AIG-301 series has implemented Modbus RTU/TCP master/client protocols which can help you to collect Modbus devices. Moreover, Azure IoT Edge software is preloaded and seamlessly integrated with the AIG-301 to enable easy, reliable, yet secure sensor-to-cloud connectivity for data acquisition and device management using the Azure Cloud solution. With the use of the ThingsPro Proxy utility, the device provisioning process is easier than ever. Thanks to the robust OTA function, you never have to worry about system failure during software upgrades. With the Secure Boot function enabled, you can prevent malicious software injection during the bootup process.

2. Getting Started

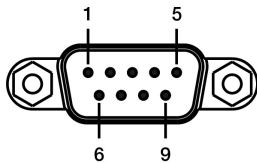
Connecting the Power

Connect the power jack (in the package) to the DC terminal block (located on the top panel), and then connect to a power line with range 12 to 48 VDC. It takes about 3 minutes for the system to boot up. Once the system is ready, the Power LED will light up. All models support dual power inputs for redundancy.



Connecting Serial Devices

The AIG device supports connections to Modbus serial devices. The serial port uses the DB9 male connector and 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	-	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 AIG's 10/100/1000M Ethernet port and the other end of the cable to the Ethernet network. The AIG will indicate a valid connection to the Ethernet by the LAN1/LAN2 LED maintaining solid green/yellow color. For details on the behavior of the LEDs, refer to the *AIG-301 Series Quick Installation Guide*.

Access to the Web Console

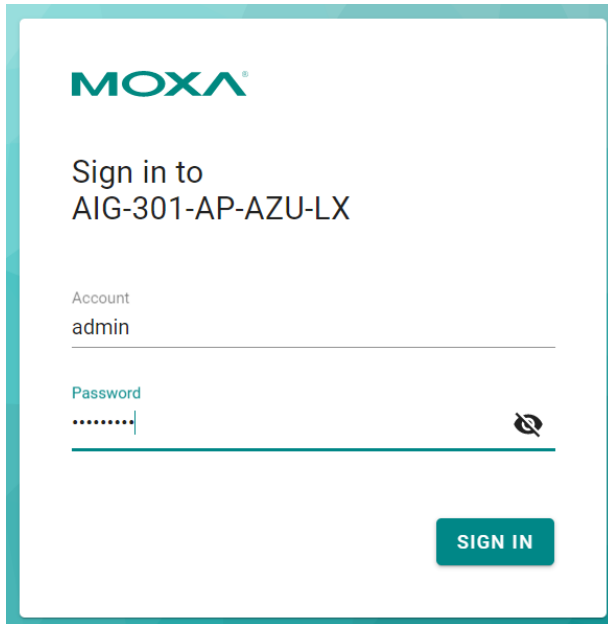
The default LAN2 IP address to access the web console of the AIG is 192.168.4.127.

To use the default IP address to access the AIG, do the following:

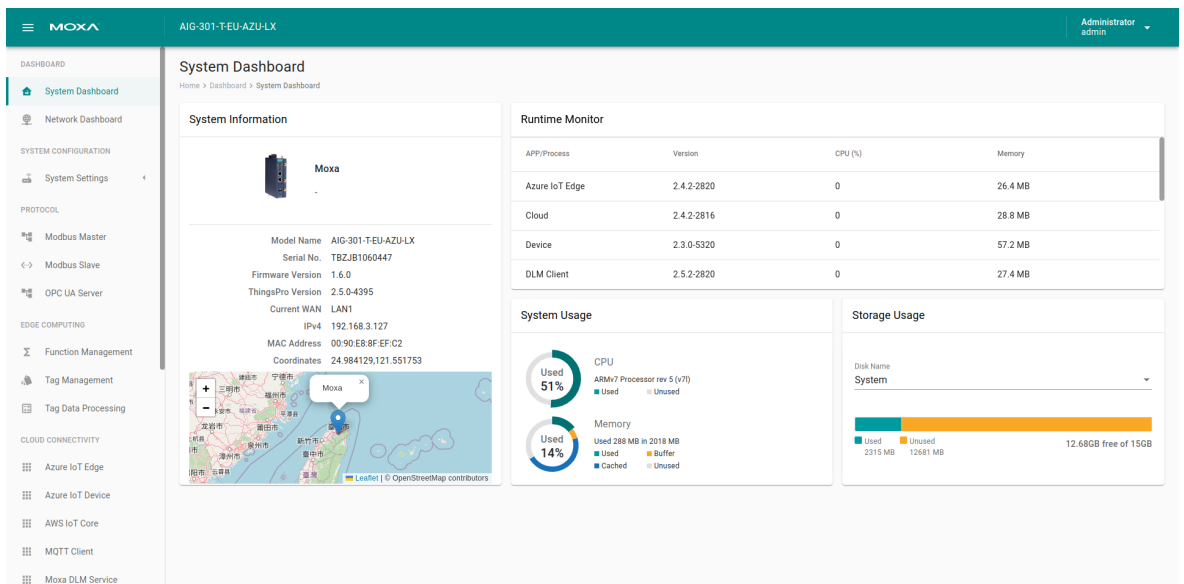
1. Ensure your host and the AIG are in the same subnet (AIG's default subnet mask is 255.255.255.0). Connect to LAN2 and enter **https://192.168.4.127:8443** in your web browser.
2. Enter the account and password information.

Default account: **admin**

Password: **admin@123**



You will see the following homepage after logging in successfully.



System Dashboard

Home > Dashboard > System Dashboard

System Information

Moxa

Model Name: AIG-301-T-EU-AZU-LX
Serial No.: TBZJB1060447
Firmware Version: 1.6.0
ThingsPro Version: 2.5.0-4395
Current WAN: LAN1
IPv4: 192.168.3.127
MAC Address: 00:90:E8:8F:EF:C2
Coordinates: 24.984129,121.551753

Runtime Monitor

APP/Process	Version	CPU (%)	Memory
Azure IoT Edge	2.4.2-2820	0	26.4 MB
Cloud	2.4.2-2816	0	28.8 MB
Device	2.3.0-5320	0	57.2 MB
DLM Client	2.5.2-2820	0	27.4 MB

System Usage

CPU: ARMv7 Processor rev 5 (v7) - Used 51% / Unused

Memory: Used 288 MB in 2016 MB - Used 14% / Buffer / Unused

Storage Usage

Disk Name: System

Used: 2315 MB | Unused: 12691 MB | 12.68GB free of 15GB

3. Web Console

Dashboard

System Dashboard

This page gives you an overview of the gateway’s system status. Basic system information such as model name, serial No., and firmware version are displayed. In addition, Storage Usage provides information on the unused storage on the system or on the SD card. Ensure that you provide accurate information when entering data so that it is useful during troubleshooting system issues.

The screenshot shows the Moxa System Dashboard web console. The top navigation bar includes the Moxa logo, the device model 'AIG-301-T-EU-AZU-LX', and the user 'Administrator admin'. The left sidebar contains navigation options: System Dashboard, Network Dashboard, System Configuration (System Settings), Protocol (Modbus Master, Modbus Slave, OPC UA Server), Edge Computing (Function Management, Tag Management, Tag Data Processing), and Cloud Connectivity (Azure IoT Edge, Azure IoT Device, AWS IoT Core, MQTT Client, Moxa DLM Service). The main content area is titled 'System Dashboard' and includes: 'System Information' with a Moxa device image and details (Model Name: AIG-301-T-EU-AZU-LX, Serial No.: TBZJ1060447, Firmware Version: 1.6.0, ThingsPro Version: 2.5.0-4395, Current WAN: LAN1, IPv4: 192.168.3.127, MAC Address: 00:90:E8:8F:EF:C2, Coordinates: 24.984129,121.551753) and a map; 'Runtime Monitor' table; 'System Usage' charts for CPU (51% used) and Memory (14% used); and 'Storage Usage' bar chart.

APP/Process	Version	CPU (%)	Memory
Azure IoT Edge	2.4.2-2820	0	26.4 MB
Cloud	2.4.2-2816	0	28.8 MB
Device	2.3.0-5320	0	57.2 MB
DLM Client	2.5.2-2820	0	27.4 MB

Category	Used	Unused
CPU	51%	49%
Memory	14%	86%

Storage Usage: System disk usage is 2315 MB used, 12681 MB unused, with 12.680GB free of 15GB total.



CAUTION

Some AIG functions utilize storage space (e.g., Store and Forward, Backup Logging and Event/System.) Hence, we recommend allocating storage space reasonably so that **the total of all the maximum storage settings does not exceed the remaining available storage. Otherwise, the functions may not work properly.**

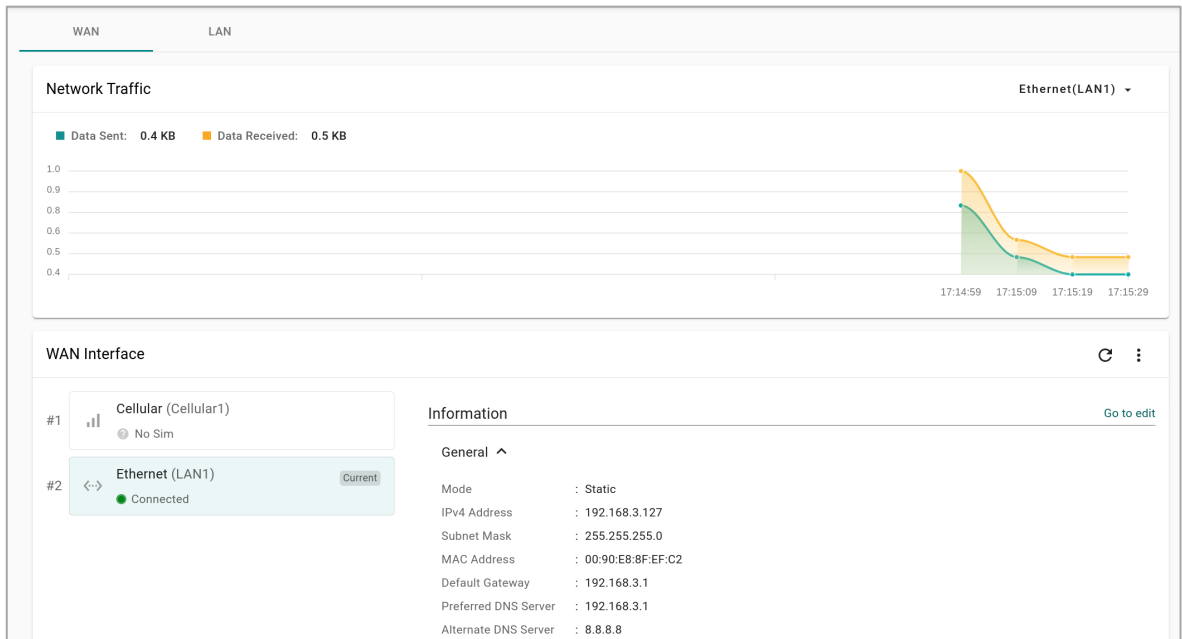
Network Dashboard

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' dashboard. It features a 'Network Status' section with a diagram showing the 'Moxa Device' connected to the 'Network', which is in turn connected to the 'Internet'. A green checkmark and the text 'Connected to the Internet' are displayed below the diagram.

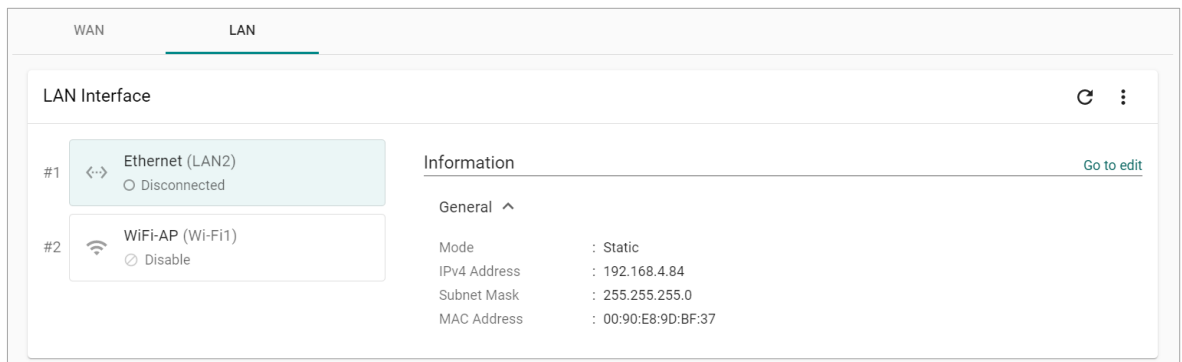
WAN

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.

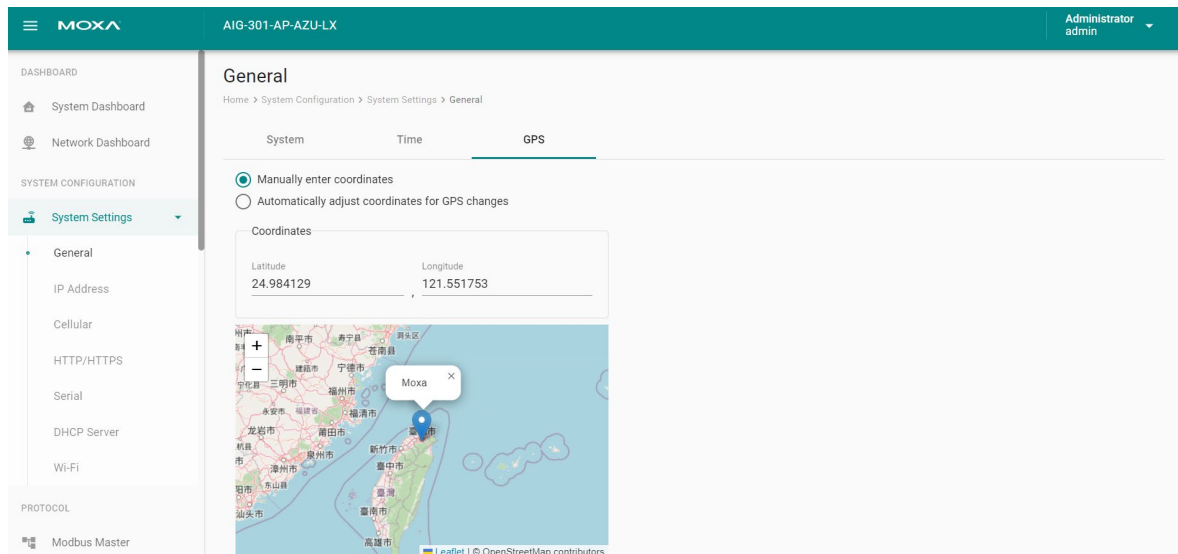
Parameter	Value	Description
Server/Host Name	Alphanumeric string	You can enter a name to identify the unit, such as a name that includes the function
Description - optional	Alphanumeric string	You can enter a description to help identify the unit location such as "Cabinet A001."

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: Enter the time parameters Auto: Automatically sync with time source. NTP and GPS can be selected as the source. 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	The time interval to sync with the time source
Source	NTP Server GPS	The way to sync with 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:

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

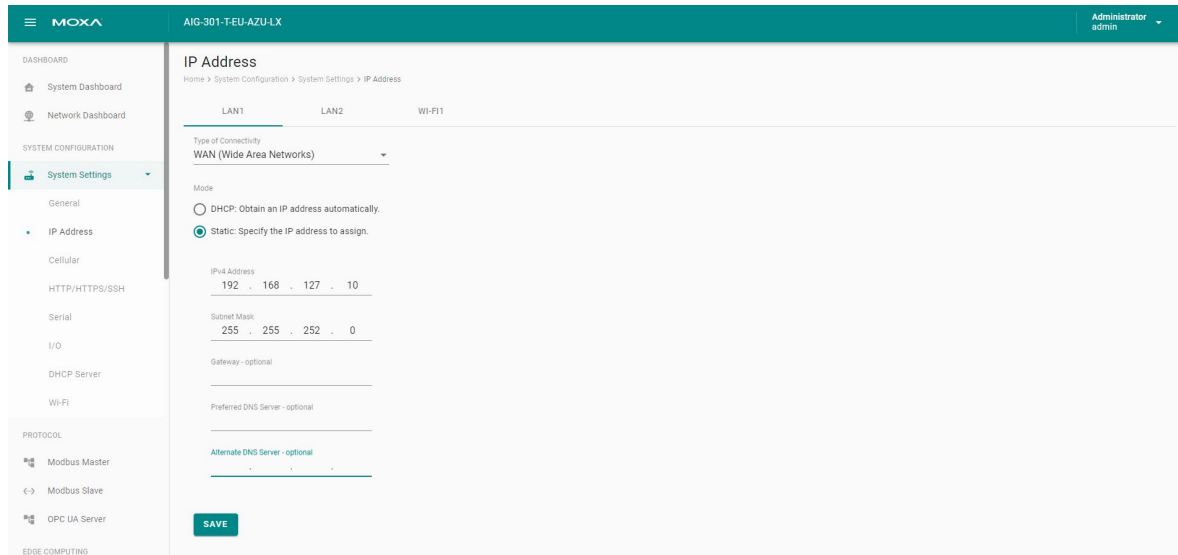


System Settings—IP Address

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: LAN2 does not support WAN.	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: DHCP LAN2 default: 192.168.4.127 (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.

The screenshot shows the MOXA web interface for the AIG-301-T-AP-AZU-LX device. The left sidebar contains navigation options like Dashboard, System Configuration, and Protocol. The main content area is titled 'Cellular' and includes a breadcrumb trail: Home > System Configuration > System Settings > Cellular. The 'CELLULAR1' section has a checked checkbox for 'Enable cellular data communication'. Below this is the 'Profile Settings' section, which includes a 'Network Type' dropdown set to 'Auto', a 'Connection Retry Timeout (sec)' field set to '120', and a 'Mode' section with 'Auto' selected (radio button) and 'Manual' unselected. The 'Check-alive' section has a checked checkbox for 'Enable check-alive' and a sub-section with an unchecked checkbox for 'Reboots the device when pings to the target host fail continuously for a specified time interval'. The 'Target Host' is '8.8.8.8' and the 'Ping Interval (sec)' is '60'. A 'SAVE' button is at the bottom.

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

APN Type
Static

APN
internet

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 device when pings 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

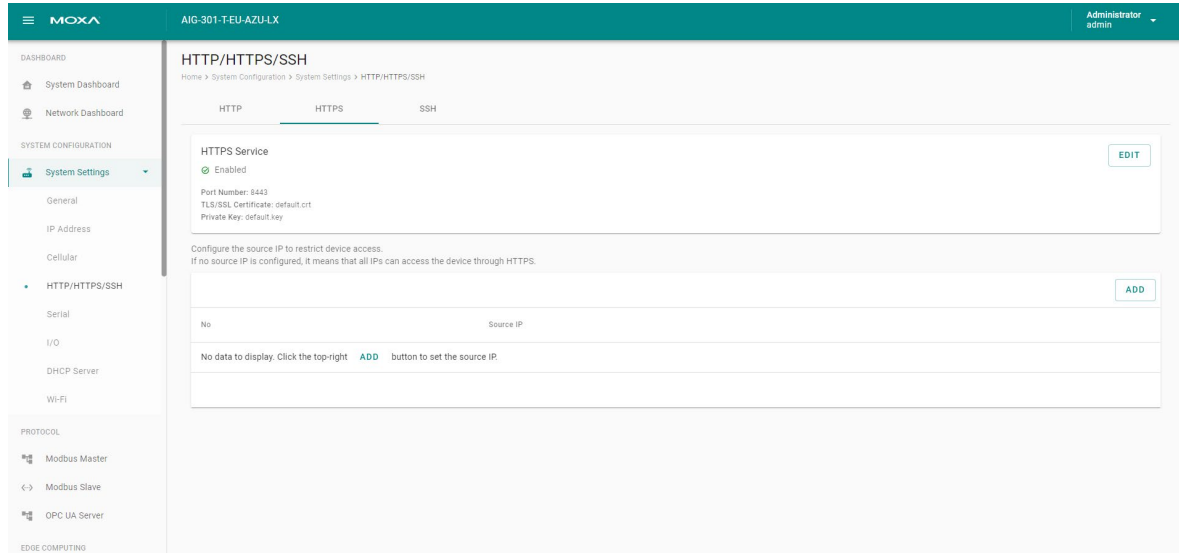
INFO: The Reboot Timer should be higher than ((total connection retry timeout) * (number of profiles)) to avoid the device from being rebooted before all the profiles are used.

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

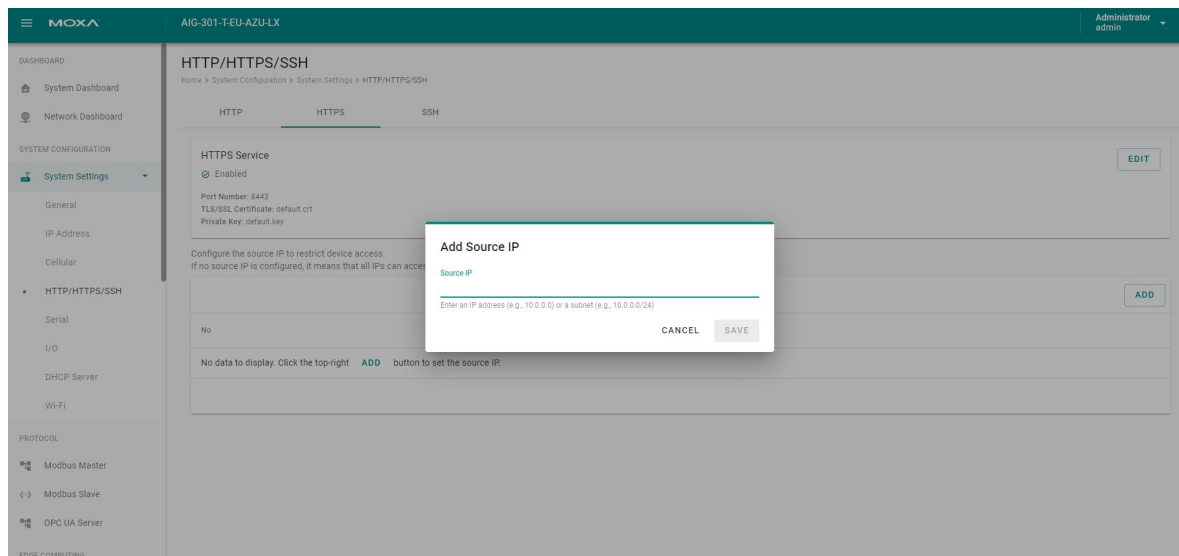
System Settings—HTTP/HTTPS

To ensure secure access to the web console of the device, we strongly recommend disabling HTTP and enabling HTTPS on the **System Settings > HTTP/HTTPS/SSH** page.

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 can generate a “AIG Series Root CA for HTTPS” certificate.



Furthermore, you can create a whitelist for allowing access to HTTP, HTTPS, and SSH connections. The maximum capacity of the whitelist is 10 entries.

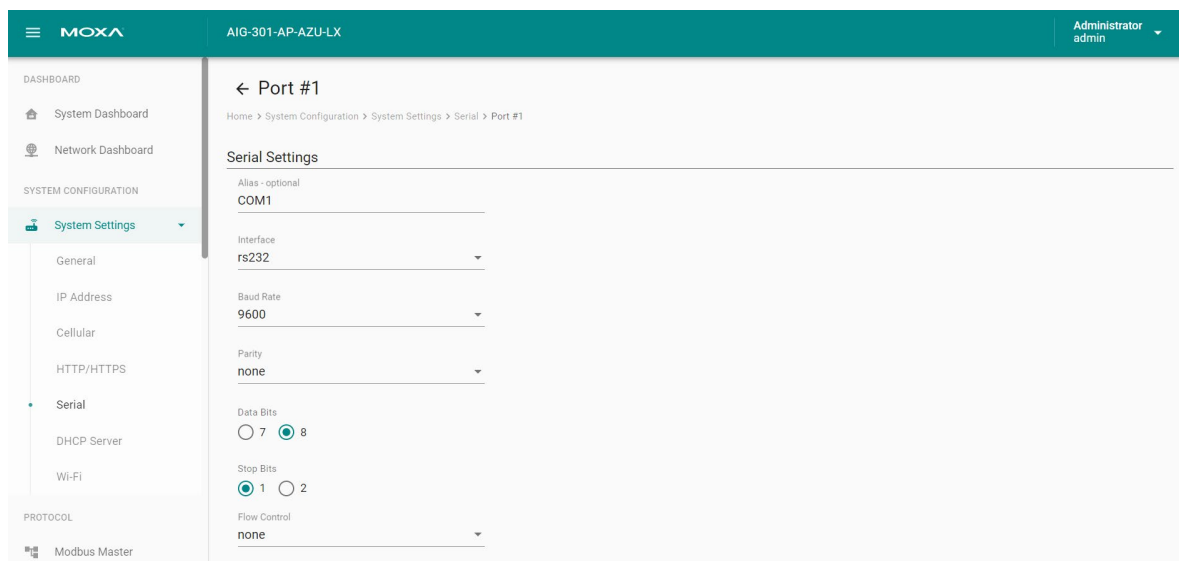
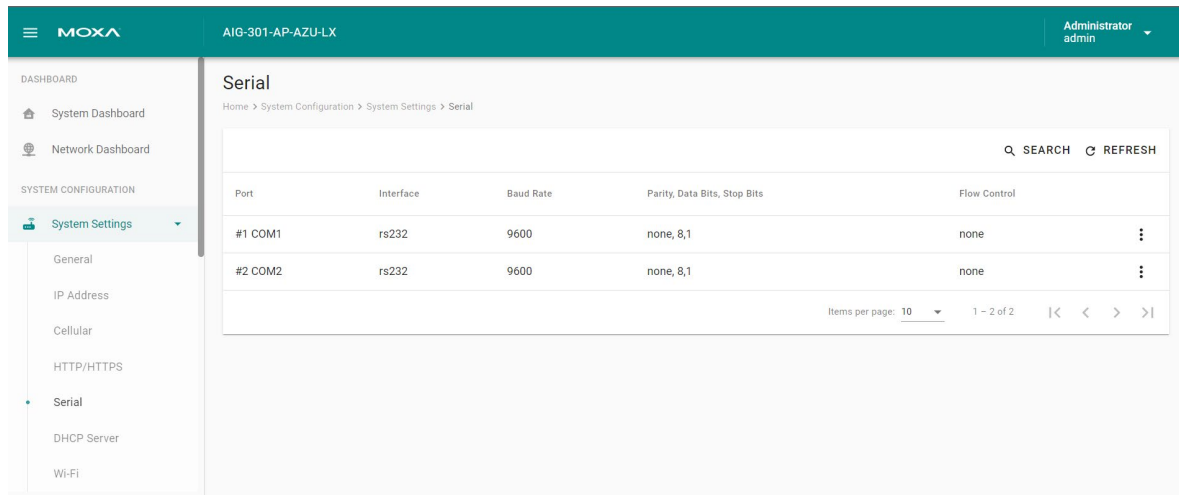


System Settings—Serial

Go to **System Settings > Serial** to view and configure serial parameters.

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.

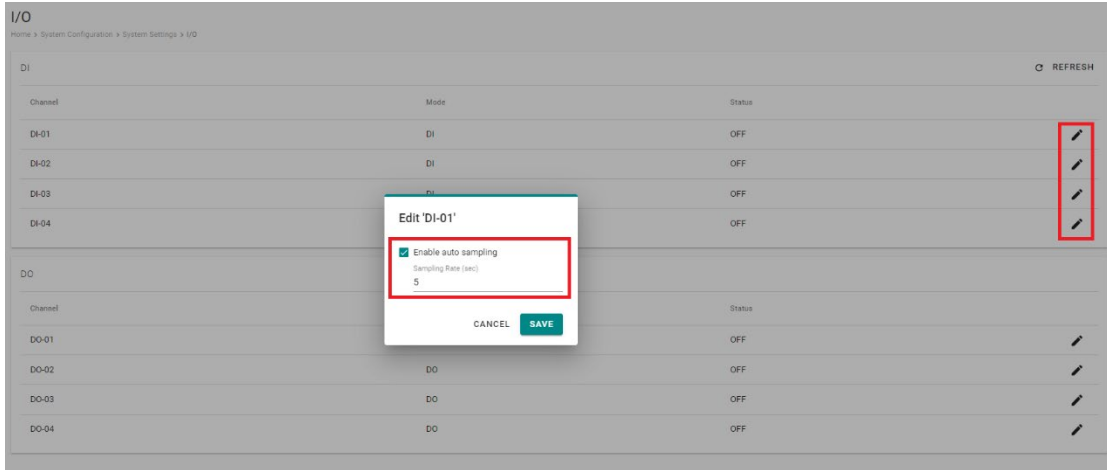


Parameter	Value	Description
Interface	rs232 rs422 rs485-2w rs-485 4w	
Baud Rate	300 to 921600	
Parity	none, odd, even, space, mark	
Data Bits	7, 8	
Stop Bits	1, 2	
Flow Control	none hardware software	Hardware: Flow control by RTS/CTS (for RS-232) Software: Flow control by XON/XOFF (for RS-232/422/485-4W)

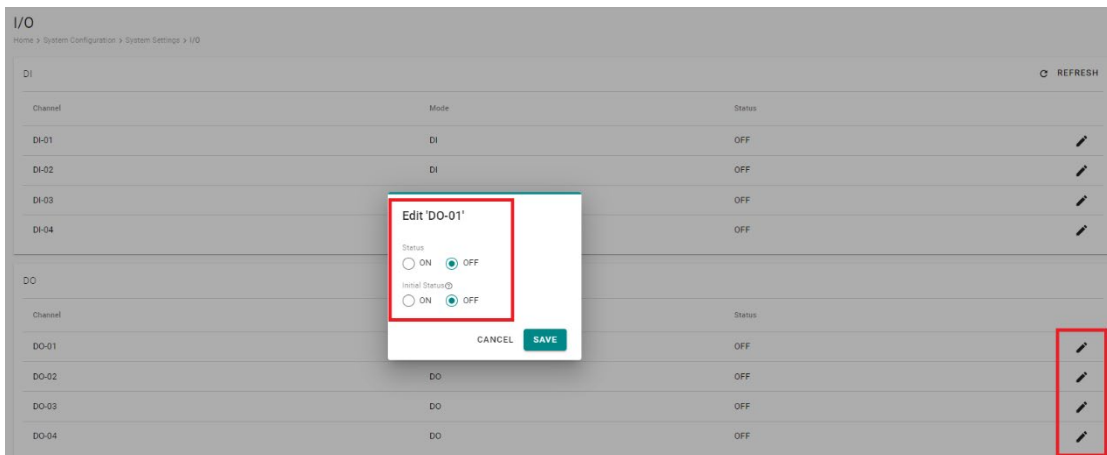
System Settings—I/O

The AIG-301 comes with 4 digital inputs (DIs) and 4 digital outputs(DOs). Tags are generated for all DI/DO interfaces which can be accessed through the tag hub.

To activate a DI, just click on the edit icon, enable auto sampling, and input sampling rates according to your requirements.



For DOs, clicking on the edit icon allows you to configure the status and initial status settings.



Parameter	Value	Description
Status	ON	High voltage
	OFF	Low voltage

System Settings—DHCP Server

Go to **System Settings > DHCP Server** to view the DHCP settings.

To configure DHCP server settings, do the following:

1. Check **Enable DHCP Server**.
2. Input **IP Address Range** parameters.
3. (Optional) Input DNS.
4. Specify **Lease Time**.
5. Click **SAVE**.
6. (Optional) input Domain Name.

The screenshot shows the MOXA network management interface for device AIG-301-AP-AZU-LX. The user is logged in as Administrator admin. The main menu on the left includes Network Dashboard, SYSTEM CONFIGURATION, System Settings, General, IP Address, Cellular, HTTP/HTTPS, Serial, DHCP Server (selected), and Wi-Fi. Under SYSTEM CONFIGURATION, there are sections for PROTOCOL (Modbus Master, OPC UA Server) and EDGE COMPUTING (Function Management). The DHCP Server configuration page is displayed, showing tabs for LAN1, LAN2, and WI-FI. The LAN1 tab is active. The Server Status is 'Stopped'. There is an unchecked checkbox for 'Enable DHCP Server'. An information box states: 'Info: The DHCP Server setting is only for LAN and static IP interfaces. You can change the settings using IP settings'. The IP Address Range section shows Start IP: 192 . 168 . 3 . 200, End IP: 192 . 168 . 3 . 250, and Netmask: 255 . 255 . 255 . 0. The DNS section shows Primary DNS - optional: 8 . 8 . 8 . 8.



NOTE

The DHCP server service is only available on LAN and static IP interfaces.

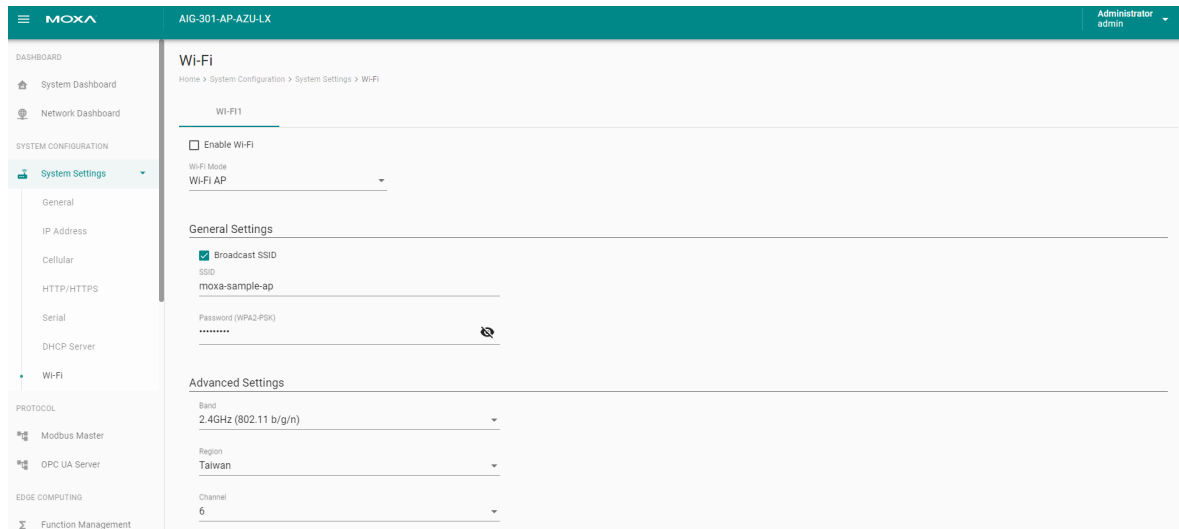
System Settings—Wi-Fi

Go to **System Settings > Wi-Fi** to view the Wi-Fi settings.

To configure Wi-Fi settings, check **Enable Wi-Fi** and select the **Wi-Fi Mode** (Wi-Fi AP / Wi-Fi Client), then do the following:

If the Wi-Fi AP is Selected

1. Disable/enable **Broadcast SSID**.
2. Input the **SSID** and **Password** for the Wi-Fi AP.
3. Specify the **Region**, **Channel** in the advanced settings.
4. Click **SAVE**.



NOTE

The maximum number of Wi-Fi clients allowed is 2.

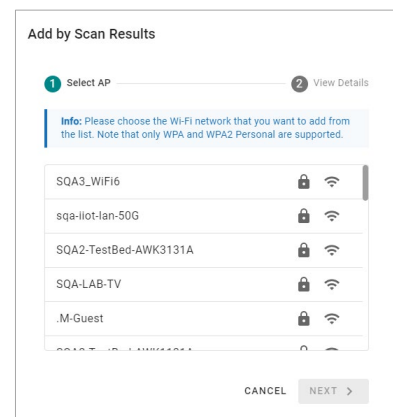
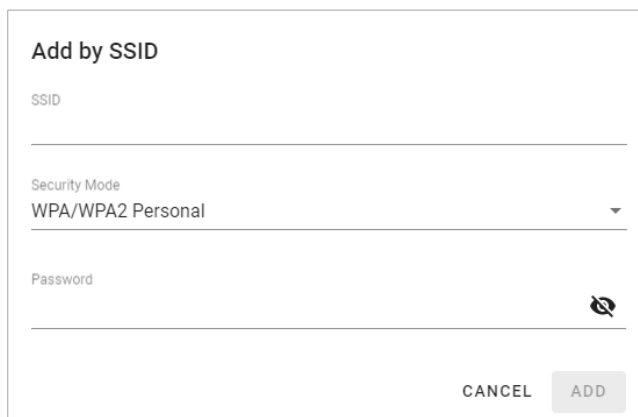


NOTE

The Wi-Fi AP mode serves as a dedicated troubleshooting feature, enabling users to conveniently access the web console or SSH for diagnostic purposes.

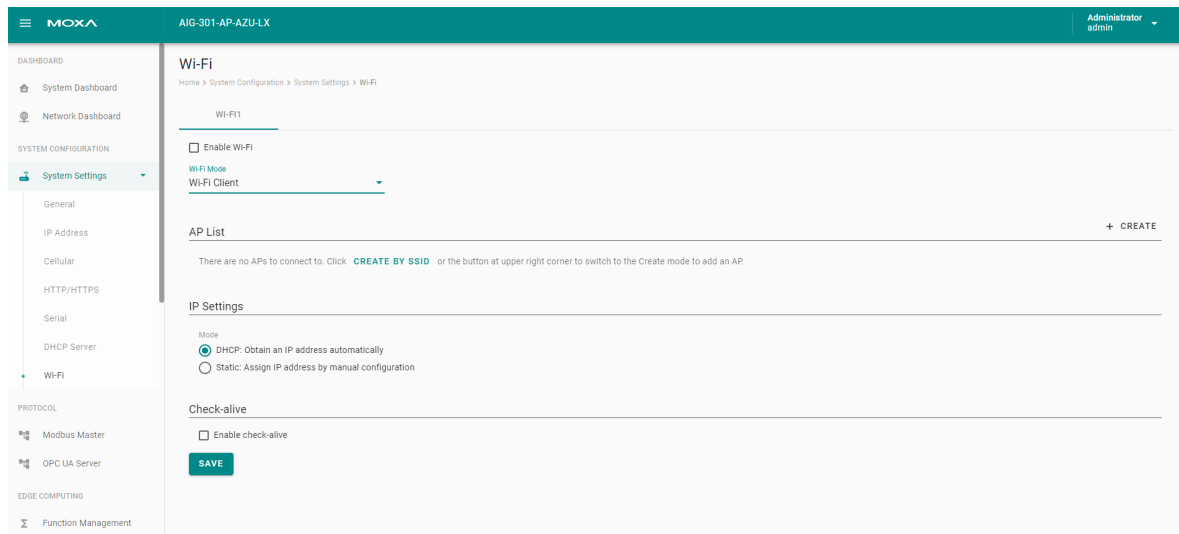
If the Wi-Fi Client is Selected

1. Click **+CREATE** to manually **Create by SSID** or be **Created by Scan Results**.



2. Select **DHCP** or **Static mode**.

3. Check **Check-alive** function which can be used to ensure Internet connectivity.
4. Click **SAVE**.



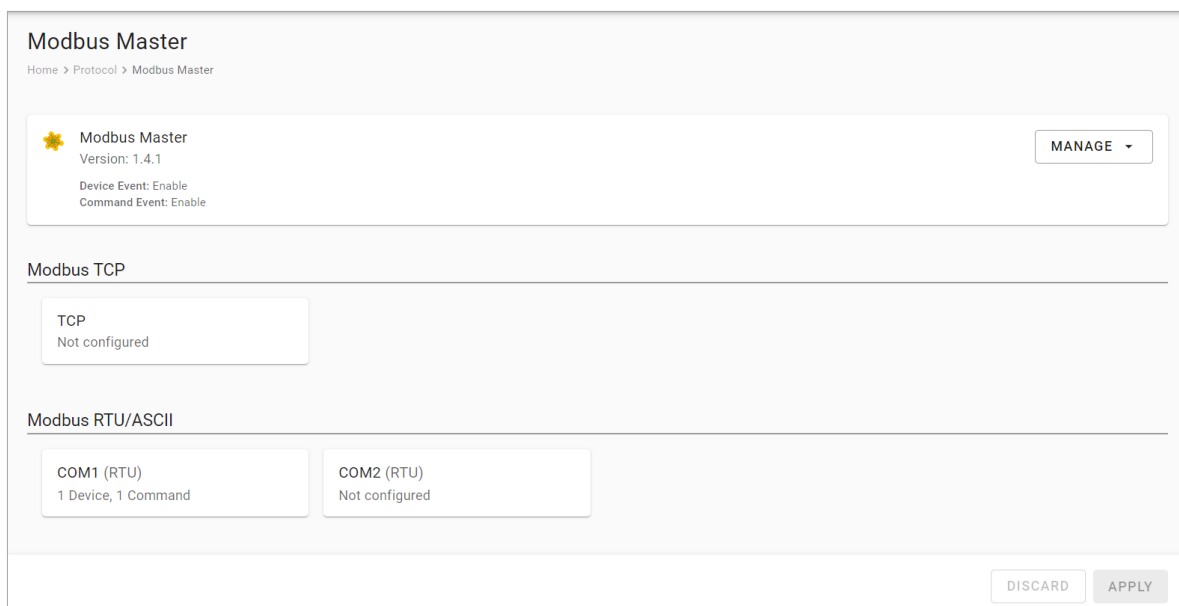
Protocol

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:

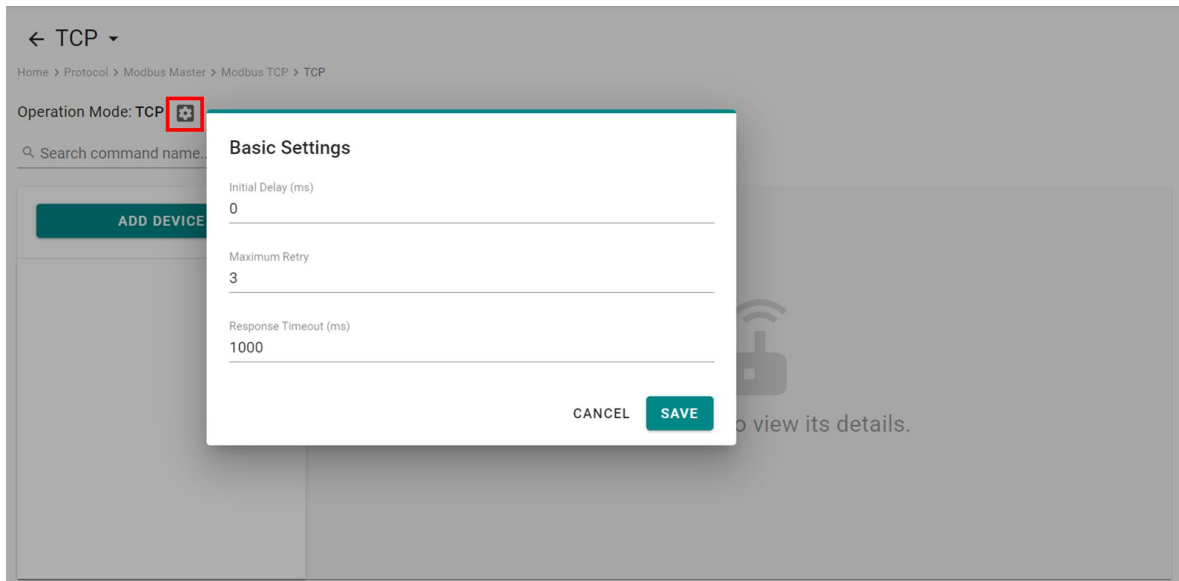
1. Click **TCP** under Modbus TCP or **COMx** under Modbus RTU/ASCII.
2. Click **ADD DEVICE** and go to the 3-step wizard page.
3. Input **device name, slave ID, IP Address,** and **TCP port,** then press **NEXT**.
4. Click **+ ADD COMMAND** to add Modbus commands to collect the data, then press **NEXT**.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

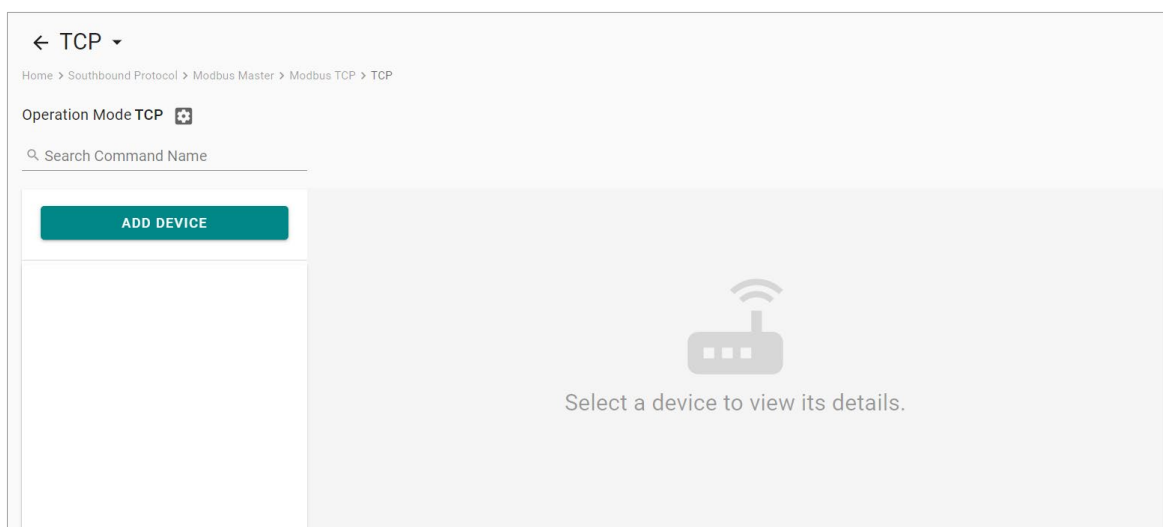
When you access the Modbus TCP setting page, you will first need to configure the basic settings.



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	Use this to configure the number of times AIG will retry to communicate with the Modbus detail 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	-	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
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	pause	The defined value of the Status Term will be effective when a read command encounters an error or times out.
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.

← 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 the settings and click **DONE** to apply them.

← 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

AIG 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 + ADD COMMAND **IMPORT** **EXPORT**

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

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 + ADD COMMAND **IMPORT** **EXPORT**

SE_Meter
Enable
Slave IP: 192.168.127.100
Slave Port: 502
Slave ID: 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

Trigger	Poll Interval (ms)	Enable
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 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

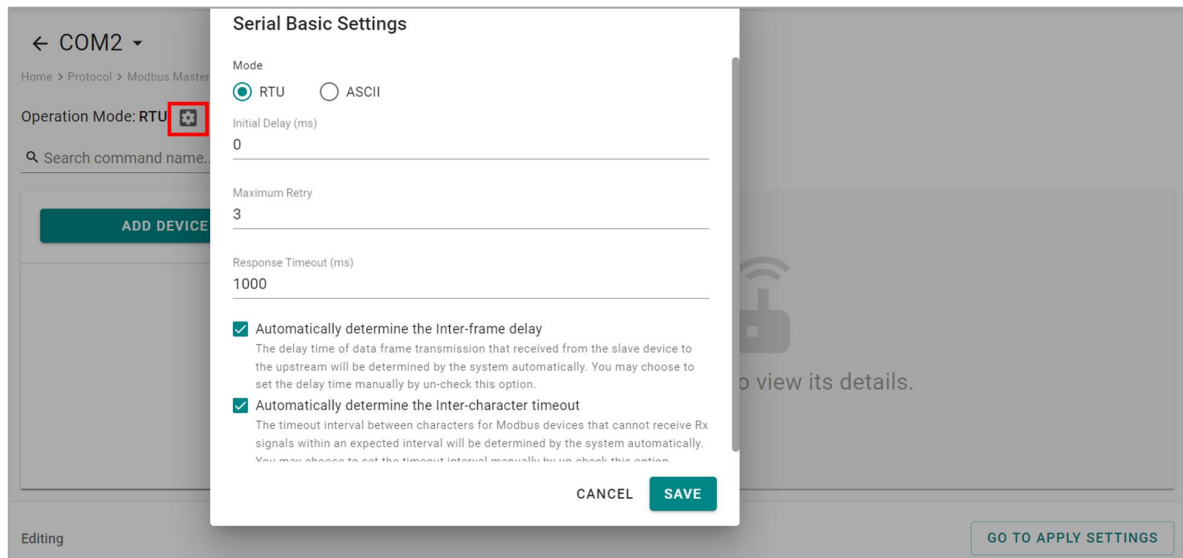
COM2 (RTU)
Not configured

Editing DISCARD **APPLY**

Modbus RTU/ASCII

Basic Settings

When you access the Modbus RTU/ASCII settings page, you will first need to configure the 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 the number of 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 cannot 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 step-by-step through the configuration process.

Step 1. Basic Settings

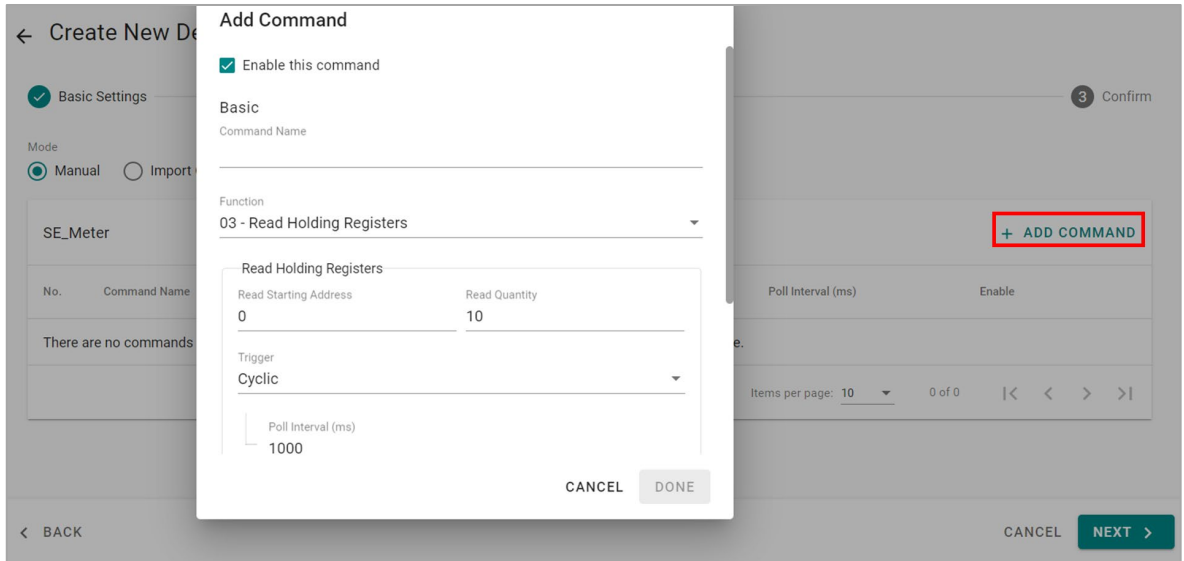
Fill in the basic parameters for the Modbus RTU/ASCII device.

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

Parameter	Value	Default	Description
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
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.
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	pause	The defined value of the Status Term will be effective when the read command encounters an error or times out.
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

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 the settings and click **DONE** to apply them.

← 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_Meter1
Slave ID: 1
Status: Enable
Number of Commands: 1

< BACK CANCEL DONE

AIG 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.

Modbus Master

Home > Protocol > Modbus Master

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

Modbus TCP

TCP
1 Device, 1 Command

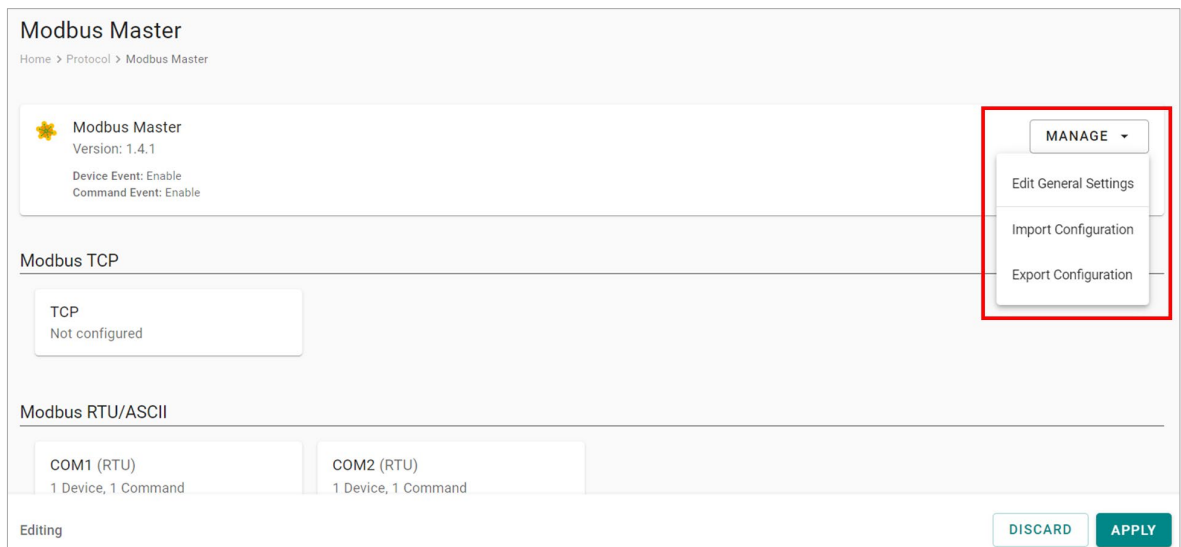
Modbus RTU/ASCII

COM1 (RTU) COM2 (RTU)
1 Device, 1 Command Not configured

Editing DISCARD **APPLY**

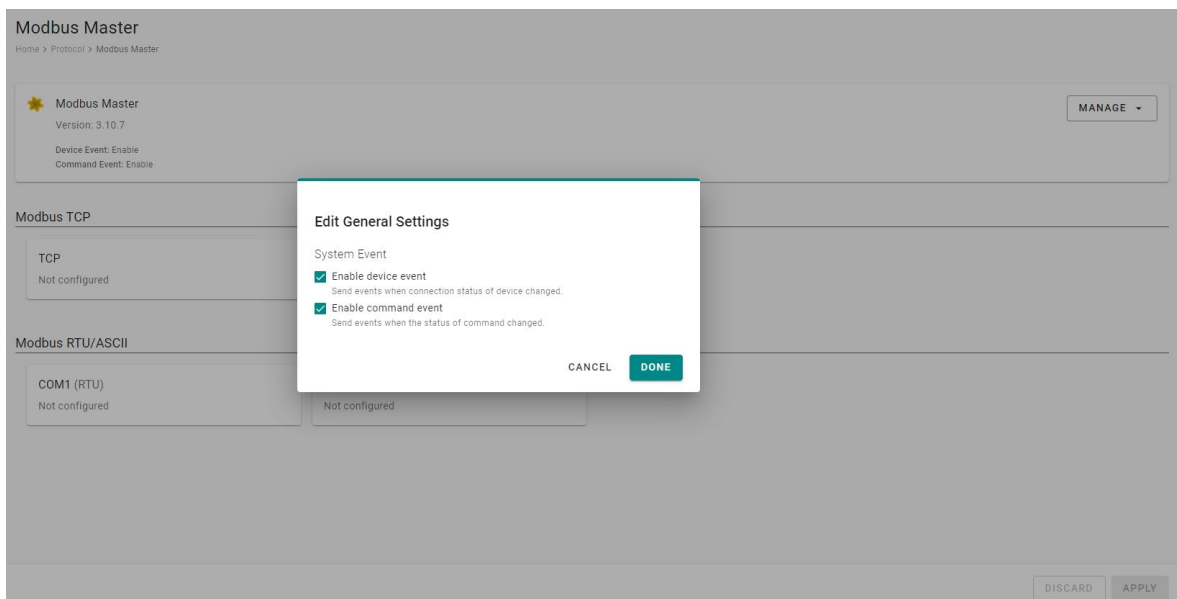
Management

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



Edit General Settings

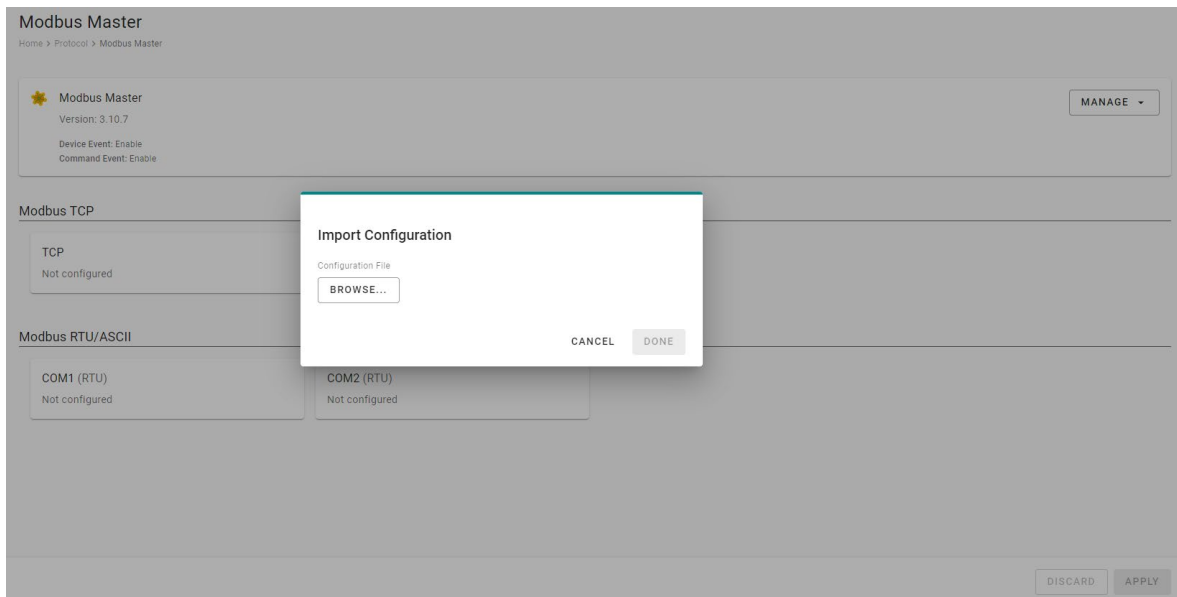
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	Check: If the Modbus communication fails, e.g., Modbus exception code is received The Modbus response timeout and 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 or Modbus response times out, 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 the **Modbus Master settings**, which will be stored in XML format.

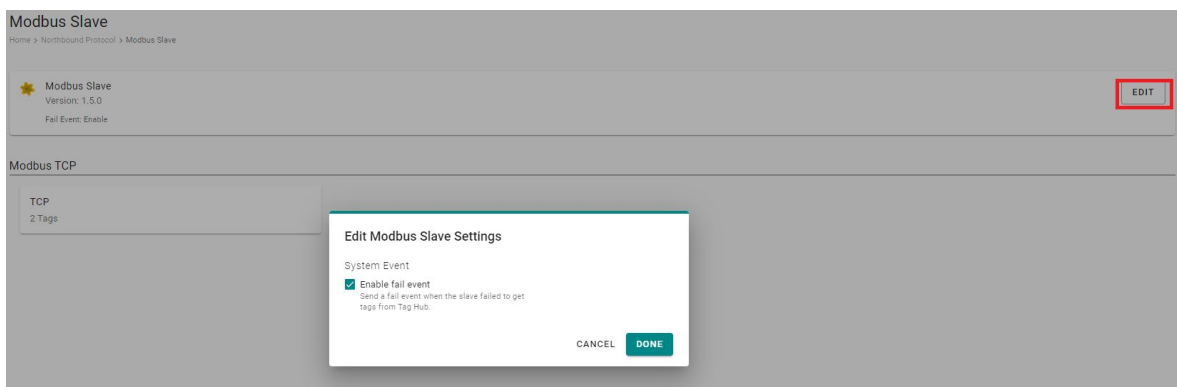


An example of an exported file that can be viewed/edited by EXCEL.

mcmnds]																										
remote	name	enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollinterv	swap	fpFunc	fpTout	fpData	scalingFu	intercept	intercept	pointSou	pointSou	pointTarg	pointTarg	tagName	data	Type	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_11	int16	r	r	20
																						Voltage_12	int16	r	r	
																						Voltage_13	int16	r	r	
																						Voltage_14	int16	r	r	
																						Voltage_15	int16	r	r	
																						Voltage_16	int16	r	r	
																						Voltage_17	int16	r	r	
																						Voltage_18	int16	r	r	

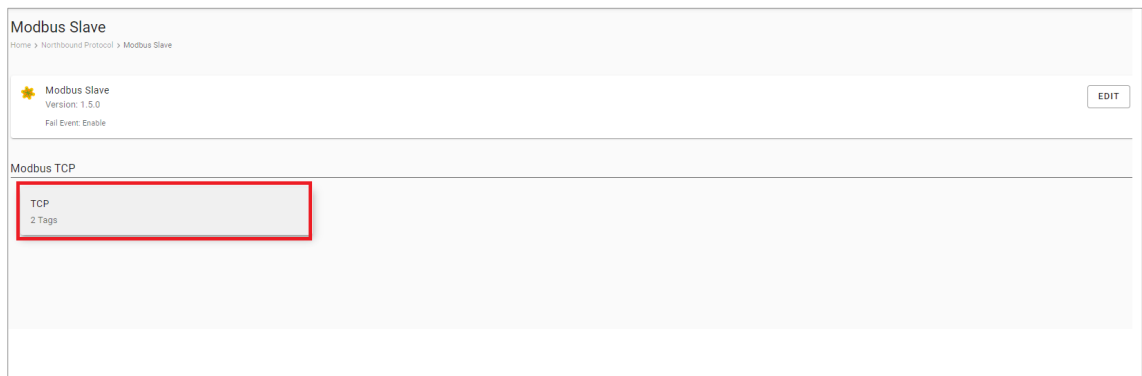
Modbus TCP Slave

Go to **Modbus Slave** and click **EDIT** to modify the Modbus Slave advanced settings. You must enable the Modbus TCP server to communicate with SCADA as a Modbus TCP client. If you want an event added to the event log when the Modbus TCP connection gets disconnected, select **Enable fail event**.

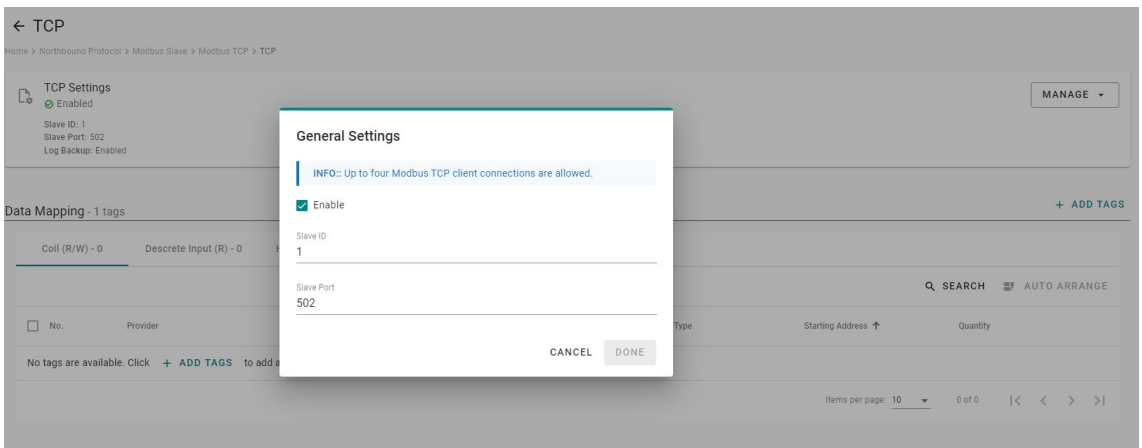


To create a Modbus TCP server (slave), do the following:

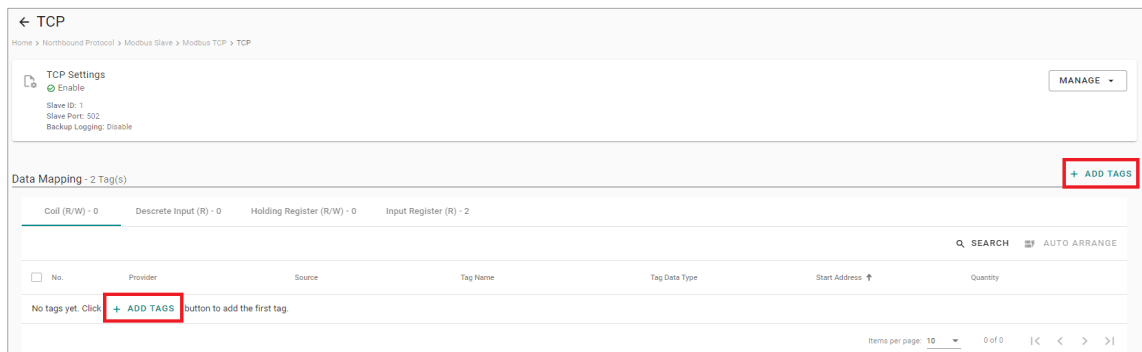
1. Go to **Modbus Slave** and click **TCP** under **Modbus TCP**.



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



3. Select **Enable**, input **Slave ID**, and **Slave Port**, and then click **DONE**.
4. Click **+ADD TAGS** to select tags (e.g., Modbus Master).



5. Click **DONE** to complete settings.

Data Mapping

You can view the selected tags under Data Mapping. The tags are organized based on tags for Coil, Discrete Input, Holding Register, and Input Register. The mapping rule for the tags 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

Data Mapping - 4 Tag(s) + ADD TAGS

Q SEARCH AUTO ARRANGE

<input type="checkbox"/> No.	Provider	Source	Tag Name	Tag Data Type	Start Address ↑	Quantity	
<input type="checkbox"/> 1	modbus_serial_master	ddd	device_info_t2	int16	00000	1	⋮
<input type="checkbox"/> 2	modbus_serial_master	ddd	Power1	int16	00001	1	⋮
<input type="checkbox"/> 3	modbus_serial_master	ddd	Power2	int16	00002	1	⋮
<input type="checkbox"/> 4	modbus_serial_master	ddd	status	int32	00003	2	⋮

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

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

Auto Arrange

Info: Auto Arrange feature is designed to re-arrange selected tags in order. Please select the item Sorting Priority, then Sort Order.

Item Sorting Priority

Provider → Source → Tag Name

Provider → Tag Name → Source

Sort Order

Ascending ▼

CANCEL
DONE

Backup Logging

If you want to enable the data logger function, go to **MANAGE > Backup Logging > Edit Settings** to enable the feature.



NOTE

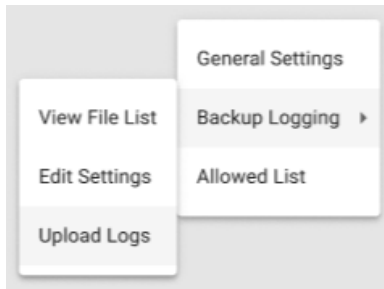
If the data is stored in an SD card, ensure that the SD card is installed before enabling this function. If you replace the SD card, reboot your device and confirm that the backup function is working properly. The SD card should have at least 1 GB free space.

To enable log backups, do that following:

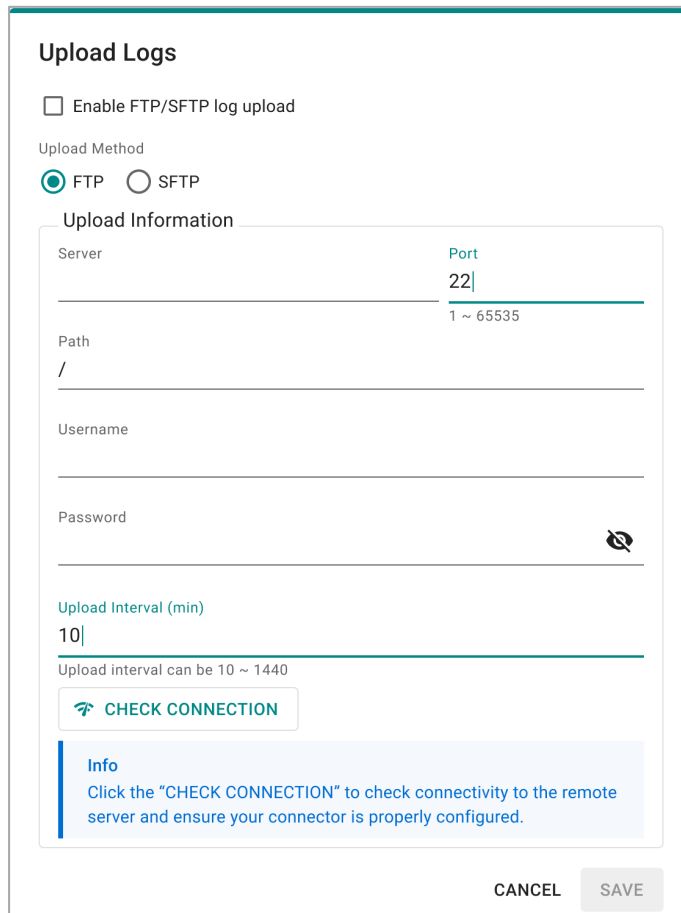
1. Select **Backup Logging** and **Edit Settings**, and then **Enable backup logging**.
2. Specify the **Folder Name**, **Maximum Storage**, and **log interval**.
3. Specify File Split Mode setting: By Time or By Size.
4. Click **DONE**.

To upload log files via FTP, do the following:

1. Select **Backup Logging** and **Upload Logs**.

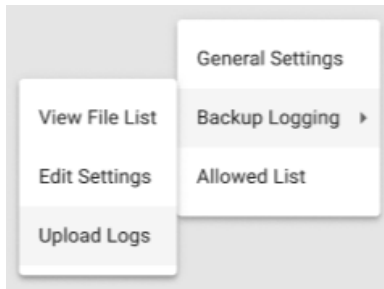


2. Select **Enable the FTP/SFTP uploader**.
3. Select **FTP** for **Upload Method**.
4. Enter the necessary parameters: **Server**, **Port**, **Path**, **Username**, and **Password**.
5. Set the **Upload Interval**.
6. (optional) Click **CHECK CONNECTION** to verify that the communication is working.
7. Click **SAVE** to apply the settings.

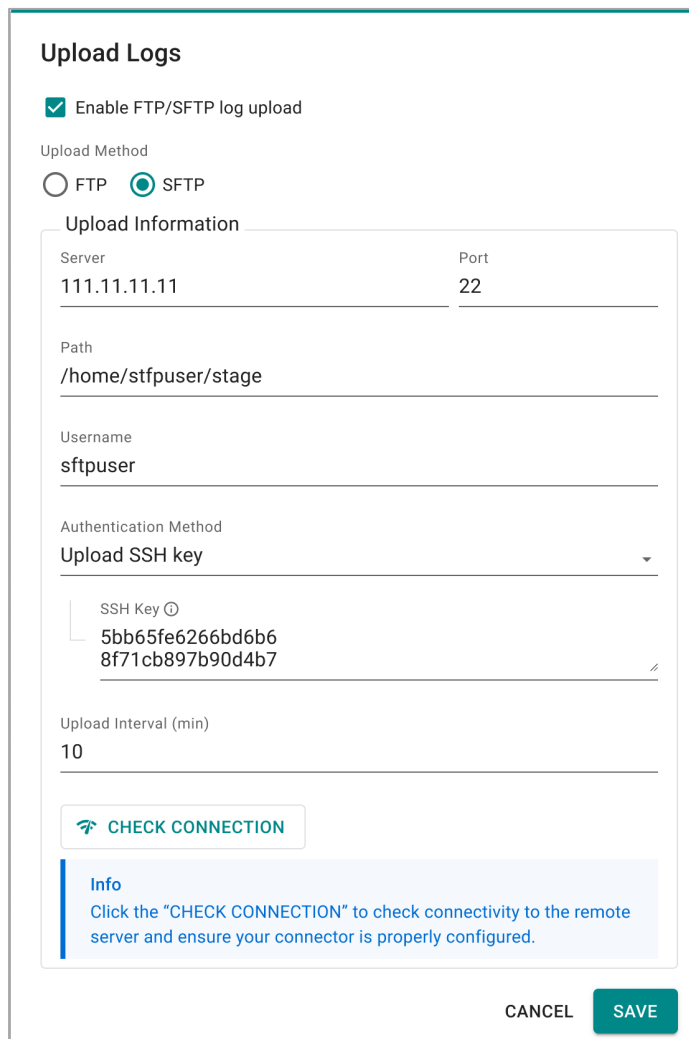
A screenshot of the 'Upload Logs' configuration window. At the top, there is a checkbox labeled 'Enable FTP/SFTP log upload'. Below it, the 'Upload Method' is set to 'FTP' (selected with a radio button) and 'SFTP' (unselected). The 'Upload Information' section contains several input fields: 'Server' (empty), 'Port' (22), 'Path' (/), 'Username' (empty), and 'Password' (empty with a toggle icon). Below these is the 'Upload Interval (min)' set to 10, with a note 'Upload interval can be 10 ~ 1440'. A 'CHECK CONNECTION' button is present. At the bottom, there is an 'Info' box with text: 'Click the "CHECK CONNECTION" to check connectivity to the remote server and ensure your connector is properly configured.' At the very bottom are 'CANCEL' and 'SAVE' buttons.

To upload files via SFTP, do the following:

1. Select **Backup Logging** and **Upload Logs**.



2. Select **Enable the FTP/SFTP uploader**.
3. Select **SFTP** as **Upload Method**.
4. Enter the necessary parameters: **Server**, **Port**, and **Path**
5. Select an SFTP authentication method:
 - a. **By Password:** Authenticate by providing a username and password combination.
 - b. **Generate New SSH Key:** Create a new SSH key pair and use it for authentication.
 - c. **Upload SSH Key:** Upload an existing SSH public key to the server for authentication.
6. Set the **Upload Interval**.
7. (optional) Click **CHECK CONNECTION** to verify that the communication is working.
8. Click **SAVE** to apply the settings.

A screenshot of a configuration form titled 'Upload Logs'. At the top, there is a checkbox labeled 'Enable FTP/SFTP log upload' which is checked. Below this, the 'Upload Method' is set to 'SFTP' (selected with a radio button). The 'Upload Information' section contains several fields: 'Server' is '111.11.11.11', 'Port' is '22', 'Path' is '/home/stfpuser/stage', 'Username' is 'stfpuser', and 'Authentication Method' is 'Upload SSH key'. Below the authentication method, there is a text area for the 'SSH Key' containing the text '5bb65fe6266bd6b68f71cb897b90d4b7'. The 'Upload Interval (min)' is set to '10'. At the bottom of the form, there is a 'CHECK CONNECTION' button with a network icon. Below the button is an 'Info' box with the text: 'Click the "CHECK CONNECTION" to check connectivity to the remote server and ensure your connector is properly configured.' At the very bottom of the form, there are 'CANCEL' and 'SAVE' buttons.



NOTE

After using **CHECK CONNECTION**, if you observe a connection failure, or if you notice in the Event Log that data cannot be uploaded via FTP/SFTP, do one the following to troubleshoot the issue:

- Check if the **Server IP** or **Port**, and **Path** are set up correctly on the server side.
- Check if the **authentication information** is accurate.

OPC UA Server

Go to **OPC UA Server** to configure the corresponding settings.

To enable the OPC UA Server, click **LAN** and do the following:

← LAN

Home > Protocol > OPC UA Server > LAN

General Advanced

Connection ^ EDIT

Server Status : Enable

Server Port : 4840

Server Address 1 : opc.tcp://10.123.13.30:4840

Server Address 2 : opc.tcp://192.168.4.127:4840

Security ^ EDIT

Enabled Policies. : Sign - Basic256Sha256
Sign & Encrypt - Basic256Sha256

Account Login : Enable [Manage Account Details >](#)

Anonymous User Login : Disable

Ignore Client Certificates : Disable [Manage Certificate Details >](#)

1. Click Connection **EDIT**, select **Enable This Server**, and click **DONE**. The service is enabled by default on port 4840.

← LAN

Home > Protocol > OPC UA Server > LAN

General Advanced

Connection ^ EDIT

Server Status : Disable

Server Port : 4840

Server Address 1 : opc.tcp://10.123.21.84:4840

Server Address 2 : opc.tcp://192.168.4.84:4840

Server Address 3 : opc.tcp://192.168.5.1:4840

Security ^ EDIT

Enabled Policies. : Sign - Basic256Sha256
Sign & Encrypt - Basic256Sha256

Account Login : Enable [Manage Account Details >](#)

Anonymous User Login : Disable

Ignore Client Certificates : Disable [Manage Certificate Details >](#)

Edit Connection

Enable This Server

Server Port
4840

CANCEL DONE

2. (Optional) Click Security **EDIT** to edit Policies, User Authentication, and Certificates.

Edit Security

Policies User Authentication Certificates

Info: For security reasons, deprecated security policies should not be activated. It is up to the administrator to enable deprecated security policies for backward compatibility.

Suggested Options

Sign and Encrypt - Basic256Sha256 (Default Choice)

Sign - Basic256Sha256

Deprecated Options

Sign and Encrypt - Basic256

Sign - Basic256

Sign and Encrypt - Basic128Rsa15

Sign - Basic128Rsa15

CANCEL DONE

3. (Optional) Click **Manage Account Details** to **CREATE** new accounts.
The default account/ password is **admin/moxa**.

← Account Management

Home > Protocol > OPC UA Server > LAN > Account Management

+ CREATE

No.	Account	
1	admin	⋮

BACK

- (Optional) Click **Manage Certificate Details** to download the server certificate or upload a client certificate.

← Certificate Management

Home > Protocol > OPC UA Server > LAN > Certificate Management

Server Certificate

My Certificates

No.	Name	SHA-1 Fingerprint	Expiration	
1	Moxa OPC UA Server	9403BE25C1FAA2A9B3FD9DBBE6887B2FAFF4A998	May 3, 2022	⋮

Client Certificate

Trusted Certificates

No.	Name	SHA-1 Fingerprint	Expiration	
1	UaExpert@DESKTOP-A6C68FO	6B7F0BB732C23E1EC68C3B08BB929D469E0C950A	Jun 1, 2026	⋮
2	UaExpert@DESKTOP-A6C68FO	FF69400D9306E439D9497551F8E0F1AC8CD62A6F	Jun 2, 2026	⋮

- Download Certificate
- Update - Manually Upload
- Update - Regenerate by ThingsPro

← Certificate Management

Home > Protocol > OPC UA Server > LAN > Certificate Management

Server Certificate

My Certificates

No.	Name	SHA-1 Fingerprint	Expiration	
1	Moxa OPC UA Server	9403BE25C1FAA2A9B3FD9DBBE6887B2FAFF4A998	May 3, 2022	⋮

Client Certificate

Trusted Certificates

No.	Name	SHA-1 Fingerprint	Expiration	
1	UaExpert@DESKTOP-A6C68FO	6B7F0BB732C23E1EC68C3B08BB929D469E0C950A	Jun 1, 2026	⋮
2	UaExpert@DESKTOP-A6C68FO	FF69400D9306E439D9497551F8E0F1AC8CD62A6F	Jun 2, 2026	⋮

Upload Client Certificate

Certificate File

5. (Optional) Click **Advanced > EDIT** to configure the subscription settings here.

The 'Edit Subscription' window contains the following settings:

Max Monitored Item Queue Size	1		
Max No. of Values per Publish	1000		
Min Publish Interval (ms)	500	Max Publish Interval (ms)	50000
Min Sampling Interval (ms)	200	Max Sampling Interval (ms)	50000
Min Lifetime (ms)	1000	Max Lifetime (ms)	100000

Buttons: CANCEL, DONE

6. Click **ADD TAGS** and select providers and tags.

The 'Add Tags' window includes an info message: "Info: Choose one or more tag providers and select tags to map data."

Providers: system

Selected Tags: cpuNice (+27 others)

28 Tags

Buttons: CANCEL, DONE

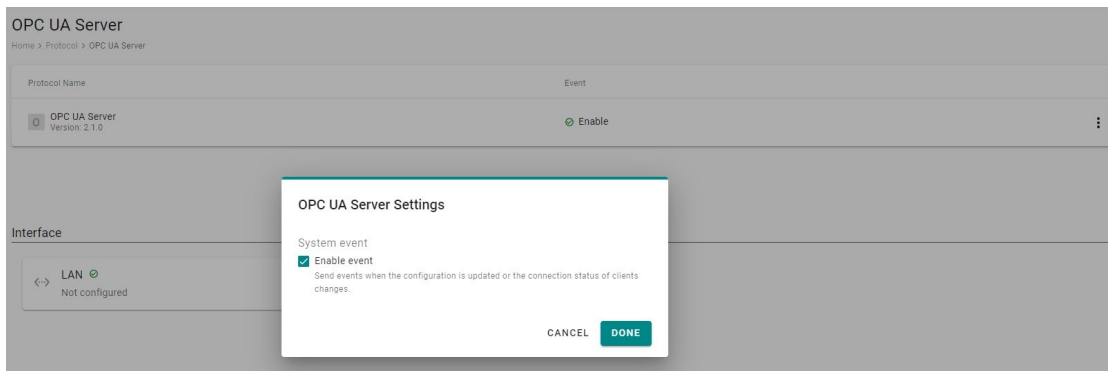
7. Click **DONE**.
8. Click **GO TO APPLE SETTINGS**.
9. Click **APPLY**.

You can also **disable/enable system event** of the OPC UA services or **Import/Export** configuration here.

The 'OPC UA Server' configuration page shows the following details:

- Protocol Name: OPC UA Server
- Version: 2.1.0
- Event: Enable
- Interface: LAN (Not configured)

A red box highlights the 'Edit', 'Import', and 'Export' options in the top right corner.



Edge Computing

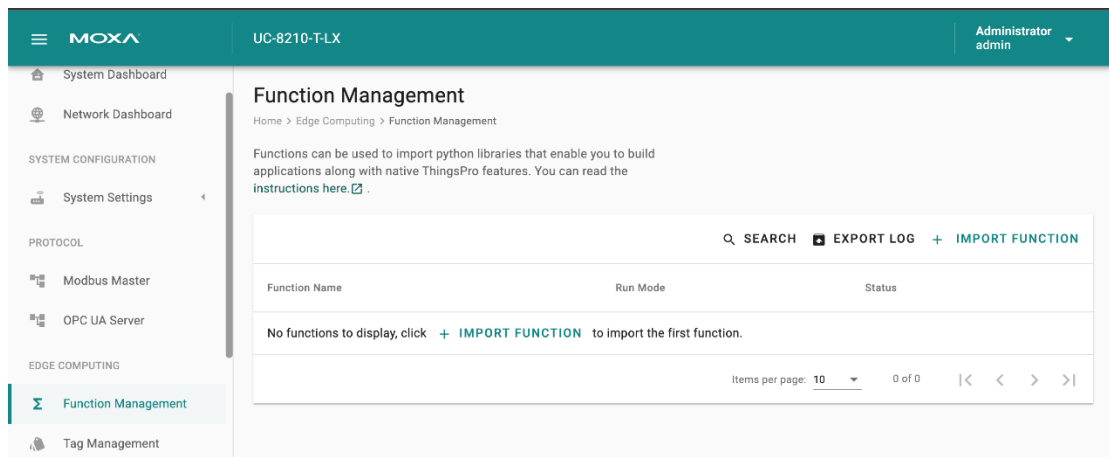
Function Management

AIG-301 Series provides a functionality to trigger actions based on specific data or time frames. For example, you can create a function that implements a defined action such as a device reboot or a **cron** job triggered by a specified change in a tag value or newly generated tags/events.

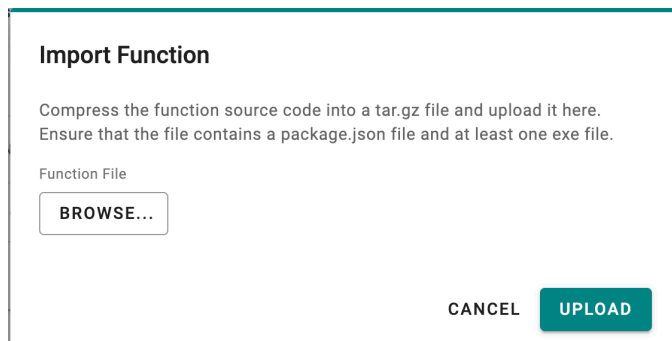
Go to **Edge Computing > Function Management** to import and manage functions. For additional information, see [build your own functions](#).

To import functions, do the following:

1. Click **IMPORT FUNCTION**.



2. Click **BROWSE** to select the application/file (*.tar.gz file) and click **UPLOAD**.



The function is displayed in the list along with the run mode and status of the function. You can click the function to check the **package.json** file.

Function Management
Home > Edge Computing > Function Management

Functions can be used to import python libraries that enable you to build applications along with native ThingsPro features. You can read the [instructions here](#).

SEARCH EXPORT LOG + IMPORT FUNCTION

Function Name	Run Mode	Status
onChangeTag	Boot Last uptime: May 20, 2022 20:42:15	Running

```

id: 1
name: "onChangeTag"
enabled: true
trigger:
  driven: "dataDriven"
  dataDriven:
    tags:
      system:
        status:
          0: "cpuUsage"
    events:
      timeDriven:
        mode: "boot"
  
```

	Run Mode
1	Boot
2	Cron job

Status	Description
Running	The function is running
Retrying	Retrying a failed function every 5 seconds (unlimited tries)
Failure	The function failed during a retry. The correspondent error message will be displayed in the table. You can click EXPORT LOG to check the logs.
Inactive	The function is disabled.

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:

1. Click **+ EDIT TAGS**.

MOXA AIG-101-T Administrator admin

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.

SEARCH + 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.						

Items per page: 10 0 of 0 |< > >|

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**

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**

CANCEL **NEXT >**



NOTE

The name of provider is "system" indicating system status whose update time is 10 seconds.

Cloud Connectivity

Azure IoT Edge


Go to **Cloud Connectivity > Azure IoT Edge** to configure the Azure IoT Edge settings. You can enable/disable the Azure IoT Edge service and enroll the device via manual setting or DPS (Device Provisioning Service) here.




NOTE

A registered Azure account is needed to manage the Azure IoT Edge service for your IoT application.

To manually create an Azure IoT Edge connection for your device, do the following:

1. Enable the Azure IoT Edge service and click on .
2. Select **Manual**.
3. Enter the **Device Connection String**.
Copy and paste the string from the Azure IoT Hub.
4. Click **SAVE**.

Provisioning Settings

 Azure IoT Edge
1.4.10 RESTORE
Current Version: 1.4.10

Info: Set up the provisioning settings to start the Azure IoT Edge on your device.

Device Connections


Source

Manual DPS

Device Connection String

CANCEL SAVE

To create an Azure IoT Edge connection for your device via DPS, do the following:

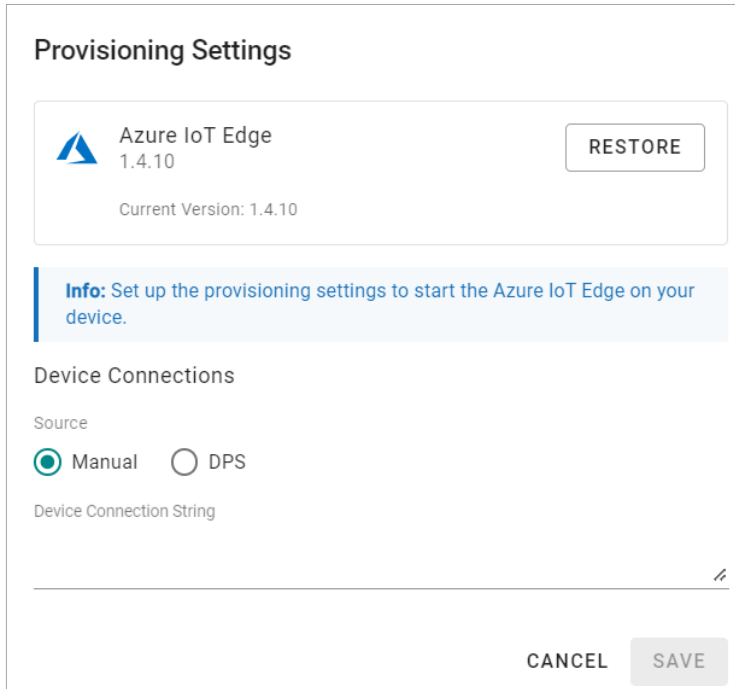
1. Enable the Azure IoT Edge service and click on .
2. Select **DPS**.
3. Select **TPM, Symmetric encryption**, or **X.509** certificate.
Select an option based on your device registered with the Azure IoT Hub.




NOTE

TPM attestation is only available for devices with a built-in TPM module.

- For the Azure IoT Hub device provisioning service and Symmetric encryption, enter the **Registration ID** and **Endorsement Key**.
 - For X.509, upload the **X.509 Certificate** and **Private Key**.
4. Click **SAVE**.



Provisioning Settings

 Azure IoT Edge
1.4.10

Current Version: 1.4.10

RESTORE

Info: Set up the provisioning settings to start the Azure IoT Edge on your device.

Device Connections

Source

Manual DPS

Device Connection String

CANCEL **SAVE**

More information about the Azure DPS configuration in the Azure IoT Hub at [Set up a DPS](#).

If you want to check the Azure IoT Edge configuration and connectivity for common issues, go to **Azure IoT Edge > AIE Checks** and click **CHECK** to see the results of the checks.

For additional information on AIE Checks, see <https://github.com/Azure/iotedge/blob/master/doc/troubleshoot-checks.md>.

If an unexpected situation occurs when you upgrade/downgrade to a certain version of Azure IoT Edge, you can restore Azure IoT Edge by clicking **RESTORE** in the Provisioning Settings. Using the restore function will remove existing settings including Message Group, Store and Forward, Device Management, and Downstream/Upstream credentials.

Telemetry Message Settings

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](#).

The screenshot shows the 'Create New Telemetry Message' dialog with three steps: 1. Basic Settings, 2. Message Tags, and 3. Properties Optional. Step 1 is active. It includes a checkbox for 'Enable Telemetry Message' which is checked. Below it is an 'Output Topic' field. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. A sub-dialog is open for 'By Interval', showing a 'Publish Interval (sec)' field with the value '60', a 'Sampling Mode' dropdown set to 'All Changed Values', and a checkbox for 'Custom sampling rate from acquired data' which is unchecked. 'CANCEL' and 'NEXT >' buttons are at the bottom right.

4. Input corresponding parameters such as publish interval, sampling mode, and publish size.
5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).

The screenshot shows the 'Create New Telemetry Message' dialog at Step 2: Message Tags. Step 1 is completed. It features a 'Select Tags' section with an info box: 'Info: Select one or more tag providers and select tags to map data.' Below this is a 'Providers' dropdown set to 'IO'. A search modal is open, showing a list of tags: '[IO] DI' (checked), 'DI-01' (checked), 'DI-02' (checked), and 'DI-03' (checked). At the bottom of the modal, it says 'Total: 8, Selected: 4' and has a 'DONE' button. To the right is a 'Default Payload' text area containing 'null' and an 'Enable Custom Payload' checkbox which is unchecked. 'CANCEL' and 'NEXT >' buttons are at the bottom right.

- (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/>).

- Click **NEXT**.
- (Optional) Enter **Property Key** and **Value**.
- Click **SAVE**.



NOTE

For information on using direct method to write tags from the cloud, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.



NOTE

If you cannot receive D2C messages, check and ensure that a default route of the modules is added. You can add routes in Azure IoT Hub by logging into **IoT Hub** > **IoT Edge** > choose a device > **Set Modules** > **Routes**.

NAME	VALUE	PRIORITY	TIME TO LIVE (SECS)
route	FROM /messages/* INTO \$upstream	0	7200
Route name	FROM /messages/* INTO \$upstream	0	7200

Device Management Settings

Go to **Cloud Connectivity > Azure IoT Edge** and click on the **Device Management** tab. Enabling this feature allows cloud service providers to manage IoT devices remotely using Device Twin and Direct Method technologies.

Azure IoT Edge

Home > Cloud Connectivity > Azure IoT Edge

Azure IoT Edge

Service Name	Status
Azure IoT Edge Version: 1.4.10	<input type="radio"/> Exited

Module List **Device Management** Telemetry Message Downstream Certificate AIE Checks

Allow managing this device from Azure IoT Hub via a Module Twin and Direct Methods technology.

Allow Device Management
This feature requires the ThingsProAgent module installed.

SAVE



NOTE

For information on managing the device using API, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>

Downstream Certificate

To prevent your device from connecting to potentially malicious gateways (Azure IoT Edge inside), you can upload **X.509 certificate**, **Private Key**, or **Trusted CA Certificate**. You can generate the certificates and the private key using ThingsPro Edge. For additional information, see [Downstream Certificate](#).

MOXA AIG-301-T-EU-AZU-LX Administrator admin

OVERVIEW

- System Overview
- Network Overview

SYSTEM CONFIGURATION

- General Settings
- System Settings

PROTOCOL

- Modbus

CLOUD CONNECTIVITY

- Azure IoT Edge**
- Azure IoT Device
- AWS IoT Core
- MQTT Client
- Sparkplug B.

SECURITY

- User Management

MAINTENANCE

- General Operation

Azure IoT Edge

Home > Cloud Connectivity > Azure IoT Edge

Azure IoT Edge

Service Name	Status
Azure IoT Edge	<input type="radio"/> Exited

Module List **Downstream Certificate** AIE Checks

This is malicious

UPDATE

Upload Downstream Certificate

X.509 Certificate

iotEdge_moxa.crt

Private Key

iotEdge_moxa.key

Trusted CA Certificate

RootCA_moxa.crt


CANCEL SUBMIT

Azure IoT Device

Go to **Cloud Connectivity > 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. Select a **Publish Mode**.

For details, see [Publish Mode](#).

The screenshot shows the 'Create New Telemetry Message' dialog in its first step, 'Basic Settings'. At the top, there are three progress indicators: '1 Basic Settings' (active), '2 Message Tags', and '3 Properties Optional'. The 'Enable Telemetry Message' checkbox is checked. Below it is an empty text field for the 'Output Topic'. Under 'Publish Mode', three radio buttons are shown: 'By Interval' (selected), 'Immediately', and 'By Size'. A sub-dialog is open for 'By Interval', showing a 'Publish Interval (sec)' field with the value '60', a 'Sampling Mode' dropdown menu set to 'All Changed Values', and an unchecked checkbox for 'Custom sampling rate from acquired data'. At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).

The screenshot shows the 'Create New Telemetry Message' dialog in its second step, 'Message Tags'. The progress indicators now show '1 Basic Settings' as completed with a checkmark, '2 Message Tags' as active, and '3 Properties Optional'. An 'Info' box states: 'Info: Select one or more tag providers and select tags to map data.' There are two main sections: 'Select Tags' and 'Default Payload'. The 'Select Tags' section has a 'Providers' dropdown set to 'IO' and a search box. A list of tags is shown with checkboxes: '[IO] DI' (checked), 'DI-01' (checked), 'DI-02' (checked), and 'DI-03' (checked). At the bottom of this list, it says 'Total: 8, Selected: 4'. There are 'SELECT ALL' and 'CLEAR' buttons. The 'Default Payload' section has a text area containing 'null' and an unchecked checkbox for 'Enable Custom Payload'. At the bottom right, 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/>).

The screenshot shows the 'Create New Telemetry Message' interface at the 'Message Tags' step. The progress bar indicates three steps: 'Basic Settings' (completed), 'Message Tags' (current), and 'Properties Optional' (skipped). On the left, there are dropdown menus for 'Providers' (IO) and 'Selected Tags' (DI-01 (+3 others)). A 'jq Filter' input field is present with a 'TEST' button. A 'Custom Payload Result' section shows a JSON payload with a 'values' array containing an 'updateTimestamp' and a 'value'. A checkbox 'Enable custom payload' is checked. Navigation buttons 'BACK', 'CANCEL', and 'NEXT >' are at the bottom.

- Click **NEXT**.

- (Optional) Enter Property Key and Value.

The screenshot shows the 'Create New Telemetry Message' interface at the 'Properties Optional' step. The progress bar indicates three steps: 'Basic Settings' (completed), 'Message Tags' (completed), and 'Properties Optional' (current). The main area contains two input fields: 'Property Key' and 'Property Value'. A '+ Add another' link is below the inputs. Navigation buttons 'BACK', 'CANCEL', and 'SAVE' are at the bottom.

- Click **SAVE**.

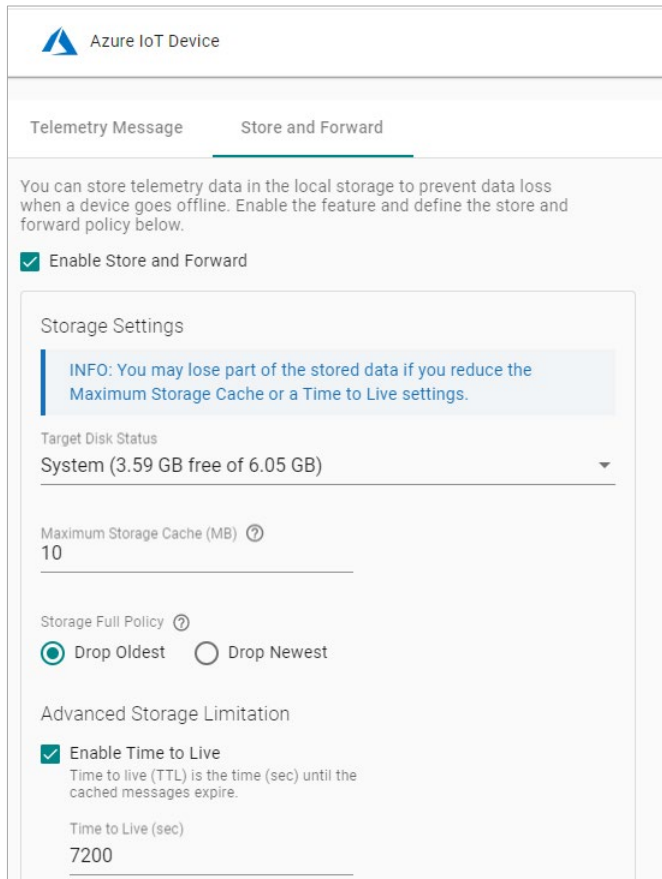


NOTE

For information on using direct method to write tags from the cloud, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

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.



The screenshot shows the 'Store and Forward' configuration page for an Azure IoT Device. The page has two tabs: 'Telemetry Message' and 'Store and Forward', with the latter being active. Below the tabs, there is a descriptive paragraph: '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.' A checkbox labeled 'Enable Store and Forward' is checked. Below this is a 'Storage Settings' section containing an information box: 'INFO: You may lose part of the stored data if you reduce the Maximum Storage Cache or a Time to Live settings.' Underneath, there is a 'Target Disk Status' dropdown menu set to 'System (3.59 GB free of 6.05 GB)'. The 'Maximum Storage Cache (MB)' is set to '10'. The 'Storage Full Policy' has two radio buttons: 'Drop Oldest' (selected) and 'Drop Newest'. An 'Advanced Storage Limitation' section includes a checked 'Enable Time to Live' checkbox, with a sub-note: 'Time to live (TTL) is the time (sec) until the cached messages expire.' The 'Time to Live (sec)' is set to '7200'.

Device Management

Go to **Cloud Connectivity > Azure IoT Device** and click on the **Device Management** tab. Enabling this feature allows cloud service providers to manage IoT devices remotely using Device Twin and Direct Method technologies.




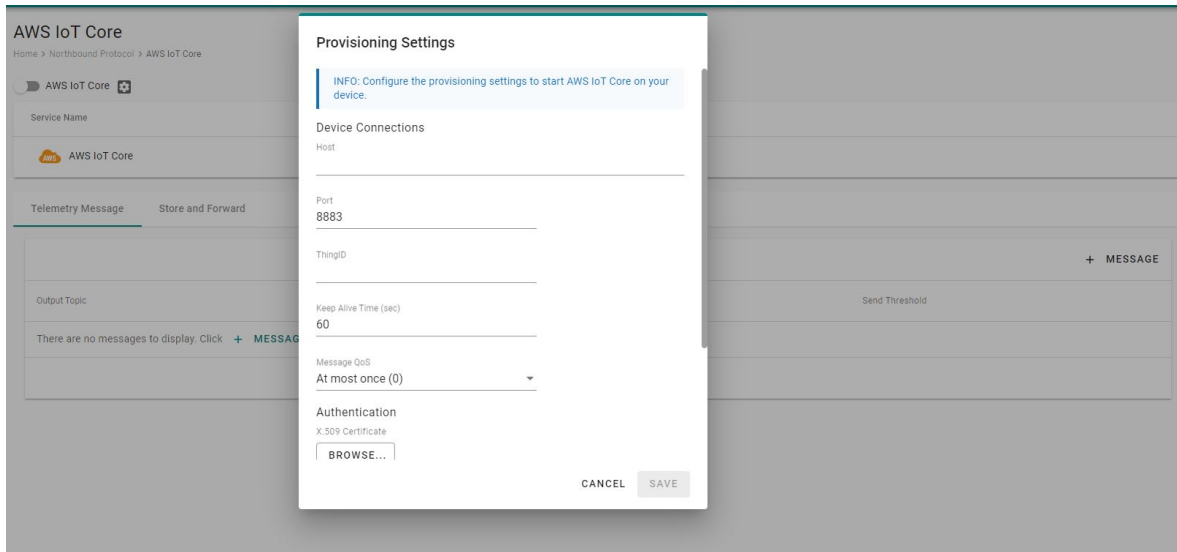
NOTE

For information on managing the device using API, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

AWS IoT Core

Go to **Cloud Connectivity > 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 size.
5. Click **NEXT**.

The screenshot shows the 'Create New Telemetry Message' dialog in its first step, 'Basic Setting'. The 'Message Tags' step is also visible and completed. The 'Enable Telemetry Message' checkbox is checked. The 'Output Topic' is '123'. The 'Publish Mode' is set to 'By Interval'. The 'Publish Interval (sec)' is '60'. The 'Sampling Mode' is 'All Changed Values'. There is an unchecked checkbox for 'Custom sampling rate from acquired data'. At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

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

The screenshot shows the 'Create New Telemetry Message' dialog in its second step, 'Message Tags'. The 'Basic Setting' step is completed. The 'Select Tags' section shows a search for 'IO' with a list of results: '[IO] DI', 'DI-01', 'DI-02', and 'DI-03'. The 'Default Payload' is 'null'. There is an unchecked checkbox for 'Enable custom payload'. At the bottom right, there are 'CANCEL' and 'SAVE' buttons. At the bottom left, there is a 'DONE' button and a status bar showing 'Total: 8, Selected: 4'.

- (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 Setting 2 Message Tags

Select Tags

Info: Select one or more tag providers to get their tags and select tags to map data.

Providers

IO

Selected Tags 8 Tags

DI-01 (+3 others)

Default Payload

Enable custom payload

```
{
  "tags": {
    "IO": {
      "DI": {
        "DI-01": {
          "values": [
            {
              "updateTimeStamp": "2020-02-14T05:53:23Z",
              "value": true
            }
          ]
        },
        "DI-02": {
          "values": [

```

< BACK CANCEL SAVE

- Click **SAVE**.



NOTE

For information on using direct method to write tags from the cloud, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

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

Device Management

Go to **Cloud Connectivity > Azure IoT Device** and click on the **Device Management** tab. Enabling this feature allows cloud service providers to manage IoT devices remotely using Device Twin and Direct Method technologies.



NOTE

For information on managing the device using API, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>

Generic MQTT Client

Go to **Cloud Connectivity > MQTT Client** to add a connection to the MQTT Broker. You can add multiple connections to the 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).

The screenshot shows a configuration window titled "Connect to New MQTT Broker" with three tabs: "General", "SSL/TLS", and "Will and Testament". The "General" tab is selected. It contains the following fields and options:

- Server:** An empty text input field.
- Port:** A text input field containing "8883".
- MQTT Version:** Two radio button options: "3.1.1" (selected) and "3.1".
- Client ID:** An empty text input field.
- Username:** A text input field containing "admin".
- Password:** A password input field with masked characters and a toggle icon.
- Keep Alive Time (sec):** A text input field containing "60".
- Clean Session:** A checked checkbox with the label "Don't persist messages on the broker when disconnected."

At the bottom right, there are two buttons: "CANCEL" and "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 are three sections, each with a "BROWSE..." button: "Client Certificate - optional", "Client Key - optional", and "Trusted Root CA - optional". At the bottom, there is an unchecked checkbox for "Ignore Server Certificate". The dialog has "CANCEL" and "SAVE" buttons 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 a progress bar at the top. The progress bar has two steps: "1 Basic Setting" (active) and "Message Tags" (completed). Under "Basic Setting", there is a checked checkbox for "Enable Telemetry Message". Below this, the "Output Topic" is set to "123". The "Publish Mode" section has three radio buttons: "By Interval" (selected), "Immediately", and "By Size". Below the radio buttons, there is a text input field for "Publish Interval (sec)" with the value "60". Below that, there is a dropdown menu for "Sampling Mode" set to "All Changed Values". At the bottom of the dialog, there is an unchecked checkbox for "Custom sampling rate from acquired data". The dialog has "CANCEL" and "NEXT >" buttons at the bottom right.

- Select a **Publish Mode**.
For details, see [Publish Mode](#).

4. Input corresponding parameters such as publish interval, sampling mode, and publish size.
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**.



NOTE

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.

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://github.com/TPE-TIGER/TPE-TIGER.github.io>.

Remote API Invocation

This function enables you to invoke nearly any RESTful API from the MQTT broker and receive responses via the specified MQTT topics.

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

This feature allows you to invoke almost all ThingsPro Edge restful APIs from the MQTT broker and receive responses using the MQTT topics listed here.

Enable Invoking of Device Restful APIs from MQTT Server

Input Topic to Subscribe [?](#)

Output Topic to Subscribe [?](#)

SAVE



NOTE

For information on managing the device using API, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

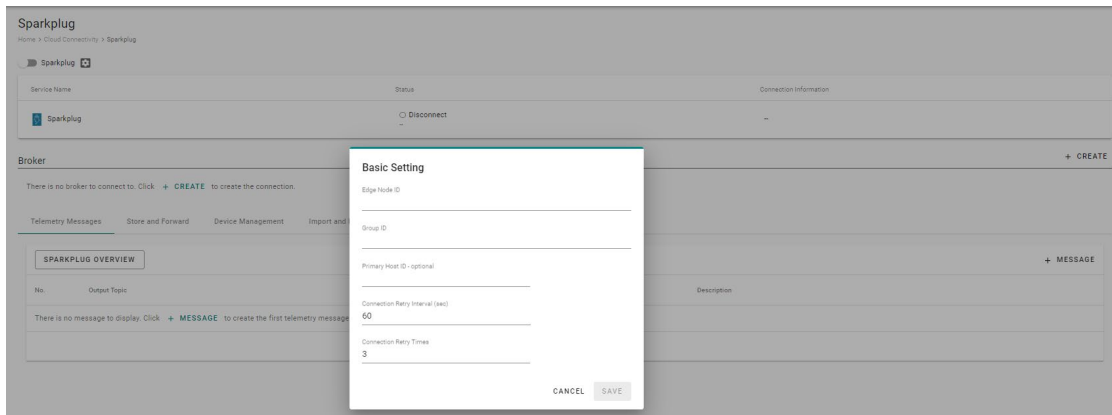
Sparkplug

Sparkplug B is a specification designed specifically for IoT applications so that MQTT devices and applications can send and receive messages in a stateful way. Go to **Cloud Connectivity > Sparkplug** to enable Sparkplug B and communication. The configuration process consists of the following:

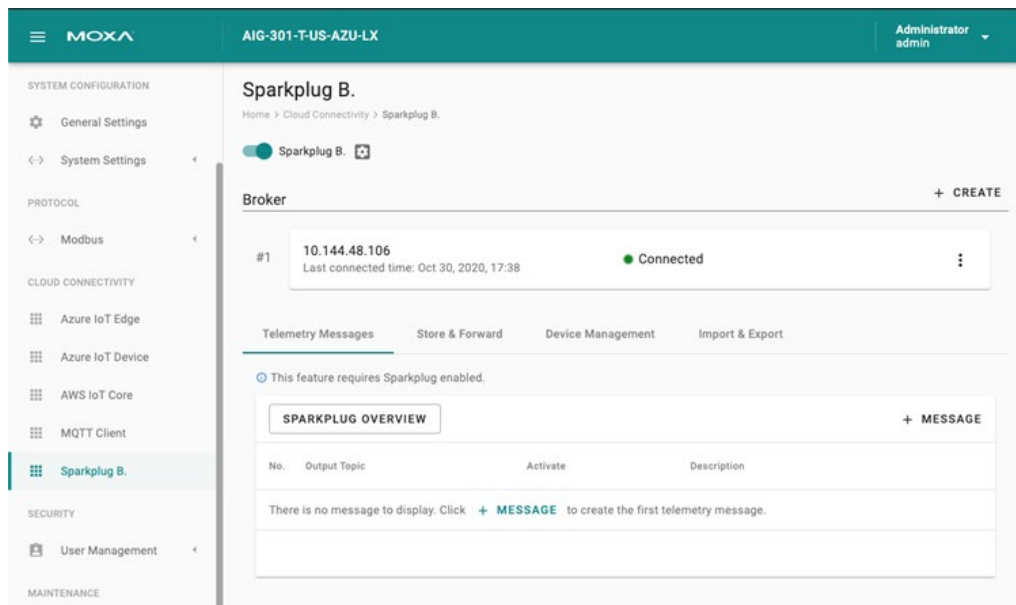
- Enabling Sparkplug
- Configuring a Broker
- Configuring a Telemetry Message

Enabling Sparkplug

1. Click on the **Sparkplug B.** link and use the scroll bar to enable Sparkplug B.
2. Specify an Edge Node ID.
3. Specify a Group ID.
4. (optional) Specify a Primary Host ID.



5. Click **SAVE**.



Configuring a Broker

1. Click on the **+ CREATE** link to create a broker for Sparkplug B.
2. Specify a **Server** (default port: 8883).
3. (optional) Enter **Client ID**, **Username**, and **Password**.
4. Specify an interval of Keep Alive Time (default 60 seconds)
5. (optional) **Enable SSL/TLS** and upload **Client Certificate**, **Key**, and **Trusted Root CA**.

Create New Broker

General **SSL/TLS**

SSL/TLS

Enable SSL/TLS

TLS Version

1.3 1.2 1.1 1.0

Client Certificate - optional

BROWSE...

Client Key - optional

BROWSE...

Trusted Root CA - optional

BROWSE...

Ignore server certificate

CANCEL SAVE

6. Click **SAVE**.



NOTE

Data loss might occur during the period of connection interval prior to network connection check (Keep Alive Time). We suggest setting a shorter interval of Keep Alive Time (e.g., 10 seconds)

Configuring a Telemetry Message

1. Click on the **+ MESSAGE** link.
2. Select tags from providers (e.g., Modbus Master).
3. Select devices or system tags.
4. Click **NEXT**.

The screenshot shows the 'Create New Telemetry Message' interface at the 'Select Tags' step. A progress bar at the top indicates three steps: '1 Select Tags' (active), '2 Set Up Transmission Setting' (completed), and '3 Confirm' (pending). Below the progress bar, there is an 'Info' box: 'Info: Select one tag provider to get its tags, and select tags to map data.' The interface is divided into two main sections: 'Select Tags' on the left and 'Selected Tags - 1 Tag' on the right. Under 'Select Tags', there are three input fields: 'Providers' with 'modbus_tcp_master' selected, 'Devices / System Tags' with 'Test' selected, and 'Selected Tags' with 'c1' selected. The 'Selected Tags' section on the right shows a list with one item: 'modbus_tcp_master (1)'. At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

5. Select a publish mode.
For details, see [Publish Mode](#).
6. Select a sampling mode.
7. Click **NEXT**.

The screenshot shows the 'Create New Telemetry Message' interface at the 'Set Up Transmission Setting' step. The progress bar at the top shows '1 Select Tags' (completed), '2 Set Up Transmission Setting' (active), and '3 Confirm' (pending). Below the progress bar, there is a 'Publish Mode' section with three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. Below this is a 'Publish Interval (sec)' input field with the value '60'. There is also a 'Sampling Mode' dropdown menu with 'All Changed Values' selected. A checkbox for 'Custom sampling rate from acquired data' is present and unchecked. At the bottom left, there is a '< BACK' button, and at the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

8. (optional) Specify a description.

9. Click **SUBMIT**.

Create New Telemetry Message

✓ Select Tags ——— ✓ Set Up Transmission Setting ——— 3 Confirm

[modbus_tcp_master] Test

c1

Message Transmission Setting

Publish Mode : By Interval
Publish Interval : 60 sec
Sampling Mode : All Changed Values
Sampling Rate : Custom disable

Message Group Description

Description

0 / 1024

Enable this message group later

< BACK CANCEL **SUBMIT**



NOTE

For information on using direct method to write tags from the cloud, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

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 in a queue temporarily when the network between your IIoT Gateway and the cloud is disconnected and transmit it to its destination after a reconnection. To enable the function, click on **Store and Forward** and select **Enable Store and Forward**. You can select a target disk and set a maximum storage cache, a retention policy, a TTL (Time to Live) value for the messages and a size of bulk transfer.

Enable Store and Forward

Storage Setting

Info: You may lose part of the data stored previously if you configure a smaller maximum Disk Size or a shorter Time to Live.

Target Disk
System (6.92GB free of 15.41GB)

Maximum Storage Cache (MB) ?
10

Storage Full Policy ?
 Drop Oldest Drop Newest

Enable Time to Live
Time to Live (TTL) is the time (sec) until the cached messages expire.
Time to Live (sec)
7200

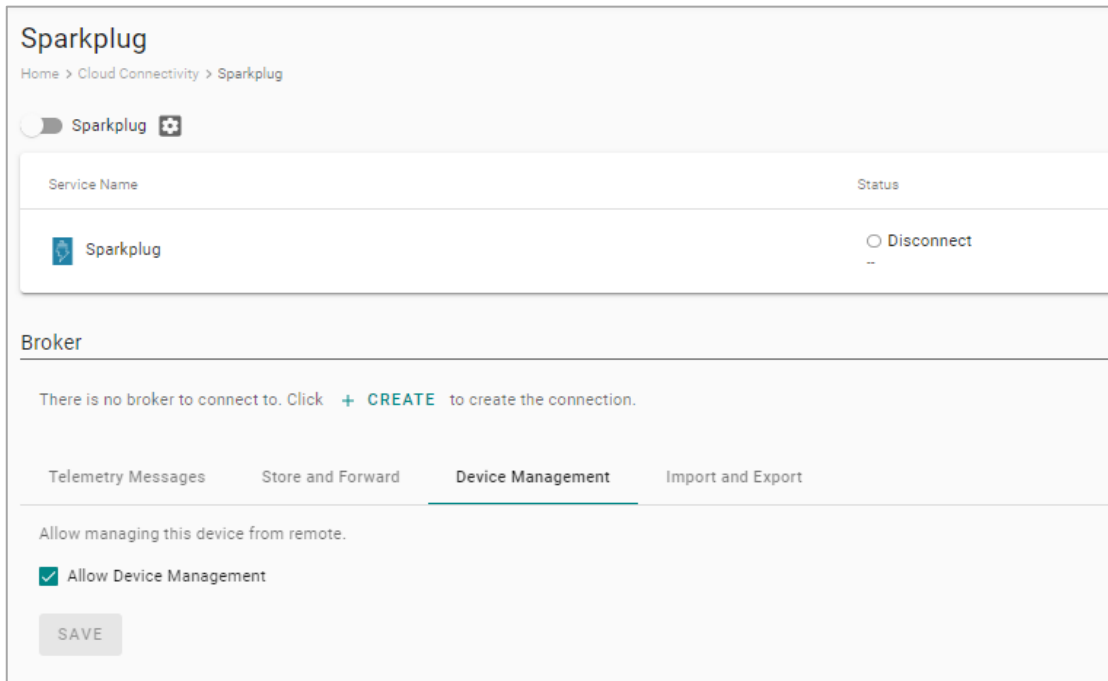
Bulk Transfer

Enable Bulk Upload
Enable bulk data upload to server after device status change to connected.
Bulk Size (KB)
128

SAVE

Device Management

Enabling this feature allows cloud service providers to manage IoT devices remotely through Device Twin and Direct Method technology.



The screenshot shows the Sparkplug configuration interface. At the top, there is a toggle switch for 'Sparkplug' which is turned on. Below this is a table with two columns: 'Service Name' and 'Status'. The table contains one entry: 'Sparkplug' with a status of 'Disconnect'. Below the table, there is a 'Broker' section with a message: 'There is no broker to connect to. Click + CREATE to create the connection.' Below this, there are four tabs: 'Telemetry Messages', 'Store and Forward', 'Device Management' (which is selected), and 'Import and Export'. Under the 'Device Management' tab, there is a section titled 'Allow managing this device from remote.' with a checked checkbox for 'Allow Device Management' and a 'SAVE' button.

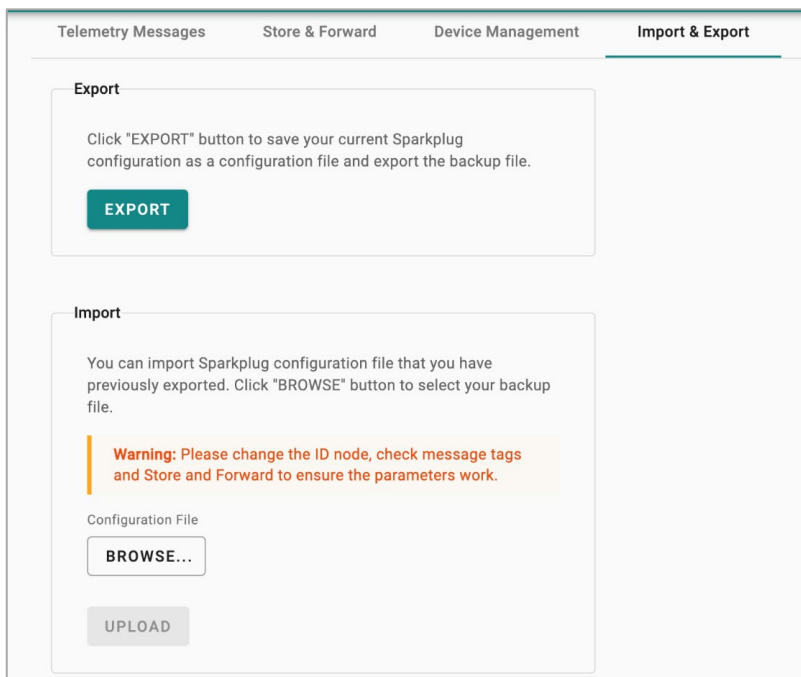


NOTE

For information on managing the device using API, see <https://github.com/TPE-TIGER/TPE-TIGER.github.io>.

Import & Export

To back up the configuration of Sparkplug, you can export the configuration as a backup file.



The screenshot shows the 'Import & Export' configuration page. At the top, there are four tabs: 'Telemetry Messages', 'Store & Forward', 'Device Management', and 'Import & Export' (which is selected). Below the tabs, there are two main sections: 'Export' and 'Import'. The 'Export' section contains the text: 'Click "EXPORT" button to save your current Sparkplug configuration as a configuration file and export the backup file.' and a green 'EXPORT' button. The 'Import' section contains the text: 'You can import Sparkplug configuration file that you have previously exported. Click "BROWSE" button to select your backup file.' Below this text is a warning box: 'Warning: Please change the ID node, check message tags and Store and Forward to ensure the parameters work.' Below the warning box is a 'Configuration File' label, a 'BROWSE...' button, and an 'UPLOAD' button.



NOTE

The exported configuration includes credentials, client ID, and policies of D2C messages. You can modify these parameters after the configuration file is imported to other gateways.

Moxa DLM Service

Moxa DLM (device lifecycle management) service is used for managing AIG devices. Imagine sitting in your office and using this service to remotely manage numerous 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 are interested in applying for this service, please use the following link to register an account: <https://dlm.thingsprocloud.com> to experience our beta DLM solution.

Once you have access to the service, go the **Moxa DLM Service** to register the product online as follows.

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

The screenshot shows the 'MOXA DLM Service' interface. A modal dialog box titled 'Add Connection' is open. It contains an information message: 'Info: Add a Moxa DLM service connection and verify it.' Below the message are two input fields: 'Email' and 'Password'. The 'Password' field has a visibility toggle icon. At the bottom of the dialog are two buttons: 'CANCEL' and 'VERIFY'. The background shows a blurred view of the service's main page with an 'ADD CONNECTION' button.

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

The screenshot shows the 'Moxa DLM Service' page. The 'Moxa DLM Service Enrollment' section is highlighted with a red border. It contains the following text: 'To start using Moxa DLM service for the device and connect to the Moxa DLM service project, add the connection in the device and select a project to enroll.' Below this is a section titled 'Configure an Moxa DLM service connection'. It shows a list of connections with a double-headed arrow icon. The first connection is 'Moxa DLM service connection' with a green checkmark and the word 'Verified' next to it. Below the connection name, the email 'Email: ichbinjoshua@gmail.com' and the password 'Password:' are displayed. At the bottom of the enrollment section is an 'ENROLL' button.

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

Moxa DLM Service
Home > Cloud Connectivity > Moxa DLM Service

Moxa DLM (Device Lifecycle Management) service provides a convenient, quick and safe working space for you to manage Moxa IIoT Gateway and IPC. Please [reach our service](#) for detail.

Moxa DLM Service Enrollment

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

Configure an Moxa DLM service connection

↔ Moxa DLM service connection

✓ Verified

Email: ichbinjoshua@gmail.com

Password: ••••••••

Enrollment setting

Project Name

Test

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 > Cloud Connectivity > Moxa DLM Service

Moxa DLM service

Project Name	Status
Test	Connected Connect on Oct 14, 2024, 12:26:31

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: moxathingpro-device-intermediate

Expires: Oct 14, 2027 04:01:22

Organization: Moxa Inc.

Model Name: AIG-301-T-AP-AZU-LX

MAC Address: 0090E99D8F3E

Serial Number: TBAIB1114968

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

All Devices
Home > Projects > All Devices

SEARCH REFRESH

Serial Number	Model Name	Host Name	Connection Status	Firmware Version	Labels
TBAIB1114968	AIG-301-T-AP-AZU-LX	Moxa	Online Connected on Oct 14, 2024 12:00:00	1.6.0	

Items per page: 10 1 - 1 of 1

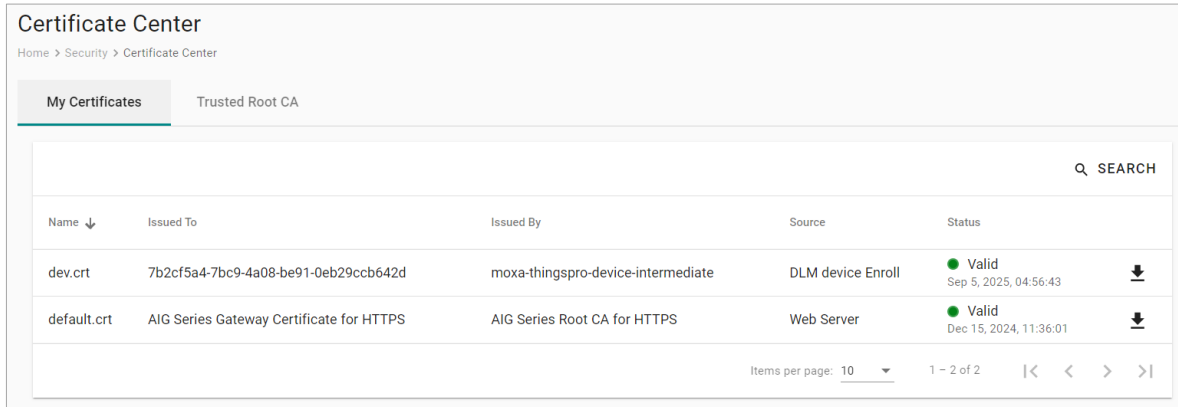
Security

Certificate Center

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.

The **rootCA.cer** certificate 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 trust the HTTPs connection between clients and 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 in the top right corner. Below the search bar is a table with the following columns: Name, Issued To, Issued By, Source, and Status. The table contains two rows of certificates. The first row is 'dev.crt' issued to '7b2cf5a4-7bc9-4a08-be91-0eb29ccb642d' by 'moxa-thingspro-device-intermediate' from 'DLM device Enroll', with a status of 'Valid' (Sep 5, 2025, 04:56:43). The second row is 'default.crt' issued to 'AIG Series Gateway Certificate for HTTPS' by 'AIG Series Root CA for HTTPS' from 'Web Server', with a status of 'Valid' (Dec 15, 2024, 11:36:01). At the bottom right of the table, there is a pagination control showing '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

Firewall

AIG provides a firewall that allows you to create rules for inbound Internet network traffic to protect your IIoT gateway.

Inbound

System Default

AIG reserves ports for the services below.

No.	Rule	Priority	Service	Port
1	Allow	1	HTTP	80
2	Allow	1	HTTPS	8443
3	Allow	1	SSH	22
4	Allow	1	Device discovery	40404
5	Forward	5	OPCUA Server	4840



NOTE

All ports (excluding the reserved ports mentioned above) on the AIG are disabled by default. To add service ports, add them to the **Allowed List**.

Firewall
Home > Security > Firewall

Inbound

System Default

Q 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	ssh service	22	TCP	Any	Localhost
Forward	5	app(opcuserver) forward port	4840	TCP	Any	172.31.9.7

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

Allowed List

Allowed List

AIG provides an allowed list for creating firewall rules. You can create, edit, and delete firewall rules here.

Firewall
Home > Security > Firewall

Inbound

System Default

Allowed List

Q SEARCH + ADD RULE

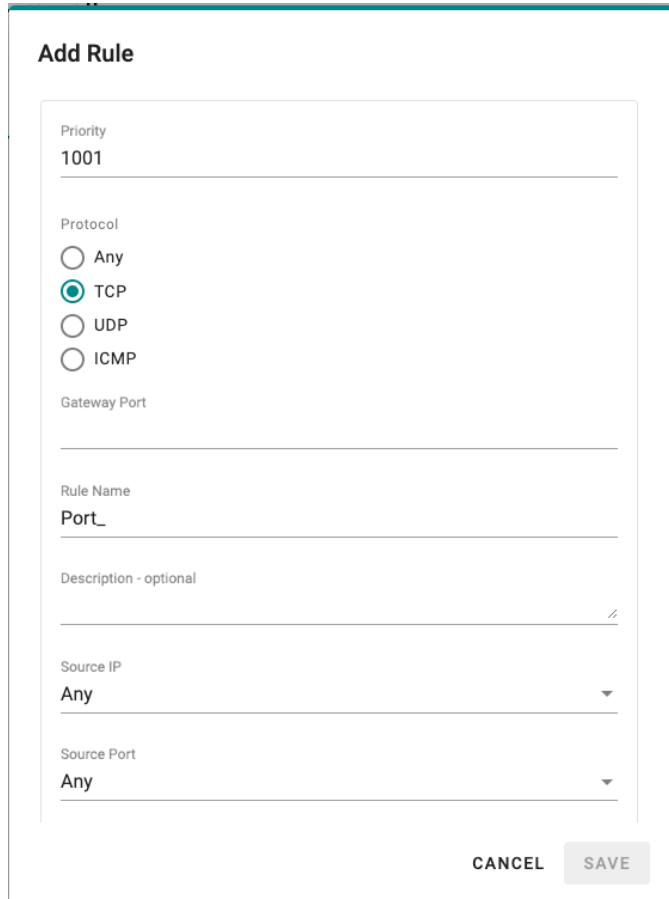
Action	Priority ↑	Rule Name	Gateway Port	Protocol	Source IP	Destination IP
No rules found. Click + ADD RULE button to add the first rule.						

Items per page: 10 0 of 0 |< < > >|

To create firewall rules, do the following:

Create Allow Rule:

1. Click **+ ADD RULE**.
2. Select action **Allow**.
3. Specify the priority, protocol, gateway port, rule name, and description (optional).
4. Specify a source IP or a subnet.
5. Specify a source port or a range of ports.
6. Click **SAVE**.



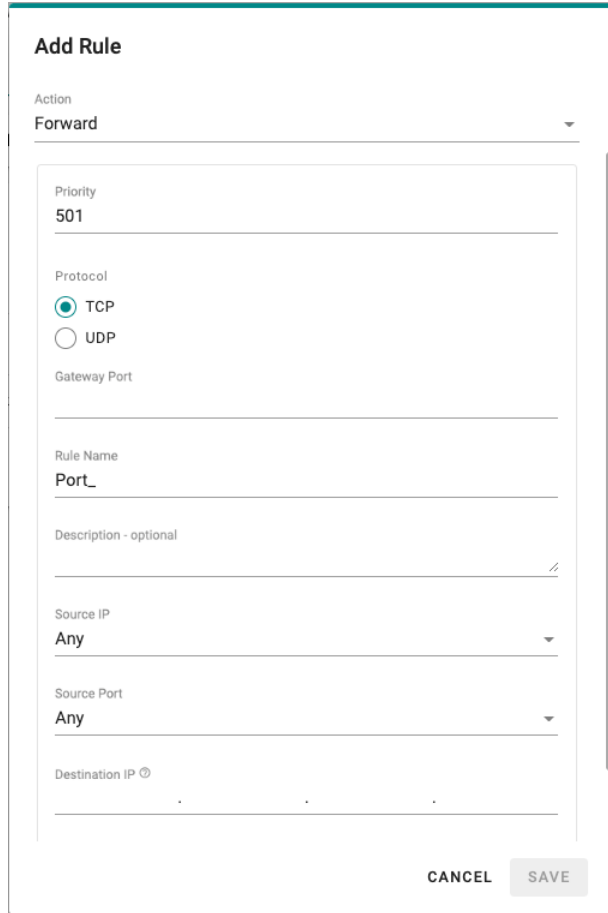
The screenshot shows a dialog box titled "Add Rule" with the following fields and options:

- Priority:** 1001
- Protocol:** Radio buttons for Any, TCP (selected), UDP, and ICMP.
- Gateway Port:** An empty text input field.
- Rule Name:** Port_
- Description - optional:** An empty text input field with a slash icon at the end.
- Source IP:** A dropdown menu with "Any" selected.
- Source Port:** A dropdown menu with "Any" selected.

At the bottom right of the dialog, there are two buttons: "CANCEL" and "SAVE".

Create Forward Rule:

1. Click **+ ADD RULE**.
2. Select action **Forward**.
3. Specify a value of priority, protocol, gateway port, rule name, and description (optional).
4. Specify a source IP or a subnet.
5. Specify a destination IP and port.



The screenshot shows the 'Add Rule' dialog box with the following fields and options:

- Action:** Forward (selected)
- Priority:** 501
- Protocol:** TCP (selected), UDP (unselected)
- Gateway Port:** (empty)
- Rule Name:** Port_
- Description - optional:** (empty)
- Source IP:** Any
- Source Port:** Any
- Destination IP:** (empty)

Buttons: CANCEL, SAVE

6. Click **SAVE**.



NOTE

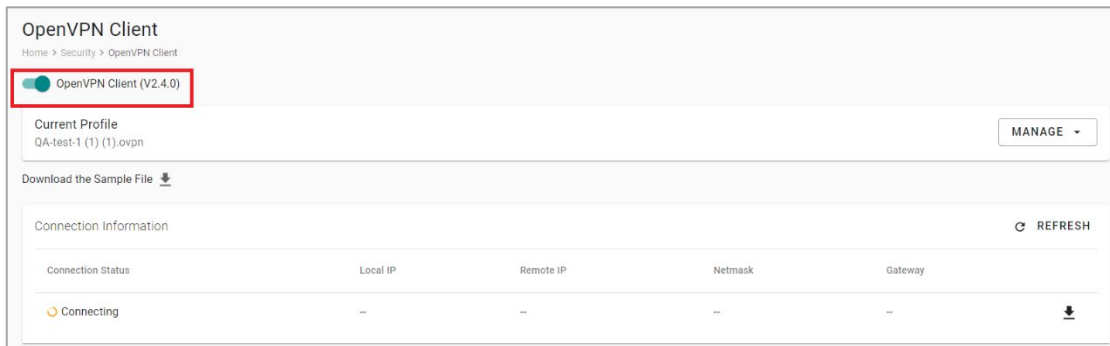
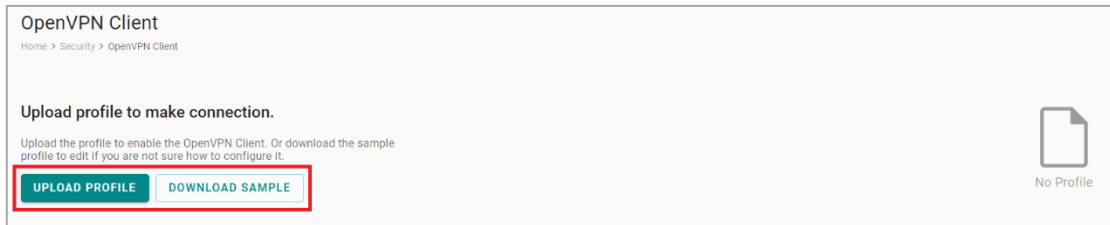
AIG Edge reserves priority 1 to 500 for system default rules. The priority range 501 to 1000 is for **Forward** action rules; while the range 1001 to 1500 is for **Allow** action rules.

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.
3. Import the OpenVPN profile.
You should see it listed in the OpenVPN client.
4. 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.



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.

Account	Role	Status
admin (you)	Administrator	Active
Josh	Administrator	Active
Justin	Administrator	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
<p>Create New Account</p> <p>Account Josh 4/16</p> <p>Role Administrator</p> <p>Password</p> <p>Contains at least 8 characters Contains at least 1 number</p> <p>Confirm Password</p> <p>Email - optional</p> <p>CANCEL SAVE</p>	<p>Create New Account</p> <p>Account Josh 4/16</p> <p>Role Administrator</p> <p>Password</p> <p>Confirm Password</p> <p>Email - optional</p> <p>CANCEL SAVE</p>

Managing Existing User Accounts

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

Accounts

Home > Security > Account Management > Accounts

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.

Roles

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

MOXA AIG-101-T Administrator admin

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	⋮
ricky --	1 account	⋮
lynn --	1 account	⋮
albert --	1 account	⋮

Items per page: 10 1 - 5 of 5 < >

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 **SAVE** to create the role in the system.

Create New Role

Basic Information

Role Name
_____ 0 / 30

Description - optional
_____ 0 / 100

Access Permissions

You must grant at least one privilege to this role.

- Azure IoT Edge
- AWS IoT Core
- Azure IoT Device
- Moxa DLM Service
- Modbus Master
- MQTT Client
- OPC UA Server
- Sparkplug
- Device Management
- User/Role Management

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

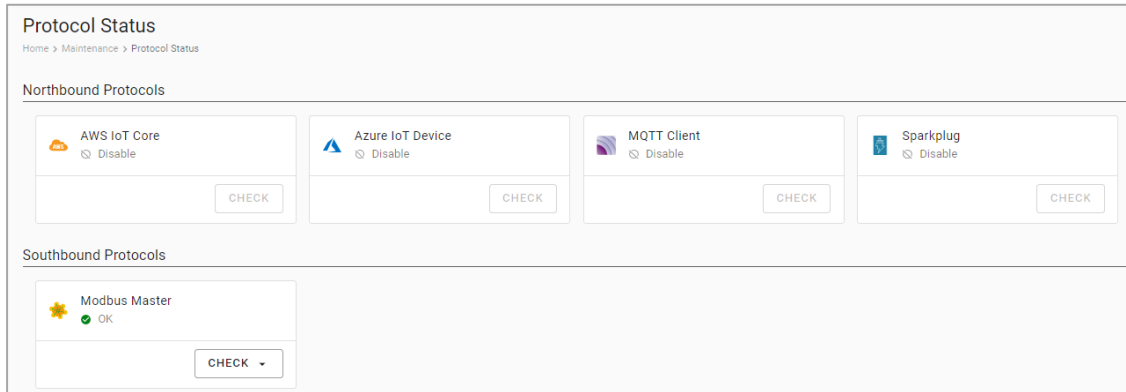
Protocol Status

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

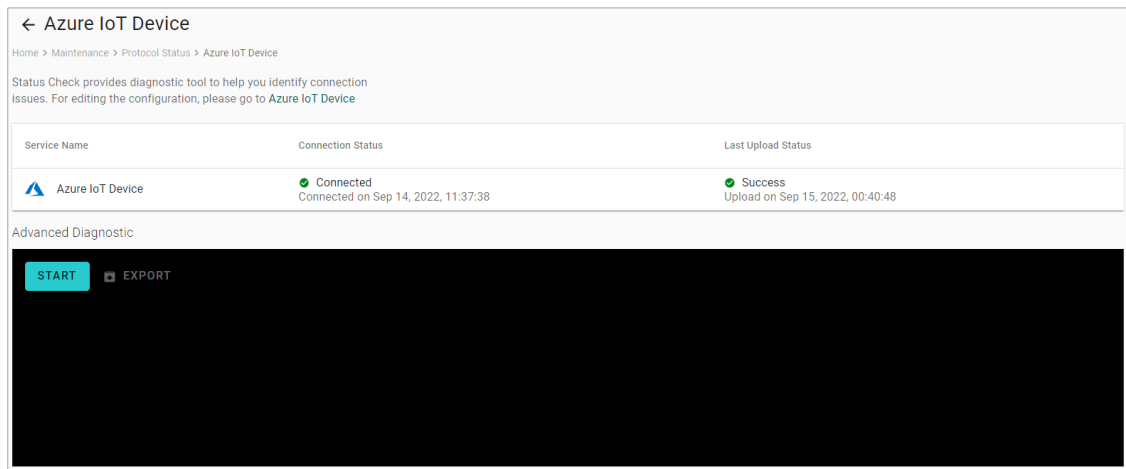
When you access the page, you can see an overview of the status for Northbound Protocols and Southbound Protocols.

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

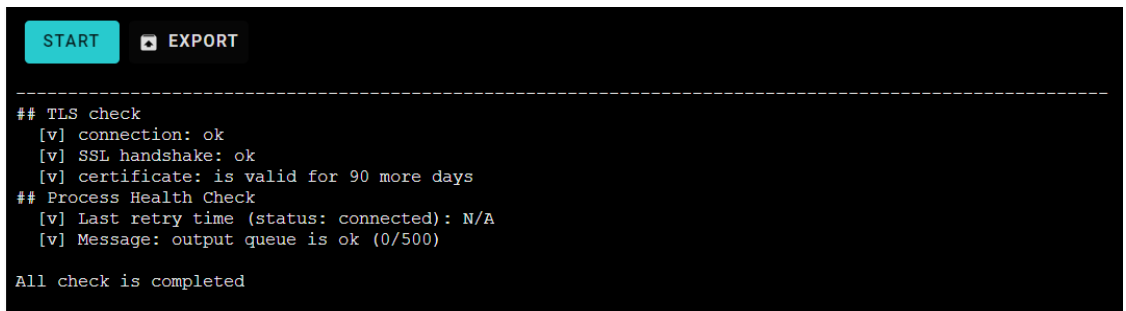
1. Click **CHECK**.



2. Click **START**. (The example below selects Azure IoT Device. The steps may vary depending on the protocol you choose.)



3. View the logs to identify the issue.



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

For Modbus troubleshooting, do the following:

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

← Modbus Master - TCP ▾

Home > Maintenance > Protocol Status > modbus master - TCP

Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to **Modbus Master TCP**.

Diagnostic Traffic Monitoring

Modbus Overview (Auto-refresh after 3s)

Number of Connections	Send Requests	Received Valid Responses	Received Invalid Responses	Received Exceptions	Timeout
1	47537	47537	0	0	0

Connections (Auto-refresh after 3s)

Slave ID	Status	Remote IP/Port	Send Requests	Received Valid Responses	Received Invalid Responses	Received Exceptions	Timeout
1	OK	10.123.12.59:502	47537	47537	0	0	0

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

← Modbus Master - TCP ▾

Home > Maintenance > Protocol Status > modbus master - TCP

Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to **Modbus Master TCP**.

Diagnostic **Traffic Monitoring**

STOP Capturing ...

Auto scroll **▼ FILTER** **EXPORT**

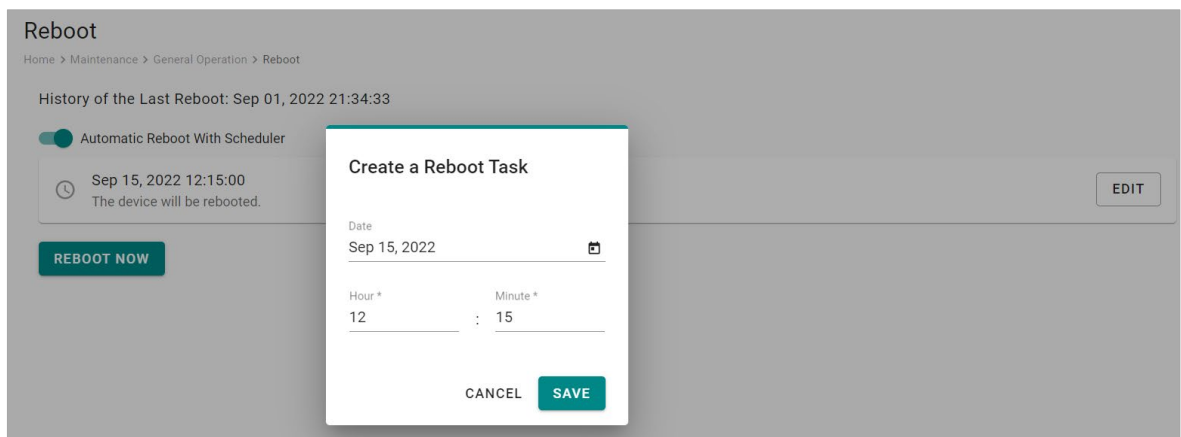
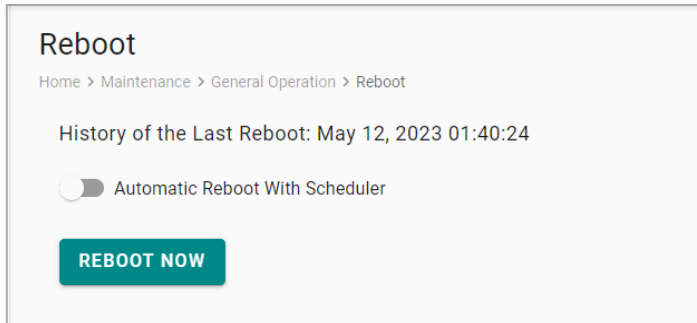
No.	Time	Send/Receive	Remote IP	Slave ID	Function Code	Data
197	16:00:29.053	WRITE	192.168.127.2:502	1	2	44B500000006010200000008
198	16:00:29.070	READ	192.168.127.2:502	1	2	44B50000000401020100
199	16:00:29.103	WRITE	192.168.127.2:502	1	4	44B600000006010400100010
200	16:00:29.120	READ	192.168.127.2:502	1	4	44B60000002301042000000000000000000000000000000000...
201	16:00:29.145	WRITE	192.168.127.2:502	1	4	44B700000006010400300001
202	16:00:29.159	READ	192.168.127.2:502	1	4	44B7000000050104020000

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

General Operation

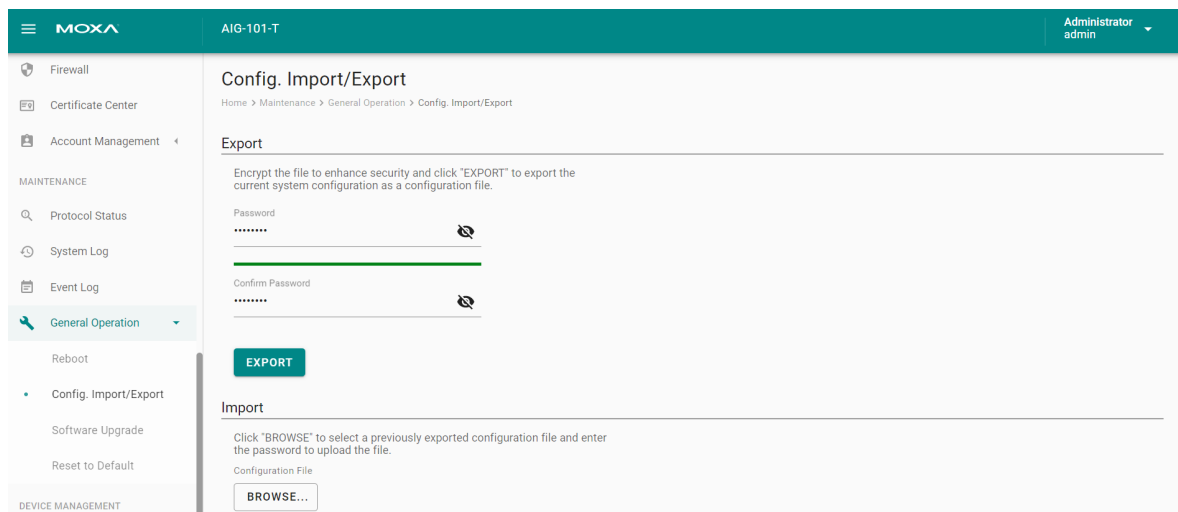
Reboot

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.



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.



Firmware Upgrade

Go to **General Operation > Firmware Upgrade** to upgrade this device with Moxa's software packages. There are two approaches to upgrading AIG: **Upgrade From the Local Drive** and **Download Over the Air**.

Upgrade From the Local Drive: click **BROWSE** and select the software package file in *.deb file format on your computer, then click **UPLOAD**.

Software Upgrade

Home > Maintenance > General Operation > Software Upgrade

Upgrade

You may upload the upgrade pack from your local drive or download it over-the-air. [Upgrade Settings](#)

Upgrade From the Local Drive
Choose the upgrade pack (*.deb) from your local drive and upload it to your IIoT gateway. The installation process will start automatically after the upload is complete.

Download Over the Air
Specify the URL of your repository or a trusted source from where the upgrade pack (*.yaml) can be downloaded and then uploaded to your IIoT gateway. The installation process will start automatically after the download is complete.

Software Upgrade File

Download Over the Air: Enter the file URL. For additional details, see <https://github.com/TPE-TIGER/AIG301-501-Technical-Document/blob/main/documents/AIG%20Software%20Upgrade.md>

Software Upgrade

Home > Maintenance > General Operation > Software Upgrade

Upgrade

You may upload the upgrade pack from your local drive or download it over-the-air. [Upgrade Settings](#)

Upgrade From the Local Drive
Choose the upgrade pack (*.deb) from your local drive and upload it to your IIoT gateway. The installation process will start automatically after the upload is complete.

Download Over the Air
Specify the URL of your repository or a trusted source from where the upgrade pack (*.yaml) can be downloaded and then uploaded to your IIoT gateway. The installation process will start automatically after the download is complete.

Upgrade File URL

Reset to Default

To clear all the settings to configuration default:

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

If you want to reset to Factory default, go to **General Operation > Reset to Default >** press **RESET** under Factory Reset.



NOTE

The configurations and firmware will be reset back to the factory default.

Reset to Default

Home > Maintenance > General Operation > Reset to Default

Configuration Reset

If you are having trouble determining the root cause of the problem with ThingsPro Edge, you can try to reset the configuration (excludes **Event Logs** and **EULA agreement**).

- > Show storage location of the log files explanation

Reserve Network Settings

RESET

Factory Reset

If you want to reset the device back to the factory default use the **Factory Reset** function.

RESET

Enablement

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

System ^

DHCP Server - LAN1 ?	<input type="checkbox"/>
DHCP Server - LAN2	<input type="checkbox"/>
Event Log	<input checked="" type="checkbox"/>
HTTP Service	<input type="checkbox"/>
HTTPS Service	<input checked="" type="checkbox"/>
Internet Check Alive Service ?	<input type="checkbox"/>
Local Console	<input checked="" type="checkbox"/>
NAT Service ?	<input type="checkbox"/>
NTP Service	<input type="checkbox"/>
SD Card	<input type="checkbox"/>
SSH Server	<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"/>
Wi-Fi1	<input type="checkbox"/>

Provision Service ^


ThingsPro Proxy	<input type="checkbox"/>
<div style="border: 1px solid #ccc; padding: 2px;"><p>Scheduled</p><p>The device provision service will be turned off 15 minutes after the service is restarted.</p></div>	<input checked="" type="checkbox"/>

Diagnostic

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 **Diagnostic > 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.

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

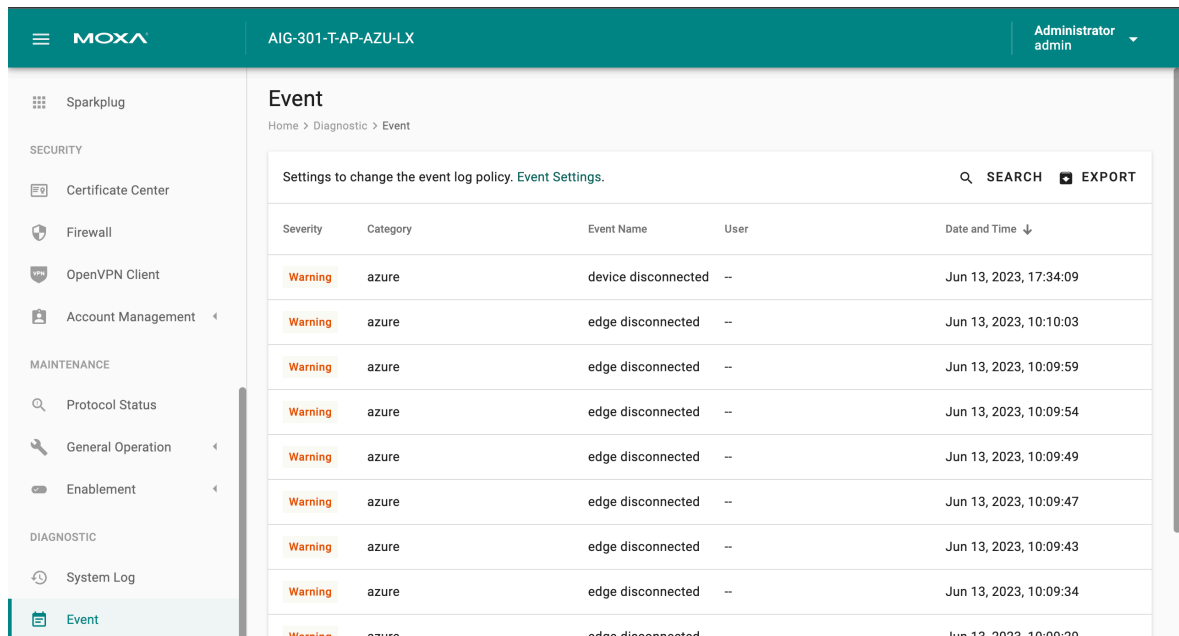
Enable Time to Live

CANCEL SAVE

Events

When you face issues, you can go to **Diagnostic** > **Event** check the event logs which record historical events that help you to narrow down the problems. If there are a lot of event logs, you can export the log to easily read and analyze it.

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.



MOXA AIG-301-T-AP-AZU-LX Administrator admin

Event

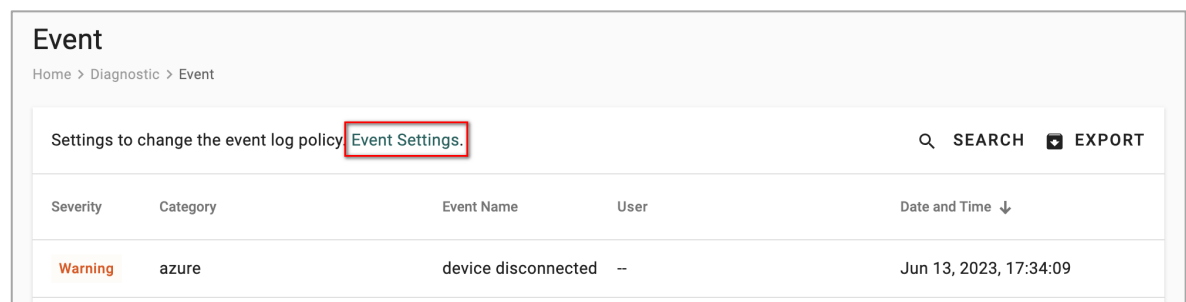
Home > Diagnostic > Event

Settings to change the event log policy. [Event Settings.](#) SEARCH

Severity	Category	Event Name	User	Date and Time ↓
Warning	azure	device disconnected	--	Jun 13, 2023, 17:34:09
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:10:03
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:59
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:54
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:49
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:47
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:43
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:34
Warning	azure	edne disconnected	--	Jun 13, 2023, 10:09:29

Configuring Event Log Settings

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



Event

Home > Diagnostic > Event

Settings to change the event log policy. [Event Settings.](#) SEARCH

Severity	Category	Event Name	User	Date and Time ↓
Warning	azure	device disconnected	--	Jun 13, 2023, 17:34:09

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

MOXA AIG-301-T-AP-AZU-LX Administrator admin

Event Settings

Home > Diagnostic > Event > 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 - 93 of 93, Selected: 58 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

Publish Mode

Publish Mode	Parameters	Value	Description
By Interval	Publish Intervals (sec)	0 to 86400	The frequency of data upload 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 to 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 when one of data item changes in the topic.
	Minimal Publish Interval (sec)	0 to 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 to 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 to 86400	The frequency to synchronize the tag values with the tag hub.
	Idle Timer (sec)	0 to 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.

B. Additional Documentation

Software Downloads

<https://moxa-srs.thingsprocloud.com/home>

Technical Documentation

<https://github.com/TPE-TIGER>

OpenAPI Documentation

<https://github.com/TPE-TIGER/TPE-TIGER.github.io>