

AIG-501 Series User Manual

Version 2.0, December 2024

www.moxa.com/products

MOXA®

© 2024 Moxa Inc. All rights reserved.

AIG-501 Series User Manual

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

Copyright Notice

© 2024 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction	4
Overview	4
2. Getting Started	5
Connecting the Power	5
Connecting Serial Devices	5
Connecting to a Network	6
Access to the Web Console	7
3. Web Console	8
Dashboard	8
System Dashboard	8
Network Dashboard	9
System Configuration	10
System Settings—General	10
System Settings—IP Address	14
System Settings—Cellular	16
System Settings—HTTP/HTTPS/SSH	18
System Settings—Serial	19
System Settings—I/O	21
System Settings—DHCP Server	22
System Settings—Wi-Fi	23
Protocol	25
Modbus Master	25
Modbus TCP Slave	44
OPC UA Server	50
Edge Computing	55
Function Management	55
Tag Management	57
Cloud Connectivity	59
Azure IoT Edge	59
Azure IoT Device	78
AWS IoT Core	82
Generic MQTT Client	86
Sparkplug	90
Moxa DLM Service	98
Security	100
Certificate Center	100
Import rootCA.cer to Google Chrome	100
Firewall	101
OpenVPN Client	104
Account Management	105
Maintenance	109
Protocol Status	109
General Operation	111
Diagnostic	116
A. Publish Modes	119
B. Module Twin Properties	121
C. Additional Documentation	143
Software Downloads	143
Technical Documentation	143
OpenAPI Documentation	143

1. Introduction

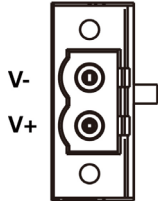
Overview

The AIG-501 Series advanced IIoT gateways are designed for Industrial IoT applications, especially for distributed and unmanned sites in harsh operating environments. AIG-501 series has implemented Modbus RTU/TCP master/client protocols which can help you to collect Modbus devices. Moreover, Azure IoT Edge software is preloaded and seamlessly integrated with the AIG-501 to enable easy, reliable, yet secure sensor-to-cloud connectivity for data acquisition and device management using the Azure Cloud solution. With the use of the ThingsPro Proxy utility, the device provisioning process is easier than ever. Thanks to the robust OTA function, you never have to worry about system failure during software upgrades. With the Secure Boot function enabled, you can prevent malicious software injection during the bootup process.

2. Getting Started

Connecting the Power

Power Input
DC 12-36 V \equiv



Connect the power jack (in the package) to the DC terminal block (located on the top panel), and then connect the power adapter. It takes about 3 minutes for the system to boot up. Once the system is ready, the power LEDs will light up.



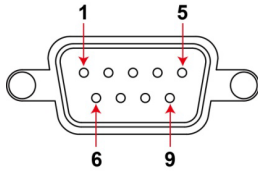
WARNING

- This product is intended to be supplied by a UL Listed Power Adapter or DC power source marked "L.P.S." (or "Limited Power Source") rated 12 to 36 VDC, 2.5 A (minimum), and TMA = 70°C (minimum).
- The power adapter should be connected to a socket outlet with an earthing connection.

If you need further information or assistance, contact a Moxa representative.

Connecting Serial Devices

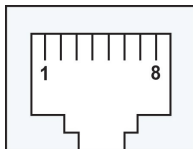
The serial port can be configured by software for RS-232, RS-422, or RS-485. The pin assignments for the port are shown in the following table:



Pin	RS-232	RS-422/ RS-485 4-wire	RS-485 2-wire
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	-	-

Connecting to a Network

The Ethernet ports are located on the front panel of the device. The pin assignments for the Ethernet port are shown in the following figure. If you are using your own cable, make sure that the pin assignments on the Ethernet cable connector match the pin assignments on the Ethernet port.



Pin	10/100 Mbps	1000 Mbps
1	Tx+	TRD(0)+
2	Tx-	TRD(0)-
3	Rx+	TRD(1)+
4	-	TRD(2)+
5	-	TRD(2)-
6	Rx-	TRD(1)-
7	-	TRD(3)+

8	-	TRD(3)-
---	---	---------

Access to the Web Console

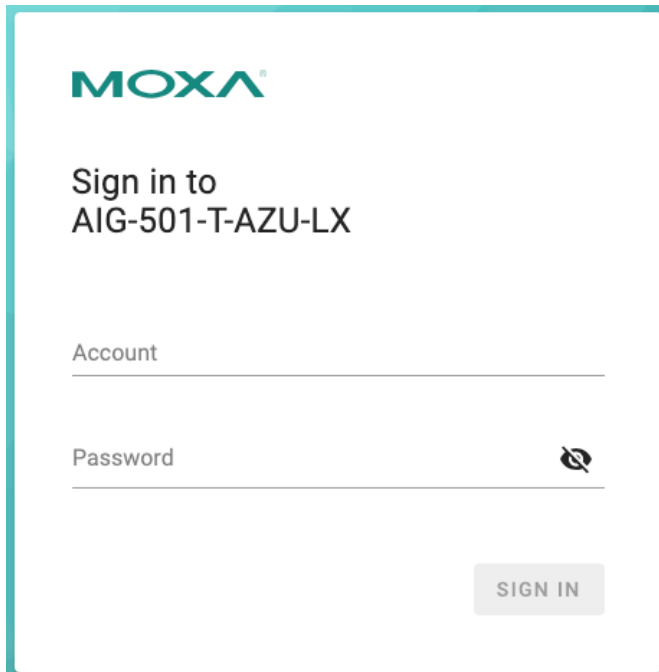
The default LAN2 IP address to access the web console of the AIG is 192.168.4.127.

When you 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**



MOXA

Sign in to
AIG-501-T-AZU-LX

Account

Password 

SIGN IN

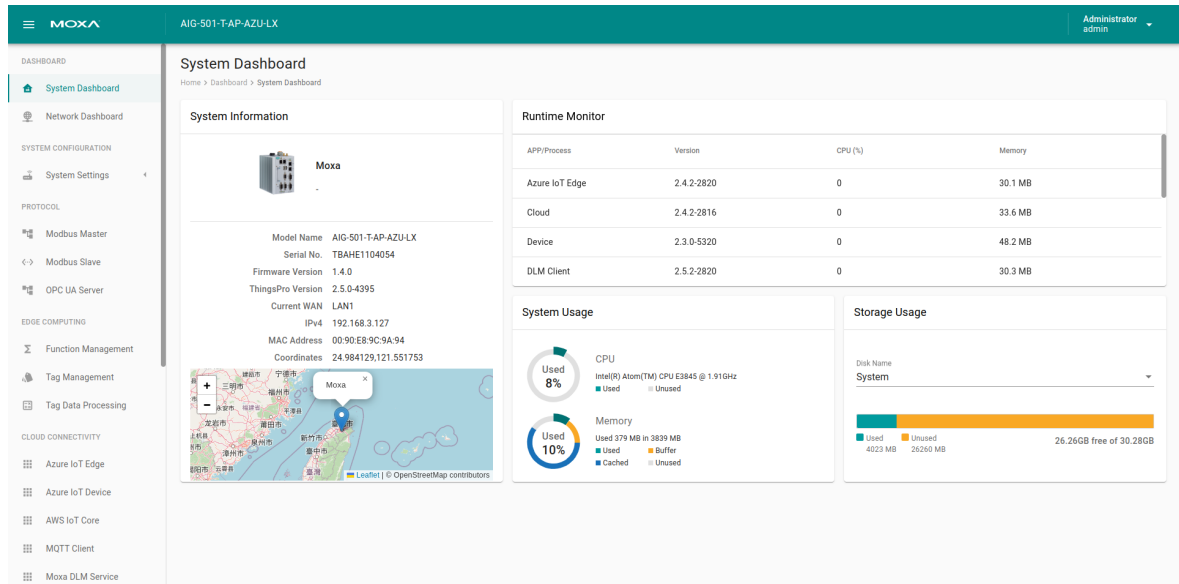
You will see the following home page after logging in successfully.

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. Ensure that you provide accurate information when entering data so that it is useful during troubleshooting system issues.

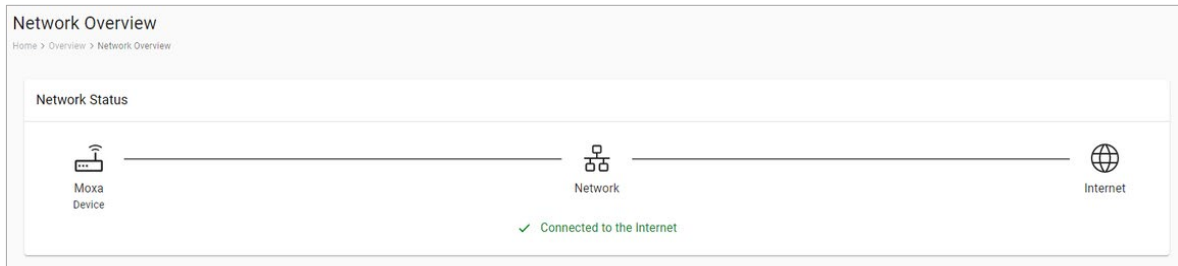


CAUTION

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

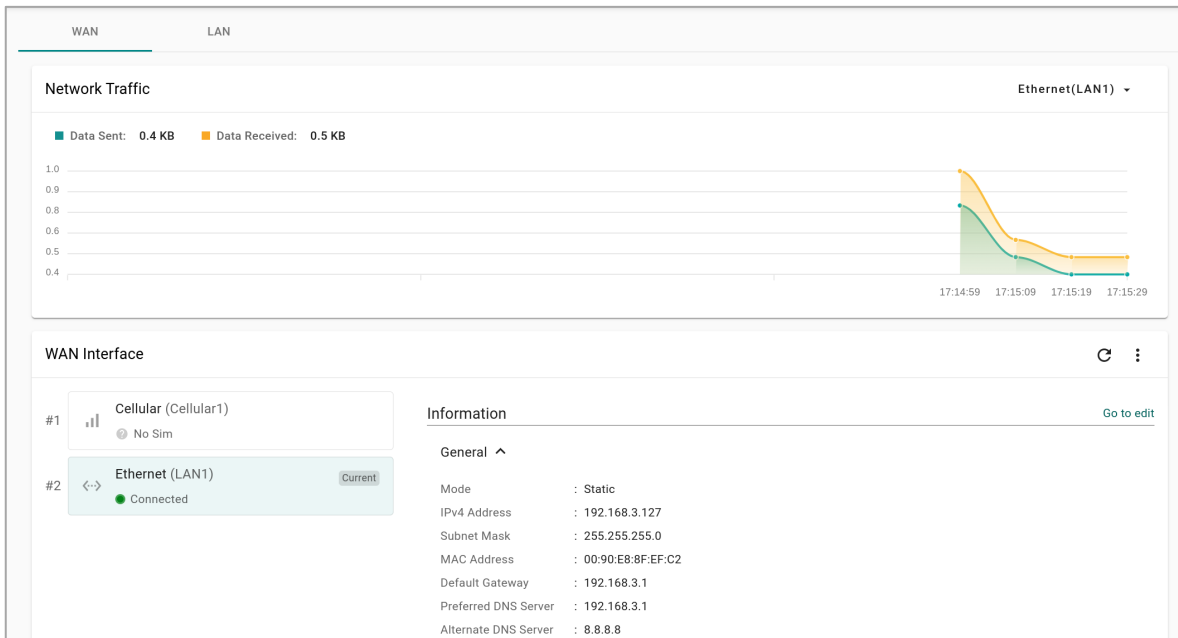
Network Dashboard

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.

The screenshot shows the LAN configuration page with two tabs: WAN and LAN. The LAN tab is active. Under 'LAN Interface', there are two entries: #1 Ethernet (LAN2) with a 'Disconnected' status, and #2 WiFi-AP (Wi-Fi1) with a 'Disable' status. The Ethernet (LAN2) interface is selected, and its configuration details are shown in the 'Information' section. The details include: Mode: Static, IPv4 Address: 192.168.4.84, Subnet Mask: 255.255.255.0, and MAC Address: 00:90:E8:9D:BF:37. There is a 'Go to edit' link next to the information section.

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 'General' configuration page for a Moxa device (AIG-501-T-AZU-LX). The page is titled 'General' and has a breadcrumb trail: Home > System Configuration > System Settings > General. There are three tabs: System, Time, and GPS. The 'System' tab is active. The 'Server/Host Name' field is set to 'Moxa' and the 'Description - optional' field is set to 'Factory A1'. There is a 'SAVE' button at the bottom of the configuration area. The left sidebar shows the navigation menu with 'System Settings' selected and 'General' highlighted. The top right corner shows the user 'Administrator admin'.

Parameter	Value	Description
Server/Host Name	Alphanumeric string	You can enter a name to identify the unit, such as the function, etc.
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 device AIG-501-T-AZU-LX. The user is logged in as Administrator admin. The left sidebar shows the navigation menu with categories: DASHBOARD (System Dashboard, Network Dashboard), SYSTEM CONFIGURATION (System Settings, General, IP Address, Cellular, HTTP/HTTPS/SSH, Serial, I/O, DHCP Server, Wi-Fi), and PROTOCOL (Modbus Master, Modbus Slave, OPC UA Server). The main content area is titled 'General' and has sub-tabs for System, Time, and GPS. The 'Time' tab is active, showing the current date and time as 'Nov 15, 2023 00:51:41'. Below this, the 'Time Zone' is set to '(GMT +08:00) Asia/Taipei'. The 'Sync Mode' is set to 'Manual' (selected with a radio button). There is a 'Sync with browser' button. A date and time picker is visible, showing 'Date: Nov 15, 2023' and a time field with 'Hour: 0', 'Minute: 51', and 'Second: 2'. A 'SAVE' button is at the bottom of the form.

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

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

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

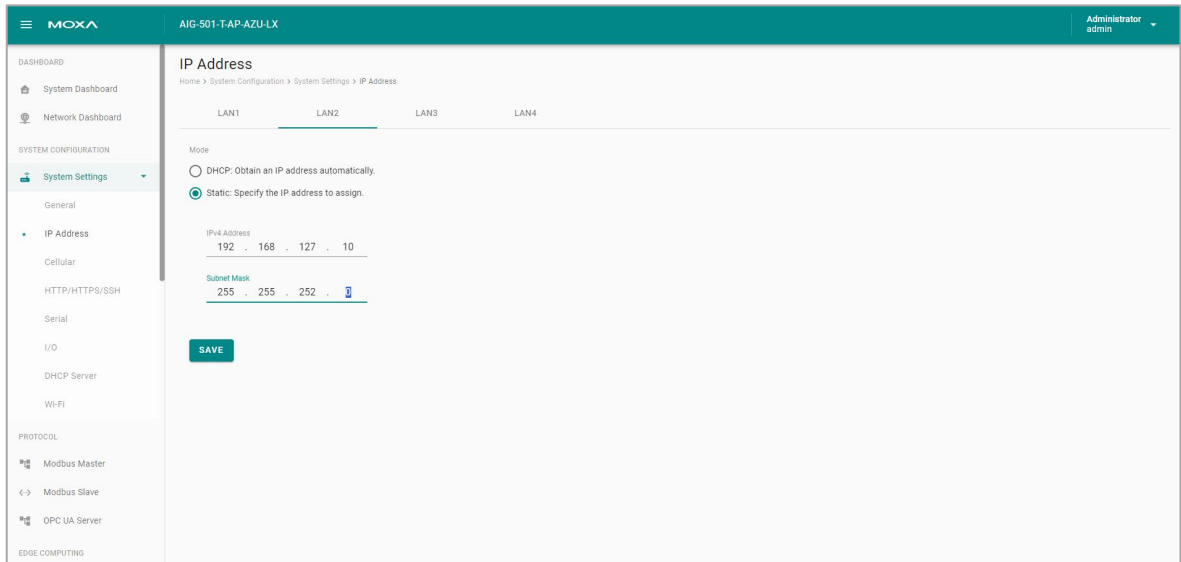
The screenshot displays the Moxa web interface for device configuration. The main content area is titled "General" and includes a breadcrumb trail: "Home > System Configuration > System Settings > General". There are three tabs: "System", "Time", and "GPS", with "GPS" being the active tab. Under the "GPS" tab, there are two radio button options: "Manually enter coordinates" (which is selected) and "Automatically adjust coordinates for GPS changes". Below these options is a "Coordinates" section with two input fields: "Latitude" containing the value "24.984129" and "Longitude" containing "121.551753". A map of Taiwan is shown below the coordinates, with a blue pin labeled "Moxa" indicating the device's location. A "SAVE" button is located at the bottom of the map area. The left sidebar shows the navigation menu with "System Settings" expanded to "General". The top right corner shows the user "Administrator admin".

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**, **LAN2**, **LAN3**, or **LAN4** 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**.

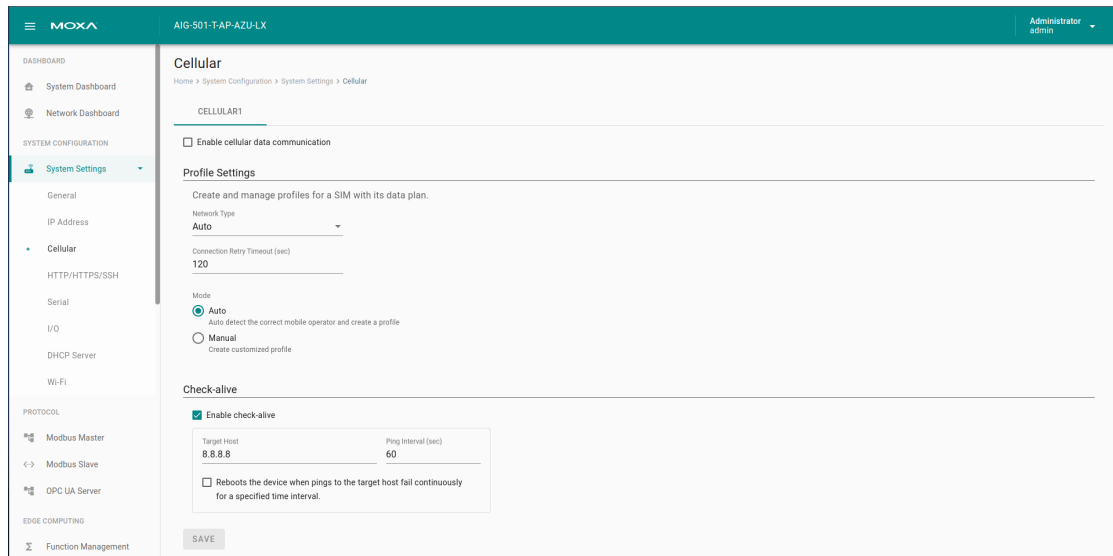


Parameter	Value	Description
Types of connectivity	WAN LAN NOTE: Only LAN1 supports WAN.	WAN: Wide Area Networks LAN: Local Area Networks
Mode	DHCP Static	DHCP: Gets the IP address automatically. Static: Specify the IP address
IPv4 Address	LAN1 default: DHCP LAN2 default: 192.168.4.127 (or other 32-bit number) LAN3 default: 192.168.5.127 (or other 32-bit number) LAN4 default: 192.168.6.127 (or other 32-bit number)	The IP (Internet Protocol) address identifies the server on the TCP/IP network

Parameter	Value	Description
Subnet Mask	Default: 255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
Gateway—optional	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server—optional	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
Alternate DNS Server— optional	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

System Settings—Cellular

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



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

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

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

1. Click **+ CREATE**.
2. Specify a unique **Profile Name**.
3. Specify the target **SIM** card.
4. Enter the **PIN Code** if your SIM card requires it.



CAUTION

Three wrong attempts will lock the SIM card.

5. Choose a **Carrier**.



NOTE

This option is displayed only if the cellular module supports carrier switching.

6. Refer to instructions from your cellular carrier to select **Static** or **Dynamic** APN and configure the corresponding settings.

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

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

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

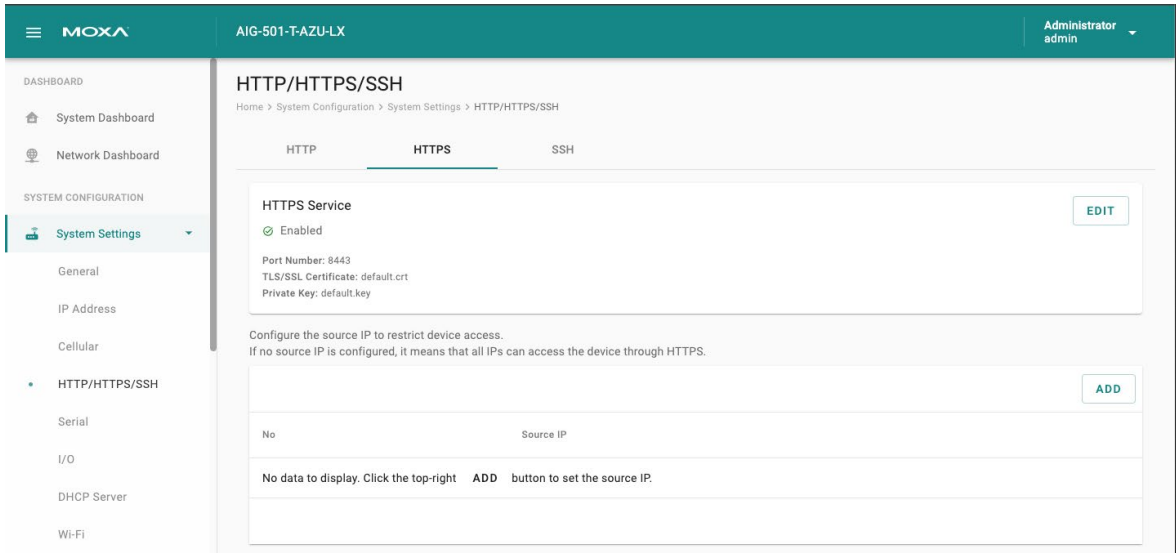
In some circumstances, a system reboot might bring an unstable or malfunctioning device back to a normal state. To enable automatic system reboot, select the **Reboot the device when pings to the target host failed continuously for a certain amount of time** option and specify a reboot interval.

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

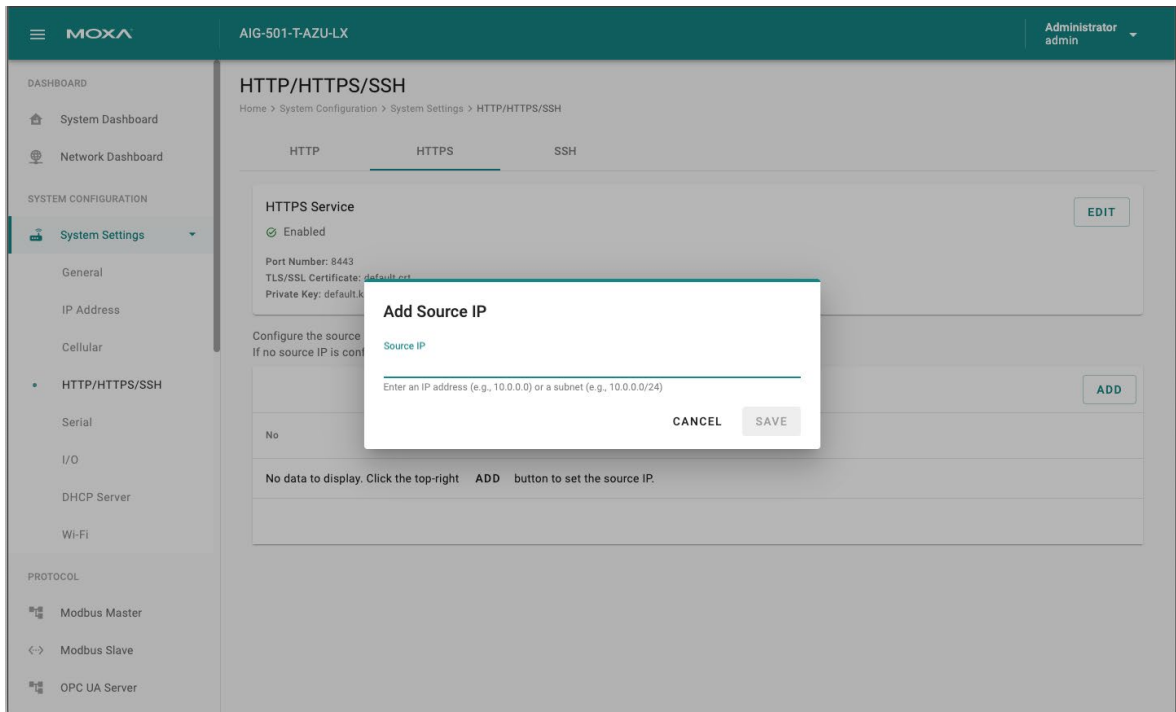
System Settings—HTTP/HTTPS/SSH

To ensure the securely access web console of the device, we strongly recommend disabling HTTP and enabling HTTPS. To do this, go to **System Settings > HTTP/HTTPS/SSH**.

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, AIG can generate a "AIG Series Root CA for HTTPS" certificate.



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



System Settings—Serial

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

To configure serial setting, do the following:

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

Port	Interface	Baud Rate	Parity, Data Bits, Stop Bits	Flow Control
#1 COM1	rs232	9600	none, 8, 1	none
#2 COM2	rs232	9600	none, 8, 1	none
#3 COM3	rs232	9600	none, 8, 1	none
#4 COM4	rs232	9600	none, 8, 1	none

Serial Settings

Interface: rs232

Baud Rate: 9600

Parity: none

Data Bits: 5 6 7 8

Stop Bits: 1 2

Flow Control*: none

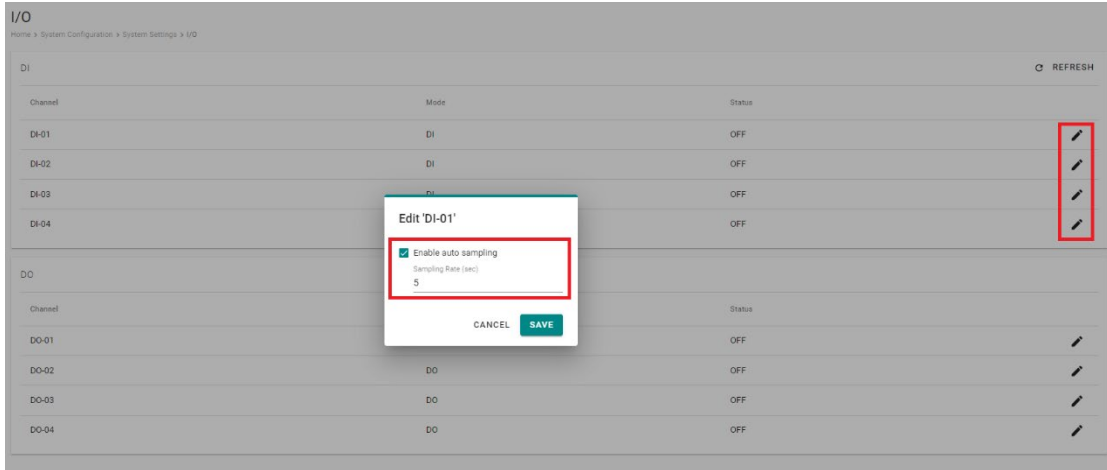
SAVE CLONE

Parameter	Value	Description
Interface	rs232 rs422 rs485-2w rs-485-4w	
Baud Rate	300 to 115200	
Parity	none, odd, even, space, mark	
Data Bits	5, 6, 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)

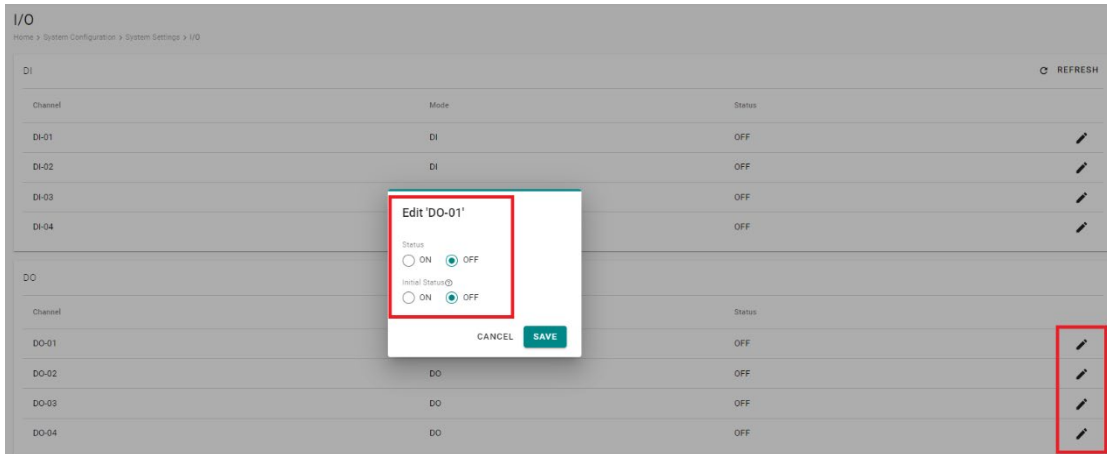
System Settings—I/O

The AIG-501 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 and enable auto sampling and input sampling rates according to your requirements.



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



Parameter	Value	Description
Status	ON	High voltage
	OFF	Low voltage

System Settings—DHCP Server

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

To configure DHCP server settings, do the following:

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

The screenshot displays the MOXA web interface for the AIG-501-T-AZU-LX device. The left sidebar shows the navigation menu with 'System Settings' selected. The main content area is titled 'DHCP Server' and includes tabs for LAN1, LAN2, LAN3, and LAN4. The 'Server Status' is currently 'Stopped'. An unchecked checkbox labeled 'Enable DHCP Server' is visible. An information box notes that the DHCP server setting is only for LAN and static IP interfaces. The 'IP Address Range' section contains input fields for Start IP (192.168.3.200), End IP (192.168.3.250), and Netmask (255.255.255.0). The 'DNS' section includes fields for Primary DNS (8.8.8.8) and Secondary DNS (8.8.4.4).



NOTE

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

System Settings—Wi-Fi

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

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

If the Wi-Fi AP is Selected

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

Wi-Fi

Home > System Configuration > System Settings > Wi-Fi

Wi-Fi1

Enable Wi-Fi

Wi-Fi Mode
Wi-Fi AP

General Settings

Broadcast SSID

SSID
moxa-sample-ap

Password (WPA2-PSK)
.....

Advanced Settings

Band
2.4GHz (802.11 b/g/n)

Region
Taiwan

Channel
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' form contains the following fields and controls:

- SSID:** A text input field.
- Security Mode:** A dropdown menu currently set to 'WPA/WPA2 Personal'.
- Password:** A text input field with a toggle icon to show/hide the password.
- Buttons:** 'CANCEL' and 'ADD' buttons at the bottom right.

The 'Add by Scan Results' form contains the following elements:

- Steps:** '1 Select AP' and '2 View Details'.
- Info:** A blue box with the text: 'Info: Please choose the Wi-Fi network that you want to add from the list. Note that only WPA and WPA2 Personal are supported.'
- AP List:** A table of detected networks with lock and signal icons.
- Buttons:** 'CANCEL' and 'NEXT >' buttons at the bottom right.

Network Name	Lock Icon	Signal Icon
SQA3_WiFi6	🔒	📶
sqa-iiot-lan-50G	🔒	📶
SQA2-TestBed-AWK3131A	🔒	📶
SQA-LAB-TV	🔒	📶
.M-Guest	🔒	📶
SQA2-TestBed-AWK3131A	🔒	📶

2. Select **DHCP** or **Static mode**.
3. Check **Check-alive** function which can be used to ensure Internet connectivity.
4. Click **SAVE**.

The 'Wi-Fi' configuration page includes the following sections:

- Wi-Fi:** A toggle for 'Enable Wi-Fi' and a dropdown for 'Wi-Fi Mode' set to 'Wi-Fi Client'.
- AP List:** A section with a '+ CREATE' button and a message: 'There are no APs to connect to. Click **CREATE BY SSID** or the button at upper right corner to switch to the Create mode to add an AP.'
- IP Settings:** Radio buttons for 'Mode': 'DHCP: Obtain an IP address automatically' (selected) and 'Static: Assign IP address by manual configuration'.
- Check-alive:** A toggle for 'Enable check-alive'.
- Buttons:** A 'SAVE' button at the bottom left.

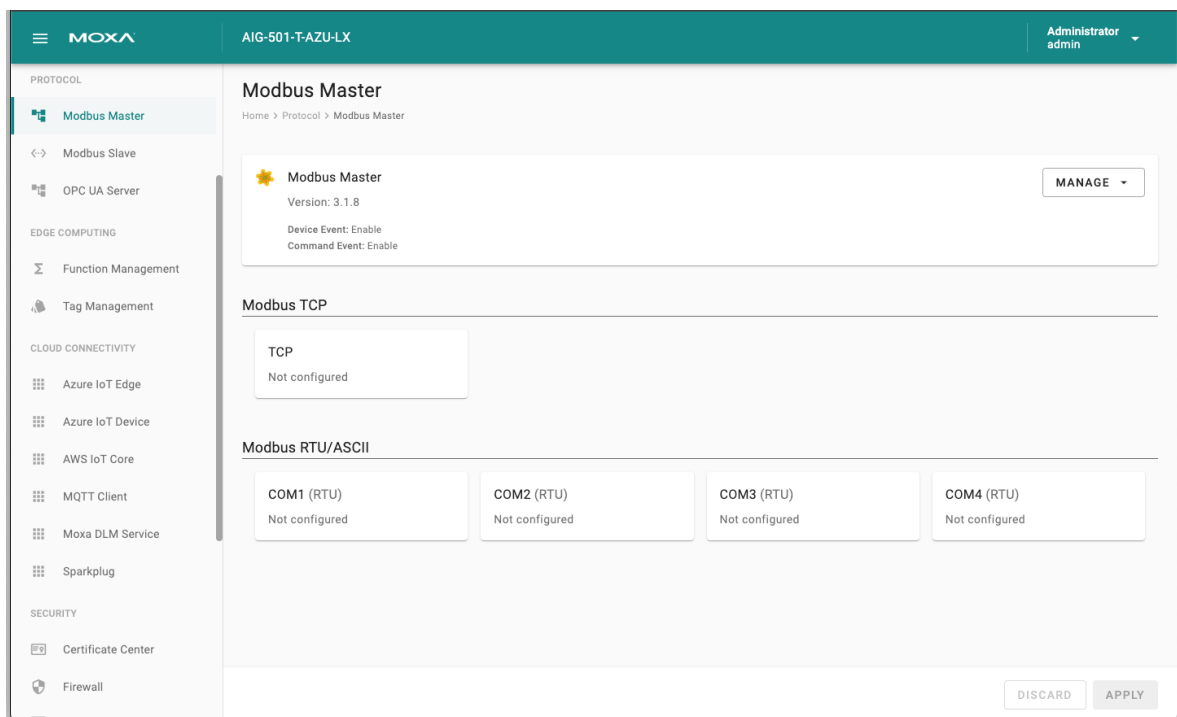
Protocol

Modbus Master

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

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

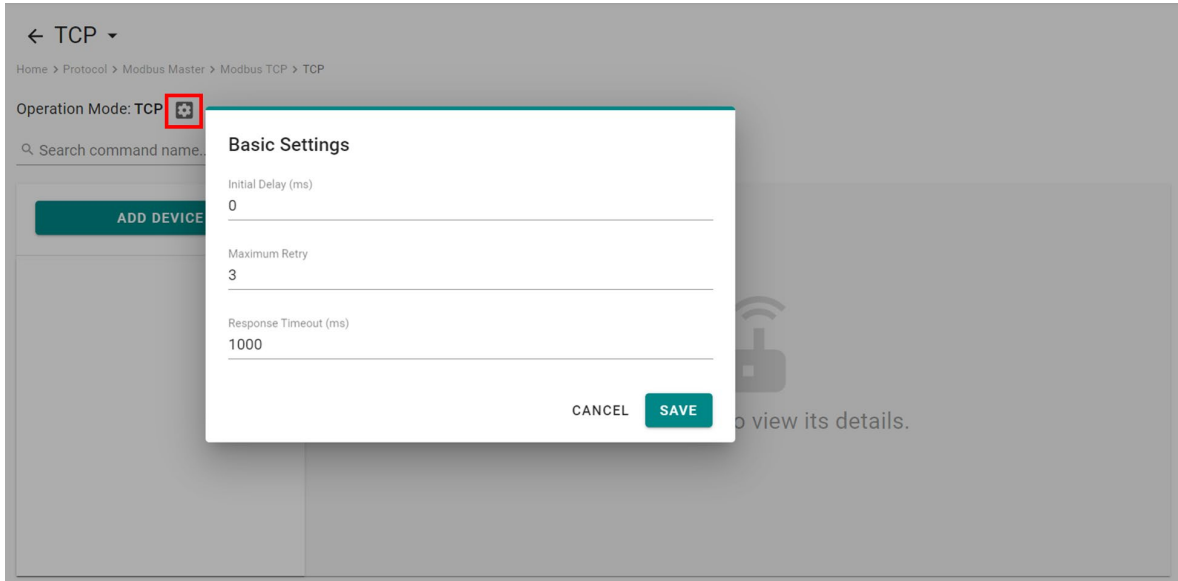
1. Click **TCP** under Modbus TCP or **COMx** under Modbus RTU/ASCII.
2. Click **ADD DEVICE** and go to the 3-step wizard page.
3. Input **device name**, **slave ID**, **IP Address**, and **TCP port**, then press **NEXT**.
4. Click **+ ADD COMMAND** to add Modbus commands to collect the data, then press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



Modbus TCP

Basic Settings

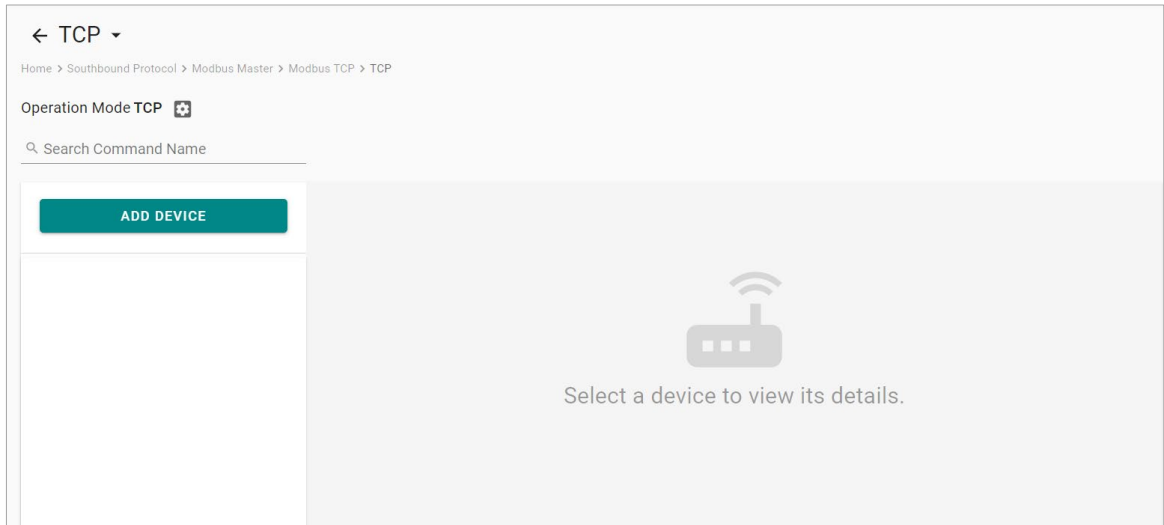
When you access the Modbus TCP setting page, you will first need to configure the basic settings.



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

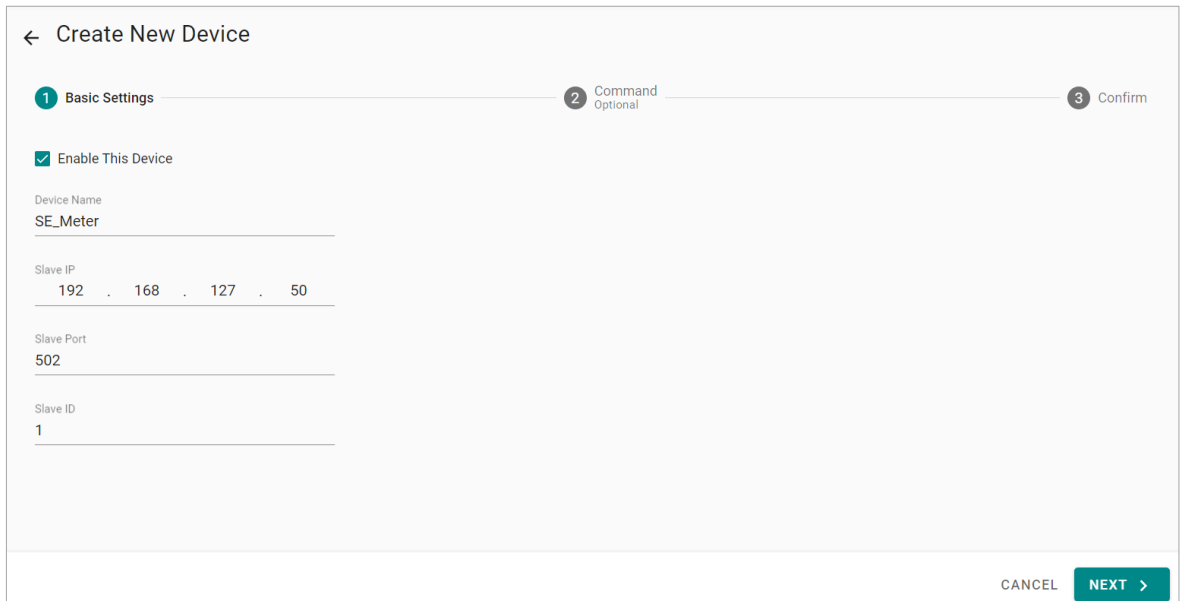
Modbus Device Settings

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



Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.



The screenshot displays the 'Create New Device' wizard, specifically the 'Basic Settings' step. The wizard has three steps: 1. Basic Settings, 2. Command Optional, and 3. Confirm. The 'Enable This Device' checkbox is checked. The following fields are filled out:

- Device Name: SE_Meter
- Slave IP: 192 . 168 . 127 . 50
- Slave Port: 502
- Slave ID: 1

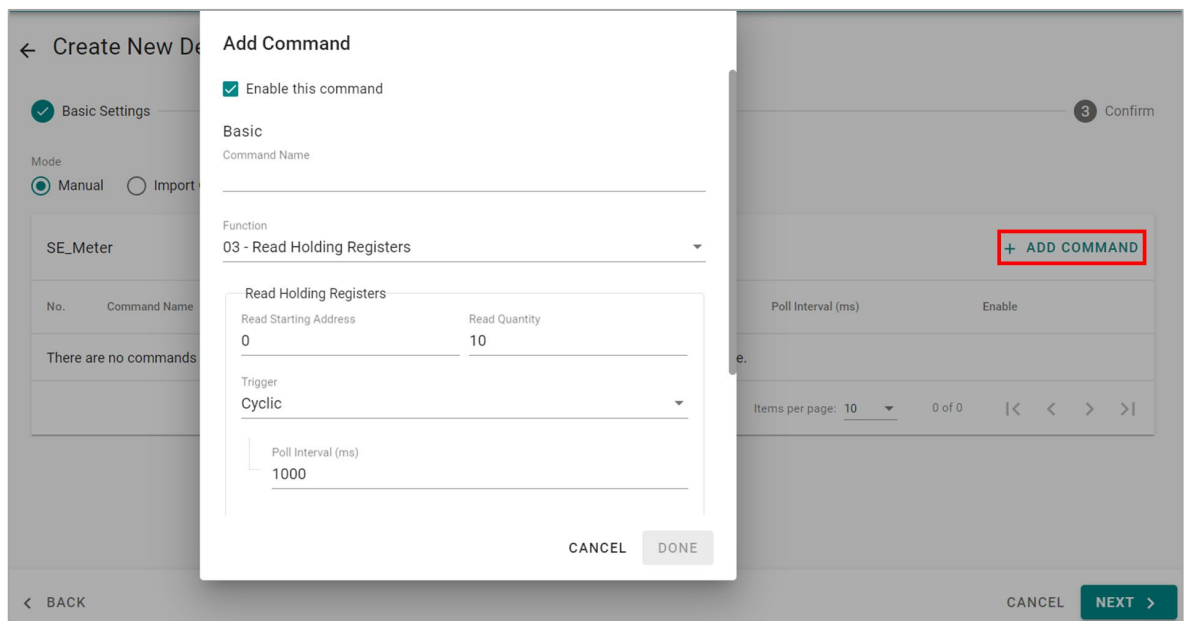
At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

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

Step 2. Command

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

The command settings will pop up.



Parameter	Value	Default	Description
Command Name	Alphanumeric string	–	Name the command
Function	01 – Read Coils 02 – Read Discrete Inputs 03 – Read Holding Registers 04 – Read Inputs Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 23 – Read/Write Multiple Registers	03 – Read Holding Registers	How to collect data from the Modbus device
Read Starting Address	0 to 65535	0	Modbus registers the address for the collected data
Read quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how much data to read
Write start address	0 to 65535	0	Modbus registers the address for the written data
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how much data to write.

Parameter	Value	Default	Description
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.
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

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

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP 🛠️

🔍 Search command name...

ADD DEVICE

SE_Meter

🟢 Enable

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

+ ADD COMMAND IMPORT EXPORT

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

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

Editing GO TO APPLY SETTINGS

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP 🛠️

🔍 Search command name...

ADD DEVICE

SE_Meter

🟢 Enable

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

+ ADD COMMAND IMPORT EXPORT

Trigger	Poll Interval (ms)	Enable	
Cyclic	1000	Enable	⋮

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

Import Command Configuration

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

Command Configuration

BROWSE...

CANCEL
DONE

Editing GO TO APPLY SETTINGS

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

Modbus Master

Home > Protocol > Modbus Master

★ Modbus Master
Version: 3.10.7
MANAGE ▾

Device Event: Enable
Command Event: Enable

Modbus TCP

TCP

1 Device, 0 Command

Modbus RTU/ASCII

COM1 (RTU)

1 Device, 0 Command

COM2 (RTU)

Not configured

COM3 (RTU)

Not configured

COM4 (RTU)

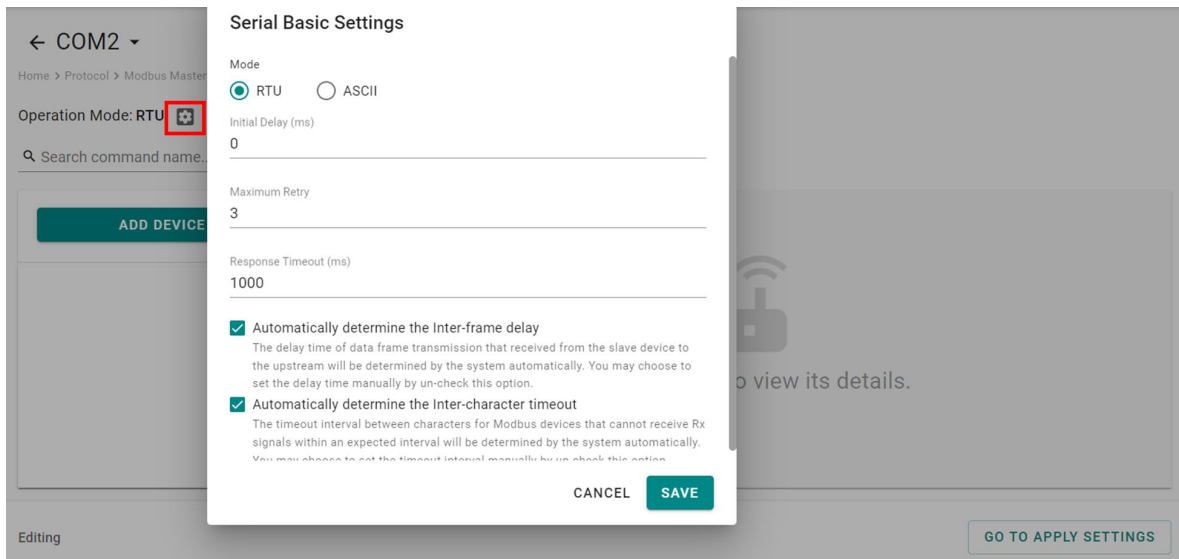
Not configured

Editing DISCARD APPLY

Modbus RTU/ASCII

Basic Settings

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



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

Modbus Device Settings

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

Step 1. Basic Settings

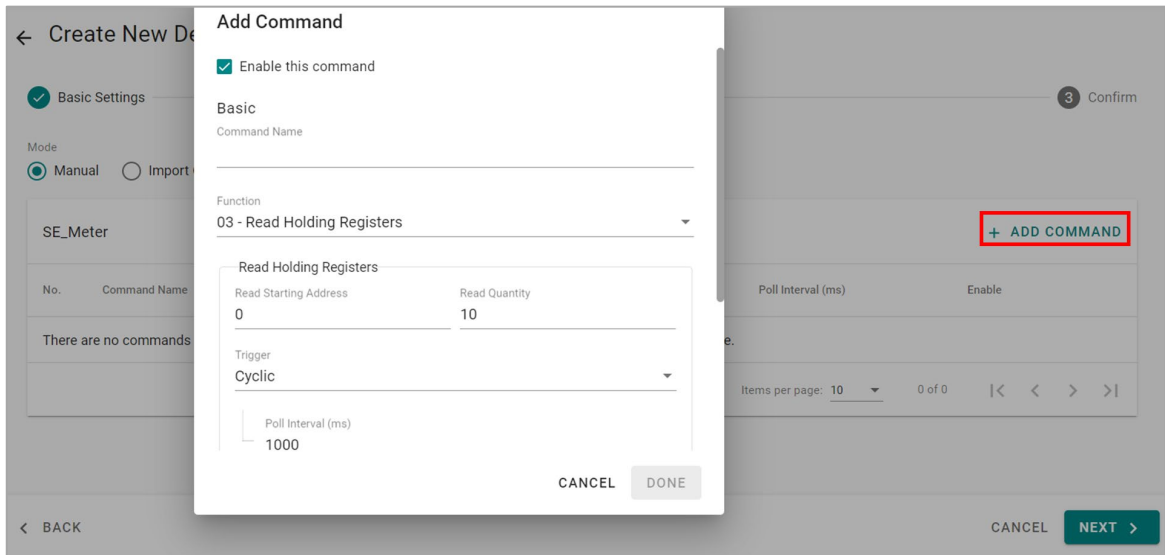
Fill in the basic parameters for the Modbus RTU/ASCII device.

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

Step 2. Command

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

The command settings will pop up.



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

Parameter	Value	Default	Description
Read quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how much data to read
Write starting address	0 to 65535	0	Modbus registers the address for the written data
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	-	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	None: not to swap Byte: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. Byte and Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.

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 the read command encounters an error or times out.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	-	The command will be generated into a meaningful tag by tag type and stored in the tag hub.

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

← Create New Device

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

✓ Basic Settings ✓ Command Optional 3 Confirm

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

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

← BACK CANCEL **DONE**

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

← COM2 ▾

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

Operation Mode: RTU 🗄

🔍 Search command name...

ADD DEVICE SE_Meter + ADD COMMAND **IMPORT** **EXPORT**

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

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

Editing **GO TO APPLY SETTINGS**

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

Modbus Master
Home > Protocol > Modbus Master

★ **Modbus Master**
Version: 3.10.7
Device Event: Enable
Command Event: Enable

MANAGE ▾

Modbus TCP

TCP
1 Device, 0 Command

Modbus RTU/ASCII

COM1 (RTU)
1 Device, 0 Command

COM2 (RTU)
Not configured

COM3 (RTU)
Not configured

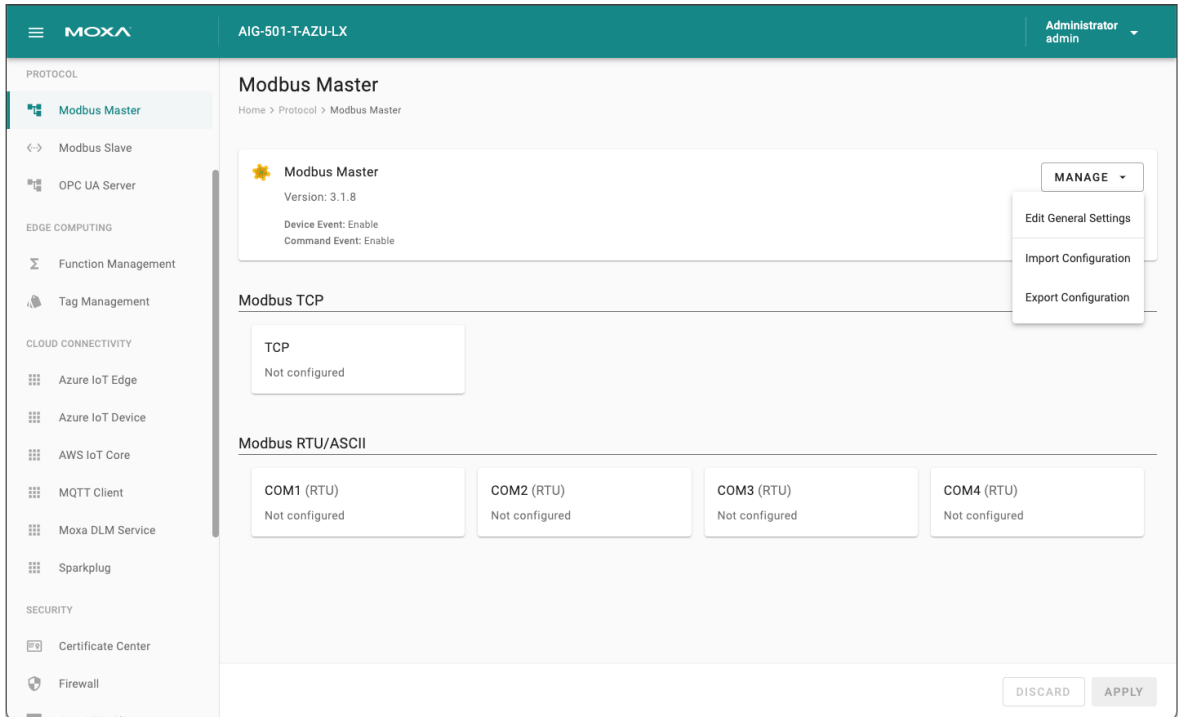
COM4 (RTU)
Not configured

Editing

DISCARD **APPLY**

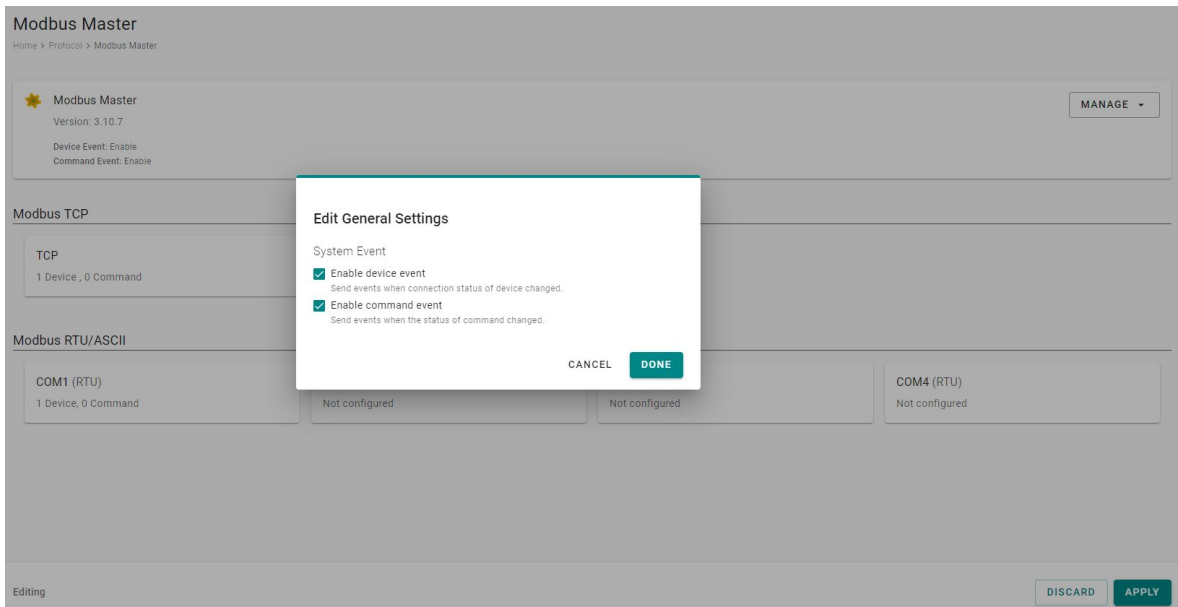
Management

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



Edit General Settings

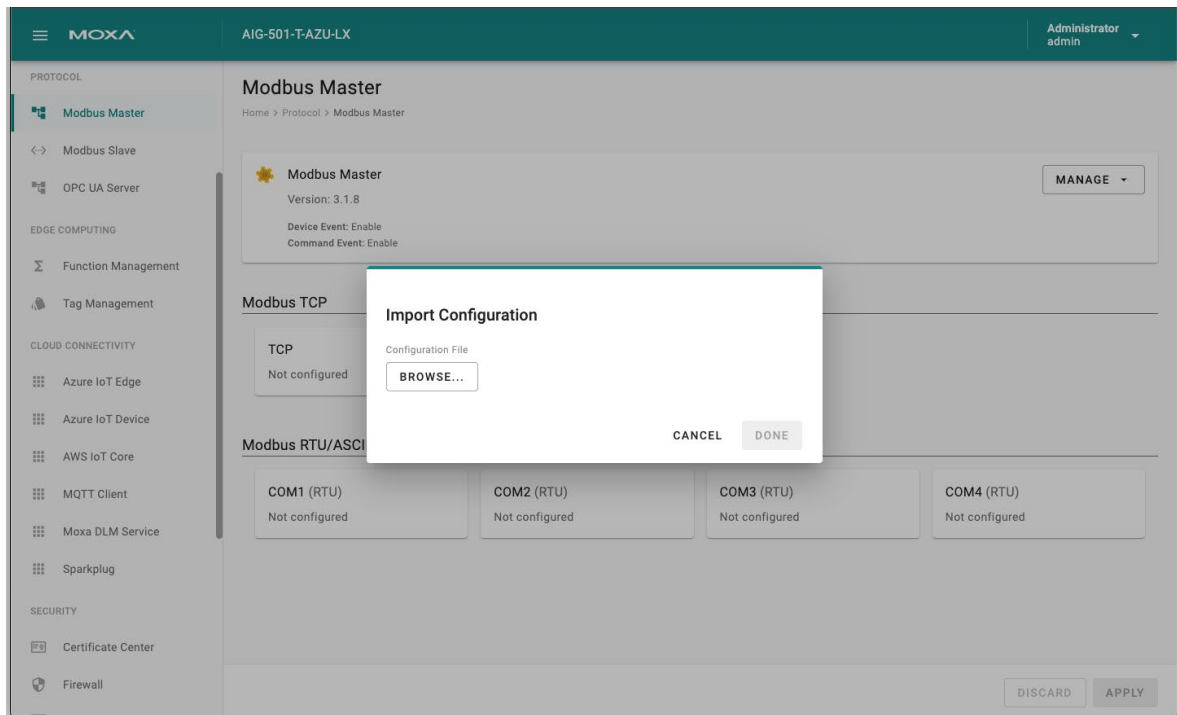
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	<p>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.</p> <p>Uncheck: Disable the function</p>
Enable command event	Check uncheck	Check	<p>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.</p> <p>Uncheck: Disable the function.</p>

Import/Export Configuration

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

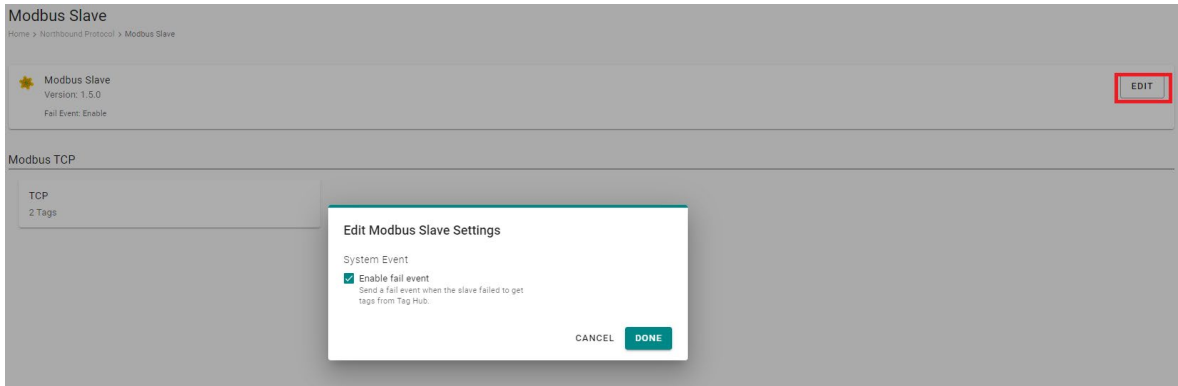


An example of an exported file that can be viewed/edited by EXCEL.

[master-tcp-faces]																										
@master	tcpMaster	initialDel	retryCour	responseTou																						
1	1	0	3	1000																						
[ser-masters]																										
@serMas	configId	name																								
1	1	modbus_serial_master																								
[master-ser-faces]																										
@master	serMaster	port	value format	initialDel	retryCour	response	frameIn	te char	interval																	
1	1	1	0	0	3	1000	0	0																		
2	1	1	0	0	3	1000	0	0																		
[remote-devs]																										
@remote	masterSer	masterTr	name	enable	slaveId	slaveIp	slaveTcpPort																			
1	1	1232	1	1	0.0.0.0	502																				
2	2	SE_Meter	1	1	0.0.0.0	502																				
3	1	GE_Meter	1	1	1.1.1.1	502																				
[mcmds]																										
@remote	name	enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollinterv	swap	fpFunc	fpTou	fpData	scalingFu	intercept	intercept	pointSou	pointSou	pointTarg	pointTarg	tagName	data	Type	dataUnit	access	dataSize
1	231	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	0	1	Voltage_t1	int16	r		20
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	0	1	Voltage_t2	int16	r		
																						Voltage_t3	int16	r		
																						Voltage_t4	int16	r		
																						Voltage_t5	int16	r		
																						Voltage_t6	int16	r		
																						Voltage_t7	int16	r		
																						Voltage_t8	int16	r		

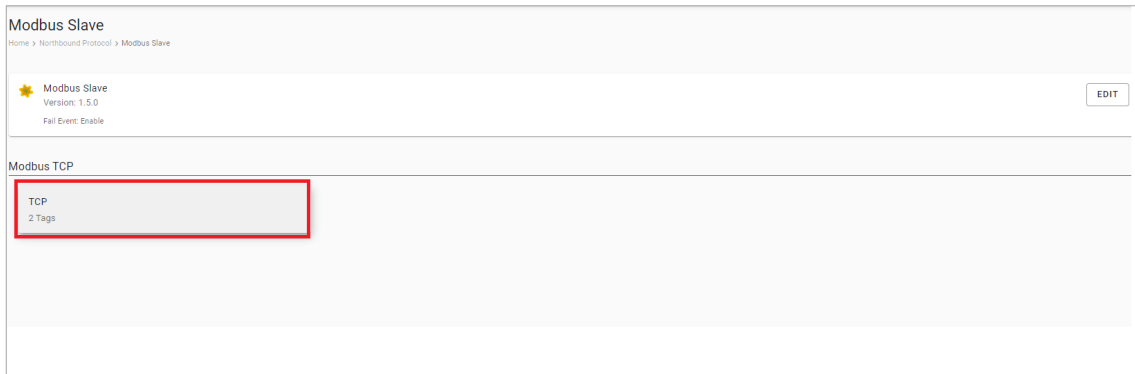
Modbus TCP Slave

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

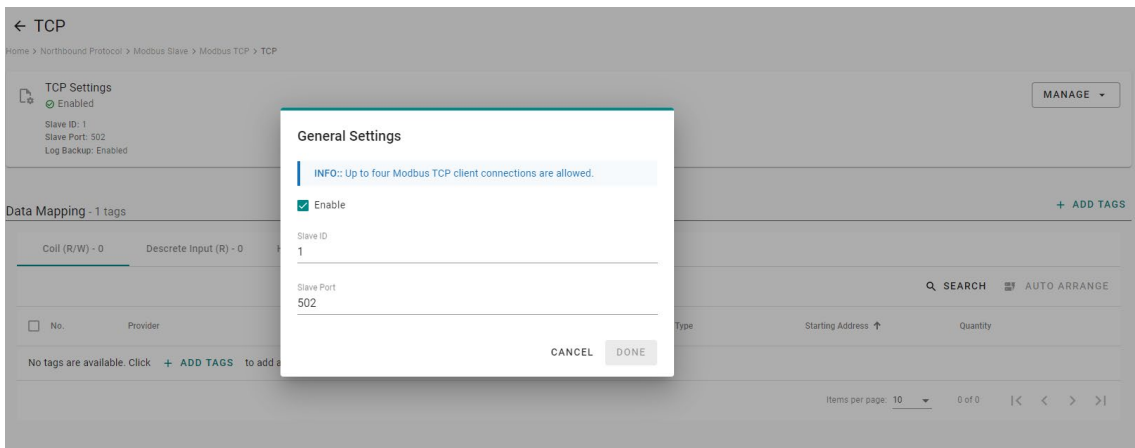


To create a Modbus TCP server (slave), following the steps below:

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

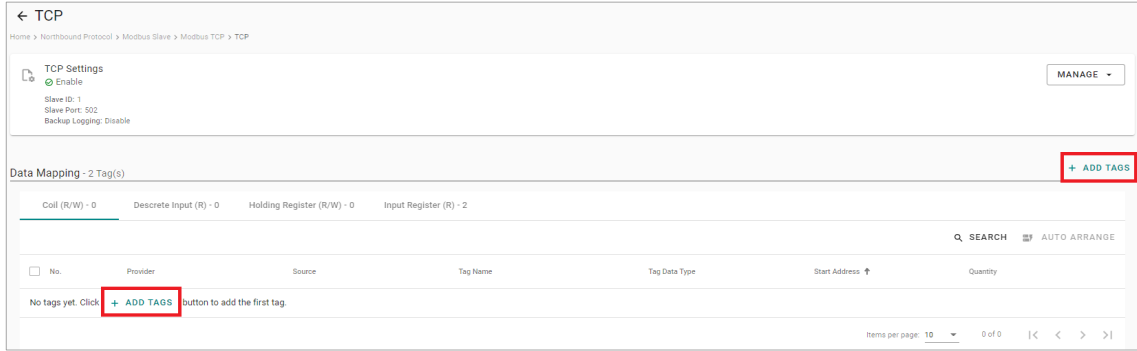


2. Click **MANAGE > General Settings**.



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

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

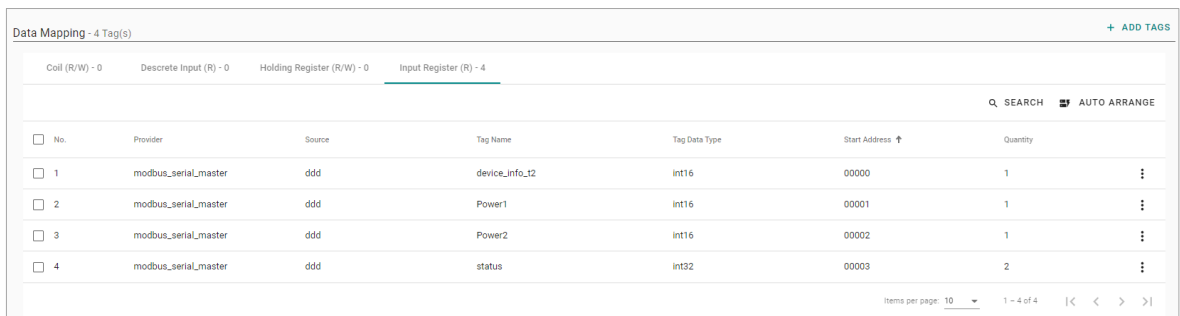


4. Click **DONE** to finish settings.

Data Mapping

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

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



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

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.

← TCP

Home > Protocol > Modbus Slave > Modbus TCP > TCP

TCP Settings

Enabled

Slave ID: 1
Slave Port: 502
Backup Logging: Enabled
FTP/SFTP Log Upload: Disabled
Last Upload Status: Unknown
Last Upload Time: Jan 01, 1970 08:00:00
Last Upload File Name: 19700101T080000Z.csv

MANAGE

- General Settings
- Backup Logging
- Edit Settings
- View File List
- Upload Logs

Data Mapping - 0 tags

+ ADD TAGS

Coil (R/W) - 0 Discrete Input (R) - 0 Holding Register (R/W) - 0 Input Register (R) - 0

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**.

Edit Backup Logging Settings

Enable backup logging

Target Storage

System (52.53GB free of 57.48GB) ▼

Folder Name

Modbus TCP Slave

Maximum Storage (MB) ⓘ

1024

Logging Interval (sec)

30

File Split Mode

By Time By Size

Time Interval (min)

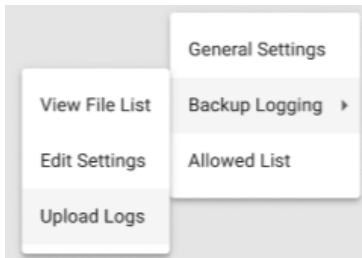
1440

CANCEL

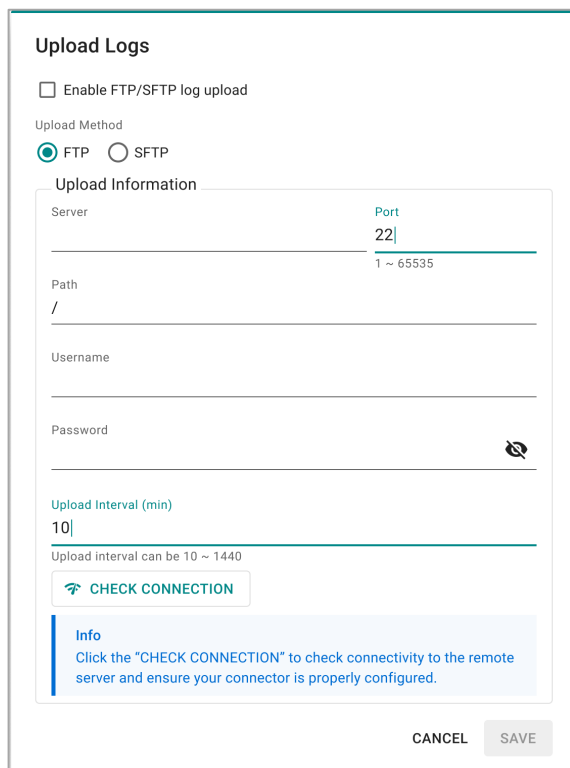
DONE

To upload files via FTP with AIG, follow these steps:

1. Click on "Backup Logging", then "Upload Logs".

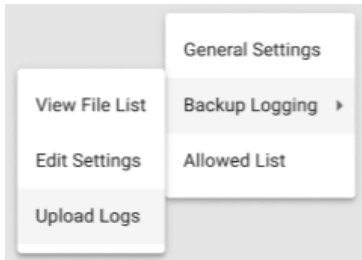


2. Enable the FTP/SFTP uploader.
3. Select FTP as upload Method.
4. Configure the necessary parameters, such as server, port, path, username, and password.
5. Configure the upload interval.
6. (Option) Click "Check Connection" to verify that the communication is functioning correctly.
7. Click "Save" to apply the settings.

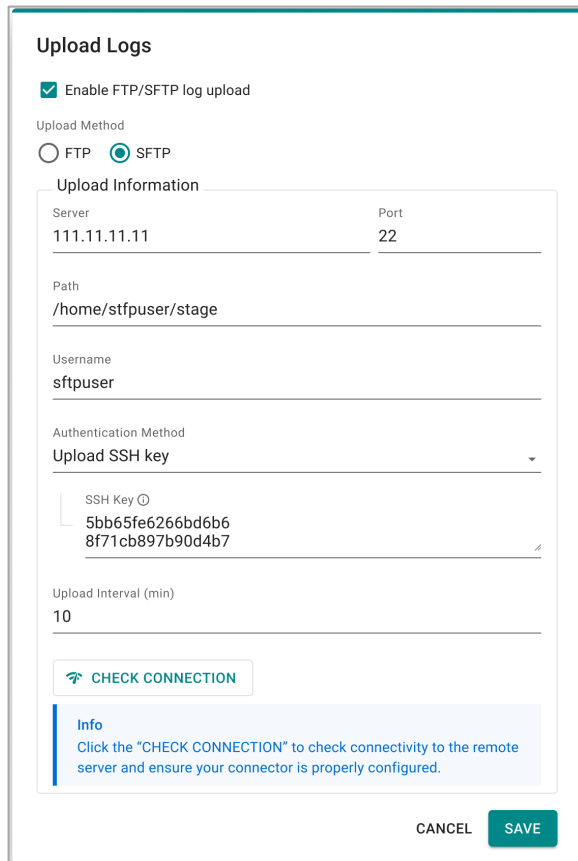
A screenshot of the "Upload Logs" configuration form. At the top, there is a checkbox labeled "Enable FTP/SFTP log upload". Below it, the "Upload Method" section has two radio buttons: "FTP" (which is selected) and "SFTP". The "Upload Information" section contains several input fields: "Server" (with a "Port" label and a value of "22" and a range "1 ~ 65535" below it), "Path" (with a value of "/"), "Username", and "Password" (with a toggle icon). Below these is the "Upload Interval (min)" field with a value of "10" and a note "Upload interval can be 10 ~ 1440". A "CHECK CONNECTION" button is located below the interval field. At the bottom, there is an "Info" box with the text: "Click the 'CHECK CONNECTION' to check connectivity to the remote server and ensure your connector is properly configured." At the very bottom of the form are "CANCEL" and "SAVE" buttons.

To upload files via SFTP with AIG, follow these steps:

1. Click on "Backup Logging", then "Upload Logs".



2. Enable the FTP/SFTP uploader.
3. Select SFTP as upload Method.
4. Configure the necessary parameters, such as server, port, and path.
5. Select the SFTP authentication method, you can use the followings:
 - 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. Configure the upload interval.
7. (Option) Click "Check Connection" to verify that the communication is functioning correctly.
8. 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" which is checked. Below this, the "Upload Method" is set to "SFTP" (selected with a radio button). The "Upload Information" section contains several fields: "Server" (111.11.11.11), "Port" (22), "Path" (/home/stfpuser/stage), and "Username" (stfpuser). The "Authentication Method" is set to "Upload SSH key". Below this, there is a text area for the "SSH Key" containing the public key: 5bb65fe6266bd6b68f71cb897b90d4b7. The "Upload Interval (min)" is set to 10. At the bottom of the form, there is a "CHECK CONNECTION" button with a Wi-Fi icon. Below the button is an "Info" box with the text: "Click the 'CHECK CONNECTION' to check connectivity to the remote server and ensure your connector is properly configured." At the very bottom of the form, there are "CANCEL" and "SAVE" buttons.



NOTE

After using the "check connection" feature, if you observe a connection failure, or if you notice in the Event Log that data cannot be uploaded via FTP/SFTP, please verify the following:

- Whether the **Server IP** or **Port**, and **Path** have been correctly set up on the server side.
- Whether the **authentication information** is accurate.

OPC UA Server

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

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

← LAN

Home > Protocol > OPC UA Server > LAN

General Advanced

Connection ^ EDIT

Server Status : Enable

Server Port : 4840

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

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

Security ^ EDIT

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

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

Anonymous User Login : Disable

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

1. Click Connection **EDIT**, select **Enable This Server**, and click **DONE**.

The service is enabled by default on port 4840.

← LAN

Home > Protocol > OPC UA Server > LAN

General Advanced

Connection ^ EDIT

Server Status : Disable

Server Port : 4840

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

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

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

Security ^ EDIT

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

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

Anonymous User Login : Disable

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

Edit Connection

Enable This Server

Server Port
4840

CANCEL **DONE**

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

Edit Security

Policies User Authentication Certificates

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

Suggested Options

- Sign and Encrypt - Basic256Sha256 (Default Choice)
- Sign - Basic256Sha256

Deprecated Options

- Sign and Encrypt - Basic256
- Sign - Basic256
- Sign and Encrypt - Basic128Rsa15
- Sign - Basic128Rsa15

CANCEL DONE

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

← Account Management

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

+ CREATE

No.	Account	
1	admin	⋮

BACK

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) Max Publish Interval (ms)
500 50000

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

Min Lifetime (ms) Max Lifetime (ms)
1000 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.

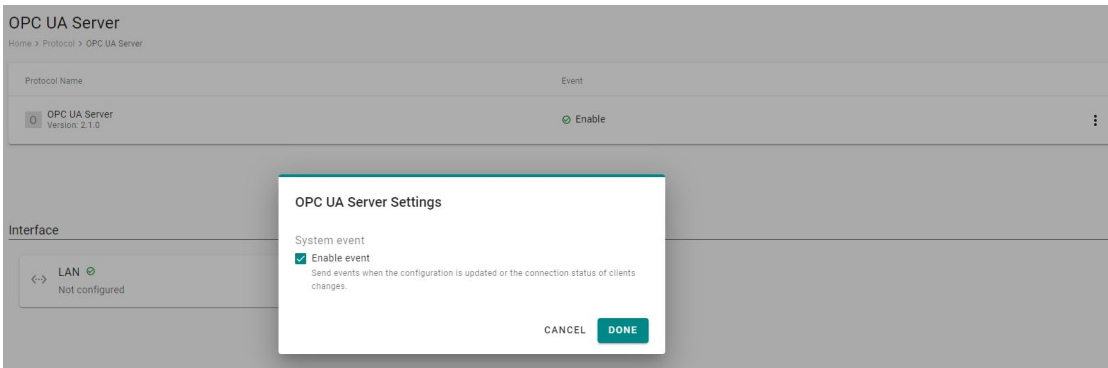
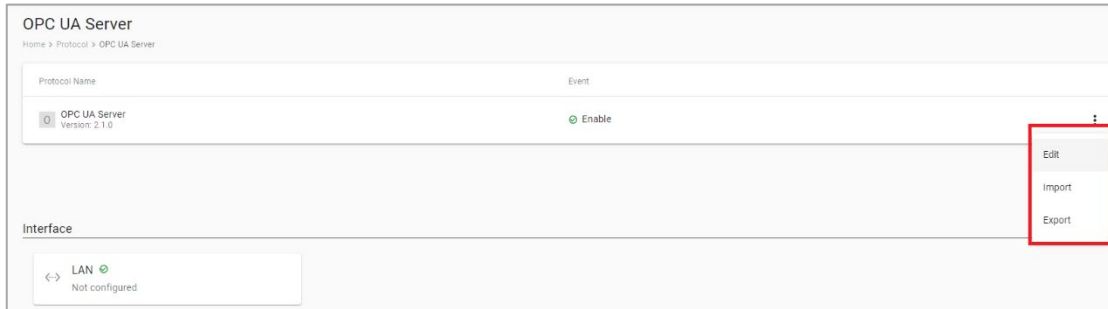
Providers
system

Selected Tags
cpuNice (+27 others)

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.



Edge Computing

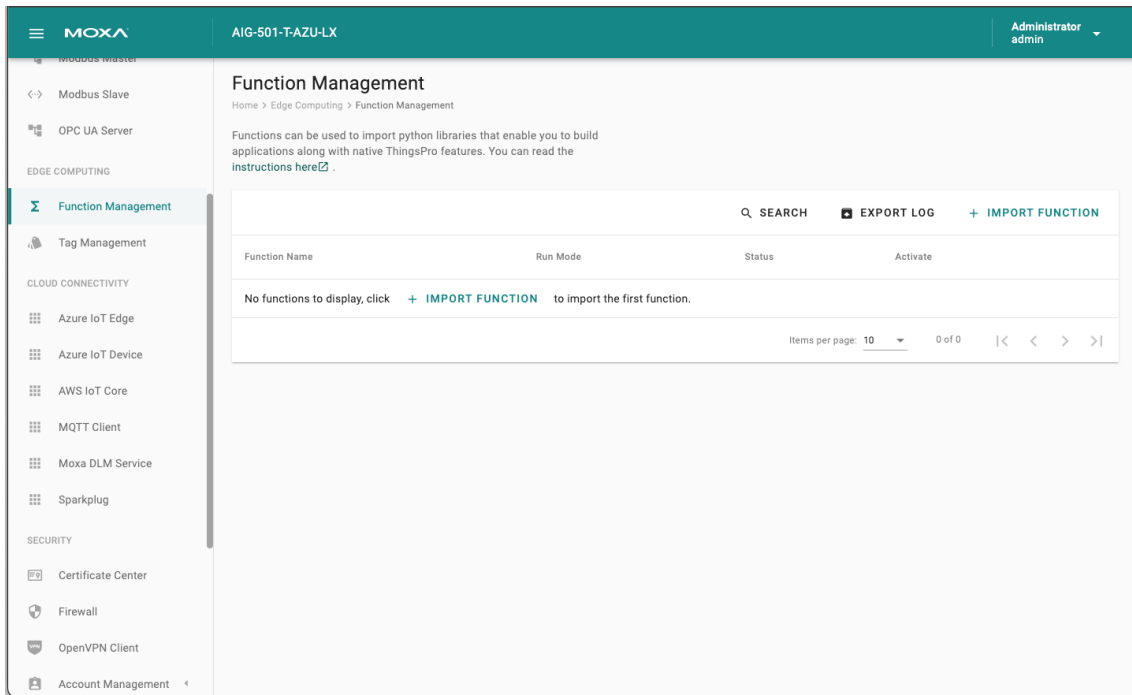
Function Management

AIG-501 Series provides a functionality to trigger actions based on specific data or time frame. 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.

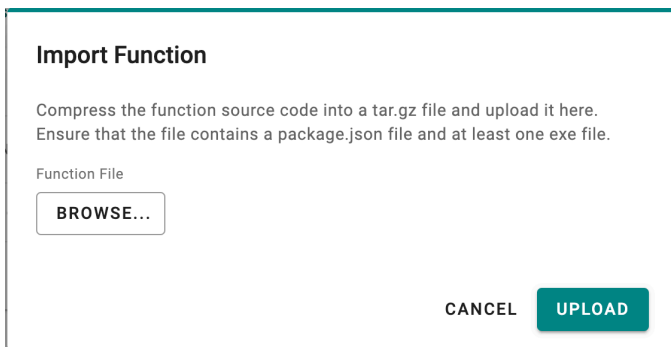
Go to **Edge Computing > Function Management** to import and manage functions. For additional information, see [build your own functions](#).

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 <small>Last uptime: May 20, 2022 20:42:15</small>	✔ Running

```

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

	Run Mode
1	Boot
2	Cron job

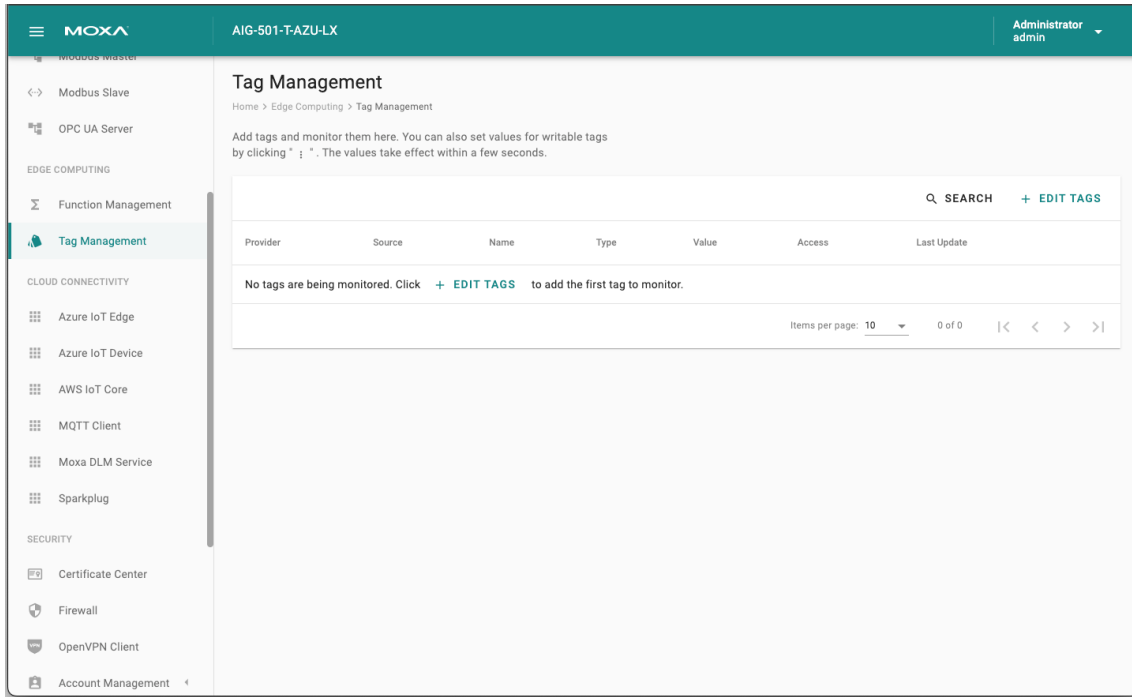
Status	Description
Running	The function is running
Retrying	Retrying a failed function every 5 seconds (unlimited tries)
Failure	The function failed during a retry. The correspondent error message will be displayed in the table. You can click EXPORT LOG to check the logs.
Inactive	The function is disabled.

Tag Management

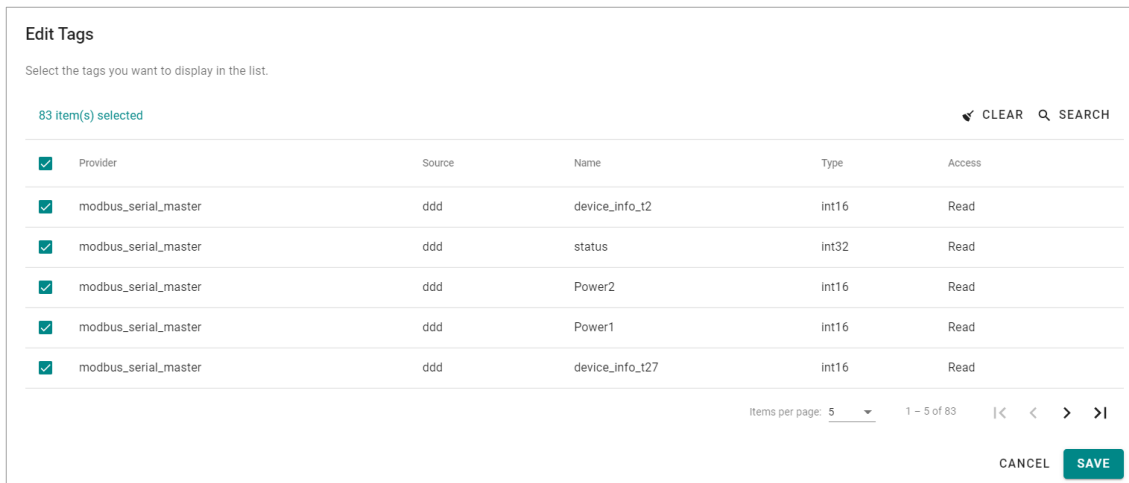
Go to **Tag Management**, where you can create and monitor the real-time tag value for troubleshooting purposes.

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

1. Click **+ EDIT TAGS**.



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



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

Tag Management
Home > Tag Hub > Tag Management

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

Monitoring tags ... SEARCH + EDIT TAGS

Provider	Source	Name	Type	Value	Access	Last Update	
modbus_serial_master	ddd	device_info_12	int16	-	Read	-	⋮
modbus_serial_master	ddd	status	int32	-2147483648	Read	Sep 14, 2022, 11:38:19	⋮
modbus_serial_master	ddd	Power2	int16	-	Read	-	⋮
modbus_serial_master	ddd	Power1	int16	-	Read	-	⋮

4. Click **SAVE**.

5. (Optional) Press the icon to deactivate the monitoring tags.

6. (Optional) Press the icon to write value for test purposes.

Tag Management
Home > Tag Hub > Tag Management

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

Monitoring tags ... SEARCH + EDIT TAGS

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

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

CANCEL **NEXT >**

Write value

Provider: modbus_serial_master

Source: 123

Name: DO

Type: boolean

Value *

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

CANCEL SAVE



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.

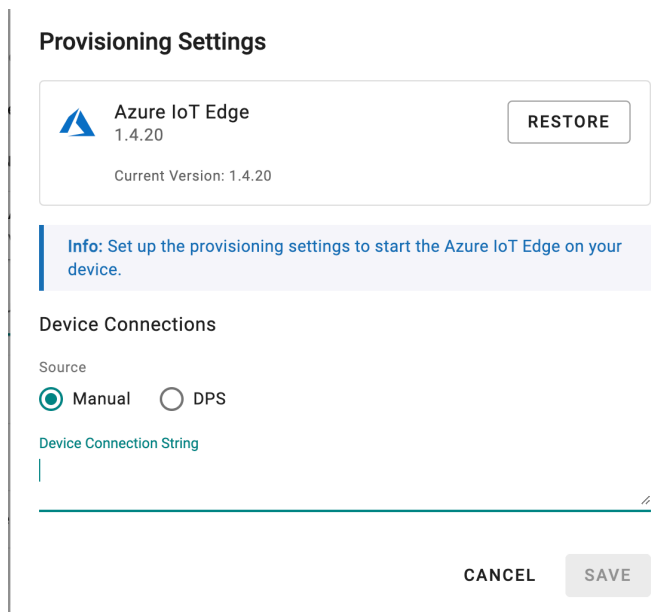


NOTE

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**.



The screenshot shows the 'Provisioning Settings' dialog box. At the top, it displays the Azure IoT Edge logo, version 1.4.20, and a 'RESTORE' button. Below this is an information box stating: 'Info: Set up the provisioning settings to start the Azure IoT Edge on your device.' Underneath, the 'Device Connections' section has a 'Source' label with two radio buttons: 'Manual' (which is selected) and 'DPS'. Below the radio buttons is a text input field labeled 'Device Connection String' with a cursor and a paste icon. At the bottom of the dialog are 'CANCEL' and 'SAVE' buttons.

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.
- 4.



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**.
- 5. Click **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.

Create New Telemetry Message

1 Basic Settings 2 Message Tags 3 Properties Optional

Enable Telemetry Message

Output Topic

Publish Mode

By Interval Immediately By Size

Publish Interval (sec)

60

Sampling Mode

All Changed Values

Custom sampling rate from acquired data

CANCEL NEXT >

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

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

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

Providers

IO

Search

SELECT ALL CLEAR

- [IO] DI
- DI-01
- DI-02
- DI-03

Total: 8, Selected: 4

DONE

Default Payload

nu11

Enable Custom Payload

CANCEL NEXT >

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

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

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": {
        "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**.

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. Log in your **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.

Azure IoT Edge

Home > Cloud Connectivity > Azure IoT Edge

Azure IoT Edge

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

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

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

Allow Device Management
This feature requires the ThingsProAgent module installed.

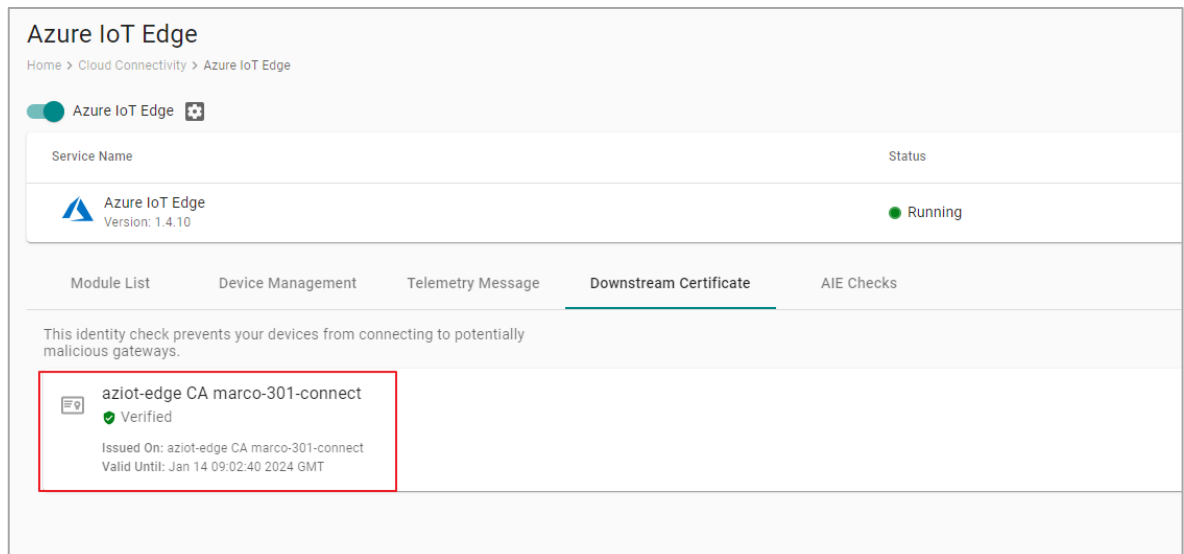
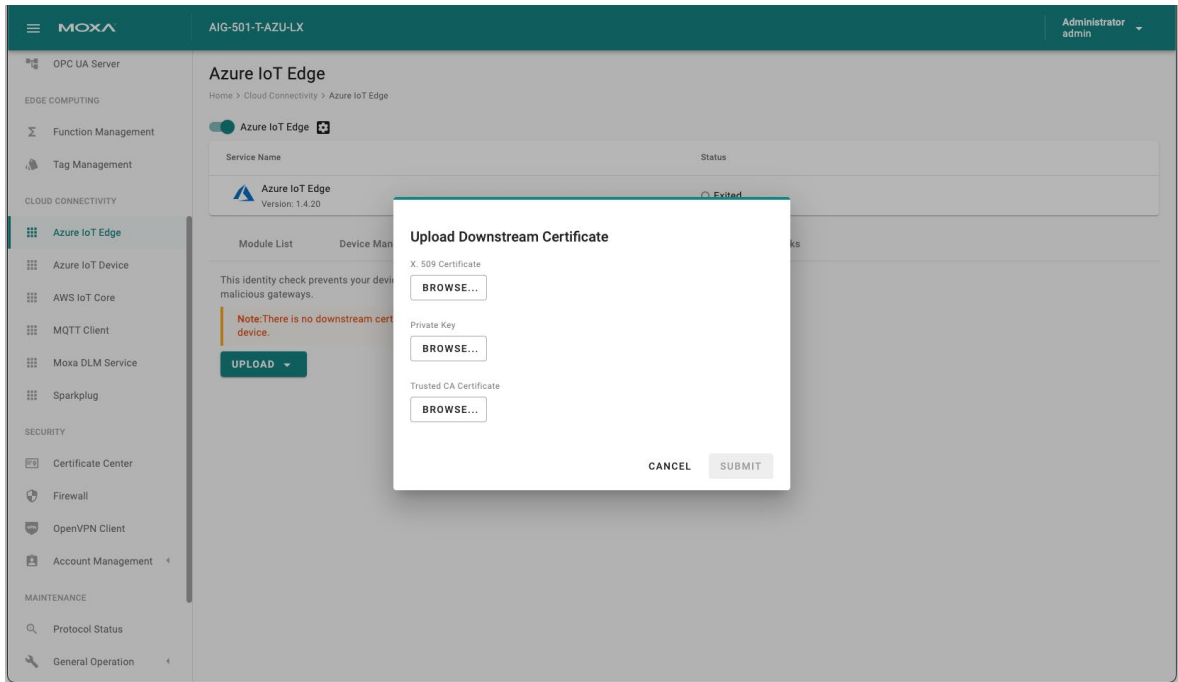


NOTE

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](#).



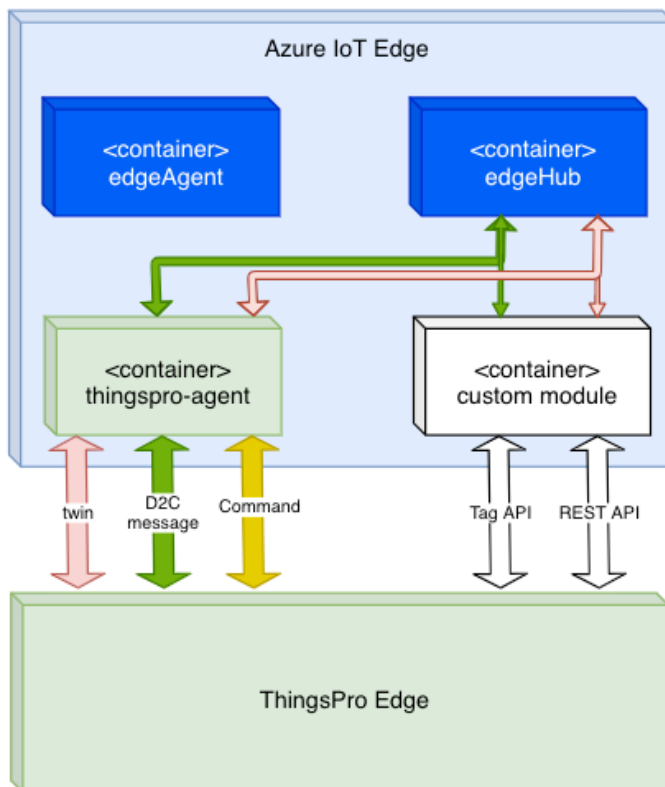


NOTE

Downstream certificate (Edge CA certificate) will be generated if there is no specific certificate assigned after Azure IoT Edge provisioned. This self-signed certificate is meant for development and testing scenarios, not production. For details, see <https://learn.microsoft.com/en-us/azure/iot-edge/how-to-manage-device-certificates?view=iotedge-1.4&tabs=ubuntu#quickstart-edge-ca>.

ThingsPro Agent

ThingsPro Agent is a module that runs on the Azure IoT Edge to enable the Azure Cloud services including **Telemetry Message, Module Twin and Direct Method**. The role of the ThingsPro Agent is shown in the diagram here.



To install the ThingsPro Agent, do the following:

1. [Create an IoT Edge device.](#)
2. Add a module from the Azure IoT Hub
 - a. Docker image:

```
moxa2019/thingspro-agent:2.2.4-amd64
```

- b. Container Create Option:

```
{
  "HostConfig": {
    "Binds": [
      "/var/thingspro/data/azureiotedge:/var/thingspro/cloud/setting/",
      "/run/tpe/azureiotedge:/run/tpe/azureiotedge/",
      "/var/thingspro/data:/var/thingspro/data/"
    ]
  }
}
```

- Module Twin

ThingsPro Agent exposes up-to-date configuration of connected devices via **Reported Properties** and allows you to re-configure devices and turn on/off services via **Desired Properties**.

- Direct Method

ThingsPro Agent offers the following seven direct methods that can be invoked when the gateway is online.

No	Method Name	Description
1	thingspro-api-v1	Universal direct method that invokes all Restful APIs of AIG-501
2	system-reboot	Restarts the gateway
3	thingspro-software-upgrade-check	Check product package is available to upgrade or up-to-date
4	thingspro-software-upgrade	Performs over-the-air (OTA) software upgrades with product package
5	message-policy-get	Retrieves the D2C message policy applied to your gateway
6	message-policy-put	Updates the D2C message policy applied to your gateway

1. Thingspro-api-v1

Method name:

```
Thingspro-api-v1
```

Request Payload: (Example to set HTTP/HTTPS configuration)

```
{
  "path": "/system/httpserver",
  "method": "PATCH",
  "headers": [],
  "requestBody": {
    "httpEnable": true,
    "httpsEnable": true
  }
}
```

Key	Description
path	AIG-501 Restful API endpoint
method	The method associated with the API endpoint
headers	Required by the application/JSON payload
requestBody	Used to post data required by the API endpoint

Response:

```
{
  "status": 200,
  "payload": {
    "data": {
      "httpEnable": true,
      "httpsEnable": true,
      "ipv6Enable": true,
      "httpPort": 80,
      "httpsPort": 8443,
      "certFileName": "ThingsPro Web",
      "keyFileName": "ThingsPro Web"
    }
  }
}
```



NOTE

We recommend changing the following timeout parameters to 30 seconds to prevent system exceptions.

Method name *

Payload

Response timeout Connection timeout

2. system-reboot

Method Name:

`system--reboot`

Request Payload:

`{}`

Response:

```
{
  "status": 200,
  "payload": {
    "data": "rebooting"
  }
}
{
  "status": 200,
  "payload": {
    "data": "rebooting"
  }
}
```

3. thingspro-software-upgrade-check

Method Name:

`thingspro-software-upgrade-check`

Request Payload:

`{}`

Response (available response):

`{`


```
"status": 200,

"payload": {

  "checktime": "2023-04-27T07:51:36Z",

  "count": 1,

  "data": [

    {

      "name": "moxa-aig-501-tpe",

      "size": 31076,

      "currentVersion": "0.11.1",

      "newVersion": "0.12.0+1533",

      "category": "software"

    }

  ]

}

}

Response (up-to-date, unavailable response):

{

  "status": 200,

  "payload": {

    "checktime": "2023-04-27T08:08:38Z",

    "count": 0,

    "data": []

  }

}
```



NOTE

- AIG allows only one active software upgrade job at a time.
- We recommend changing the following timeout parameters to 1 minute to prevent system exceptions.

4. Thingspro-software-upgrade

Method Name:

```
thingspro-software-upgrade
```

Request Payload:

```
{  
  Response:  
  {  
    "status": 200,  
    "payload": {  
      "data": [  
        "moxa-aig-501-tpe"  
      ],  
      "message": "Successfully trigger"  
    }  
  }  
}
```



NOTE

- AIG allows only one active software upgrade job at a time.
- We recommend changing the following timeout parameters to 1 minute to prevent system exceptions.

The screenshot shows a REST client interface with the following fields and values:

- Method name:** thingspro-software-upgrade
- Payload:** {}
- Response timeout:** 1 minute
- Connection timeout:** Module must already be connected
- Invoke method:** A blue button.
- Result:** A JSON response: { "status": 200, "payload": { "data": ["moxa-aig-502-tpe"], "message": "Successfully trigger" } }

5. message-policy-get

Method Name:

```
message-policy-get
```

Request Payload:

```
{}
```

Response:

```
{
  "status": 200,
  "payload": {
    "data": {
      "groups": [
        {
          "id": 1,
          "description": "",
          "enable": true,
          "outputTopic": "sample",
          "format": "{ (.tagName): .dataValue, ts: .ts}"
          "properties": [ { "key": "messageType", "value":
"deviceMonitor" } ],
          "tags": {"system": {"status": ["memoryUsage"]}},
          "sendOutThreshold": {
            "mode": "immediately",
            "size": 4096,
            "time": 0,
            "sizeIdleTimer": {
              "enable": true,
              "time": 60
            }
          },
          "minPublishInterval": 1,
          "samplingMode": "allValues",
          "customSamplingRate": false,
          "pollingInterval": 0,
        }
      ]
    }
  }
}
```

```
}  
}  
}
```

Key	Description
groups	Type: array Description: The message group; you can define multiple messages by demand.
id	Type: integer Description: The message ID.
description	Type: string Description: The message description.
enable	Type: boolean Description: Enable or disable this message policy.
outputTopic	Type: string Description: The output topic required by Azure IoT Edge; helps manage the message route in Azure IoT Edge.
format	Type: string Description: A jq script to transform a default payload to a custom payload.
properties	Type: string Description: Application properties of the message. This allows cloud applications to access certain messages without deserializing the JSON payload.
tags	Type: string Description: The tag data to send in the message. You can retrieve all available tags defined by ThingsPro Edge RESTful API.

Key	Description
sendOutThreshold	<p>Type: object</p> <p>Define conditions to send out messages to Azure Edge Hub based on:</p> <ul style="list-style-type: none"> mode Type: string Enum: byTime, bySize immediately size (mode: bySize) Type: integer Unit: bytes time (mode: byTime) Type: integer Unit: second value 0 almost real time sizeIdleTimer (mode: bySize, optional): Description: A fixed publish time between the two bySize mode publish. Type: object enable Type: boolean time Type: integer Unit: second
minPublishInterval	<p>Type: integer</p> <p>Unit: second</p> <p>Description: A fixed interval between the two immediately mode publish</p>
samplingMode	<p>Type: string</p> <p>Enum: allValues, latestValues, allChangedValues, latestChangedValues</p>
customSampling	<p>Type: boolean</p> <p>Description: Enable will use the pollingInterval that user input.</p>
pollingInterval	<p>Type: integer</p> <p>Description: The interval at which to poll tag data. For example,</p> <ul style="list-style-type: none"> value 10 : Every 10 second value 0 : when the data is pushed into the tag (almost real time)

6. message-policy-put

Method Name:

```
message-policy-put
```

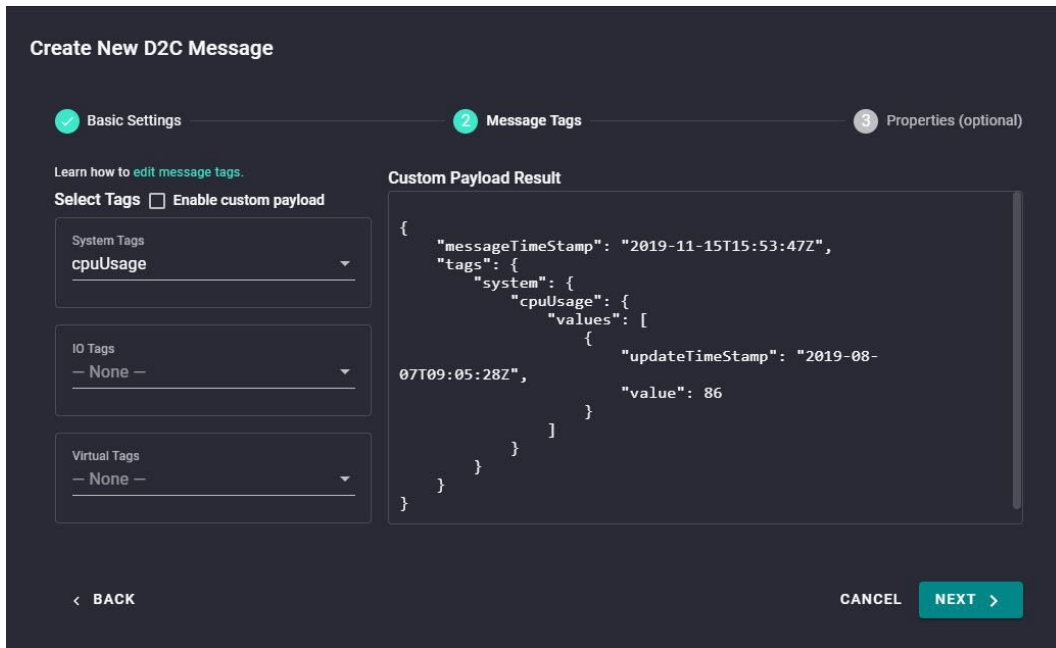
Request Payload:

```
{
  "groups": [
    {
      "id": 1,
      "description": "",
      "enable": true,
      "outputTopic": "sample",
      "format": "{ (.tagName): .dataValue, ts: .ts}"
      "properties": [ { "key": "messageType", "value": "deviceMonitor" }],
      "tags": {"system": {"status": ["memoryUsage"]}},
      "sendOutThreshold": {
        "mode": "bySize",
        "size": 4096,
        "time": 0,
        "sizeIdleTimer": {
          "enable": true,
          "time": 60
        }
      },
      "minPublishInterval": 0,
      "samplingMode": "allValues",
      "customSamplingRate": false,
      "pollingInterval": 0,
    }
  ]
}
```

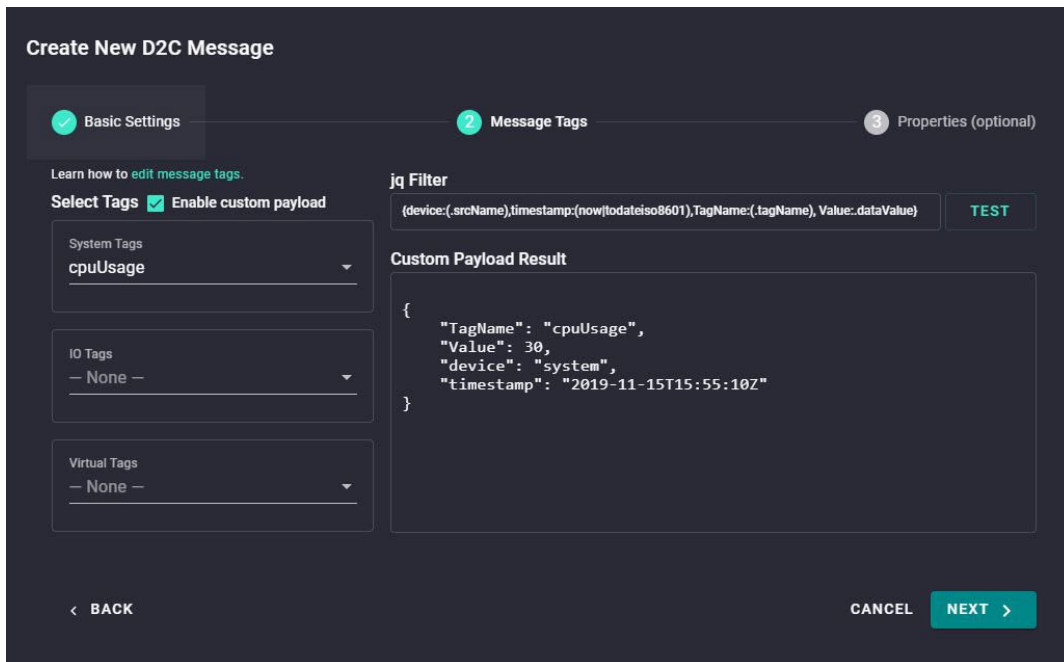
The D2C message policy allows you to transform a default payload to your desired payload schema via a jq filter. For additional details, visit the jq website ([jq Manual \(development version\)](#)). The AIG Web GUI offers an easy way to apply the jq filter and test the transformed result as shown in the following examples.

- Default D2C message schema

Select the tags that you want using the tag-selector panel on the left. The default result for the selected tags will show in the right panel.



- Custom payload after transforming the default payload
Enable custom payload and input the jq Filter to display the custom payload for your selection.



Variable	Description
.srcName	Prints the source of the tag data
.tagName	Prints the tag name
.dataValue	Prints the tag value
.ts	Prints the timestamp of tag value be collected
.dataUnit	Prints data unit of tag value (e.g.: %)
.dataType	Prints data type of tag value (e.g.: int64)

To use the above variables as the key of a JSON element, use parentheses as shown here.

```
(.tagName): .dataValue
```

Example:

```
{device:(.srcName),timestamp:(now|todayiso8601),(.tagName):.dataValue}
```

```
Custom Payload Result
{
  "cpuUsage": 52,
  "device": "system",
  "memoryUsage": 40,
  "networkUsage": 67,
  "timestamp": "2019-11-20T01:10:29Z"
}
```


When the jq Filter has been confirmed, you can include the "format" key into the D2C message policy to enable a custom payload.

```
{
  "groups": [
    {
      "enable": true,
      "outputTopic": "sample",
      "format": "",
      "properties": [
        { "key": "messageType", "value": "deviceMonitor" }
      ],
      "tags": {
        "system": {
          "status": ["cpuUsage", "memoryUsage"]
        }
      },
      "pollingInterval": 2,
      "sendOutThreshold": { "size": 4096, "time": 5 },
      "format":
      "{device:(.srcName),timestamp:(now|todateiso8601),TagName:(.tagName),
      Value:.dataValue}"
    }
  ]
}
```

Azure IoT Device


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



NOTE

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

Telemetry Message

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

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

For details, see Publish Mode.

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

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

The screenshot shows the 'Create New Telemetry Message' dialog in its second step, 'Message Tags'. The progress bar now shows '1 Basic Settings' as completed and '2 Message Tags' as active. The 'Select Tags' section has an info box: 'Info: Select one or more tag providers and select tags to map data.' Below this, a 'Providers' dropdown menu is set to 'IO'. A search modal is open, showing a list of tags: '[IO] DI', 'DI-01', 'DI-02', and 'DI-03'. The first three are checked. The modal has 'SELECT ALL' and 'CLEAR' buttons. At the bottom of the modal, it says 'Total: 8, Selected: 4' and has a 'DONE' button. The 'Default Payload' section has a text area containing 'null' and an unchecked checkbox for 'Enable Custom Payload'. At the bottom right, there are 'CANCEL' and 'NEXT >' buttons.

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/>).

1. 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.

1. Basic Settings

2. Message Tags

3. Properties Optional

Property Key

Property Value

+ Add another

< BACK

CANCEL

SAVE

10. Click **SAVE**.

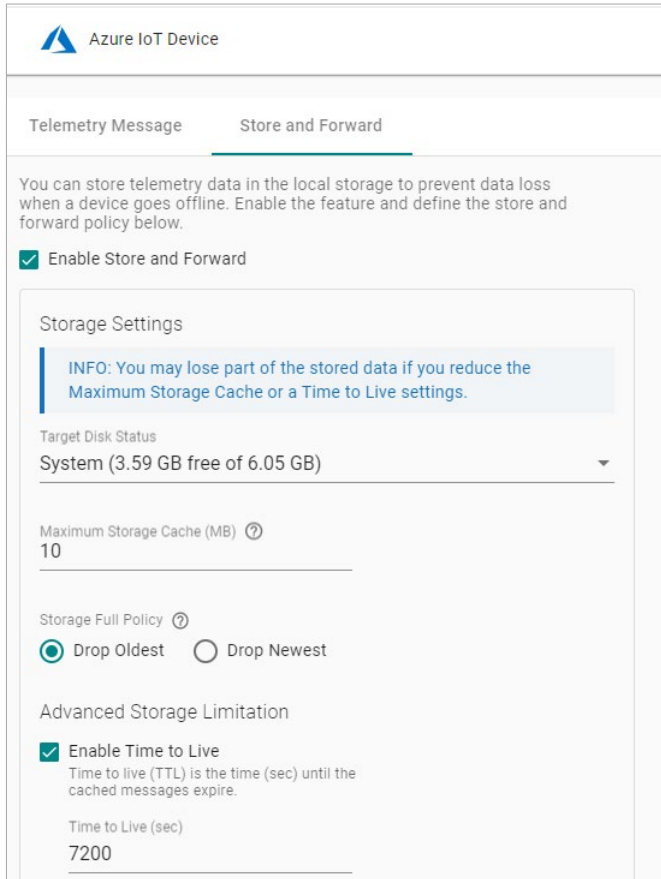


NOTE

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. At the top, there are two tabs: 'Telemetry Message' and 'Store and Forward', with the latter being active. Below the tabs, a brief explanation states: '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. Under 'Storage Settings', there is an informational message: 'INFO: You may lose part of the stored data if you reduce the Maximum Storage Cache or a Time to Live settings.' Below this, the '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' is set to 'Drop Oldest'. Under 'Advanced Storage Limitation', the 'Enable Time to Live' checkbox is checked, and 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.




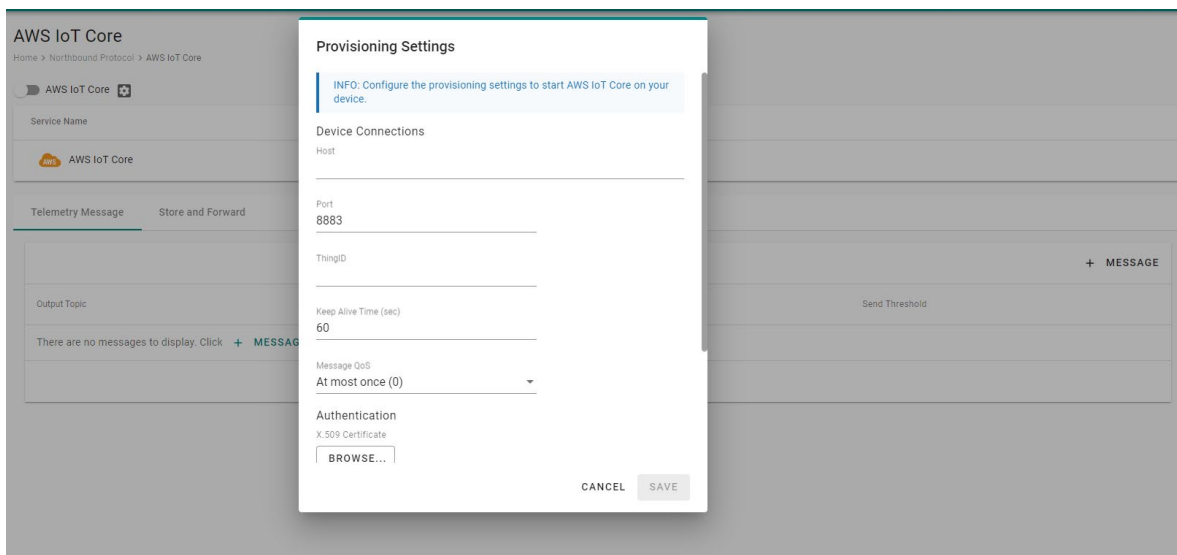
NOTE

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' form at the 'Basic Setting' step. The progress bar indicates '1 Basic Setting' is active and '2 Message Tags' is completed. The form includes the following fields and options:

- Enable Telemetry Message**
- Output Topic: 123
- Publish Mode: By Interval, Immediately, By Size
- Publish Interval (sec): 60
- Sampling Mode: All Changed Values
- Custom sampling rate from acquired data

Buttons at the bottom right: CANCEL, NEXT >

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

The screenshot shows the 'Create New Telemetry Message' form at the 'Message Tags' step. The progress bar indicates '1 Basic Setting' is completed and '2 Message Tags' is active. The form includes the following fields and options:

- Select Tags: Info: Select one or more tag providers to get their tags and select tags to map data.
- Providers: IO
- Default Payload: null
- Enable custom payload

A modal window is open for selecting tags from the 'IO' provider:

- Search: [Empty]
- SELECT ALL CLEAR
- [IO] DI
- DI-01
- DI-02
- DI-03
- ... (more items)
- Total: 8, Selected: 4
- DONE

Buttons at the bottom right: CANCEL, SAVE

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 8 Tags

DI-01 (+3 others)

Default Payload

Enable custom payload

```
{
  "tags": {
    "IO": {
      "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**, and you can add many connections to MQTT Broker.



NOTE

You need to first create a connection 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 active. Under the "SSL/TLS" heading, there is a checked checkbox for "Enable SSL/TLS". Below this, there is a "TLS Version" section with three radio buttons: "1.2" (selected), "1.1", and "1.0". There are three "BROWSE..." buttons for "Client Certificate - optional", "Client Key - optional", and "Trusted Root CA - optional". At the bottom, there is an unchecked checkbox for "Ignore Server Certificate". "CANCEL" and "SAVE" buttons are at the bottom right.

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" (active) and "Message Tags". Under "Basic Setting", there is a checked checkbox for "Enable Telemetry Message". The "Output Topic" field contains "123". The "Publish Mode" section has three radio buttons: "By Interval" (selected), "Immediately", and "By Size". Below this, there is a "Publish Interval (sec)" field with "60" and a "Sampling Mode" dropdown menu set to "All Changed Values". There is an unchecked checkbox for "Custom sampling rate from acquired data". "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).

Create New Telemetry Message

Basic Setting 2 Message Tags

Select Tags Enable custom payload

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

Providers: IO

Search

SELECT ALL CLEAR

- [IO] DI
- DI-01
- DI-02
- DI-03

Total: 8, Selected: 4 DONE

Default Payload: null CANCEL SAVE

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

Create New Telemetry Message

Basic Setting 2 Message Tags

Select Tags Enable custom payload

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

Providers: IO

Selected Tags: 8 Tags

DI-01 (+3 others)

Default Payload:

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

```

< BACK CANCEL SAVE

8. Click **SAVE**.

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

Store and Forward

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

The screenshot shows the 'Store and Forward' configuration page. On the left, there is a sidebar with an 'ADD CONNECTION' button and a list of connections, including 'test.mosquitto.org' which is 'Connected'. The main content area has three tabs: 'Telemetry Message', 'Store and Forward' (which is active), and 'Remote API Invocation'. Below the tabs, there is a description: 'Stores telemetry data in the local storage to prevent data loss when device goes offline. You can enable this feature by defining policies here.' A checkbox labeled 'Enable Store and Forward' is checked. Below this is a 'Storage Setting' section with an info box: 'INFO: You may lose part of stored data stored if you reduce the maximum Disk Size or Time to Live settings.' The 'Target Disk' is set to 'System (3.59GB 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 checked checkbox for 'Enable Time to Live' with a description: 'Time to live (TTL) is the time (sec) until the cache messages expire.' The 'Time to Live (sec)' is set to '7200'. A 'SAVE' button is at the bottom.

Remote API Invocation

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

The screenshot shows the 'Remote API Invocation' configuration page. It has three tabs: 'Telemetry Message', 'Store and Forward', and 'Remote API Invocation' (which is active). Below the tabs, there is a description: '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.' A checkbox labeled 'Enable Invoking of Device Restful APIs from MQTT Server' is checked. Below this are two input fields: 'Input Topic to Subscribe' and 'Output Topic to Subscribe', both with a help icon. A 'SAVE' button is at the bottom.



NOTE

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

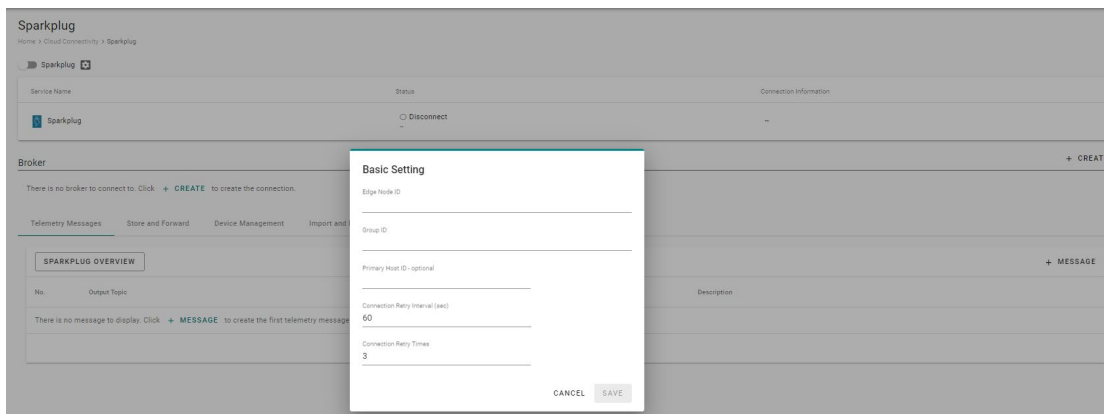
Sparkplug

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:

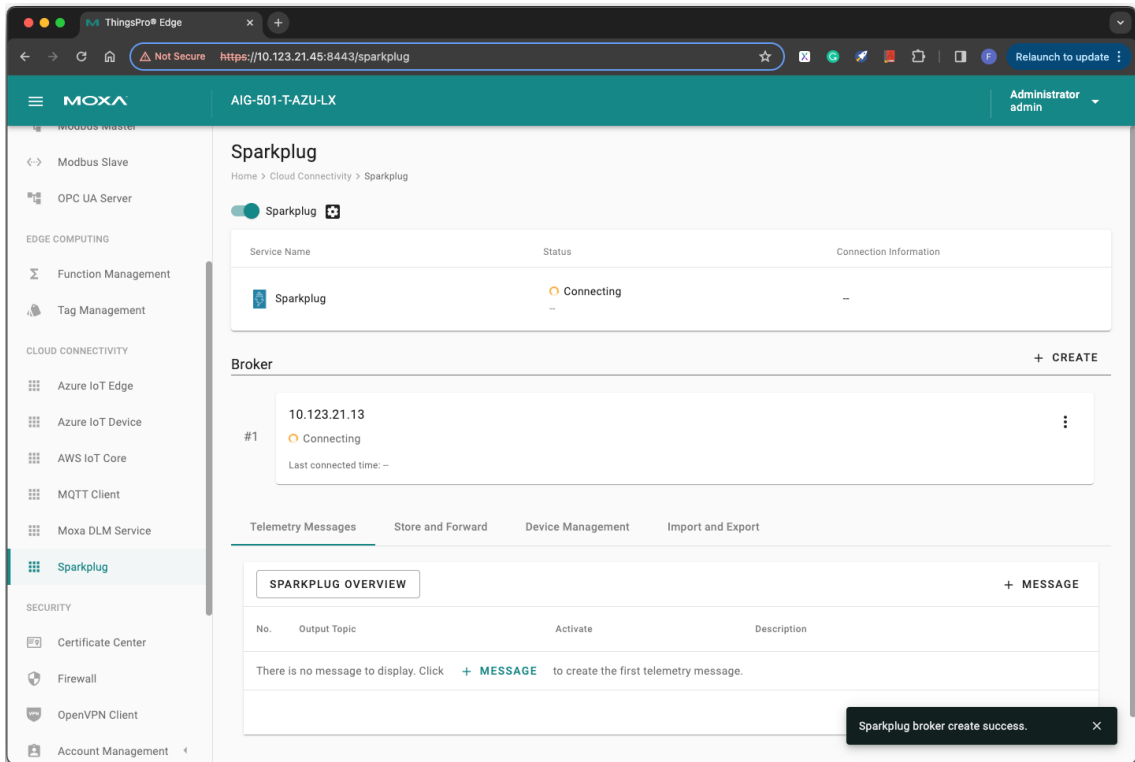
- Enabling Sparkplug
- Configuring a Broker
- Configuring a Telemetry Message

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: 1883).
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 a 'Create New Broker' dialog box with two tabs: 'General' and 'SSL/TLS'. The 'SSL/TLS' tab is active. Under the 'SSL/TLS' heading, there is a checked checkbox for 'Enable SSL/TLS'. Below this, there is a 'TLS Version' section with four radio buttons: 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 of the dialog, there is an unchecked checkbox for 'Ignore server certificate' and two buttons: 'CANCEL' and 'SAVE'.

6. Click **SAVE**.



NOTE

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

Configuring a Telemetry Message

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

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

5. Select a publish mode.
For details, see Publish Mode.
6. Select a sampling mode.
7. Click **NEXT**.

The screenshot shows the 'Create New Telemetry Message' interface at the 'Set Up Transmission Setting' step. The progress bar at the top shows '1 Select Tags' (completed), '2 Set Up Transmission Setting' (active), and '3 Confirm' (pending). Below the progress bar, the 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. The 'Publish Interval (sec)' field contains the value '60'. The 'Sampling Mode' dropdown menu is set to 'All Changed Values'. There is an unchecked checkbox for 'Custom sampling rate from acquired data'. 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

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	<input type="radio"/> 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

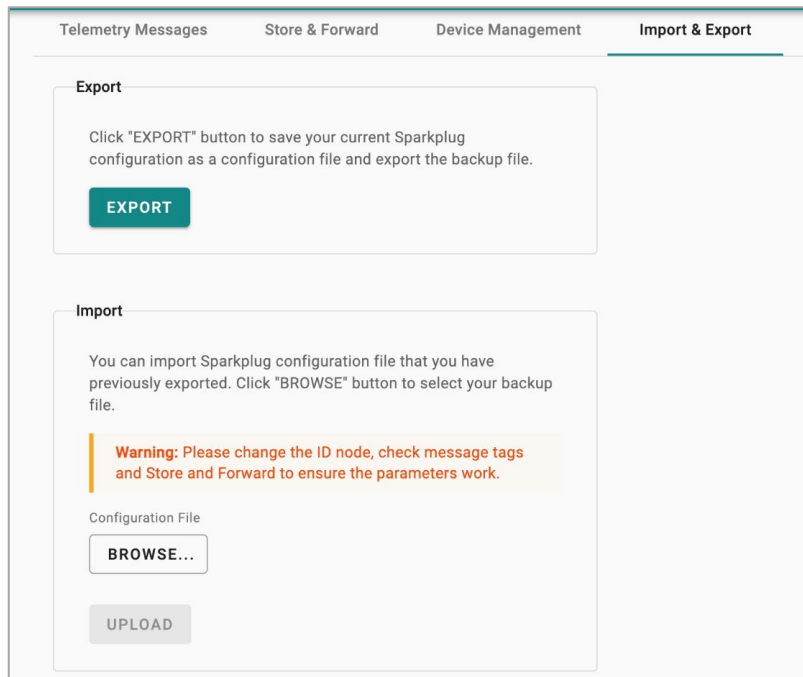


NOTE

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

Import & Export

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



The screenshot shows a web interface with a navigation bar at the top containing four tabs: "Telemetry Messages", "Store & Forward", "Device Management", and "Import & Export". The "Import & Export" tab is active and highlighted. Below the navigation bar, there are two main sections: "Export" and "Import".

Export

Click "EXPORT" button to save your current Sparkplug configuration as a configuration file and export the backup file.

EXPORT

Import

You can import Sparkplug configuration file that you have previously exported. Click "BROWSE" button to select your backup file.

Warning: Please change the ID node, check message tags and Store and Forward to ensure the parameters work.

Configuration File

BROWSE...

UPLOAD



NOTE

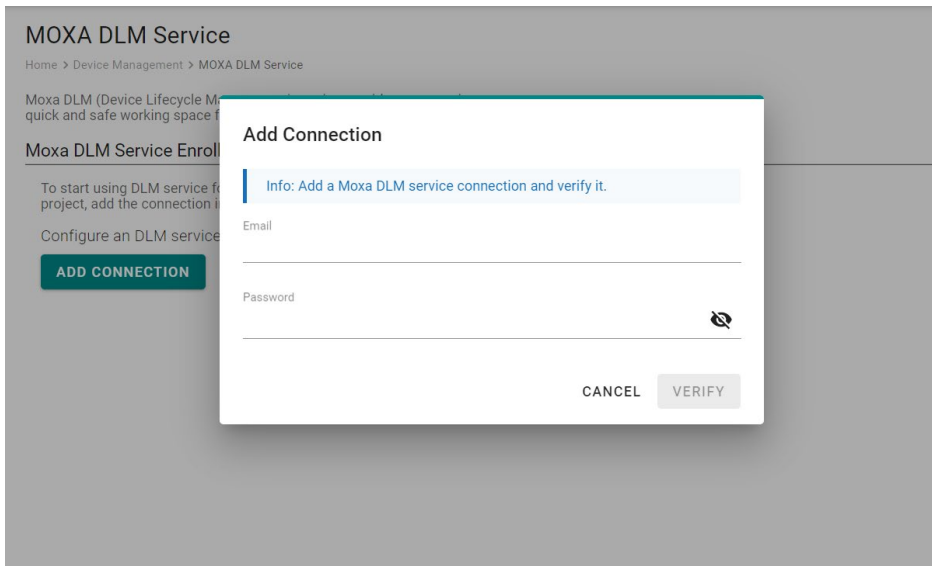
The exported configuration includes credentials, client ID, and policies of D2C messages. You can modify these parameters after the configuration file is imported to other gateways.

Moxa DLM Service

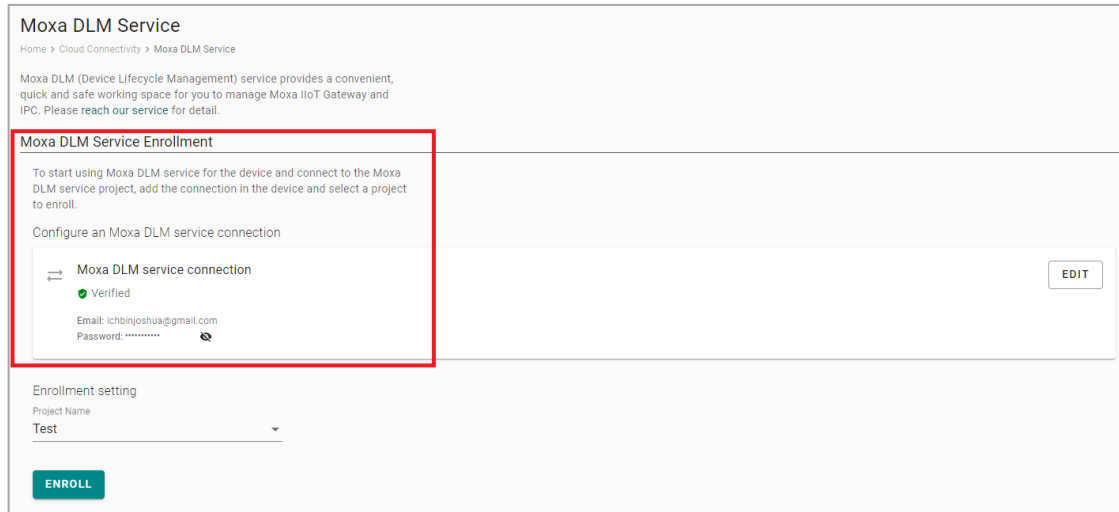
Moxa DLM (device lifecycle management) service is used for managing the AIG devices. Imagine sitting in your office and using this service to remotely manage numerous devices distributed around the world. You can monitor the device's health status, upgrade firmware, import/export configuration, and remotely 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**.



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



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, 12:14:01

Moxa DLM Service Certificate

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

📄 dev.crt

✔ Verified

Issued By: moxa-thingspro-device-intermediate
Expires: Oct 14, 2027 04:14:47
Organization: Moxa Inc.

Model Name: AIG-501-TAP-AZU-LX
MAC Address: 0090E88F9A95
Serial Number: TBZJE1013036

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

Serial Number	Model Name	Host Name	Connection Status	Firmware Version	Labels
<input type="checkbox"/> TBZJE1013036	AIG-501-T-AP-AZU-LX	Moxa	● Online Connected on Oct 14, 2024 12:	1.3	-

Security

Certificate Center

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

The **rootCA.cer** certificate is used to sign the HTTP SSL X.509 certificate, default.crt. You can download this root CA and import it to your client devices to trust the HTTPs connection between clients and AIG.

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

Import rootCA.cer to Google Chrome

Adding the rootCA certificate to prevent an unsafe message shown by Google Chrome during accessing ThingsPro Edge via HTTPS.

- Download the rootCA.cer from **Certificate Center > Trusted Root CA**, and extract the download file (i.e. rootCA.cer).
- Launch Google Chrome. Click **Settings > Privacy and security > Security > Manage certificates**. Normally, a Certificate dialog will be popped up.
- Go to **Trusted Publishers**, and click **Import** button to trigger **Certificate Import Wizard** to import rootCA 2.cer.
- Once the rootCA has been imported, **AIG Series Root CA for HTTPS** will be shown in the Trusted Publishers.

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

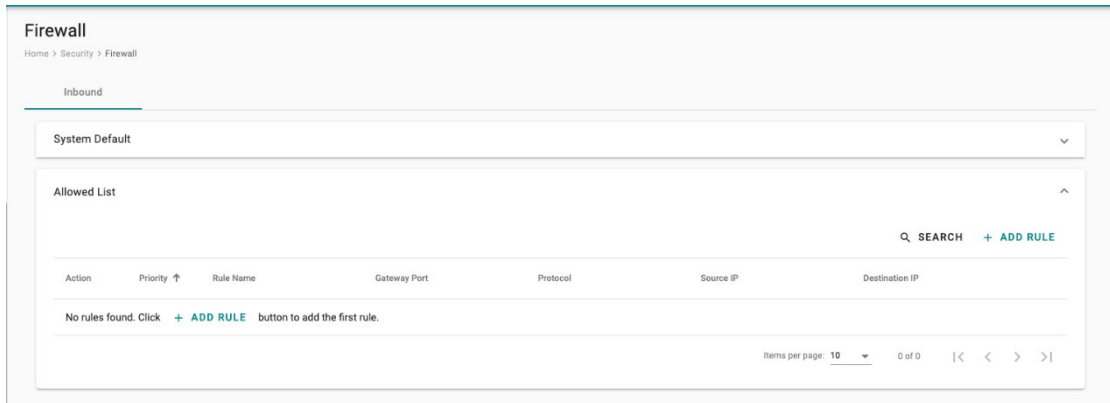
The AIG disables all ports by default excluding the reserved ports mentioned above. To add service ports, add them to the **Allowed List**.

The screenshot shows the 'Firewall' configuration page with the 'Inbound' tab selected. Under 'System Default', there is a table of rules. The table has columns for Action, Priority, Rule Name, Gateway Port, Protocol, Source IP, and Destination IP. The rules listed are: 'default deny all' (Deny, Priority 1), 'https service' (Allow, Priority 1, Gateway Port 8443, Protocol TCP), 'ssh service' (Allow, Priority 1, Gateway Port 22, Protocol TCP), and 'app(opcusever) forward port' (Forward, Priority 5, Gateway Port 4840, Protocol TCP). A search bar and pagination controls are also visible.

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(opcusever) forward port	4840	TCP	Any	172.31.9.7

Allowed List

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



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**.

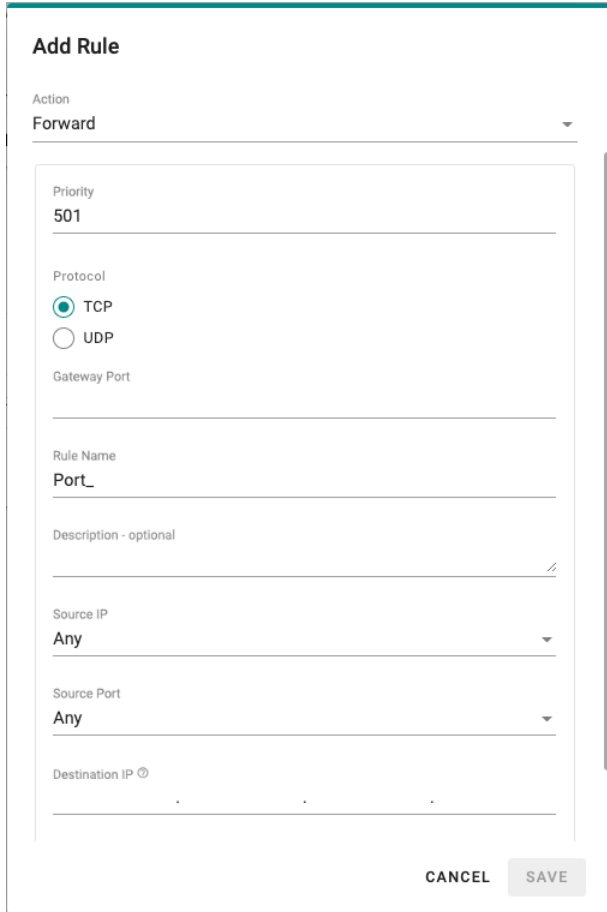
The 'Add Rule' form is shown with the following fields and options:

- Priority:** 1001
- Protocol:** Radio buttons for Any, TCP (selected), UDP, and ICMP.
- Gateway Port:** Empty text field.
- Rule Name:** Port_
- Description - optional:** Empty text area with a slash icon for help.
- Source IP:** Dropdown menu set to Any.
- Source Port:** Dropdown menu set to Any.

At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

Create Forward Rule:

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



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

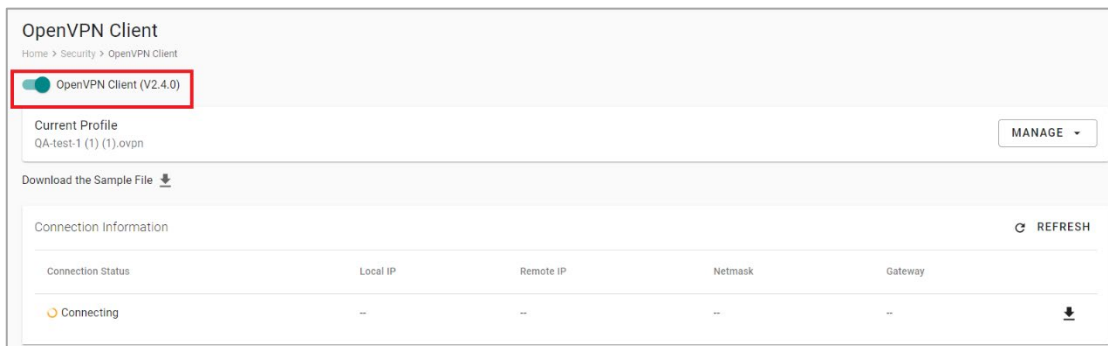
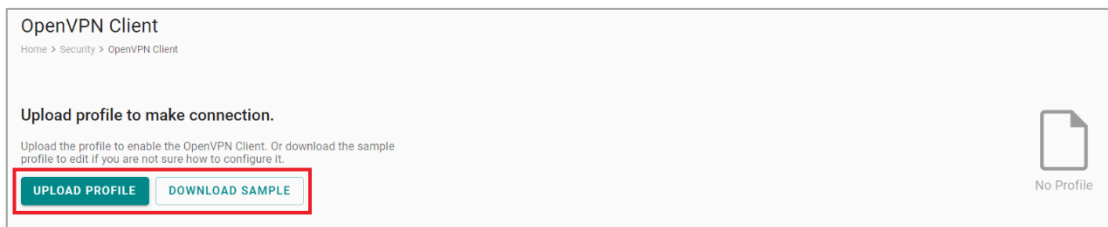
AIG Edge reserves priority 1 to 500 for system default rules. The priority range 501 to 1000 is for **Forward** action rules; while the range 1001 to 1500 is for **Allow** action rules.

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.



NOTE

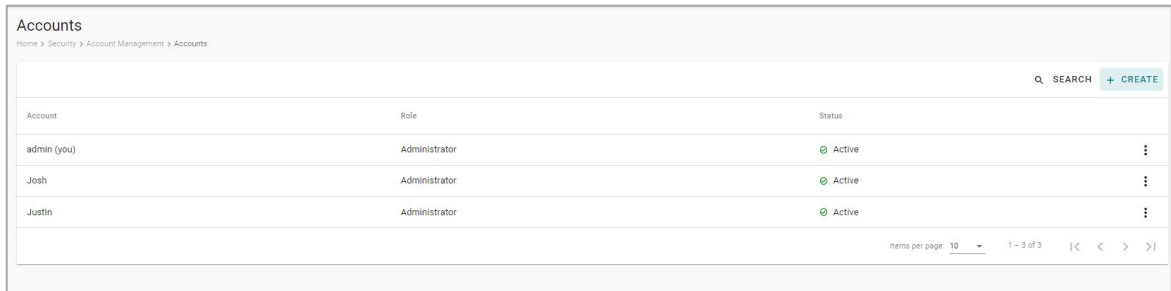
if your AIG is connected to Moxa DLM Service, the OpenVPN Client cannot be used because the Moxa DLM Service requires the OpenVPN Client for communication.

Account Management

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

Accounts

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



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

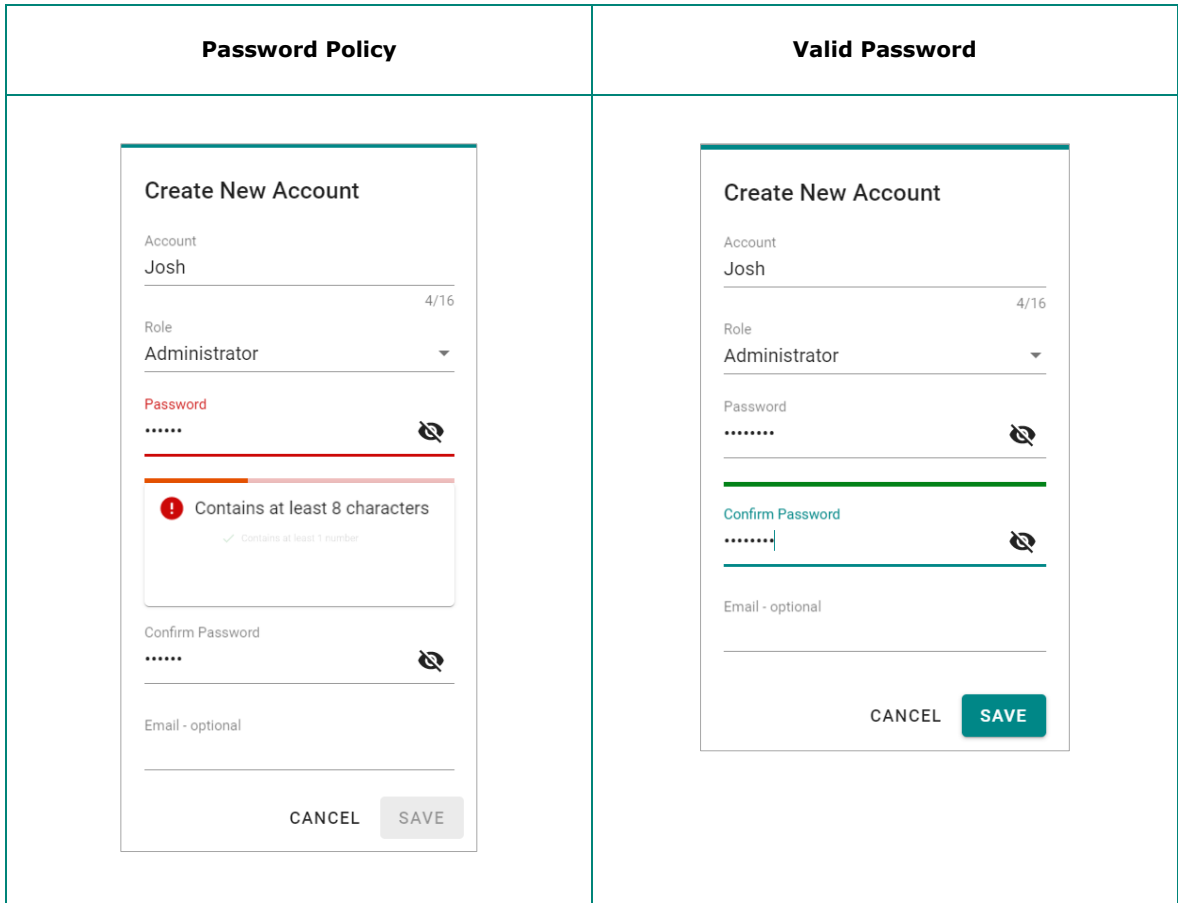
Creating a New User Account

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



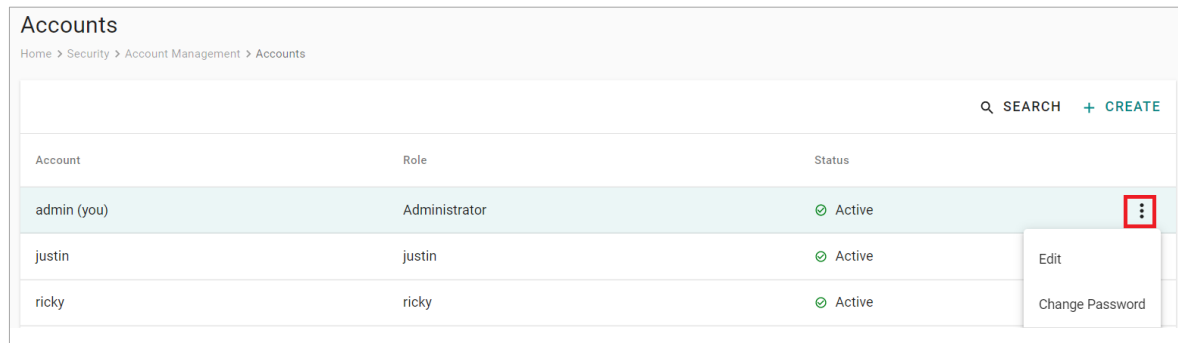
NOTE

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



Managing Existing User Accounts

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



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



NOTE

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

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.

The screenshot displays the 'Roles' management page in the MOXA ThingsPro Edge interface. The page title is 'Roles' and the breadcrumb is 'Home > Security > Account Management > Roles'. The interface includes a search bar and a '+ CREATE' button. The roles listed are:

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

At the bottom right, there is a pagination control showing 'Items per page: 10' and '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 on the button **"SAVE"** to create the role in the system.

Create New Role

Basic Information

Role Name
_____ 0 / 30

Description - optional
_____ 0 / 100

Access Permissions

You must grant at least one privilege to this role.

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

CANCEL **SAVE**

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

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

Maintenance

Protocol Status

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

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

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

1. Click **CHECK**.

The screenshot shows the 'Protocol Status' page. At the top, there is a breadcrumb trail: 'Home > Maintenance > Protocol Status'. Below this, the page is divided into two main sections: 'Northbound Protocols' and 'Southbound Protocols'. Under 'Northbound Protocols', there are five protocol cards: 'Modbus TCP Slave' (OK), 'AWS IoT Core' (Disable), 'Azure IoT Device' (Disable), 'MQTT Client' (Disable), and 'Sparkplug' (Warning). Each card has a 'CHECK' button. Under 'Southbound Protocols', there is one card: 'Modbus Master' (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.)

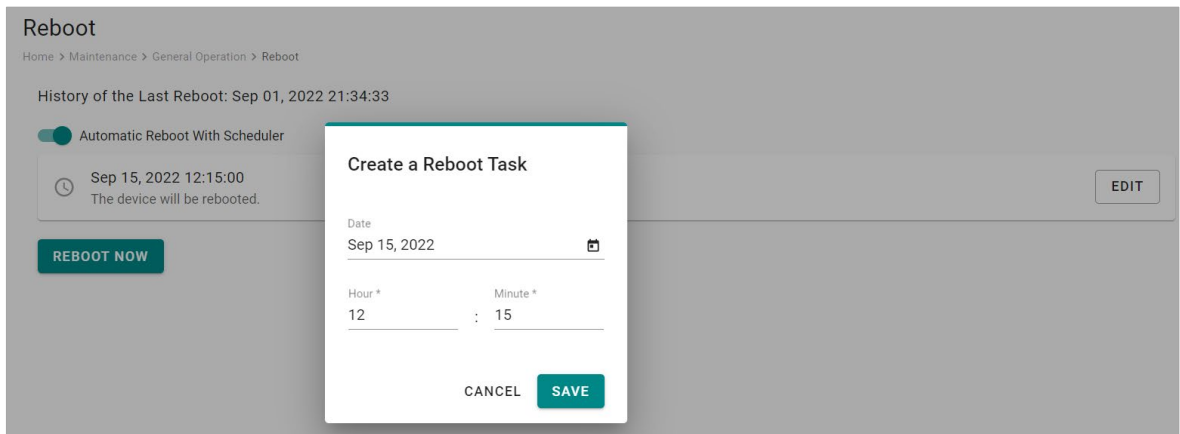
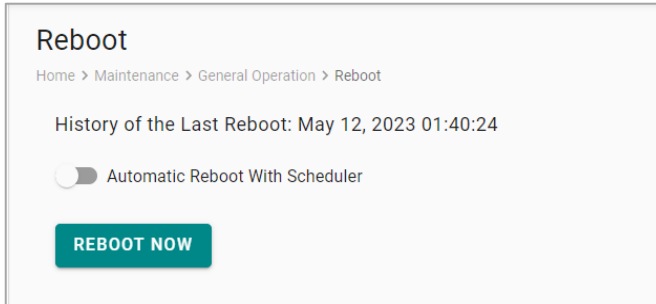
The screenshot shows the 'Azure IoT Device' diagnostic page. At the top, there is a breadcrumb trail: 'Home > Maintenance > Protocol Status > Azure IoT Device'. Below this, there is a description: 'Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to Azure IoT Device'. A table shows the service name, connection status, and last upload status. Below the table, there is an 'Advanced Diagnostic' section with a 'START' button and an 'EXPORT' button.

Service Name	Connection Status	Last Upload Status
Azure IoT Device	Connected Connected on Sep 14, 2022, 11:37:38	Success Upload on Sep 15, 2022, 00:40:48

General Operation

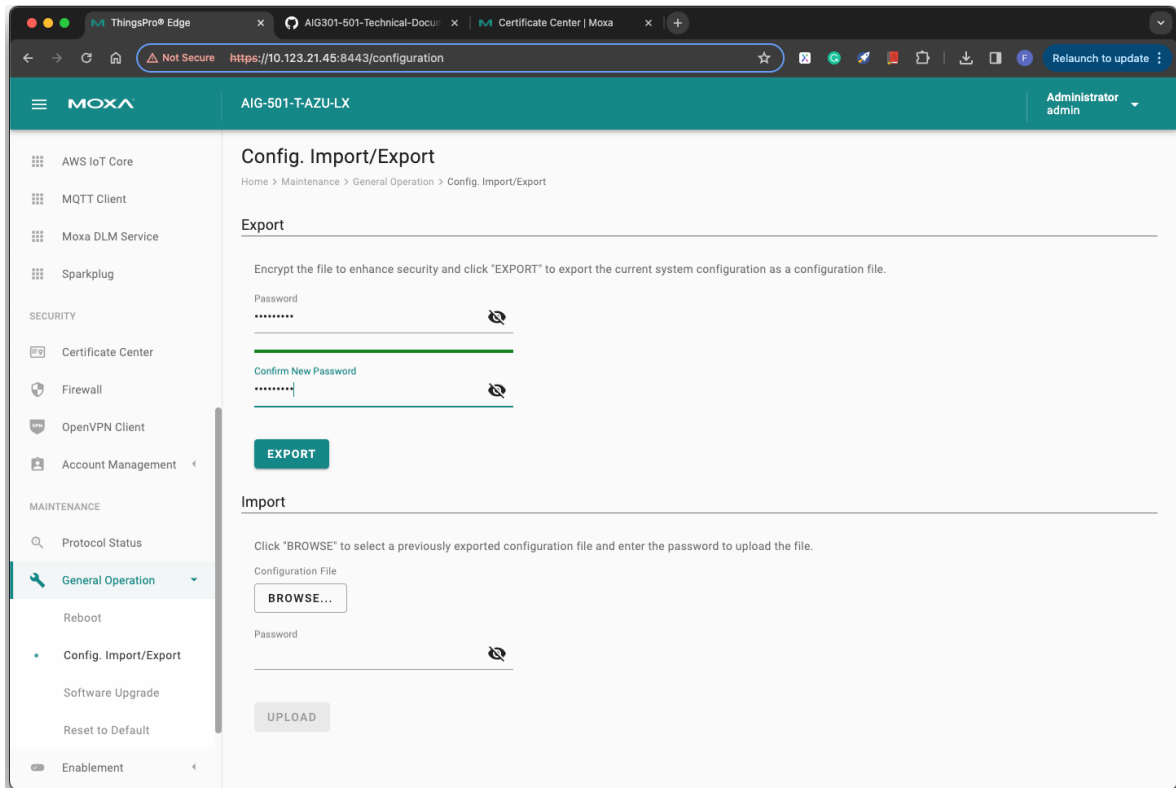
Reboot

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



Config. Import/Export

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



The exported configuration settings include:

Function	Description
Device Configuration	Provision, Syslog, Reboot, Local console, Events, NAT, HTTP/ HTTPS/ SSH, Internet check alive, SD Card, HTTPS certificate & private key, DHCP Server, Firewall, Time (NTP), and Host name.
Interfaces Configuration	Cellular, Wi-Fi, Ethernet, GPS, Route priority, IO, and Serials.
Services Configuration	Tag Service, Function Management, all cloud connectivity excluding Moxa DLM Service and all protocols.

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

The upgrade pack can be downloaded from the Moxa SRS: <https://moxa-srs.thingsprocloud.com/series/S000001843>

Software Upgrade

Home > Maintenance > General Operation > Software Upgrade

Upgrade

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

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

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

Software Upgrade File

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

Software Upgrade

Home > Maintenance > General Operation > Software Upgrade

Upgrade

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

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

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

Upgrade File URL



NOTE

The upgrade process requires incremental updates, such as from version 1.0 to 1.1 to 1.2, or can be automated using the Utility ThingsPro Proxy. For details on ThingsPro Proxy, see <https://cdn-cms.azureedge.net/getmedia/a28fef01-c1e1-4d61-9bd4-c3fdc7c148c3/moxa-thingspro-proxy-manual-v4.1.pdf>.

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 factory default.

Reset to Default

Home > Maintenance > General Operation > Reset to Default

Configuration Reset

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

- > Show storage location of the log files explanation

Reserve Network Settings

RESET

Factory Reset

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

RESET

Enablement

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

System ^

DHCP Server - LAN1 ?	<input type="checkbox"/>
DHCP Server - LAN2	<input type="checkbox"/>
DHCP Server - LAN3	<input type="checkbox"/>
DHCP Server - LAN4	<input type="checkbox"/>
Event Log	<input checked="" type="checkbox"/>
HTTP Service	<input type="checkbox"/>
HTTPS Service	<input checked="" type="checkbox"/>
Internet Check Alive Service ?	<input type="checkbox"/>
Local Console	<input checked="" type="checkbox"/>
Login Policy	<input type="checkbox"/>
NAT Service ?	<input type="checkbox"/>
NTP Service	<input checked="" type="checkbox"/>
SD Card	<input type="checkbox"/>
SSH Server	<input checked="" type="checkbox"/>
System Log	<input checked="" type="checkbox"/>

Network ^


Cellular1	<input checked="" type="checkbox"/>
LAN1	<input checked="" type="checkbox"/>
LAN2	<input checked="" type="checkbox"/>
LAN3	<input checked="" type="checkbox"/>
LAN4	<input checked="" type="checkbox"/>
Wi-Fi1	<input type="checkbox"/>

Diagnostic

System Log

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

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

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

Storage Settings

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

Target Storage
System

Used 2209 MB 3.59GB free of 6.05GB

Limiting Condition
Desired Storage Cache Size (MB) ⓘ
100

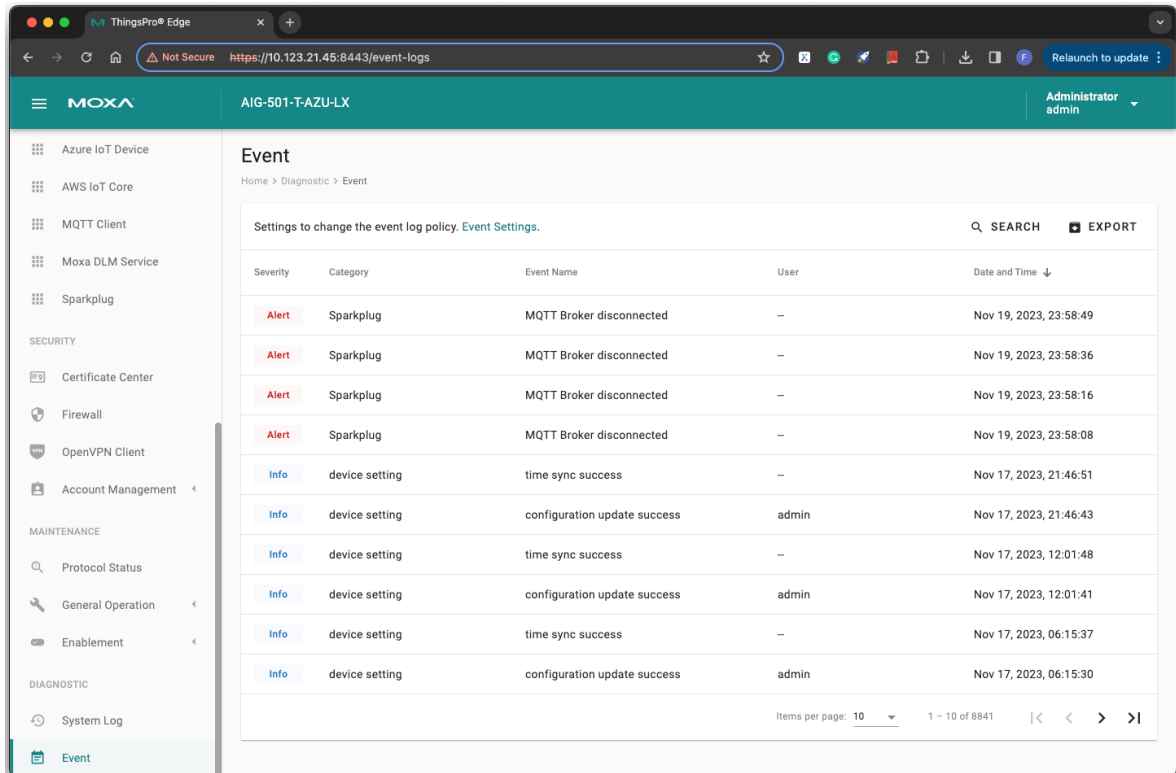
Enable Time to Live

CANCEL SAVE

Events

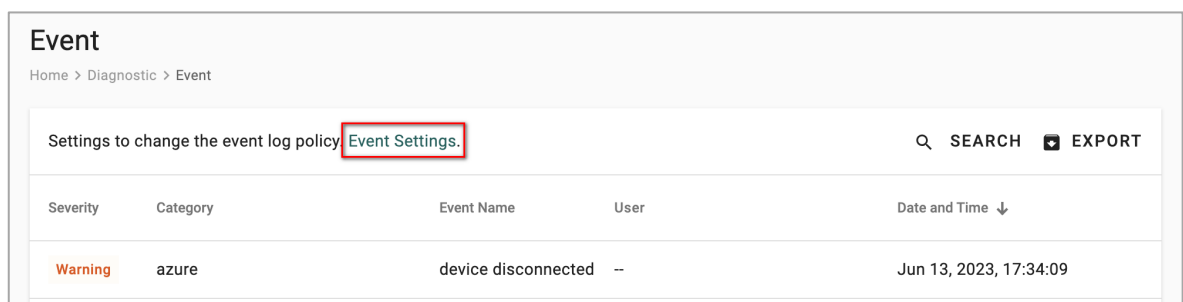
When you face issues, you can go to **Diagnostic > Event** check the event logs which record historical events that help you to narrow down the problems. If there are plenty of event logs, you can export the log to read easily.

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

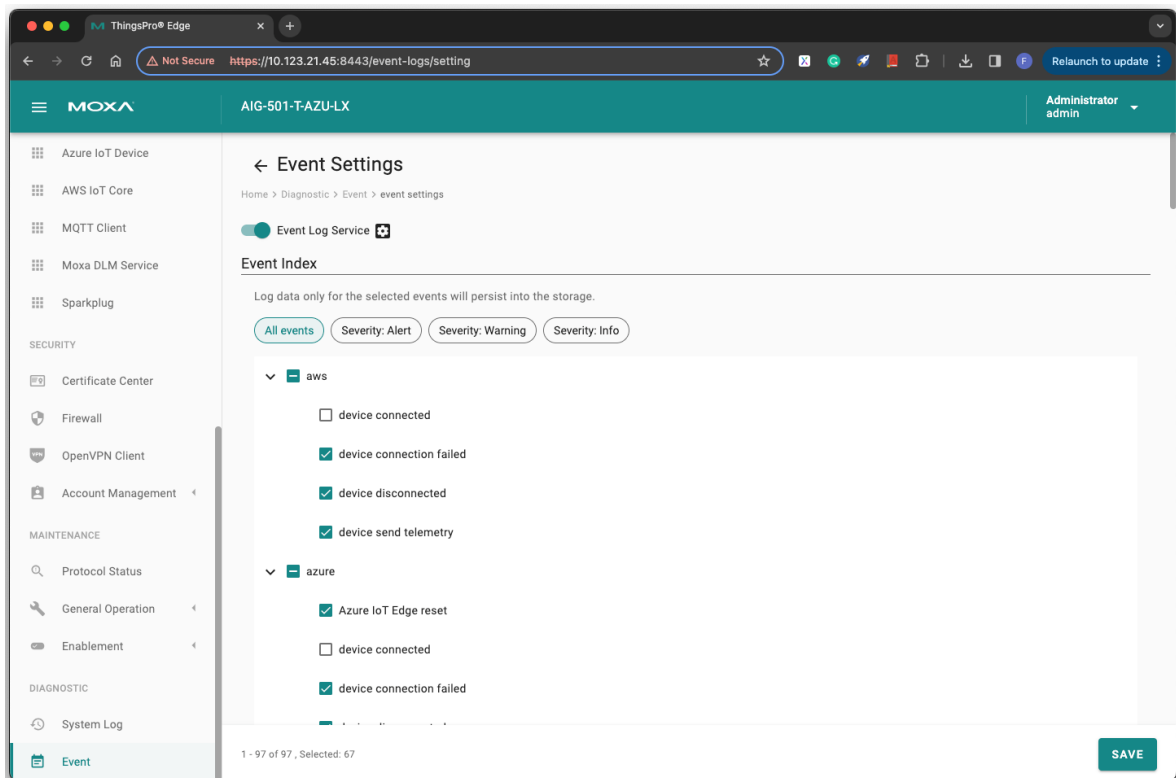



Configuring Event Log Settings

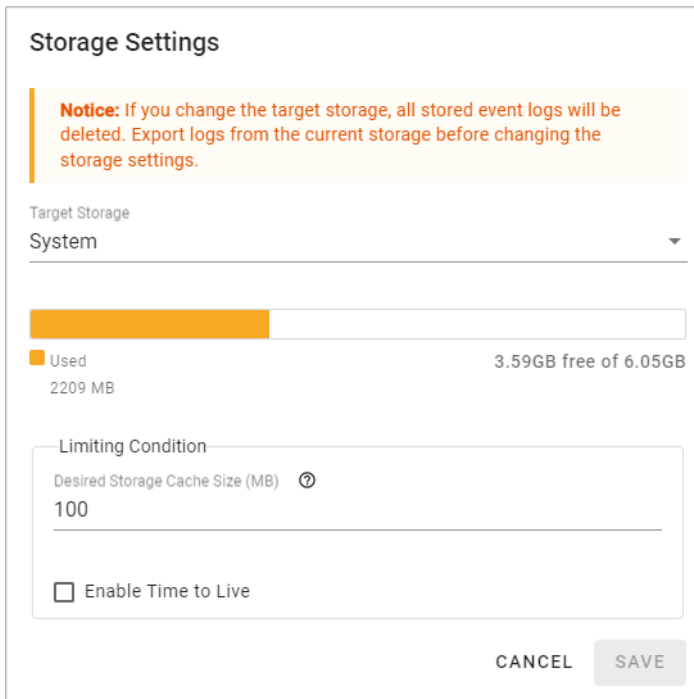
Choose the type of events to be stored, specify where to keep the logs, and the maximum storage size to use. Click the **Event Settings** to access these settings.



You can select the type of events to be stored by clicking on the different levels of 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.



A. Publish Modes

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

Publish Mode	Parameters	Value	Description
	Idle Timer (sec)	0 - 86400	To avoid situations where the data takes a long time to reach the desired size, a threshold value can be set to ensure that the data is sent out as soon as it reaches the specified timer setting.

B. Module Twin Properties

Reported Properties

Properties	Sample
httpserver	<pre>{ "httpserver": { "httpPort": 80, "httpsEnable": true, "httpsPort": 8443, "ipv6Enable": true, "keyFileName": "", "certFileName": "", "httpEnable": true } }</pre>
discovery	<pre>{ "discovery": { "enable": true, "schedule": { "enable": true, "disableAfterSec": 900 } } }</pre>

Properties	Sample
wan	<pre> { "wan": { "displayName": "LAN1", "dns": { "0": "", "arraySize": 1 }, "gateway": "", "ip": "", "name": "eth0", "netmask": "255.255.252.0" } } </pre>
route	<pre> { "route": { "defaultRoute": "LAN1", "priorityList": { "0": "Cellular1", "1": "LAN1", "arraySize": 2 } } } </pre>

Properties	Sample
serials	<pre> { "serials": { "0": { "baudRate": 9600, "dataBits": 8, "device": "/dev/ttyM0", "displayName": "PORT 1", "flowControl": "none", "id": 1, "mode": "rs232", "parity": "none", "stopBits": 1 }, "arraySize": 1 } } </pre>
time	<pre> { "time": { "lastUpdateTime": "2023-05-24T23:22:05+00:00", "ntp": { "enable": false, "interval": 7200, "server": "time.cloudflare.com", "source": "timeserver" }, "timezone": "Asia/Taipei" } } </pre>

Properties	Sample
ethernets	<pre> { "ethernets": { "0": { "enable": true, "enableDhcp": false, "id": 1, "name": "enp0s31f6", "status": "connected", "displayName": "LAN1", "gateway": "192.168.88.88", "ip": "192.168.88.8", "linkSpeed": 1000, "mac": "", "netmask": "255.255.252.0", "wan": true, "dns": { "0": "192.168.200.11", "1": "192.168.200.12", "arraySize": 2 } }, "arraySize": 1 } } </pre>

Properties	Sample
general	<pre> { "general": { "biosVersion": "V1.0.0S01", "firmwareVersion": "1.3.0", "serialNumber": "TBBCE10709X9", "softwareVersion": "0.15.0+2045", "cpu": "Intel(R) Atom(TM) CPU E3845@ 1.91GHz", "description": "", "hostName": "moxa-tbbce1070929", "lastBootTime": "2023-05-24T23:06:57+00:00", "memorySize": 16635346944, "modelName": "AIG-501-T-AP-AZU-LX" } } </pre>
gps	<pre> { "gps":{ "mode": "manual", "interface": "", "location": { "lat": 24.984129, "lng": 121.551753 } } } </pre>

Properties	Sample
SoftwareUpgrade	<pre>{ "softwareUpgrade": { "allowOverCellular": true, "allowUpdate": true, "autoScan": false, "autoScanExpression": "0 0 * * 0", "snapshotBeforeUpdate": true } }</pre>

cellulars	<pre> { "cellulars": { "0": { "operatorName": "", "pinRetryRemain": 3, "profiles": { "0": { "name": "Profile-1", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", "simSlot": 1 }, "1": { "name": "Profile-2", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", </pre>
-----------	---

	<pre> "simSlot": 2 }, "arraySize": 1 }, "currentProfileName": "Profile-1", "imsi": "", "keepalive": { "enable": true, "intervalSec": 60, "targetHost": "8.8.8.8" }, "mac": "", "gateway": "", "id": 1, "name": "wwan0", "profileTimeout": 120, "cellId": "", "displayName": "Cellular1", "dns": { "arraySize": 0 }, "enable": false, "status": "sim_pin_locked", "signalStrength": 0, "capabilities": { "sim": 2 }, "iccId": "", "ip": "", "mode": "unknown", </pre>
--	---

Properties	Sample
	<pre>"imei": "", "lac": "", "netmask": "", "tac": "" }, "arraySize": 1 } }</pre>

cellulars	<pre> { "cellulars": { "0": { "operatorName": "", "pinRetryRemain": 3, "profiles": { "0": { "name": "Profile-1", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", "simSlot": 1 }, "1": { "name": "Profile-2", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", </pre>
-----------	---

	<pre> "simSlot": 2 }, "arraySize": 1 }, "currentProfileName": "Profile-1", "imsi": "", "keepalive": { "enable": true, "intervalSec": 60, "targetHost": "8.8.8.8" }, "mac": "", "gateway": "", "id": 1, "name": "wwan0", "profileTimeout": 120, "cellId": "", "displayName": "Cellular1", "dns": { "arraySize": 0 }, "enable": false, "status": "sim_pin_locked", "signalStrength": 0, "capabilities": { "sim": 2 }, "iccId": "", "ip": "", "mode": "unknown", </pre>
--	---

Properties	Sample
	<pre>"imei": "", "lac": "", "netmask": "", "tac": "" }, "arraySize": 1 } }</pre>

cellulars	<pre> { "cellulars": { "0": { "operatorName": "", "pinRetryRemain": 3, "profiles": { "0": { "name": "Profile-1", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", "simSlot": 1 }, "1": { "name": "Profile-2", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "", </pre>
-----------	---

	<pre> "simSlot": 2 }, "arraySize": 1 }, "currentProfileName": "Profile-1", "imsi": "", "keepalive": { "enable": true, "intervalSec": 60, "targetHost": "8.8.8.8" }, "mac": "", "gateway": "", "id": 1, "name": "wwan0", "profileTimeout": 120, "cellId": "", "displayName": "Cellular1", "dns": { "arraySize": 0 }, "enable": false, "status": "sim_pin_locked", "signalStrength": 0, "capabilities": { "sim": 2 }, "iccId": "", "ip": "", "mode": "unknown", </pre>
--	---

Properties	Sample
	<pre> "imei": "", "lac": "", "netmask": "", "tac": "" }, "arraySize": 1 } } </pre>

Desired Properties

Properties	Sample
httpserver	<pre> { "desired": { "httpserver": { "httpEnable": true, "httpsEnable": true, "httpsPort": 8443 "ipv6Enable": true } } } </pre>

Properties	Sample
discovery	<pre> { "desired": { "discovery": { "enable": true, "schedule": { "enable": true, "disableAfterSec": 900 } } } } </pre>
serials	<pre> { "desired": { "serials": { "0": { "mode": "rs232", "stopBits": 1, "baudRate": 9600, "dataBits": 8, "parity": "none", "flowControl": "none", "id": 1 }, "arraySize": 1 } } } </pre>

Properties	Sample
time	<pre> Update NTP Settings: { "desired": { "time": { "ntp": { "enable": true, "interval": 7200, "server": "time.cloudflare.com", "source": "timeserver" } } } } Update Time zone: { "desired": { "time": { "timezone": "Asia/Taipei" } } } </pre>

Properties	Sample
<p>general</p>	<p>Update gateway host name:</p> <pre>{ "desired": { "general": { "hostName": "MyHost" } } }</pre> <p>Update gateway description:</p> <pre>{ "desired": { "general": { "description": "MyDevice" } } }</pre>
<p>route</p>	<pre>{ "route": { "priorityList": { "0": "Cellular1", "1": "LAN1", } } }</pre>

Properties	Sample
gps	<p>Update GPS latitude and longitude by manual mode:</p> <pre> { "desired": { "gps":{ "mode": "manual", "location": { "lat": 11, "lng": 12 } } } } </pre> <p>Update GPS by auto mode:</p> <pre> { "desired": { "gps":{ "mode": "auto", "interface": "GPS1" } } } </pre>

Properties	Sample
ethernets	<pre> { "ethernets": { "0": { "dns": { "0": "192.168.88.88", "arraySize": 1 }, "enable": true, "enableDhcp": false, "gateway": "192.168.88.8", "id": 1, "ip": "192.168.88.80", "netmask": "255.255.252.0", "wan": true }, "arraySize": 1 } } </pre>

Properties	Sample
SoftwareUpgrade	<pre> { "desired": { "softwareUpgrade": { "allowUpdate": true, "allowOverCellular": false, "snapshotBeforeUpdate": true, "autoScan": false, "autoScanExpression": "0 3 * * 1-5" } } } </pre>

cellulars	<pre> { "cellulars": { "0": { "enable": false, "keepalive": { "enable": false, "intervalSec": 120, "targetHost": "8.8.8.8" }, "profileTimeout": 140, "profiles": { "0": { "name": "SIM1", "pdpContext": { "apn": "internet", "auth": { "password": "", "username": "" }, "type": "ipv4" }, "pinCode": "0000", "simSlot": 1 }, "arraySize": 1 } }, "arraySize": 1 } } </pre>
-----------	---

C. Additional Documentation

Software Downloads

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

Technical Documentation

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

OpenAPI Documentation

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