

AIG-301 Series User Manual

Version 2.3, November 2025

www.moxa.com/products



© 2025 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

© 2025 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	35
OPC UA Server	41
Edge Computing	45
Function Management	45
Tag Management	46
Cloud Connectivity	48
Azure IoT Edge	48
Azure IoT Device	53
AWS IoT Core	57
Generic MQTT Client	61
Sparkplug	65
Moxa DLM Service	73
Sign Up DLM Account	75
Security	76
Certificate Center	76
Firewall	76
OpenVPN Client	80
Account Management	81
Maintenance	84
Protocol Status	84
General Operation	86
Diagnostic	90
4. Security Hardening Guide	93
A. Appendix	96
Publish Mode	96
B. Additional Documentation	97
Software Downloads	97
Technical Documentation	97
OpenAPI Documentation	97

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 collect data from 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 via cloud solutions such as Azure Device Twin. 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 attacks during the bootup process.

The AIG QuickON utility simplifies the device provisioning process, and the Moxa DLM Service offers a solution to further streamline operations for efficient remote device management.



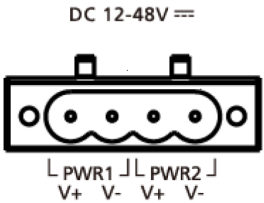
NOTE

The AIG is not designed to operate in NAT mode. Doing so may compromise its performance and security. Refrain from using NAT mode to ensure optimal functionality. For further guidance on strengthening security, see [Security Hardening Guide](#).

2. Getting Started

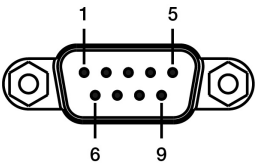
Connecting the Power

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

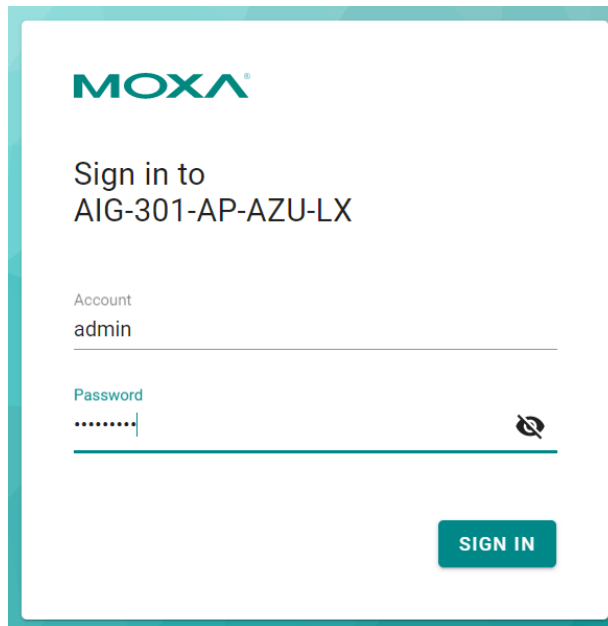
The default LAN2 IP address to access the web console of the AIG is 192.168.4.127.

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**



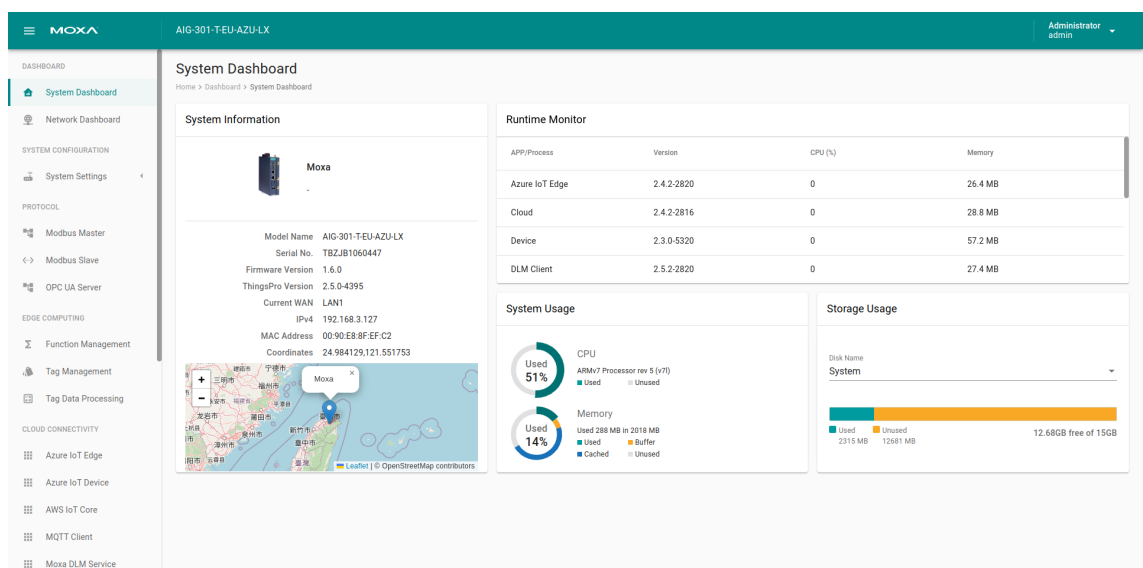
The login page features the Moxa logo at the top. Below it, the text 'Sign in to AIG-301-AP-AZU-LX' is displayed. There are two input fields: 'Account' with the value 'admin' and 'Password' with masked characters. A 'SIGN IN' button is located at the bottom right of the form area.



NOTE

After the first login, we force a password change to comply with general security policies and practices and to increase the security of your device.

You will see the following homepage after logging in successfully.

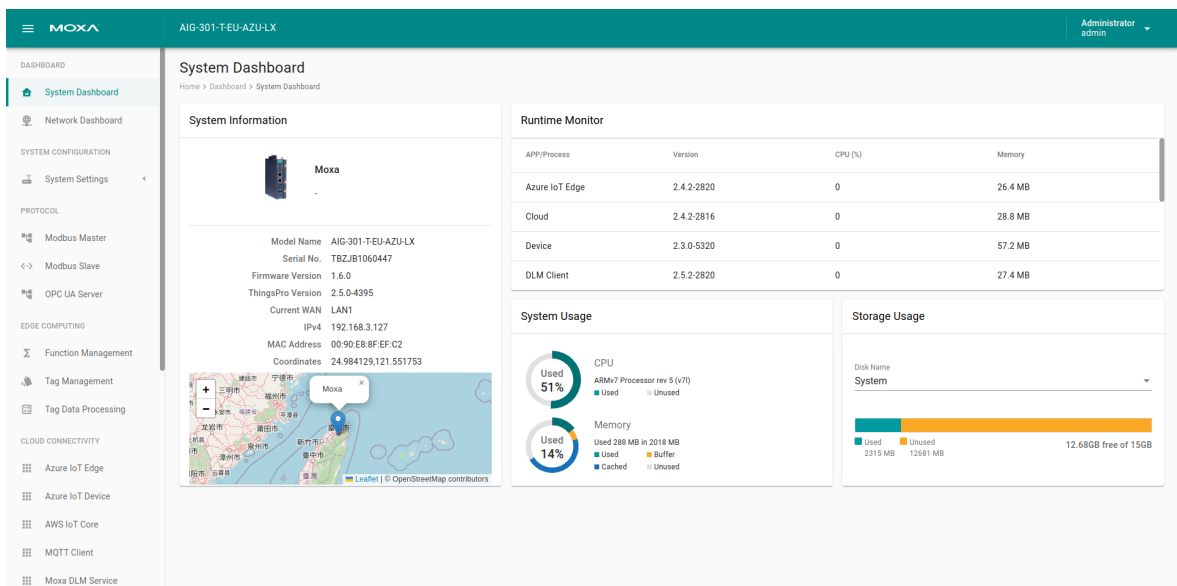


3. Web Console

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.

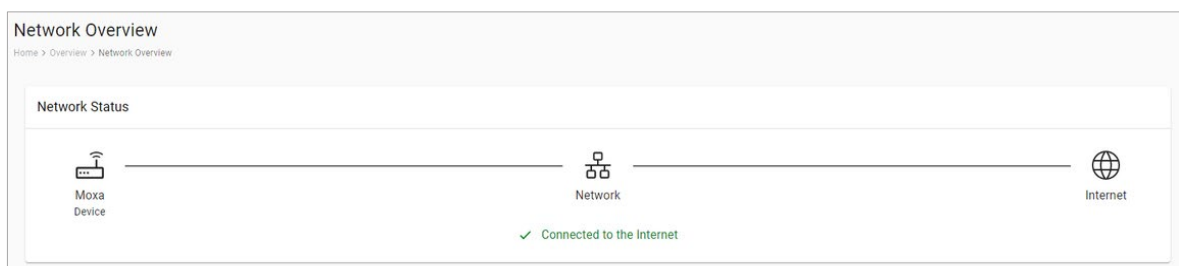


CAUTION

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.**

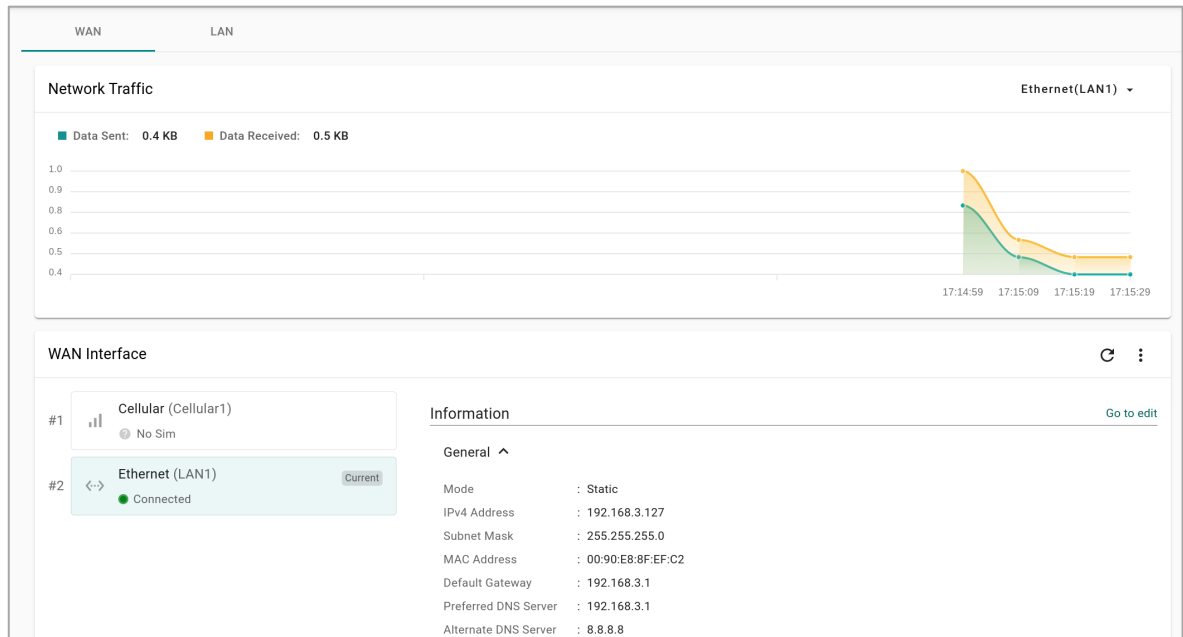
Network Dashboard

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.



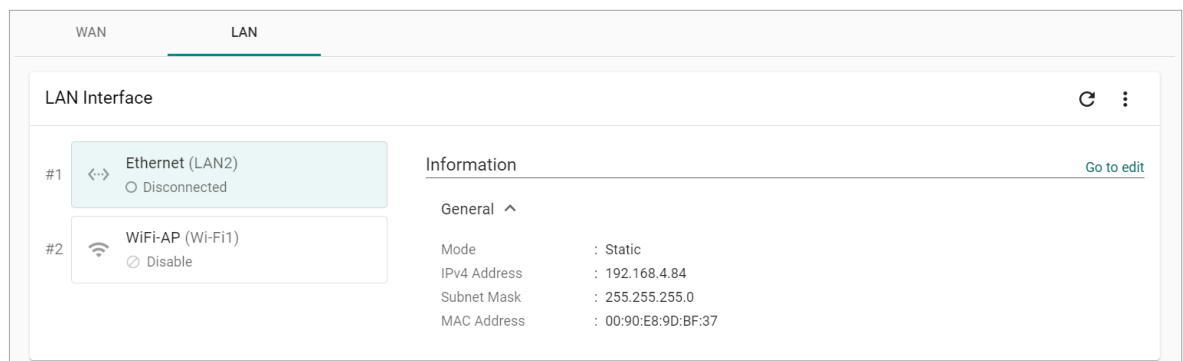
WAN

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.

The screenshot shows the Moxa web interface for the AIG-301-AP-AZU-LX device. The left sidebar contains navigation options: DASHBOARD (System Dashboard, Network Dashboard) and SYSTEM CONFIGURATION (System Settings, General, IP Address, Cellular). The main content area is titled 'General' and shows the 'System' tab selected. It contains two text input fields: 'Server/Host Name' with the value 'Moxa' and 'Description - optional' with the value 'Factory A1'. A 'SAVE' button is located at the bottom of the form.

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."

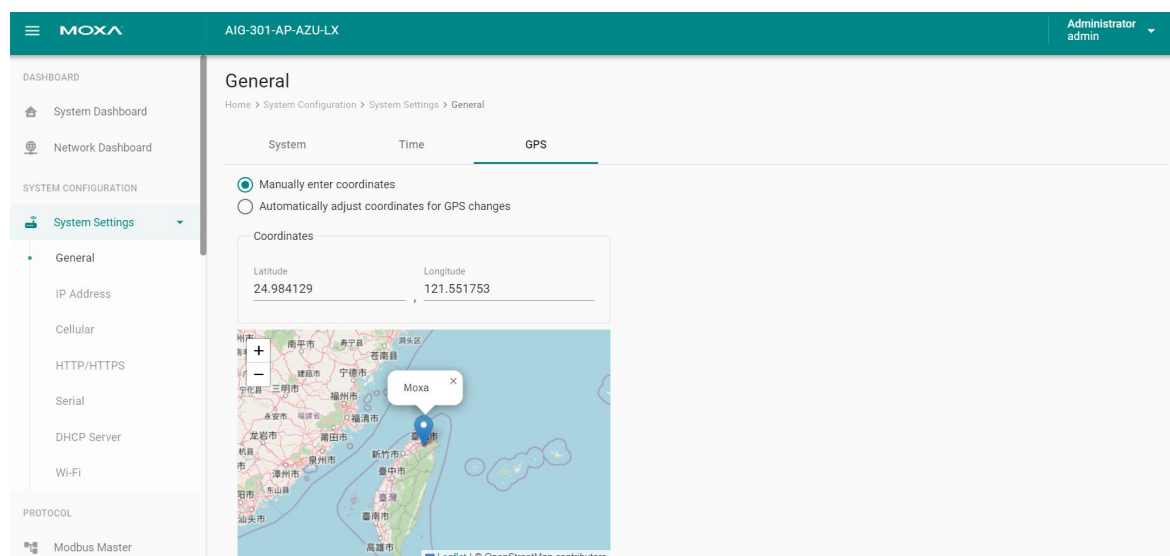
Go to **System Settings > General > Time** to select a time zone. Choose between the Manual or Auto option to update the system time.

The screenshot shows the Moxa web interface for the AIG-301-AP-AZU-LX device, specifically the 'Time' tab under 'General' settings. It displays the 'Current date and time' as Mar 07, 2023 18:02:45. The 'Time Zone' is set to '(GMT +08:00) Asia/Taipei'. Under 'Sync Mode', the 'Manual' radio button is selected. There is a 'Sync with browser' button and a date/time picker showing 'Mar 07, 2023' with fields for Hour (18), Minute (1), and Second (51). A 'SAVE' button is at the bottom.

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.

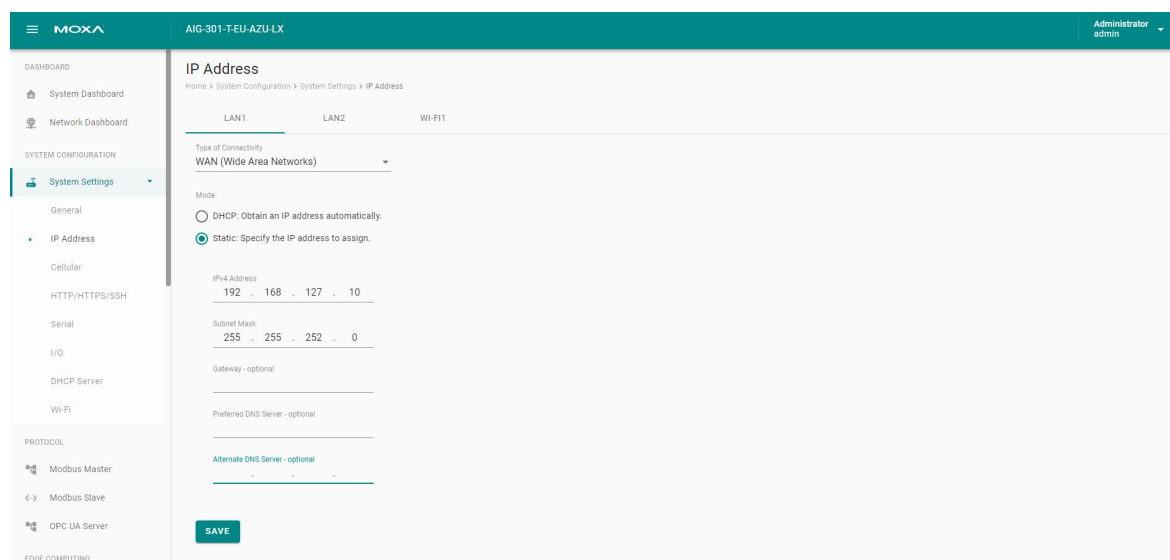


System Settings—IP Address

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.

To maintain a reliable connection, we recommend enabling the **Check-alive** function and the **Store and Forward** function. These features help prevent unexpected issues, such as those caused by base station handovers or module resets.

Cellular

Home > System Configuration > System Settings > Cellular

CELLULAR1

☒ Enable cellular data communication

Profile Settings

Create and manage profiles for a SIM with its data plan.

Network Type
Auto

Connection Retry Timeout (sec)
180

Mode
☐ Auto
Auto detect the correct mobile operator and create a profile
☒ Manual
Create customized profile

Profile List

#1

SIM1
SIM1 · Static APN

+ CREATE

Check-alive

☒ Enable check-alive

Target Host
8.8.8.8

Ping Interval (sec)
60

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

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

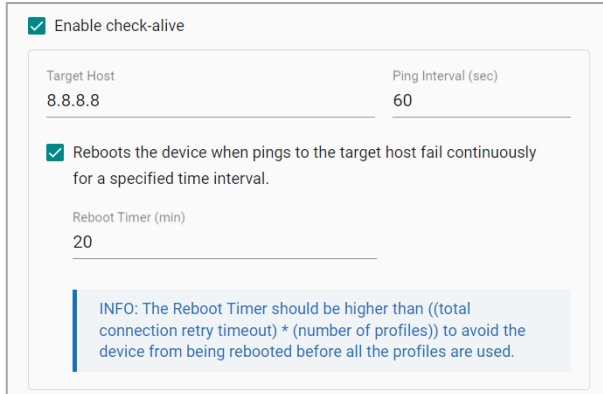
CANCEL DONE

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.



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



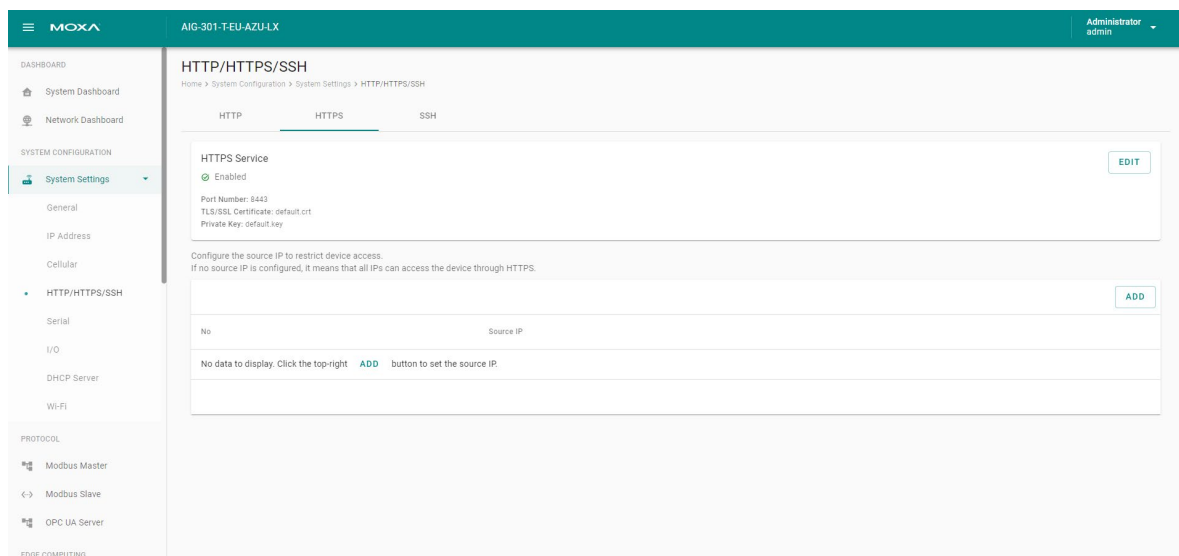
NOTE

If you are using a private APN without DNS configuration, the Enable check-alive process will fail. An accessible DNS server is required to verify connectivity.

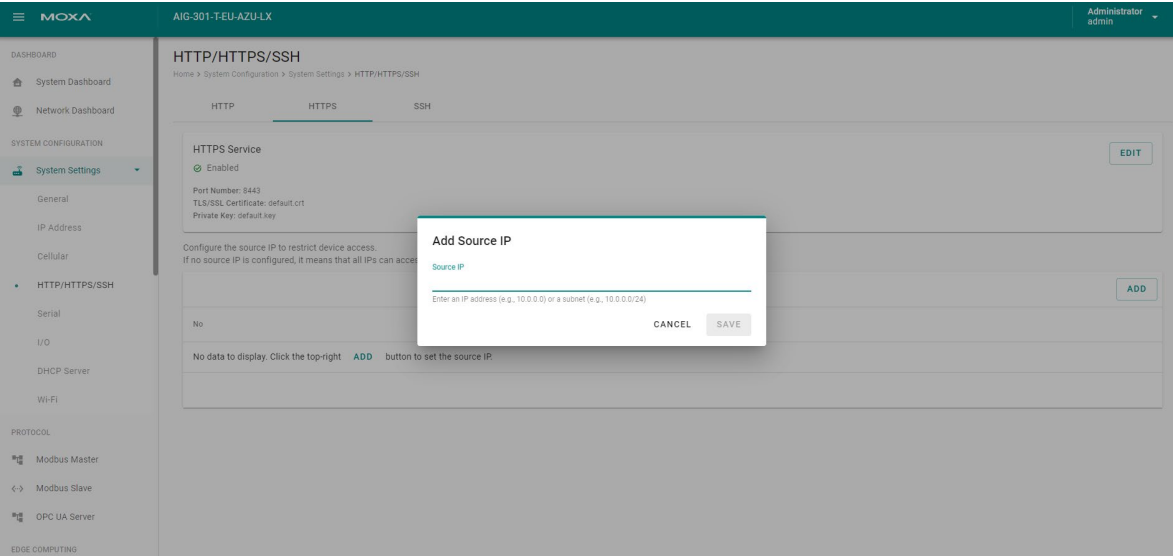
System Settings—HTTP/HTTPS

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.

The default setting for **HTTP redirect to HTTPS** is **Enabled** (starting with firmware version v1.8.0) to enhance security capabilities. 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.



NOTE

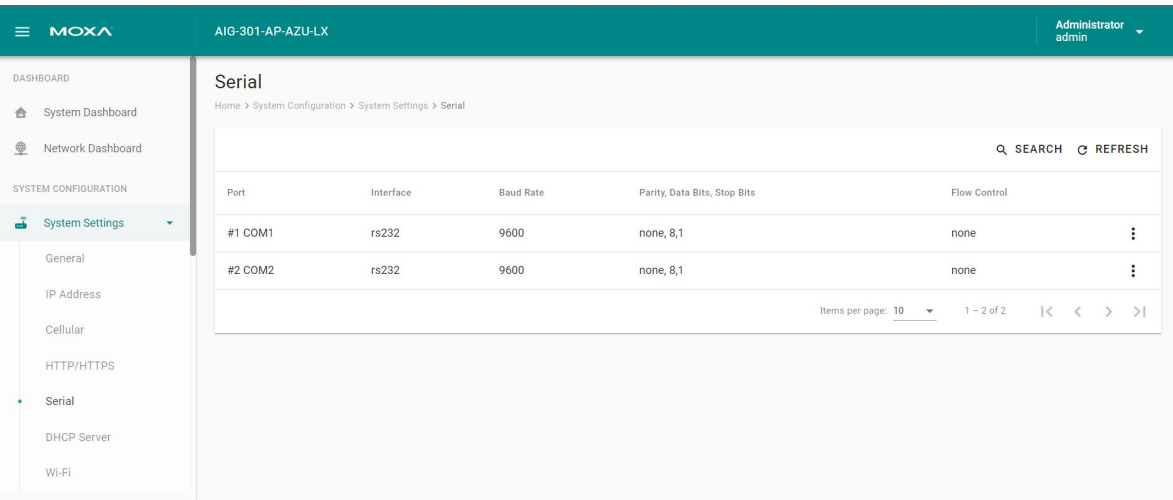
After the first SSH login, we force a password change to comply with general security policies and practices and to increase the security of your device.

System Settings—Serial

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

To configure serial settings, 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.



MOXA

AIG-301-AP-AZU-LX

Administrator admin

DASHBOARD

System Dashboard

Network Dashboard

SYSTEM CONFIGURATION

System Settings

General

IP Address

Cellular

HTTP/HTTPS

Serial

DHCP Server

Wi-Fi

PROTOCOL

Modbus Master

← Port #1

Home > System Configuration > System Settings > Serial > Port #1

Serial Settings

Alias - optional

COM1

Interface

rs232

Baud Rate

9600

Parity

none

Data Bits

☐ 7
☒ 8

Stop Bits

☒ 1
☐ 2

Flow Control

none

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.

I/O

Home > System Configuration > System Settings > I/O

REFRESH

Channel	Mode	Status	
DI-01	DI	OFF	
DI-02	DI	OFF	
DI-03	DI	OFF	
DI-04	DI	OFF	

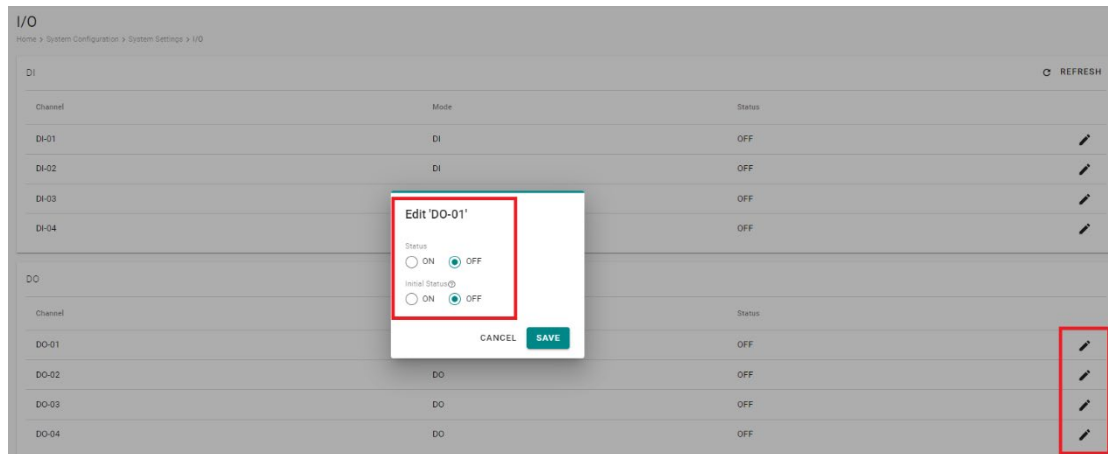
Edit 'DI-01'

☒ Enable auto sampling
Sampling Rate (sec)
5

CANCEL SAVE

Channel	Mode	Status	
DO-01	DO	OFF	
DO-02	DO	OFF	
DO-03	DO	OFF	
DO-04	DO	OFF	

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



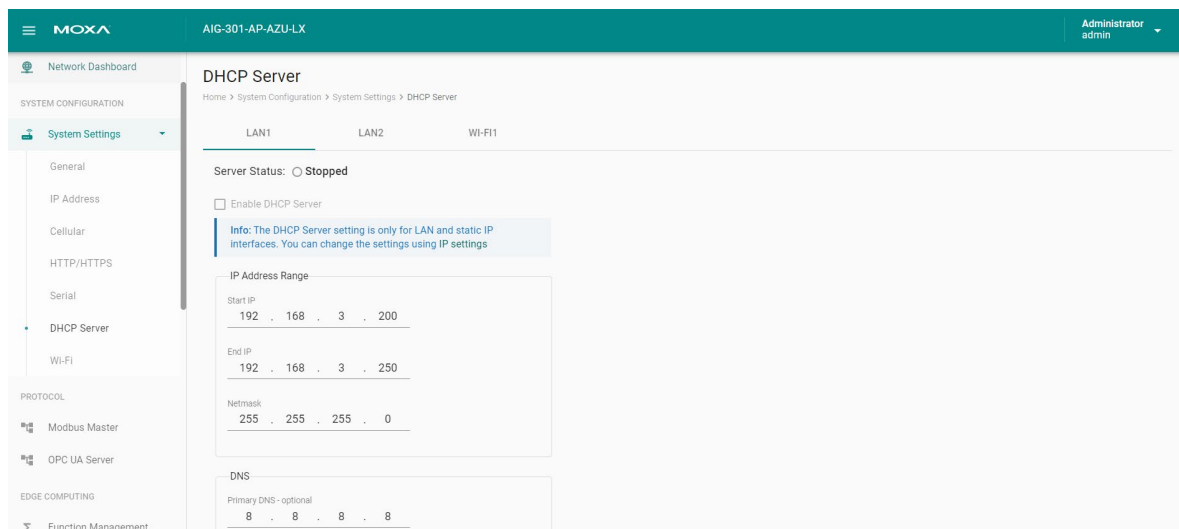
Parameter	Value	Description
Status	ON OFF	High voltage Low voltage

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.



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 specify a **Password** for the Wi-Fi AP.
3. Specify the **Region**, **Channel** in the advanced settings.
4. Click **SAVE**.

The screenshot shows the MOXA web interface for the AIG-301-AP-AZU-LX device. The left sidebar contains navigation menus for Dashboard, System Configuration, and Protocol. The main content area is titled 'Wi-Fi' and shows the configuration for 'Wi-Fi1'. The 'Enable Wi-Fi' checkbox is checked. The 'Wi-Fi Mode' is set to 'Wi-Fi AP'. Under 'General Settings', 'Broadcast SSID' is checked, the SSID is 'moxa-sample-ap', and the Password (WPA2-PSK) is masked. Under 'Advanced Settings', the Band is '2.4GHz (802.11 b/g/n)', the Region is 'Taiwan', and the Channel is '6'.



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**.

The 'Add by SSID' dialog box has three input fields: 'SSID', 'Security Mode' (a dropdown menu currently showing 'WPA/WPA2 Personal'), and 'Password'. At the bottom right, there are two buttons: 'CANCEL' and 'ADD'.

The 'Add by Scan Results' dialog box shows a list of detected Wi-Fi networks. The list includes: SQA3_WiFi6, sqa-llot-lan-50G, SQA2-TestBed-AWK3131A, SQA-LAB-TV, and .M-Guest. Each entry has a lock icon and a signal strength indicator. At the bottom, there are 'CANCEL' and 'NEXT >' buttons.

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

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

The screenshot shows the Moxa AIG-301-AP-AZU-LX web interface. The left sidebar contains a navigation menu with sections: DASHBOARD, SYSTEM CONFIGURATION, PROTOCOL, and EDGE COMPUTING. Under SYSTEM CONFIGURATION, 'System Settings' is selected. The main content area is titled 'Wi-Fi' and shows configuration options: 'Enable Wi-Fi' (checkbox), 'Wi-Fi Mode' (dropdown), 'Wi-Fi Client' (dropdown), 'AP List' (with a '+ CREATE' button), 'IP Settings' (with radio buttons for 'DHCP: Obtain an IP address automatically' and 'Static: Assign IP address by manual configuration'), and 'Check-alive' (checkbox). A green 'SAVE' button is located at the bottom of the configuration area.

Protocol

Modbus Master

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

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

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

The screenshot shows the 'Modbus Master' configuration page. The top section is titled 'Modbus Master' and includes a 'MANAGE' button. Below this, there are two main sections: 'Modbus TCP' and 'Modbus RTU/ASCII'. The 'Modbus TCP' section shows a 'TCP' button with the text 'Not configured'. The 'Modbus RTU/ASCII' section shows two buttons: 'COM1 (RTU)' with '1 Device, 1 Command' and 'COM2 (RTU)' with 'Not configured'. At the bottom right of the page, there are 'DISCARD' and 'APPLY' buttons.

Modbus TCP

Basic Settings

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

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

Search command name:

ADD DEVICE

Basic Settings

Initial Delay (ms)
0

Maximum Retry
3

Response Timeout (ms)
1000

CANCEL SAVE

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.

← TCP ▾

Home > Southbound Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

Search Command Name

ADD DEVICE

Select a device to view its details.

Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.

← Create New Device

1 Basic Settings 2 Command Optional 3 Confirm

☒ Enable This Device

Device Name
SE_Meter

Slave IP
192 . 168 . 127 . 50

Slave Port
502

Slave ID
1

CANCEL NEXT >

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.

← Create New Device

1 Basic Settings 2 Command Optional 3 Confirm

☒ Enable this command

Basic

Command Name

Function
03 - Read Holding Registers

Read Holding Registers

Read Starting Address 0 Read Quantity 10

Trigger
Cyclic

Poll Interval (ms)
1000

CANCEL DONE

+ ADD COMMAND

Poll Interval (ms) Enable

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

CANCEL NEXT >

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
Enable

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

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

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

🔍 Search command name...

ADD DEVICE

SE_Meter
Enable

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

SE_Meter

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

Trigger	Poll Interval (ms)	Enable
Cyclic	1000	Enable

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

Import Command Configuration

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

Command Configuration

BROWSE...

CANCEL DONE

Editing GO TO APPLY SETTINGS

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

Modbus Master

Home > Protocol > Modbus Master

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

MANAGE ▾

Modbus TCP

TCP
1 Device, 1 Command

Modbus RTU/ASCII

COM1 (RTU)
1 Device, 1 Command

COM2 (RTU)
Not configured

Editing DISCARD **APPLY**

Regarding the exported CSV file, here is the description of each column.

Parameter	Value	Default	Description
name	Alphanumeric string	–	Name the command
enable	0: disable command 1: enable command		Enable/ Disable the command
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.
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	–	How to collect data from the Modbus device
readAddress	0 to 65535	–	Modbus registers the address for the collected data Note: Not applicable for write commands.
readQuantity	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	–	How much data to read. Note: Not applicable for write commands.
writeAddress	0 to 65535	–	Modbus registers the address for the written data. Note: Not applicable for read commands.
writeQuantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	–	How much data to write. Note: Not applicable for read commands.
pollInterval	100 to 86400000	–	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.
swap	0: Big-endian (None, conversion AB CD → AB CD) 1: Big-endian byte swap (Byte, conversion AB CD → BA DC) 4: Little-endian (conversion AB CD → DC BA) 5: Little-endian byte swap (conversion AB CD → CD AB)	–	Byte swap mode

Parameter	Value	Default	Description
fpFunc	Applicable only when the function code is 5, 6, 15, 16, or 23. For other function codes, set this value to 0. When the command trigger mode (mode) is cyclic (0): 0: Continue – retain the latest data 1: Continue – clear data to zero 2: Continue – set to user-defined value (fpData) When the command trigger mode (mode) is data change (1): 0: Pause 1: Continue – clear data to zero 2: Continue – set to user-defined value (fpData)		Fail-safe Mode Note: Not applicable for read commands.
fuTout	Applicable only when the function code is 5, 6, 15, 16, or 23. Type: Integer Minimum: 1 Maximum: 86400		Fail-safe Timeout (seconds) Note: Not applicable for read commands.
fpData	Applicable only when the function code is 5, 6, 15, 16, or 23. Represented as a hexadecimal string, with bytes separated by spaces. For function codes 5, 15: Byte count = $\lceil \text{writeQuantity} \div 8 \rceil$ Modbus addresses are grouped in sets of 8 (from low to high), mapped left to right into each byte of fpData. Within a byte, the lowest address is mapped to the LSB, and the highest address to the MSB. For function codes 6, 16, 23: Byte count = $\text{writeQuantity} \times 2$ Modbus addresses are grouped in sets of 1 (from low to high), mapped left to right into two bytes of fpData.		User-defined Fail-safe Value Note: Not applicable for read commands.
scalingFunc	0: None 1: Slope-intercept 2: Point-slope		Scaling Note: The Modbus Master does not support write command scaling, so the value in the exported file will not take effect
interceptSlope	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double)		Slope
interceptOffset	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double)		Offset
pointSourceMin	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double)		Source data minimum value

Parameter	Value	Default	Description
pointSourceMax	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double) Note: pointSourceMax cannot be the same as pointSourceMin		Source data maximum value
pointTargetMin	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double)		Target data minimum value
pointTargeMax	Double precision floating-point number (double) Range: $\pm 1.79 \times 10^{(-308)} \sim \pm 1.79 \times 10^{(+308)}$ (IEEE 754 Double)		Target data maximum value
sfFunc	Applies when function codes are 1, 2, 3, 4, 23; set to 0 for others 0: Pause 1: Continue – Clear data to zero 2: Continue – Set to user-defined value (stData)		Status Function (applies when a read command error or timeout occurs) Note: Not applicable for write commands.
stData	Required only for function codes 1, 2, 3, 4, 23 Hexadecimal string, bytes separated by spaces For function codes 1, 2: - Byte count = $\lceil (\text{readQuantity})/8 \rceil$ - Modbus addresses grouped in sets of 8, mapped from left to right in stData Within each byte: smallest address → LSB; largest address → MSB For function codes 3, 4, 23: - Byte count = $\text{readQuantity} \times 2$ - Modbus addresses grouped by 1, mapped left to right in stData (two bytes per address)		Custom Status Value. Note: Not applicable for write commands.
tagName	String, length 1–128 characters. Allowed characters: uppercase/lowercase letters, digits, ".", "_", "~", "-". Must not duplicate other tag names in the device. Reserved name "status" cannot be used.		Tag Name

Parameter	Value	Default	Description
dataType	String For function codes 1, 2, 5, 15: Options: "boolean", "int8", "uint8", "string", "raw" "int8" and "uint8" allowed only if readQuantity or writeQuantity is a multiple of 8 For function codes 3, 4, 6, 16, 23: Options: "boolean", "int8", "int16", "int32", "int64", "uint8", "uint16", "uint32", "uint64", "float", "double", "string", "raw" "int32", "uint32", "int64", "uint64", "float", "double" allowed only if (readQuantity × 2) or (writeQuantity × 2) is an integer multiple of the size of the selected type		Tag data type
dataUnit	String		Tag value unit
access	String Valid options: "r", "w", "rw" r: read-only w: write-only rw: read/write		Tag access permission
dataSize	Integer For function codes 1, 2, 5, 15: dataSize = [(readQuantity or writeQuantity)/8] For function codes 3, 4, 6, 16, 23: dataSize = readQuantity × 2 or writeQuantity × 2		Tag data size (bytes); Required only when tag type is "string" or "raw"
offset	Integer Minimum: 0 Maximum: For "string"/"raw" types: max = 0 (one tag per Modbus command) For other types: max = (total number of tags - 1) Total tags = Modbus command data size (bytes) / tag type size (bytes)		Tag index Note: A Modbus command may map to multiple tags. offset specifies the index of this tag within that command.

Modbus RTU/ASCII

Basic Settings

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

Serial Basic Settings

Mode
☒ RTU ☐ ASCII

Initial Delay (ms)
0

Maximum Retry
3

Response Timeout (ms)
1000

☒ Automatically determine the Inter-frame delay
The delay time of data frame transmission that received from the slave device to the upstream will be determined by the system automatically. You may choose to set the delay time manually by un-check this option.

☒ Automatically determine the Inter-character timeout
The timeout interval between characters for Modbus devices that cannot receive Rx signals within an expected interval will be determined by the system automatically. You may choose to set the timeout interval manually by un-check this option.

CANCEL SAVE

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.

← COM2 ▾

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

Operation Mode: RTU

🔍 Search command name...

ADD DEVICE

Select a device to view its details.

Editing

GO TO APPLY SETTINGS

Step 1. Basic Settings

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

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

☒ Enable this device

Device Name
SE_Meter

Slave ID
1

CANCELNEXT >

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 time 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

SE_Meter

Enable

Slave ID: 1

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

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

AIG-301 Series User Manual

33

Management

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

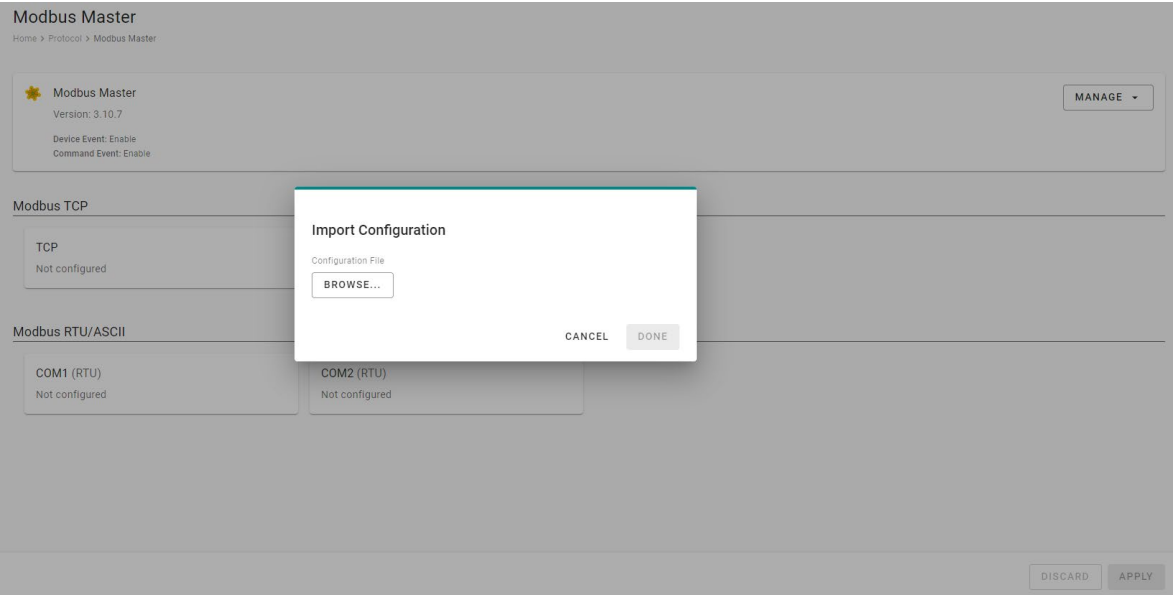
Edit General Settings

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.

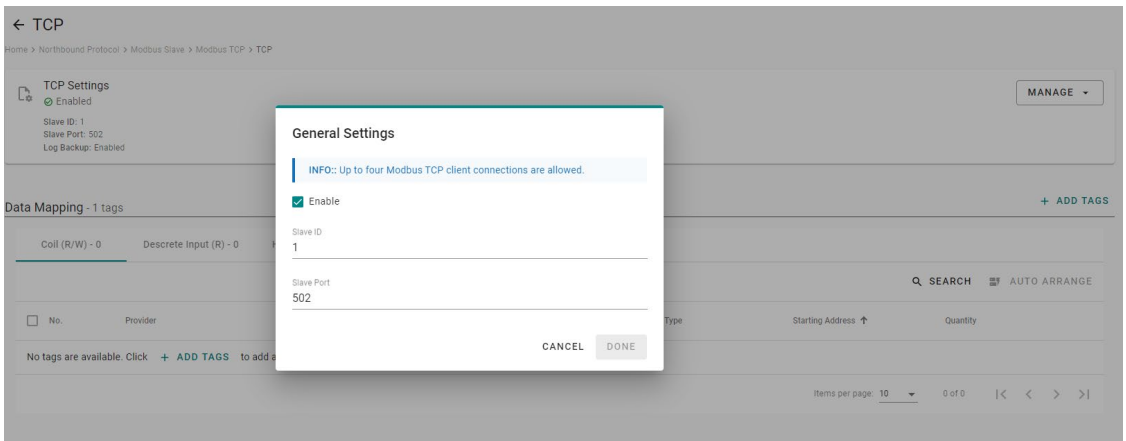
master-tcp-ifaces																																											
@master-tcpMaster		initialDelay	retryCount	responseTou																																							
1	1	0	3	1000																																							
ser-masters																																											
@serMas configId		name																																									
1	1	modbus_serial_master																																									
master-ser-ifaces																																											
@master-serMaster		port	Value format	initialDelay	retryCount	responseT	frameInt	charInterval																																			
1	1	0	0	0	3	1000	0	0																																			
2	1	1	0	0	3	1000	0	0																																			
remote-devs																																											
@remote-masterSer		masterTq	name	enable	slaveId	slaveIp	slaveTcpPort																																				
1	1	1232	1	1.0.0.0	502																																						
2	2	SE_Meter	1	1.0.0.0	502																																						
3	1	GE_Meter	1	1.1.1.1	502																																						
mcmds																																											
@remote name		enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollInterval	swap	fpFunc	fpTouT	fpData	scalingFu	intercept	intercept	pointSou	pointSou	pointTarg	pointTarg	tagName	dataType	dataUnit	access	dataSize																		
1	231	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	Voltage_t1	int16	r		20																			
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	Voltage_t2	int16	r																					
																				1	Voltage_t3	int16	r																				
																				1	Voltage_t4	int16	r																				
																				1	Voltage_t5	int16	r																				
																				1	Voltage_t6	int16	r																				
																				1	Voltage_t7	int16	r																				
																				1	Voltage_t8	int16	r																				

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

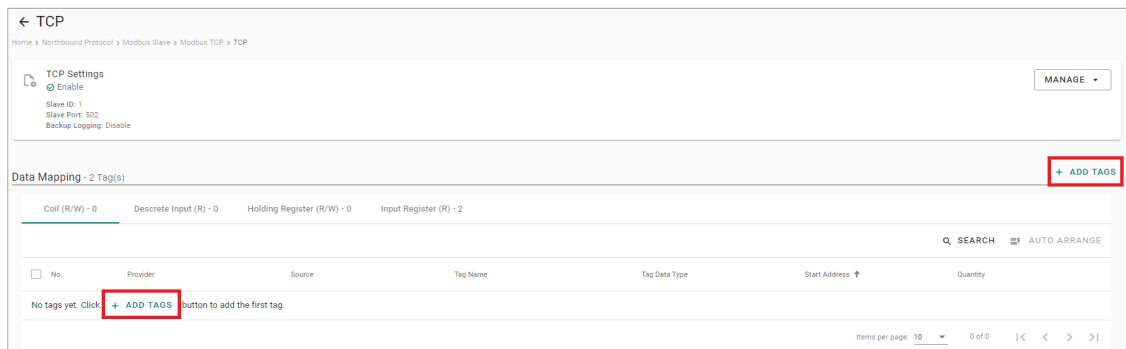
1. Go to **Modbus Slave** and click **TCP** under **Modbus TCP**.



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

Coil (R/W) - 0

Discrete Input (R) - 0

Holding Register (R/W) - 0

Input Register (R) - 4

SEARCH

AUTO ARRANGE

☐ No.	Provider	Source	Tag Name	Tag Data Type	Start Address ↑	Quantity	
☐ 1	modbus_serial_master	ddd	device_info_t2	int16	00000	1	⋮
☐ 2	modbus_serial_master	ddd	Power1	int16	00001	1	⋮
☐ 3	modbus_serial_master	ddd	Power2	int16	00002	1	⋮
☐ 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

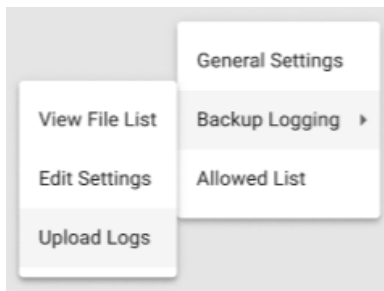
If the data is stored in an SD card, ensure that the SD card is installed before enabling this function. If you replace the SD card, reboot your device and confirm that the backup function is working properly. The SD card should have at least 1 GB free space.

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**.

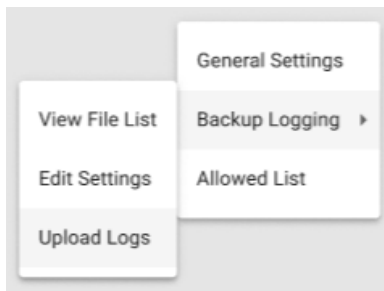


2. Select **Enable the FTP/SFTP uploader**.
3. Select **FTP** for **Upload Method**.
4. Enter the necessary parameters: **Server**, **Port**, **Path**, **Username**, and **Password**.
5. Set the **Upload Interval**.
6. (optional) Click **CHECK CONNECTION** to verify that the communication is working.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

A screenshot of the 'Upload Logs' configuration form. At the top, there is a checkbox labeled 'Enable FTP/SFTP log upload'. Below it, the 'Upload Method' section has two radio buttons: 'FTP' (selected) and 'SFTP'. The 'Upload Information' section contains several input fields: 'Server' (with a 'Port' label and value '22' next to it, and a range '1 ~ 65535' below), 'Path' (with a '/' character), 'Username', and 'Password' (with a toggle icon). Below these is the 'Upload Interval (min)' field with the value '10' and a note 'Upload interval can be 10 ~ 1440'. A 'CHECK CONNECTION' button with a checkmark icon is located below the interval field. 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 of the form 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.

Upload Logs

☒ Enable FTP/SFTP log upload

Upload Method

☐ FTP ☒ SFTP

Upload Information

Server	Port
111.11.11.11	22

Path

/home/stfpuser/stage

Username

sftpuser

Authentication Method

Upload SSH key

SSH Key

5bb65fe6266bd6b6
8f71cb897b90d4b7

Upload Interval (min)

10

CHECK CONNECTION

Info

Click the "CHECK CONNECTION" to check connectivity to the remote server and ensure your connector is properly configured.

CANCEL SAVE

Modbus Capability:

Max. # of Serial Slave Device 31

Max. # of TCP Slave Device 64

Max. # of Command 2048 (Supports Max. 2048 commands across all slave devices)

Max. # of Tags for Modbus Master 3000

Max. # of Tags for Modbus Slave 4500

Max. # of Commands for a Slave Device 256

Max. # of Commands for a TCP Slave Device 2048



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. Click **Manage Account Details** to **CREATE** new accounts.
The default account/password is **admin/moxa** (for firmware version of v1.7.0 and prior).
- Click **CREATE**.
 - Specify an **Account** and **Password**.
 - Click **DONE**.

← Account Management

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

CREATE

No.	Account	
1	admin	⋮

BACK

4. (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

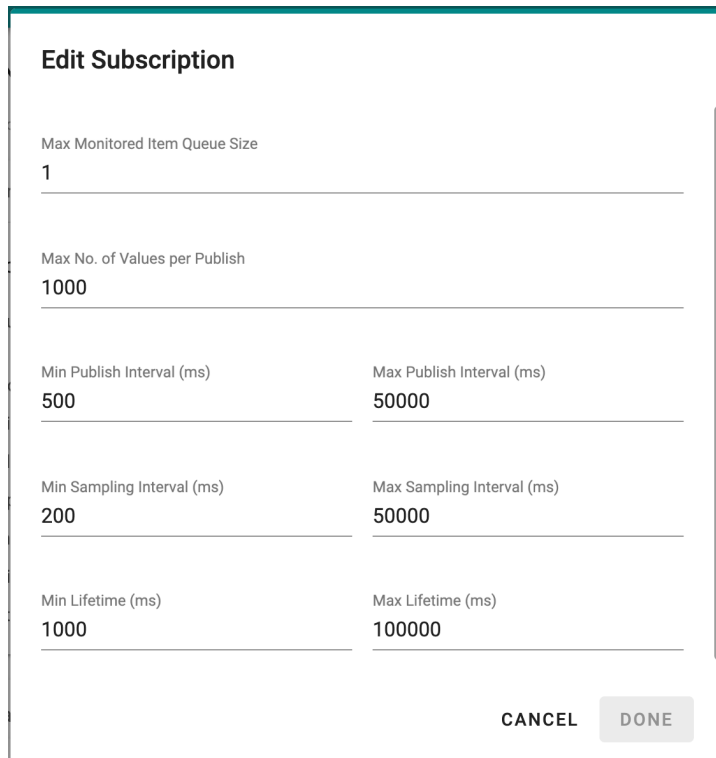
Certificate File

BROWSE...

CANCEL DONE

UPLOAD

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



Edit Subscription

Max Monitored Item Queue Size
1

Max No. of Values per Publish
1000

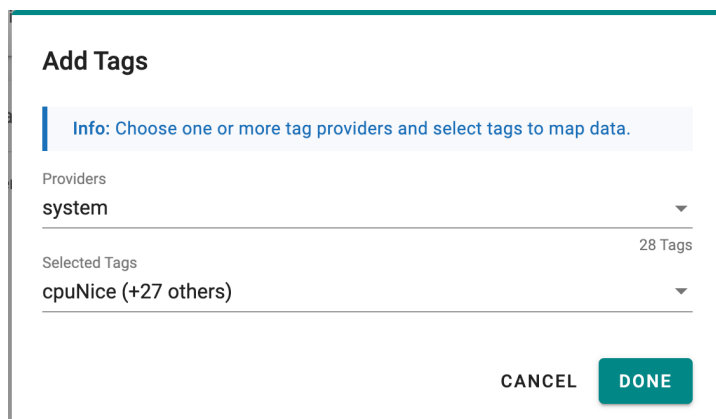
Min Publish Interval (ms) 500 Max Publish Interval (ms) 50000

Min Sampling Interval (ms) 200 Max Sampling Interval (ms) 50000

Min Lifetime (ms) 1000 Max Lifetime (ms) 100000

CANCEL DONE

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



Add Tags

Info: Choose one or more tag providers and select tags to map data.

Providers
system

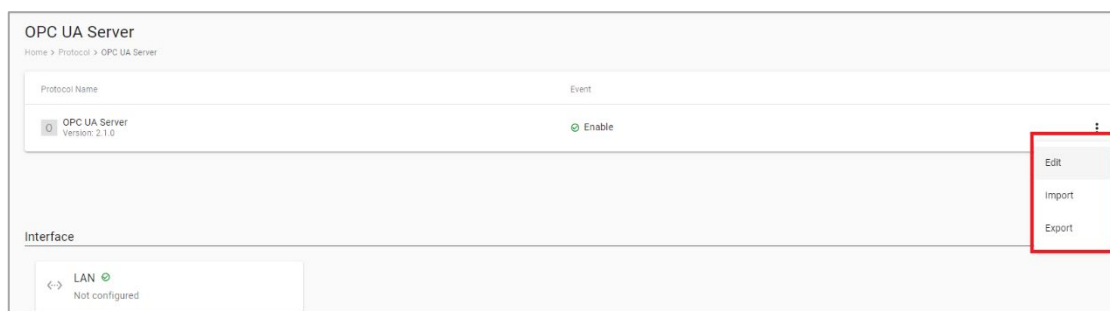
Selected Tags
cpuNice (+27 others)

28 Tags

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.



OPC UA Server

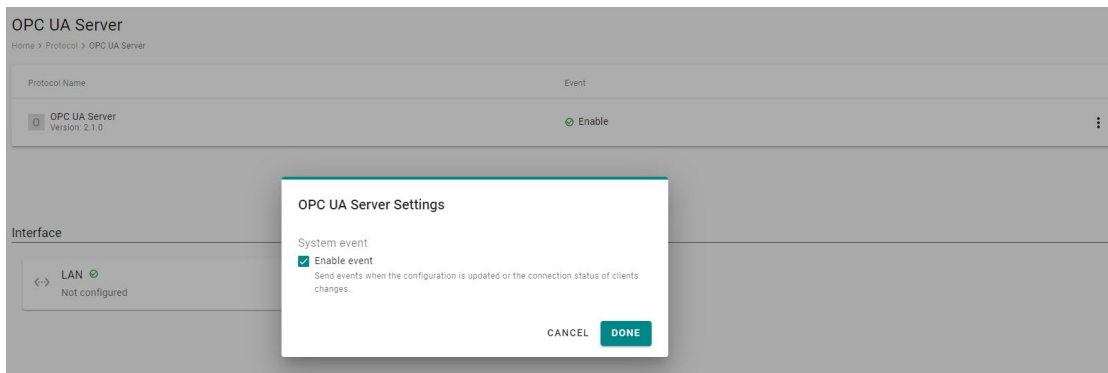
Home > Protocol > OPC UA Server

Protocol Name	Event
OPC UA Server Version: 2.1.0	Enable

Interface

LAN Not configured

Edit
Import
Export



Edge Computing

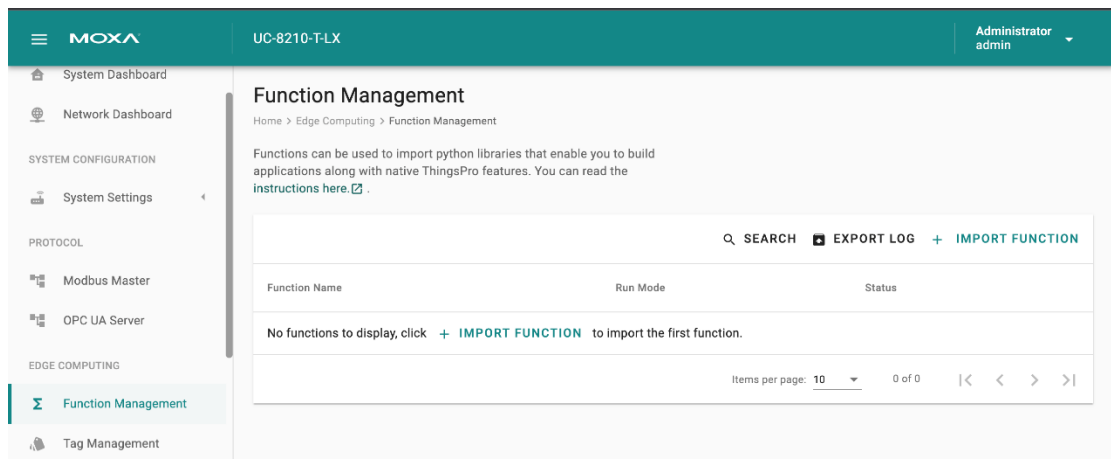
Function Management

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.

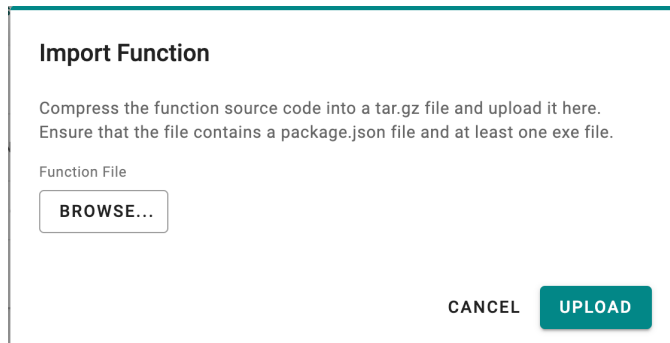
Go to **Edge Computing > Function Management** to import and manage functions. For additional information, see [build your own functions](#).

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 ⋮ <pre> id: 1 name: "onChangeTag" enabled: true trigger: driven: "dataDriven" dataDriven: tags: system: status: 0: "cpuUsage" events: timeDriven: mode: "boot" </pre>

	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

Home > Tag Hub > Tag Management

Southbound Protocol

Modbus Master

Tag Hub

Tag List

Tag Management

Tag Data Processing

Northbound Protocol

Azure IoT Device

AWS IoT Core

MQTT Client

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

☒	Provider	Source	Name	Type	Access
☒	modbus_serial_master	ddd	device_info_t2	Int16	Read
☒	modbus_serial_master	ddd	status	Int32	Read
☒	modbus_serial_master	ddd	Power2	Int16	Read
☒	modbus_serial_master	ddd	Power1	Int16	Read
☒	modbus_serial_master	ddd	device_info_t27	Int16	Read

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 "i". 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. You can also set values for writable tags by clicking "i". 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
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

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

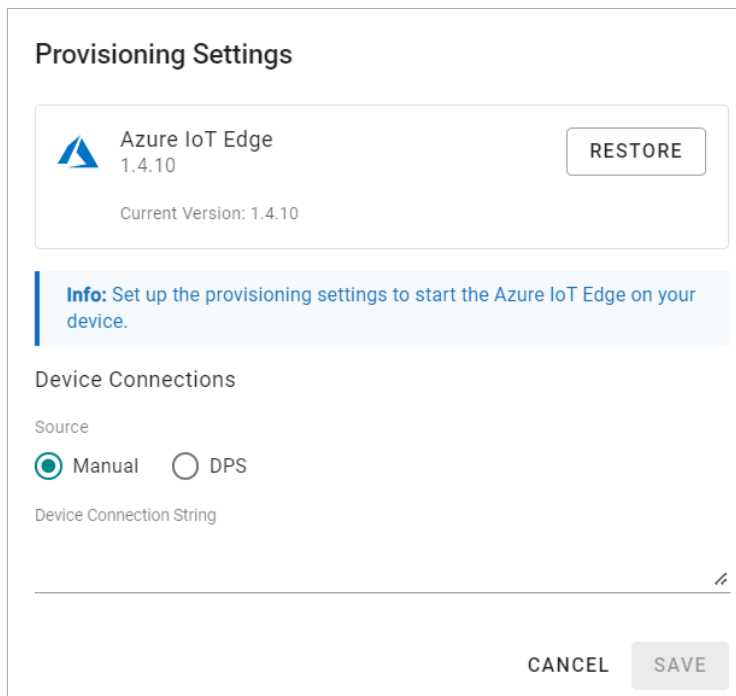
1. Enable the Azure IoT Edge service and click on .
2. Select **DPS**.
3. Select **TPM, Symmetric encryption**, or **X.509** certificate.
Select an option based on your device registered with the Azure IoT Hub.



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 a text field for 'Output Topic'. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. A modal window is open for 'Publish Interval (sec)' with the value '60'. It also has a 'Sampling Mode' dropdown set to 'All Changed Values' and a checkbox for 'Custom sampling rate from acquired data' which is unchecked. At the bottom right are 'CANCEL' and 'NEXT >' buttons.

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 now complete with a green checkmark. The 'Select Tags' section has an info box: 'Info: Select one or more tag providers and select tags to map data.' Below it is a 'Providers' dropdown set to 'IO'. A modal window is open showing a list of tags: '[IO] DI', 'DI-01', 'DI-02', and 'DI-03', all of which are checked. The modal has 'SELECT ALL' and 'CLEAR' buttons. At the bottom of the modal, it says 'Total: 8, Selected: 4' and a 'DONE' button. The 'Default Payload' text area contains the text 'null'. There is a checkbox for 'Enable Custom Payload' which is unchecked. At the bottom right are 'CANCEL' and 'NEXT >' buttons.

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

Create New Telemetry Message

Basic Settings

2 Message Tags

3 Properties Optional

Select Tags

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

Providers

IO

Selected Tags

DI-01 (+3 others)

8 Tags

jq Filter

TEST

Custom Payload Result

Enable custom payload

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

BACK

CANCEL

NEXT

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

Create New Telemetry Message

Basic Settings

2 Message Tags

3 Properties Optional

Property Key

Property Value

+ Add another

BACK

CANCEL

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**.

Routes

Routes direct messages between modules, giving the flexibility to send messages where they need to go without the need for additional services to process messages or to write additional code.

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.

The screenshot shows the 'Azure IoT Edge' configuration page. At the top, there's a toggle switch for 'Azure IoT Edge' which is turned on. Below it, a table lists the service name 'Azure IoT Edge' with version '1.4.10' and status 'Exited'. A tabbed interface at the bottom includes 'Module List', 'Device Management' (which is selected), 'Telemetry Message', 'Downstream Certificate', and 'AIE Checks'. Under the 'Device Management' tab, there's a checkbox labeled 'Allow Device Management' which is checked, with a note that this feature requires the ThingsProAgent module installed. A 'SAVE' button is at the bottom left.



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](#).

The screenshot shows the Moxa AIG-301-T-EU-AZU-LX interface. On the left is a sidebar menu with categories like OVERVIEW, SYSTEM CONFIGURATION, PROTOCOL, CLOUD CONNECTIVITY, SECURITY, and MAINTENANCE. The 'Azure IoT Edge' option under CLOUD CONNECTIVITY is selected. The main panel shows the 'Azure IoT Edge' settings. A modal dialog titled 'Upload Downstream Certificate' is open in the foreground. It has three input fields: 'X.509 Certificate' with the value 'iotEdge_moxa.crt', 'Private Key' with 'iotEdge_moxa.key', and 'Trusted CA Certificate' with 'RootCA_moxa.crt'. Each field has a clear (X) button. At the bottom of the dialog are 'CANCEL' and 'SUBMIT' buttons. The background settings page is dimmed.

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=Vq2qbpoo7I/PUFt0s

Connection Protocol

mqtt (Port: 8883)

Authentication Type

☒ Symmetric Key ☐ X.509 Certificate

Trusted Root CA - optional

BROWSE...

CANCEL

SAVE

Telemetry Message

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

1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a **Publish Mode**.

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

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 a text field for 'Output Topic'. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. A modal window is open for 'Publish Interval (sec)' with the value '60'. Below that is a 'Sampling Mode' dropdown menu set to 'All Changed Values'. At the bottom of the modal is a checkbox for 'Custom sampling rate from acquired data' which is unchecked. At the bottom right of the dialog 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 at Step 2: Message Tags. Step 1 is now completed with a green checkmark. The 'Select Tags' section has an info box: 'Info: Select one or more tag providers and select tags to map data.' Below it is a 'Providers' dropdown menu set to 'IO'. A modal window is open showing a list of tags: '[IO] DI', 'DI-01', 'DI-02', and 'DI-03'. The first three are checked. At the bottom of the modal is a 'DONE' button. The 'Default Payload' text area contains the text 'null'. To the right of the text area is a checkbox for 'Enable Custom Payload' which is unchecked. At the bottom right of the dialog are 'CANCEL' and 'NEXT >' buttons.

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

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

The screenshot shows the 'Create New Telemetry Message' form at the 'Message Tags' step. The progress bar at the top indicates three steps: 'Basic Settings' (completed), 'Message Tags' (current), and 'Properties Optional' (skipped). On the left, under 'Select Tags', there is an info box that says 'Info: Select one or more tag providers and select tags to map data.' Below this, the 'Providers' dropdown is set to 'IO', and the 'Selected Tags' dropdown shows 'DI-01 (+3 others)'. To the right, the 'jq Filter' field is empty, with a 'TEST' button next to it. Below the filter, the 'Custom Payload Result' section shows a JSON payload:

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

. A checkbox labeled 'Enable custom payload' is checked. At the bottom, there are 'BACK', 'CANCEL', and 'NEXT >' buttons.

8. Click **NEXT**.

9. (Optional) Enter Property Key and Value.

The screenshot shows the 'Create New Telemetry Message' form at the 'Properties Optional' step. The progress bar at the top indicates three steps: 'Basic Settings' (completed), 'Message Tags' (completed), and 'Properties Optional' (current). The form has two input fields: 'Property Key' and 'Property Value'. Below these fields is a link that says '+ Add another'. At the bottom, there are 'BACK', 'CANCEL', and 'SAVE' buttons.

10. Click **SAVE**.

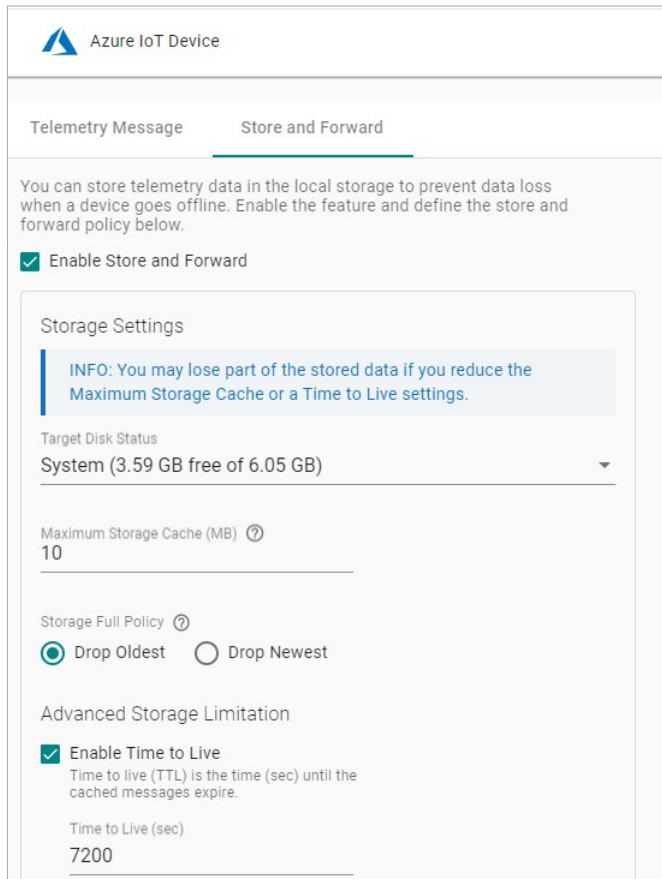


NOTE

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 text: '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. It contains an information box stating: 'INFO: You may lose part of the stored data if you reduce the Maximum Storage Cache or a Time to Live settings.' Underneath, 'Target Disk Status' is 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 options: 'Drop Oldest' (selected) and 'Drop Newest'. The 'Advanced Storage Limitation' section has a checkbox 'Enable Time to Live' which is checked, with a subtext: '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.



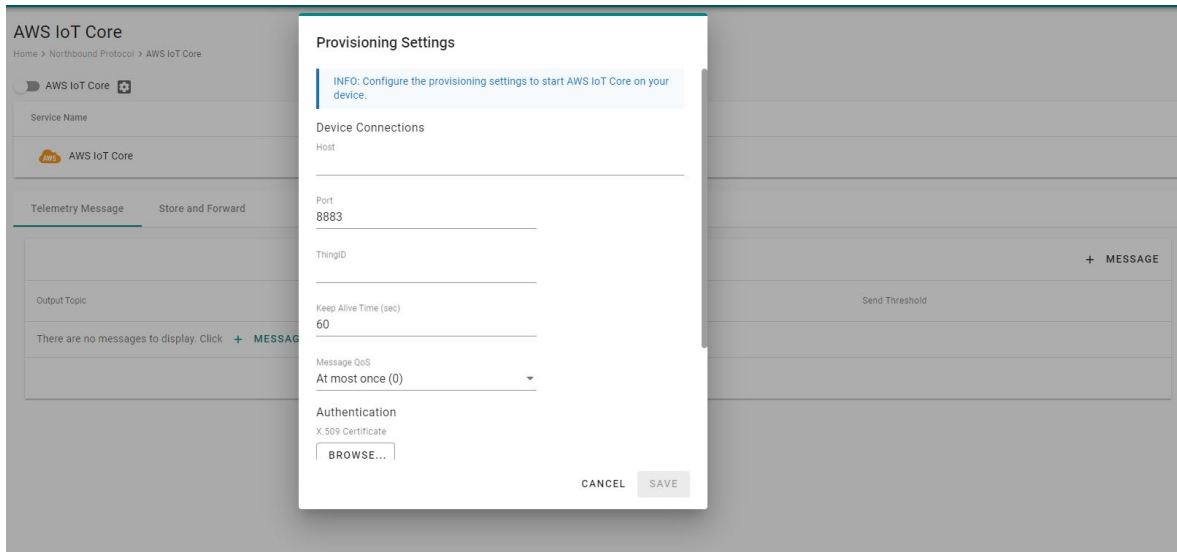
NOTE

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 with the 'Basic Setting' tab selected. The progress bar at the top shows '1 Basic Setting' and '2 Message Tags'. The 'Enable Telemetry Message' checkbox is checked. The 'Output Topic' is '123'. The 'Publish Mode' is 'By Interval' (selected), with 'Immediately' and 'By Size' as options. The 'Publish Interval (sec)' is '60'. The 'Sampling Mode' is 'All Changed Values'. There is a checkbox for 'Custom sampling rate from acquired data' which is unchecked. At the bottom right are 'CANCEL' and 'NEXT >' buttons.

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

The screenshot shows the 'Create New Telemetry Message' dialog with the 'Message Tags' tab selected. The progress bar at the top shows '1 Basic Setting' and '2 Message Tags'. The 'Select Tags' section has an info box: 'Info: Select one or more tag providers to get their tags and select tags to map data.' Below it, the 'Providers' dropdown is set to 'IO'. A search modal is open, showing a list of tags: 'DI-01', 'DI-02', and 'DI-03', all of which are selected. The 'Default Payload' is 'null'. There is a checkbox for 'Enable custom payload' which is unchecked. At the bottom right are 'CANCEL' and 'SAVE' buttons. At the bottom left of the modal, it says 'Total: 8, Selected: 4' and there is a 'DONE' button.

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

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

Create New Telemetry Message

✓ 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

DI-01 (+3 others)

8 Tags

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

8. 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).

Connect to New MQTT Broker

General SSL/TLS Will and Testament

Server _____ Port 8883

MQTT Version
☒ 3.1.1 ☐ 3.1

Client ID _____

Username
admin

Password
.....

Keep Alive Time (sec)
60

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

CANCEL SAVE

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

7. (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 selected. Under the "SSL/TLS" heading, there is a checked checkbox for "Enable SSL/TLS". Below this, there is a section for "TLS Version" with three radio buttons: "1.2" (selected), "1.1", and "1.0". There are three optional fields, each with a "BROWSE..." button: "Client Certificate - optional", "Client Key - optional", and "Trusted Root CA - optional". At the bottom of the dialog, there is an unchecked checkbox for "Ignore Server Certificate". The "CANCEL" and "SAVE" buttons are at the bottom right.

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

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

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

The screenshot shows a dialog box titled "Create New Telemetry Message" with two tabs: "Basic Setting" and "Message Tags". The "Basic Setting" tab is selected. Under the "Basic Setting" heading, there is a checked checkbox for "Enable Telemetry Message". Below this, there is a text field for "Output Topic" with the value "123". There is a section for "Publish Mode" with three radio buttons: "By Interval" (selected), "Immediately", and "By Size". Below this, there is a text field for "Publish Interval (sec)" with the value "60". There is a dropdown menu for "Sampling Mode" with the value "All Changed Values". There is an unchecked checkbox for "Custom sampling rate from acquired data". The "CANCEL" and "NEXT >" buttons are at the bottom right.

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**.
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.

ADD CONNECTION

test.mosquitto.org
Connected

Telemetry Message Store and Forward Remote API Invocation

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

☒ Enable Store and Forward

Storage Setting

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

Target Disk
System (3.59GB free of 6.05 GB)

Maximum Storage Cache (MB) ⓘ
10

Storage Full Policy ⓘ
☒ Drop Oldest ☐ Drop Newest

Advanced Storage Limitation

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

Time to Live (sec)
7200

SAVE



NOTE

if you want to use the direct method to write tags from the cloud, refer to <https://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>.

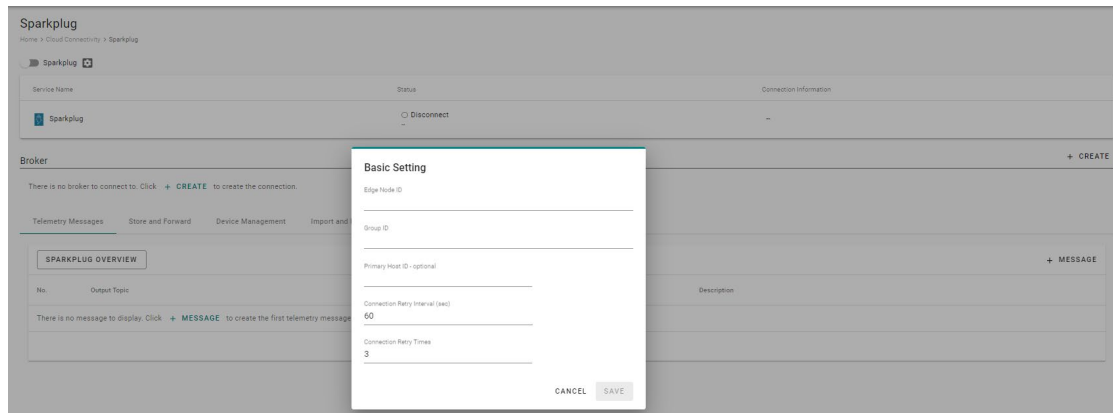
Sparkplug

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:

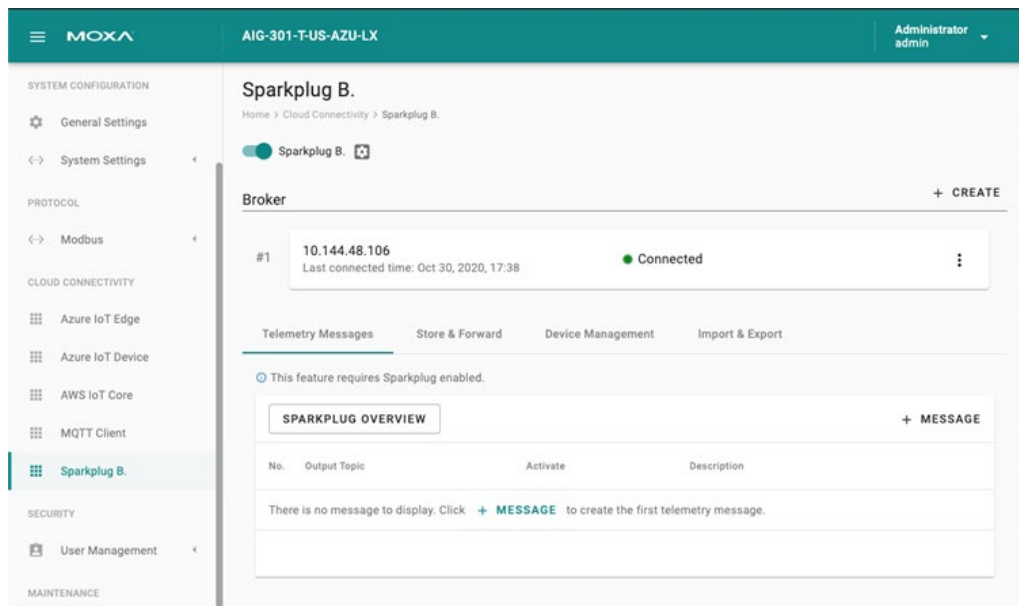
- Enabling Sparkplug
- Configuring a Broker
- Configuring a Telemetry Message

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**.

The screenshot shows the 'Create New Broker' dialog box with the 'SSL/TLS' tab selected. The 'General' tab is also visible. The 'SSL/TLS' section has a checkbox for 'Enable SSL/TLS' which is checked. Below this, there is a 'TLS Version' section with radio buttons for 1.3, 1.2 (selected), 1.1, and 1.0. There are three 'BROWSE...' buttons for 'Client Certificate - optional', 'Client Key - optional', and 'Trusted Root CA - optional'. At the bottom, there is an unchecked checkbox for 'Ignore server certificate' and 'CANCEL' and 'SAVE' buttons.

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 stating: 'Info: Select one tag provider to get its tags, and select tags to map data.' The 'Providers' section shows 'modbus_tcp_master' selected. The 'Devices / System Tags' section shows 'Test' selected. The 'Selected Tags' dropdown menu shows 'c1' selected. On the right, a box titled 'Selected Tags - 1 Tag' displays '> 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, the 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'By Size', and 'Immediately'. The 'Publish Interval (sec)' input field is set to '60'. The 'Sampling Mode' dropdown menu is set to 'All Changed Values'. There is a checkbox for 'Custom sampling rate from acquired data' which is currently unchecked. At the bottom left, there is a '< BACK' button. 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

AIG-301 Series User Manual

70

Device Management

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

Sparkplug

Home > Cloud Connectivity > Sparkplug

☐ Sparkplug

Service Name	Status
Sparkplug	☐ Disconnect --

Broker

There is no broker to connect to. Click [+ CREATE](#) to create the connection.

Telemetry Messages Store and Forward **Device Management** Import and Export

Allow managing this device from remote.

☒ Allow Device Management

SAVE



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.



NOTE

Applying the Sparkplug configuration takes time when a large number of messages or tags are selected. In such cases, wait at least one minute after saving the configuration.

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



NOTE

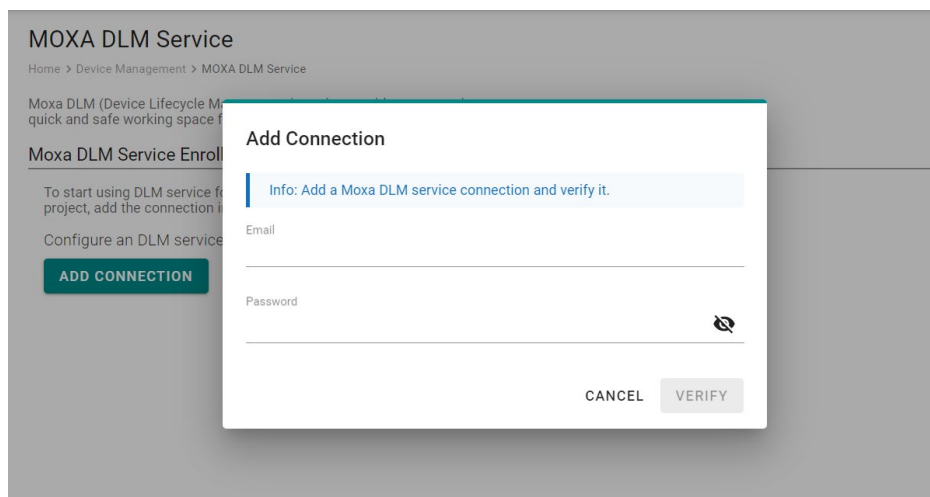
The exported configuration includes credentials, client ID, and policies of D2C messages. You can modify these parameters after the configuration file is imported to other gateways.

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.

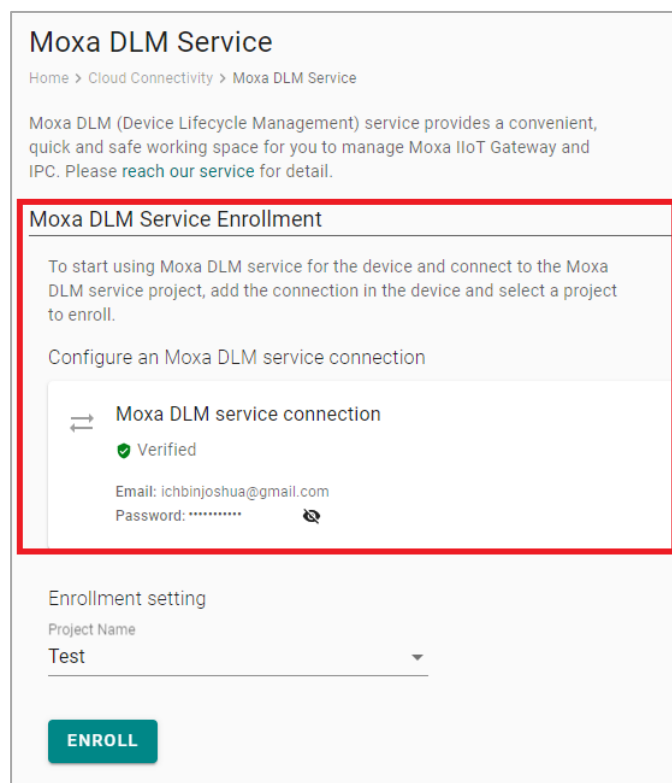
Once you have access to the service, go the **Moxa DLM Service** to register the product online as follows.

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



The screenshot shows the 'Moxa DLM Service' interface with a modal dialog titled 'Add Connection'. The dialog contains an information message: 'Info: Add a Moxa DLM service connection and verify it.' Below this are input fields for 'Email' and 'Password'. The 'Password' field has a toggle icon for visibility. At the bottom of the dialog are 'CANCEL' and 'VERIFY' buttons. The background shows the 'Moxa DLM Service Enrollment' 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 Enrollment' page. A red box highlights the 'Moxa DLM service connection' section, which shows a green checkmark and the text 'Verified'. Below this, the email 'ichbinjoshua@gmail.com' and a masked password are displayed. The 'Enrollment setting' section shows a dropdown menu for 'Project Name' with 'Test' selected. An 'ENROLL' button is at the bottom.

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: 0090E99DF3E

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

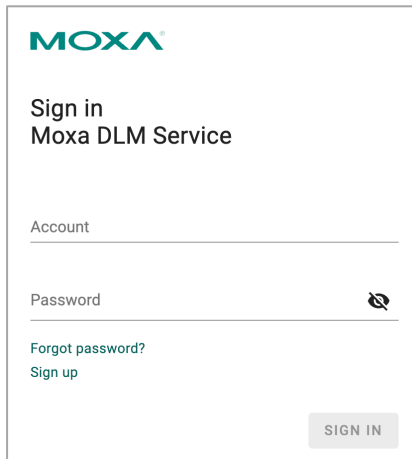
REFRESH

☐	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	1.6.0	-

Items per page: 10 1 - 1 of 1

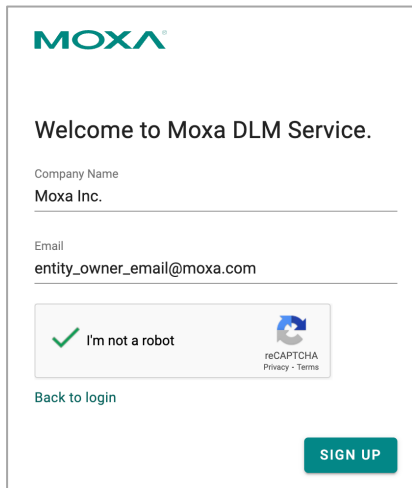
Sign Up DLM Account

1. Go to the website: <https://dlm.thingsprocloud.com/>



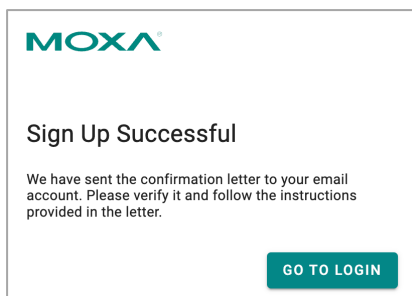
The image shows the 'Sign in Moxa DLM Service' page. At the top is the MOXA logo. Below it, the text 'Sign in Moxa DLM Service' is displayed. There are two input fields: 'Account' and 'Password'. The 'Password' field has a toggle icon for visibility. Below the 'Password' field are two links: 'Forgot password?' and 'Sign up'. At the bottom right is a 'SIGN IN' button.

2. Enter your company name and email. Click SIGN UP. Note that each company name can be associated with only one email account. If your company has multiple organizations, please specify the detailed organization name instead of using the general company name.



The image shows the 'Welcome to Moxa DLM Service' page. At the top is the MOXA logo. Below it, the text 'Welcome to Moxa DLM Service.' is displayed. There are two input fields: 'Company Name' (with 'Moxa Inc.' entered) and 'Email' (with 'entity_owner_email@moxa.com' entered). Below the 'Email' field is a reCAPTCHA widget with a green checkmark and the text 'I'm not a robot'. To the right of the reCAPTCHA widget are links for 'reCAPTCHA', 'Privacy', and 'Terms'. At the bottom left is a 'Back to login' link. At the bottom right is a 'SIGN UP' button.

3. Go to the email inbox you entered in step 2, and follow the instructions to complete the sign-up process.



The image shows the 'Sign Up Successful' page. At the top is the MOXA logo. Below it, the text 'Sign Up Successful' is displayed. Below that is a paragraph: 'We have sent the confirmation letter to your email account. Please verify it and follow the instructions provided in the letter.' At the bottom right is a 'GO TO LOGIN' button.

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 purposes.

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

Certificate Center					
Home > Security > Certificate Center					
My Certificates		Trusted Root CA			
					Q SEARCH
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	↓
Items per page: 10 1 - 2 of 2 < < > >					

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(opcuaerver) 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

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.						

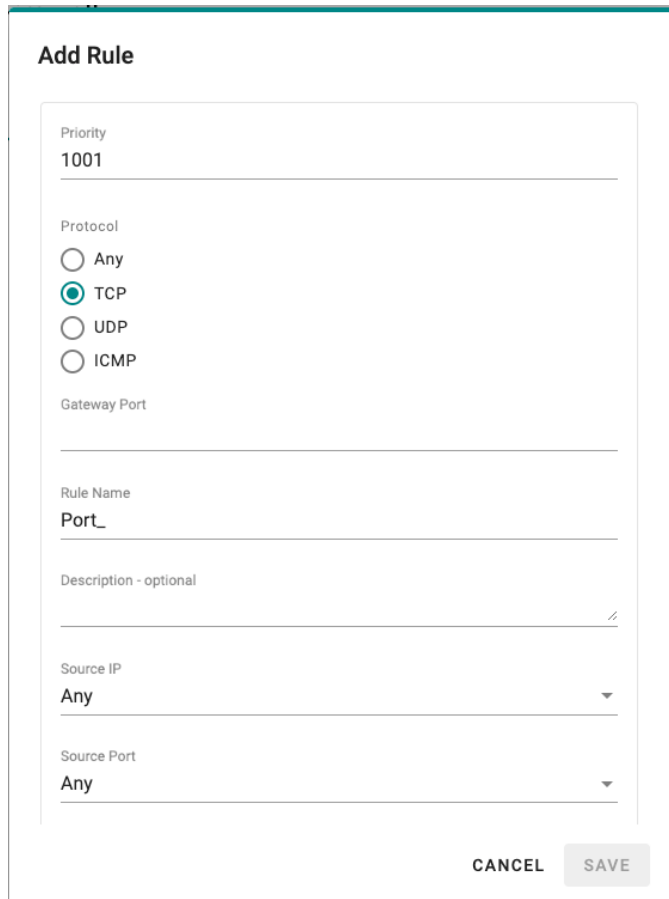
Items per page: 10 0 of 0 |< < > >|

Allowed List

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 modal dialog titled "Add Rule". It contains several input fields and a list of radio buttons. The "Priority" field is set to "1001". The "Protocol" section has four radio buttons: "Any", "TCP" (which is selected), "UDP", and "ICMP". The "Gateway Port" field is empty. The "Rule Name" field is set to "Port_". The "Description - optional" field is empty. The "Source IP" dropdown menu is set to "Any". The "Source Port" dropdown menu is set to "Any". At the bottom right of the dialog are two buttons: "CANCEL" and "SAVE".

Add Rule

Priority
1001

Protocol

☐ Any

☒ TCP

☐ UDP

☐ ICMP

Gateway Port

Rule Name
Port_

Description - optional

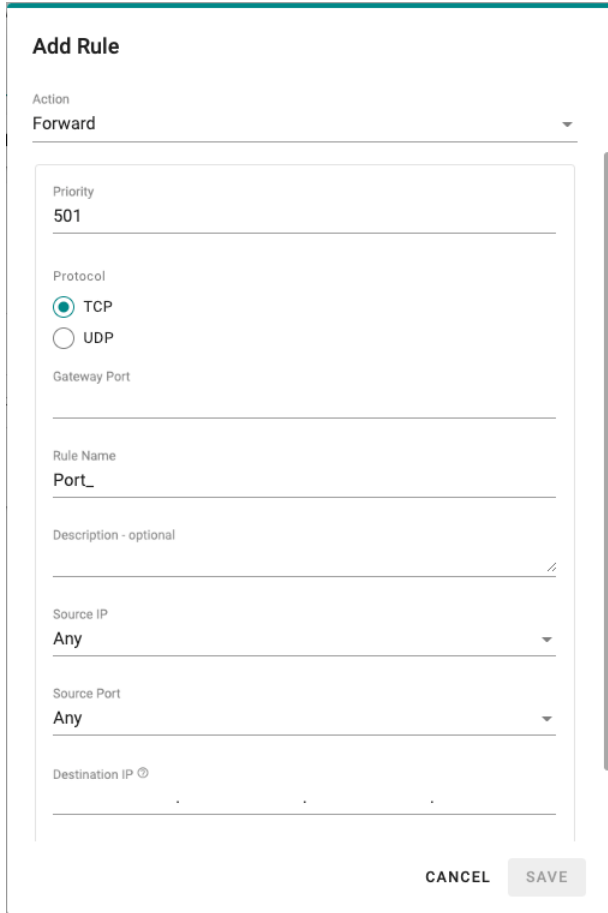
Source IP
Any

Source Port
Any

CANCEL SAVE

Create Forward Rule:

1. Click **+ ADD RULE**.
2. Select action **Forward**.
3. Specify the **Priority**, **Protocol**, **Gateway Port**, **Rule Name**, and **Description** (optional).
4. Specify the **Source IP** or **Subnet**.
5. Specify the **Destination IP** and **Port**.



Add Rule

Action
Forward

Priority
501

Protocol
☒ TCP
☐ UDP

Gateway Port

Rule Name
Port

Description - optional

Source IP
Any

Source Port
Any

Destination IP

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.

OpenVPN Client
Home > Security > OpenVPN Client

Upload profile to make connection.
Upload the profile to enable the OpenVPN Client. Or download the sample profile to edit if you are not sure how to configure it.

UPLOAD PROFILE **DOWNLOAD SAMPLE**

No Profile

OpenVPN Client
Home > Security > OpenVPN Client

☒ OpenVPN Client (V2.4.0)

Current Profile
QA-test-1 (1) (1).ovpn **MANAGE**

Download the Sample File

Connection Information **REFRESH**

Connection Status	Local IP	Remote IP	Netmask	Gateway
Connecting	--	--	--	--

Account Management

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

Accounts

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

Accounts

Home > Security > Account Management > Accounts

Q SEARCH

+ CREATE

Account	Role	Status	
admin (you)	Administrator	Active	
Josh	Administrator	Active	
Justin	Administrator	Active	

Items per page: 10 1 - 3 of 3 |< > >|

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

Create New Account

Account

Josh

4/16

Role

Administrator

▼

Password

Contains at least 8 characters

Contains at least 1 number

Confirm Password

Email - optional

CANCEL SAVE

Valid Password

Create New Account

Account

Josh

4/16

Role

Administrator

▼

Password

Confirm Password

Email - optional

CANCEL SAVE

Managing Existing User Accounts

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

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

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
Modbus Slave		Roles	
SECURITY		Home > Security > Account Management > Roles	
Service Enablement		Q SEARCH + CREATE	
HTTP/HTTPS		Role Name	
Firewall		Administrator (built-in)	
Certificate Center		Users of this role have full permissions. This is a built-in role and can't be modify or delete.	
Account Management		justin	
Accounts		ricky	
Roles		lynn	
MAINTENANCE		albert	
Protocol Status		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		
		Q SEARCH + CREATE
Role Name		
Administrator (built-in)	1 account	⋮
Users of this role have full permissions. This is a built-in role and can't be modify or delete.		
justin	1 account	⋮
--		

Taking into consideration the security requirements of the AIG-301, we recommend creating these roles with the specified permissions.

Role	Permissions
Administrator	All
OT – Field site operator	Device Maintenance Modbus Master
IT – maintenance personnel	Device Maintenance (optional) Add-on Applications

Maintenance

Protocol Status

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

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**.

The screenshot shows the 'Protocol Status' page. At the top, there's a breadcrumb: 'Home > Maintenance > Protocol Status'. Below this, the page is divided into two sections: 'Northbound Protocols' and 'Southbound Protocols'. Under 'Northbound Protocols', there are four cards: 'AWS IoT Core', 'Azure IoT Device', 'MQTT Client', and 'Sparkplug'. Each card has a 'Disable' link and a 'CHECK' button. Under 'Southbound Protocols', there is one card: 'Modbus Master', which shows a green checkmark and 'OK', with a 'CHECK' button that has a dropdown arrow.

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

The screenshot shows the 'Azure IoT Device' diagnostic page. It has a breadcrumb: 'Home > Maintenance > Protocol Status > Azure IoT Device'. Below the breadcrumb, there's a description: 'Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to [Azure IoT Device](#)'. A table shows the service name 'Azure IoT Device', its connection status 'Connected' (with a green checkmark), and the last upload status 'Success' (with a green checkmark). Below the table, there's an 'Advanced Diagnostic' section with a 'START' button and an 'EXPORT' button. The main area below these buttons is a large black rectangle, likely representing a terminal or log output.

3. View the logs to identify the issue.

The screenshot shows the diagnostic log output. At the top, there are 'START' and 'EXPORT' buttons. Below them, the log text is as follows:
TLS check
[v] connection: ok
[v] SSL handshake: ok
[v] certificate: is valid for 90 more days
Process Health Check
[v] Last retry time (status: connected): N/A
[v] Message: output queue is ok (0/500)
All check is completed

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

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.

Reboot

Home > Maintenance > General Operation > Reboot

History of the Last Reboot: May 12, 2023 01:40:24

☐ Automatic Reboot With Scheduler

REBOOT NOW

Reboot

Home > Maintenance > General Operation > Reboot

History of the Last Reboot: Sep 01, 2022 21:34:33

☒ Automatic Reboot With Scheduler

Sep 15, 2022 12:15:00
The device will be rebooted.

REBOOT NOW

CREATE A REBOOT TASK

Date
Sep 15, 2022

Hour * : Minute *
12 : 15

CANCEL **SAVE**

EDIT

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.

MOXA

AIG-101-T

Administrator
admin

Firewall

Certificate Center

Account Management

MAINTENANCE

Protocol Status

System Log

Event Log

General Operation

Reboot

Config. Import/Export

Software Upgrade

Reset to Default

DEVICE MANAGEMENT

Config. Import/Export

Home > Maintenance > General Operation > Config. Import/Export

Export

Encrypt the file to enhance security and click "EXPORT" to export the current system configuration as a configuration file.

Password

Confirm Password

EXPORT

Import

Click "BROWSE" to select a previously exported configuration file and enter the password to upload the file.

Configuration File
BROWSE...

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

BROWSE...

UPLOAD

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

DOWNLOAD

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 ?

DHCP Server - LAN2

Event Log

HTTP Service

HTTPS Service

Internet Check Alive Service ?

Local Console

NAT Service ?

NTP Service

SD Card

SSH Server

System Log

Network

Cellular1

LAN1

LAN2

Wi-Fi1

Provision Service

ThingsPro Proxy

Scheduled

The device provision service will be turned off 15 minutes after the service is restarted.

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. The event logs can also be exported for convenient offline analysis.

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.

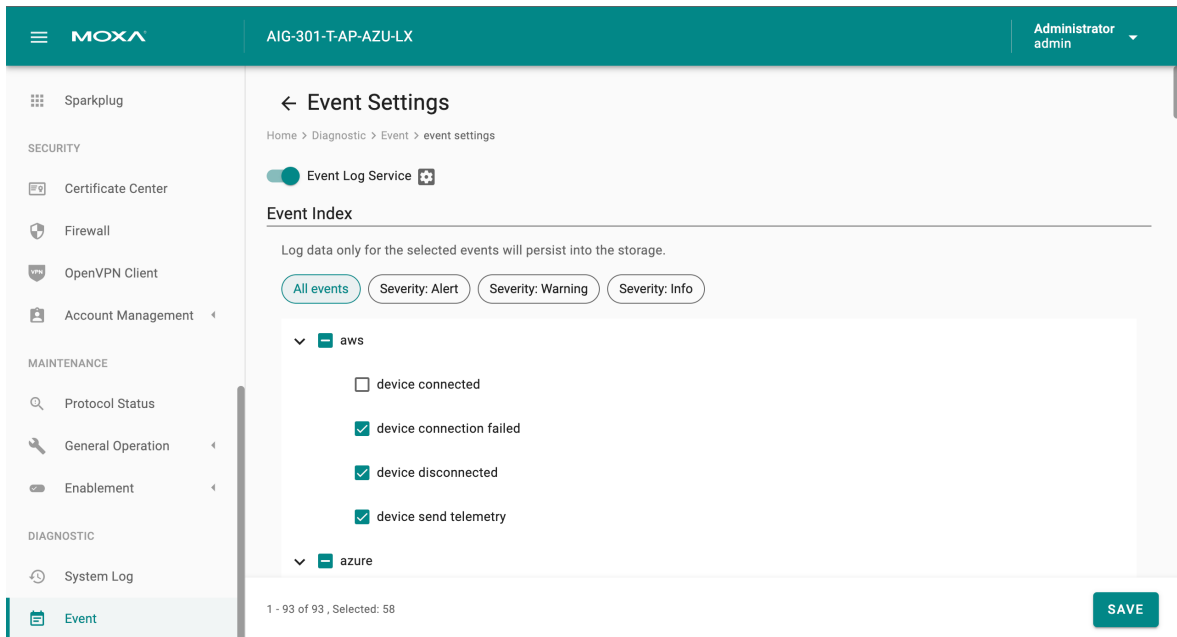
Severity	Category	Event Name	User	Date and Time ↓
Warning	azure	device disconnected	--	Jun 13, 2023, 17:34:09
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:10:03
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:59
Warning	azure	edge disconnected	--	Jun 13, 2023, 10:09:54
Warning	azure	edge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

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.



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

4. Security Hardening Guide

In this chapter, we discuss some security aspects and guidelines for operating the AIG more securely.

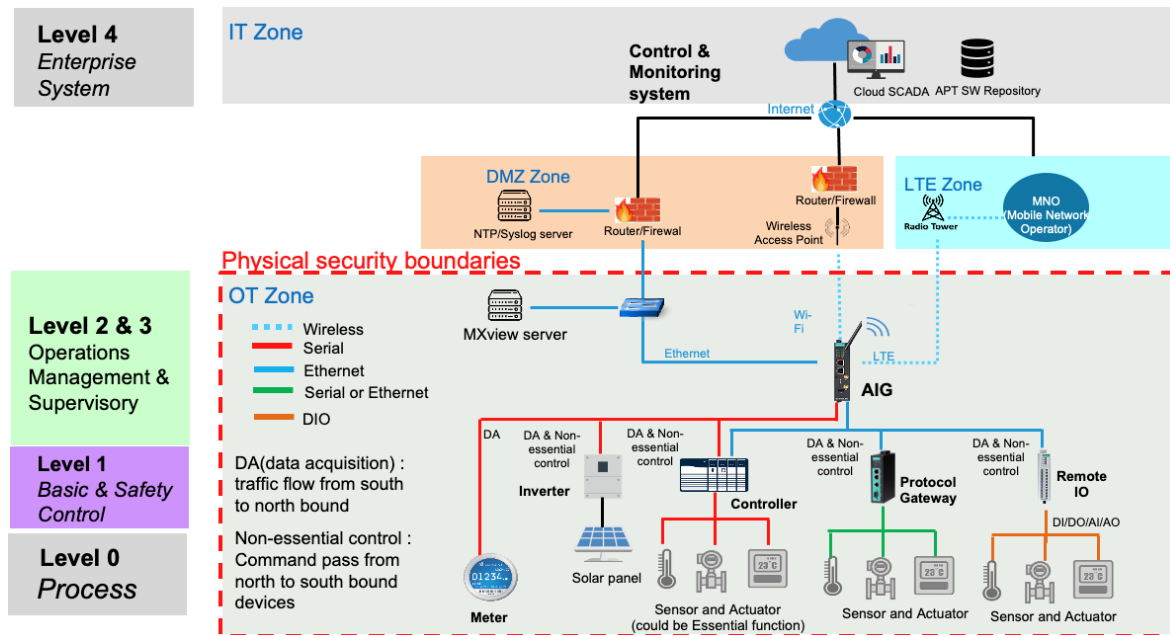
Communication Integrity and Authentication

The AIG supports the following network communication services and protocols as a server.

Communication Interface	Protocol	TCP/ UDP Port	Authenticator	Default Configuration
WEB	HTTP	TCP 80	password	Disabled
	HTTPS	TCP 443	password	Enabled
DHCP server	DHCP	UDP 67, 68	N/A	Disabled
DNS client	DNS	TCP 53	N/A	Disabled
OPCUA Server	HTTPS	TCP 4840	Password & certificate	Disabled
Modbus Master	TCP	TCP 502	N/A	Disabled
openssh-server (Debug mode used)	SSH	TCP 22	password	Disabled

Potential Threats and Corresponding Security Measures

The following diagram depicts the security architecture and the location of the AIG.



A list of potential security threats to the AIG and the corresponding security measures that need to be taken by the asset owner if these threats apply is listed in the following table:

Threat ID	Threat mitigated/ handled	Security measures
1	Unauthorized access to nginx configuration allows an attacker to alter execution flow	Enable HTTP to HTTPS redirection to ensure secure protocol with encryption and authentication during data transmission.
2	An attacker spoofs a browser via WAN, mimicking an external entity.	
3	An intruder gains elevated privileges through impersonation tactics	
4	An unauthorized party intercepts data flow, capturing sensitive information in transit.	
5	An attacker masquerades as the nginx web server process, deceiving users and gaining unauthorized access	
6	Excessive resource usage by edgeHub (container) or system storage (mSATA), like frequent log writing, could lead to system slowdowns or data loss, especially when storage space is low.	- Configure maximum storage capacity for individual Azure IoT Edge modules. - Utilize iotedge metrics monitor on Azure IoT Hub for Azure IoT modules' monitoring. More information about the Azure IoT module's monitoring: https://learn.microsoft.com/en-us/azure/iot-edge/how-to-collect-and-transport-metrics?view=iotedge-1.5&tabs=iothub
7	Excessive resource usage by system logs might dominate storage space, reducing room for critical information or telemetry message buffers when the network is down.	Store system logs on external storage, freeing the log partition exclusively for system logs.
8	Network data flow could be potentially interrupted, crashed, or stopped by a DOS attack.	- Configure an alternative WAN interface, like Ethernet or Wi-Fi, for connection failover. - Configure keep-alive for cellular connections.
9	Excessive write-tag requests from an IoT Edge module affect Modbus data acquisition.	Restrict internal HTTPS API server usage to a maximum of 10 requests per second maximum. Note: The shared memory used by tagHub is not publicly accessible. For data sampling from tagHub, we recommend intervals of at least 1 second.
10	Frequent telemetry message uploads from an IoT Edge module impact other uploads via edgeHub (container).	
11	High volumes of HTTPS requests from an IoT Edge module, like massive data downloads, slow down web GUI interaction.	
12	An excessive number of tags generated by an IoT Edge module can overwhelm tagHub (system service), causing it to be busy while refreshing or monitoring tag values.	

Installation

- Physical Installation
 - a. The AIG MUST be protected by physical security that can include CCTV surveillance, security guards, protective barriers, locks, access control, perimeter intrusion detection, etc. The proper form of physical security should apply depending on the environment and the physical attack risk level.
 - b. The AIG MUST NOT be used to control the operation of mission-critical IACS component which failure to maintain control of such device could result in threat to human, safety, environment or massive financial loss.
- Environment Requirement
 - a. If the AIG connects to untrusted networks (e.g., Internet) via Ethernet or Wi-Fi, it MUST NOT directly connect to the untrust network, which means a firewall must be set up between the Ethernet and Wi-Fi connection from the AIG to the untrust network.
 - b. For security-critical applications, we strongly recommend using a private APN for cellular networks.
- Access Control
 - a. The default password policy requires the password to be at least 8 characters in length.
 - b. Update user passwords on a regular basis.
For the administrator account, we recommend refreshing password at least every 3 months.
 - c. Enabling debug mode activates the SSH Server service for remote terminal access.
Asset owners MUST disable debug mode in the production stage.

- Operation
 - a. Disabled communication interfaces that are not in use.
 - b. Make sure only trusted and reliable people are registered and have access to the AIG.
 - c. We recommend resetting the AIG to the factory default upon receiving it to avoid the risk of potential software tampering before it reached your hand.
- Maintenance
 - a. Perform software upgrade frequently to enhance features, security patches, and fix bugs.
 - b. Perform backup of system on a regular basis.
 - c. Examine events or system logs frequently to detect any anomalies.
 - d. To report vulnerabilities of Moxa products, submit your findings to us at the following webpage:
<https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability>.

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

Upgrade Packs:

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

Utility (QuickON):

<https://www.moxa.com/en/products/industrial-computing/iiot-gateways/programmable-iiot-gateways/aig-301-series#resources>

Technical Documentation

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

OpenAPI Documentation

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