

AIG-501 Series User Manual

Version 2.1, November 2025

www.moxa.com/products



© 2025 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

© 2025 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction	4
Overview	4
2. Getting Started	5
Connecting the Power	5
Connecting Serial Devices	5
Connecting to a Network	5
Access to the Web Console	6
3. Web Console	7
Dashboard	7
System Dashboard	7
Network Dashboard	8
System Configuration	9
System Settings—General	9
System Settings—IP Address	12
System Settings—Cellular	13
System Settings—HTTP/HTTPS/SSH	15
System Settings—Serial	16
System Settings—I/O	17
System Settings—DHCP Server	18
System Settings—Wi-Fi	19
Protocol	21
Modbus Master	21
OPC UA Server	44
Edge Computing	48
Function Management	48
Tag Management	50
Cloud Connectivity	52
Azure IoT Edge	52
Azure IoT Device	64
AWS IoT Core	68
Generic MQTT Client	72
Sparkplug	76
Moxa DLM Service	82
Sign Up DLM Account	84
Security	85
Certificate Center	85
Import rootCA.cer to Google Chrome	85
Firewall	86
OpenVPN Client	89
Account Management	90
Maintenance	93
Protocol Status	93
General Operation	95
Diagnostic	100
4. Security Hardening Guide	103
A. Publish Modes	106
B. Module Twin Properties	107
C. Additional Documentation	116
Software Downloads	116
Technical Documentation	116
OpenAPI Documentation	116

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 via cloud solutions such as Azure Device Twin. Thanks to the robust OTA function, you never have to worry about system failure during software upgrades. With the Secure Boot function enabled, you can prevent malicious software-injection attacks during the bootup process.

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



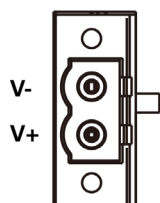
NOTE

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

2. Getting Started

Connecting the Power

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.



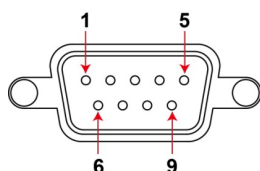
WARNING

- 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

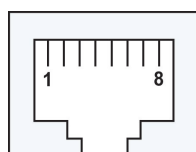
The serial port can be configured by software for RS-232, RS-422, or RS-485. The pin assignments for the port are shown in the following table:



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

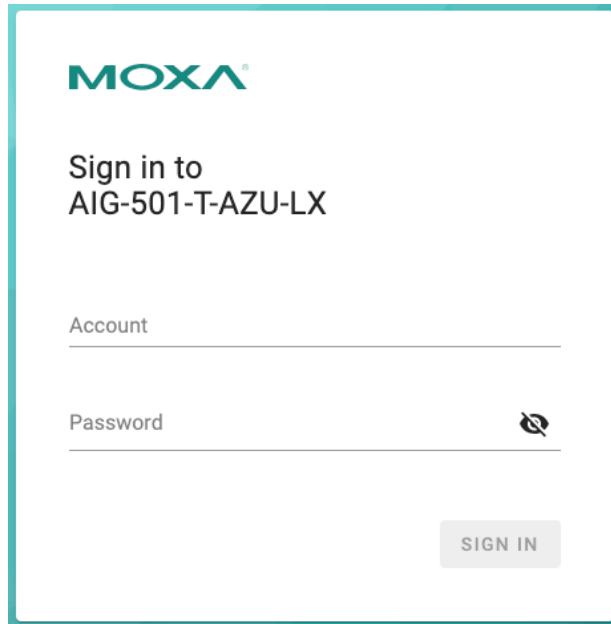
The default LAN2 IP address to access the web console of the AIG is 192.168.4.127.

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**



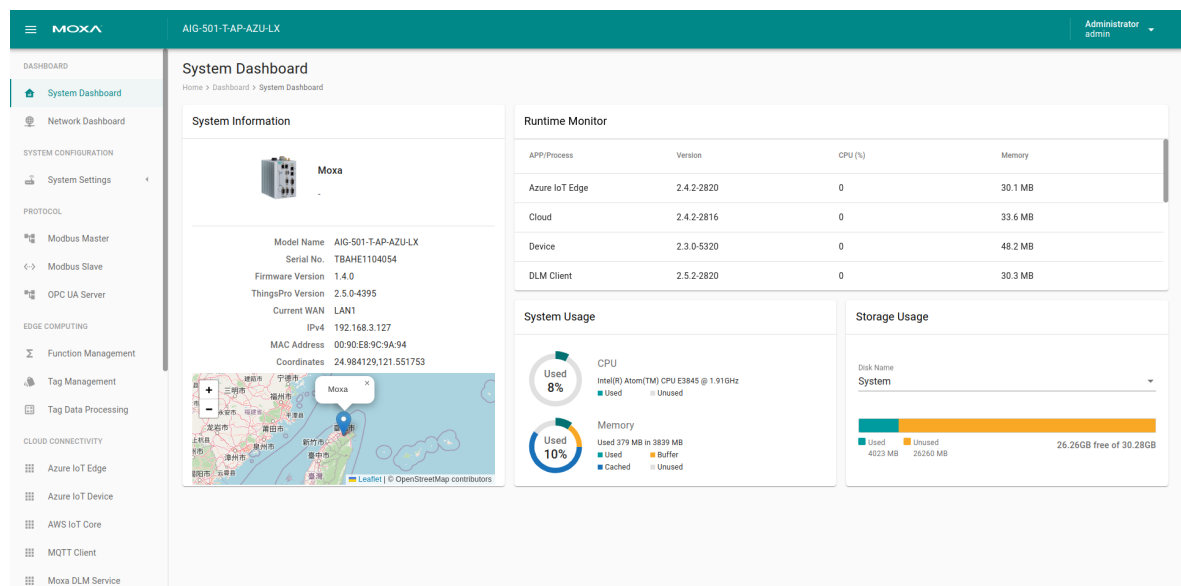
The image shows the login page for the Moxa AIG-501-T-AZU-LX. It features the Moxa logo at the top, followed by the text "Sign in to AIG-501-T-AZU-LX". Below this are two input fields: "Account" and "Password". The "Password" field has a toggle icon for visibility. At the bottom right, there is a "SIGN IN" button.



NOTE

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

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



The screenshot shows the Moxa System Dashboard for the AIG-501-T-AP-AZU-LX. The dashboard includes a sidebar with navigation options like System Dashboard, Network Dashboard, and System Configuration. The main content area displays System Information (Model Name, Serial No., Firmware Version, etc.), Runtime Monitor (APP/Process, Version, CPU %, Memory), System Usage (CPU, Memory), and Storage Usage (Disk Name, System). The System Information section also includes a map showing the device's location.

APP/Process	Version	CPU (%)	Memory
Azure IoT Edge	2.4.2-2820	0	30.1 MB
Cloud	2.4.2-2816	0	33.6 MB
Device	2.3.0-5320	0	48.2 MB
DLM Client	2.5.2-2820	0	30.3 MB

Category	Used	Unused
CPU	8%	92%
Memory	10%	90%

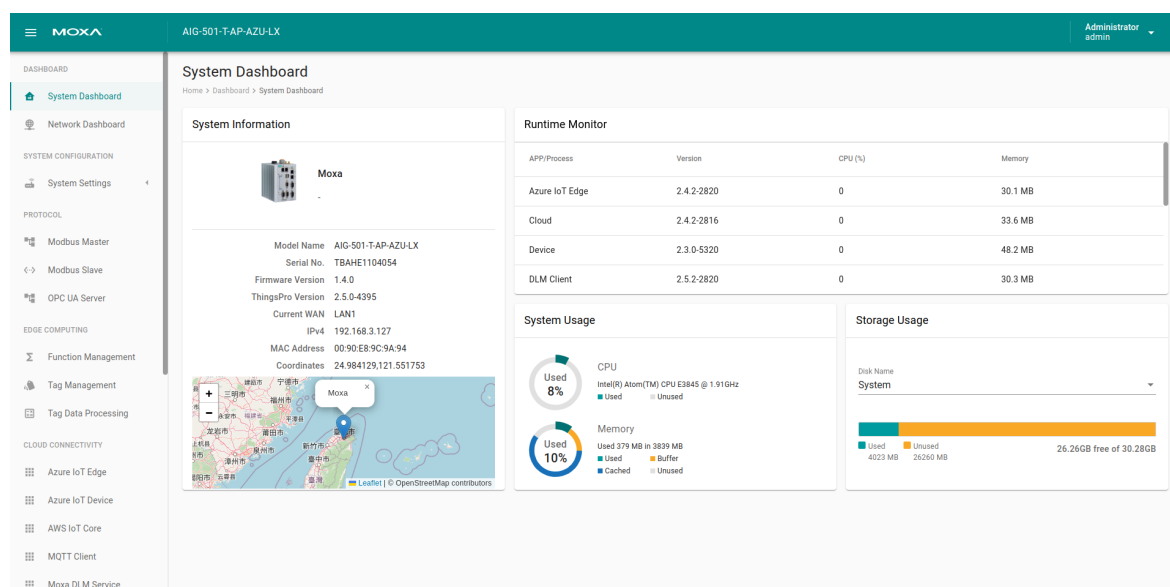
Disk Name	System	Used	Unused
System	4023 MB	26260 MB	26.26GB free of 30.28GB

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.

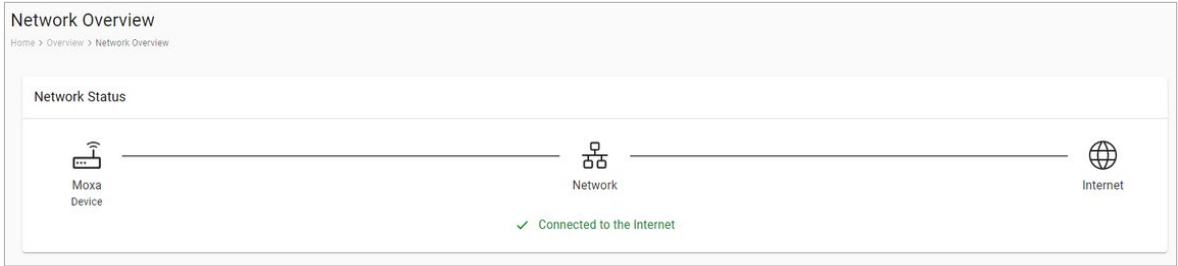


CAUTION

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.

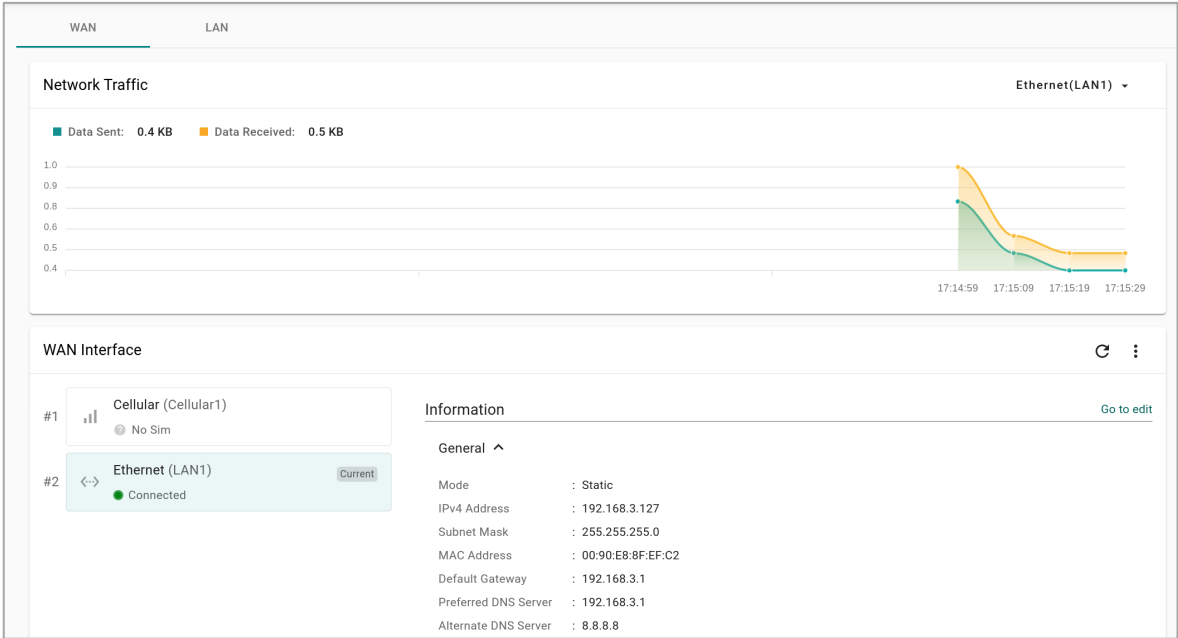
Network Dashboard

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.



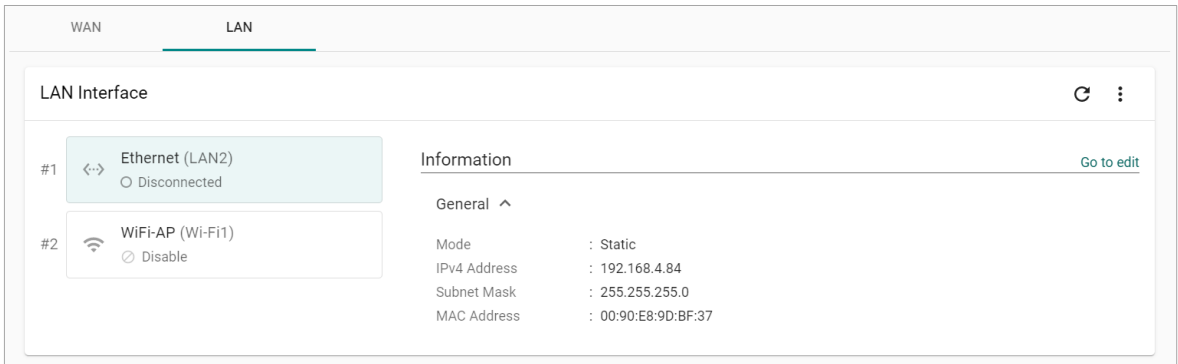
WAN

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.



System Configuration

System Settings—General

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

The screenshot shows the Moxa AIG-501-T-AZU-LX web interface. The header is teal and contains the Moxa logo, the device name 'AIG-501-T-AZU-LX', and the user 'Administrator admin'. The left sidebar is divided into three sections: 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 shows the 'System' tab selected. It contains two text input fields: 'Server/Host Name' with the value 'Moxa' and 'Description - optional' with the value 'Factory A1'. A 'SAVE' button is located at the bottom left of the main content area.

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 CONFIGURATION, and PROTOCOL. Under SYSTEM CONFIGURATION, 'System Settings' is expanded, showing 'General' as the selected option. The main content area is titled 'General' and has tabs for 'System', 'Time', and 'GPS'. The 'Time' tab is active, showing the 'Current date and time: 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' (radio button selected). There is a 'Sync with browser' button and a date picker showing 'Nov 15, 2023'. Below the date, there are input fields for '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:

Input latitude and longitude in **manual**.

check the **Automatically adjust coordinates for GPS changes** option if you want the system to automatically update the device coordinates.

The screenshot shows the Moxa web interface for device configuration. The top header includes the Moxa logo, the device model 'AIG-501-T-AZU-LX', and the user 'Administrator admin'. The left sidebar lists navigation categories: DASHBOARD, SYSTEM CONFIGURATION, and PROTOCOL. Under SYSTEM CONFIGURATION, 'System Settings' is expanded, showing options like General, IP Address, Cellular, HTTP/HTTPS/SSH, Serial, I/O, DHCP Server, and Wi-Fi. The main content area is titled 'General' and shows the 'GPS' tab. It features two radio button options: 'Manually enter coordinates' (selected) and 'Automatically adjust coordinates for GPS changes'. Below these are input fields for 'Latitude' (24.984129) and 'Longitude' (121.551753). A map of Taiwan is shown with a blue location pin labeled 'Moxa' over Taipei. A 'SAVE' button is located at the bottom of the map area.

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**.

The screenshot shows the MOXA web interface for the AIG-501-TAP-AZU-LX device. The 'IP Address' configuration page for LAN2 is active. The 'Static' mode is selected, and the IP address is 192.168.4.127 with a subnet mask of 255.255.252.0. The interface includes a sidebar with navigation options like System Dashboard, Network Dashboard, System Configuration, and Protocol. The top navigation bar shows the device name and the user is logged in as Administrator admin.

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

System Settings—Cellular

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

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

The screenshot shows the Moxa web interface for the AIG-501-TAP-AZU-LX device. The left sidebar contains navigation menus for Dashboard, System Configuration, and Protocol. The main content area is titled 'Cellular' and shows settings for 'CELLULAR1'. It includes a checkbox to 'Enable cellular data communication', a 'Profile Settings' section with 'Network Type' set to 'Auto', 'Connection Retry Timeout (sec)' set to '120', and 'Mode' set to 'Auto'. The 'Check-alive' section has a checkbox to 'Enable check-alive' and a checkbox to 'Reboots the device when pings to the target host fail continuously for a specified time interval'. The 'Check-alive' section also displays 'Target Host' as '8.8.8.8' and 'Ping Interval (sec)' as '60'. A 'SAVE' button is located at the bottom right of the settings area.

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.

Create New Profile

Profile Name

SIM
SIM1

Pin Code - optional

APN Type
Static

APN
internet

CANCEL DONE

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

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

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

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

☒ Enable check-alive

Target Host
8.8.8.8

Ping Interval (sec)
60

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

Reboot Timer (min)
20

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

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



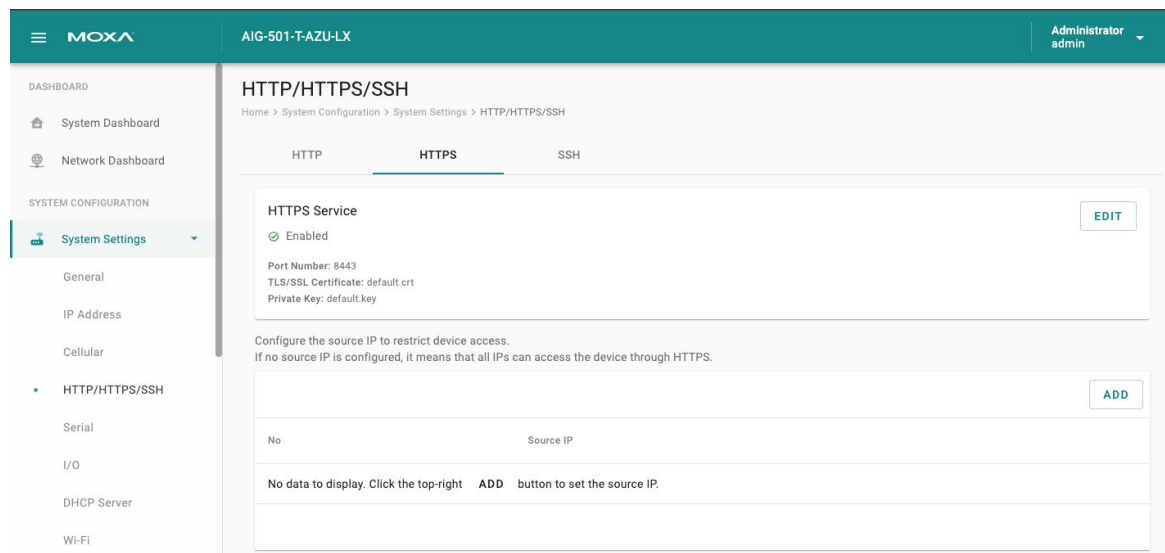
NOTE

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

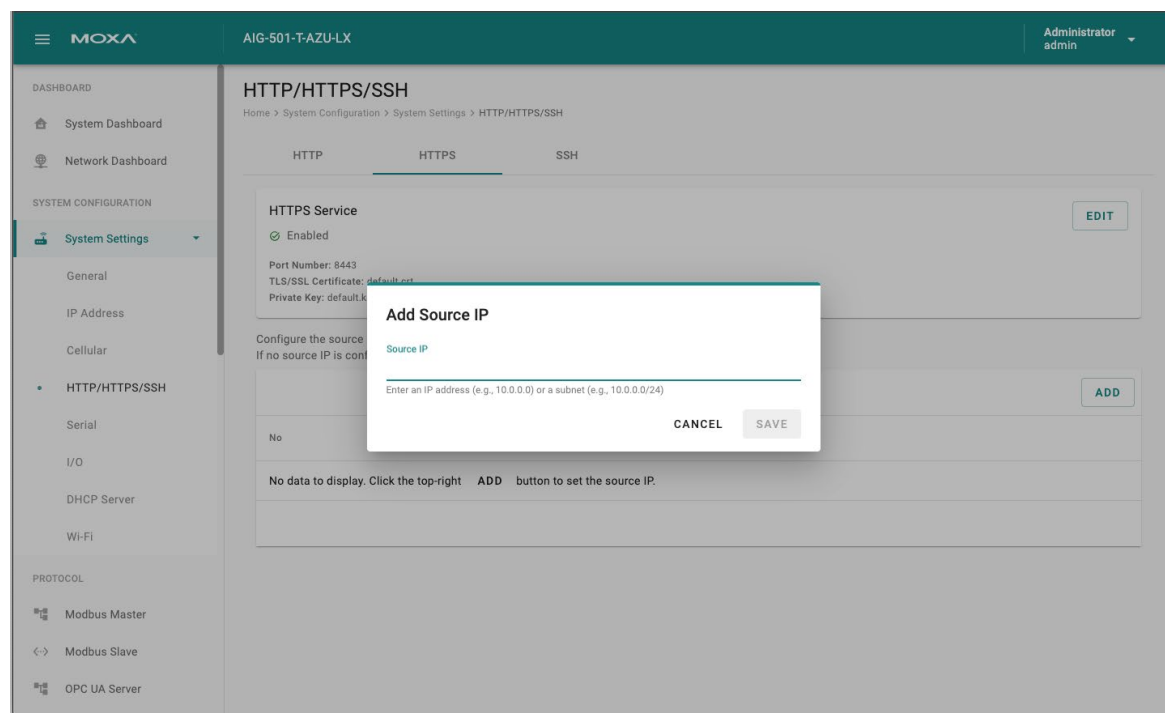
System Settings—HTTP/HTTPS/SSH

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 enhance cybersecurity, the default setting for **HTTP redirect to HTTPS** is **Enabled** (starting with firmware version v1.8.0). 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.



NOTE

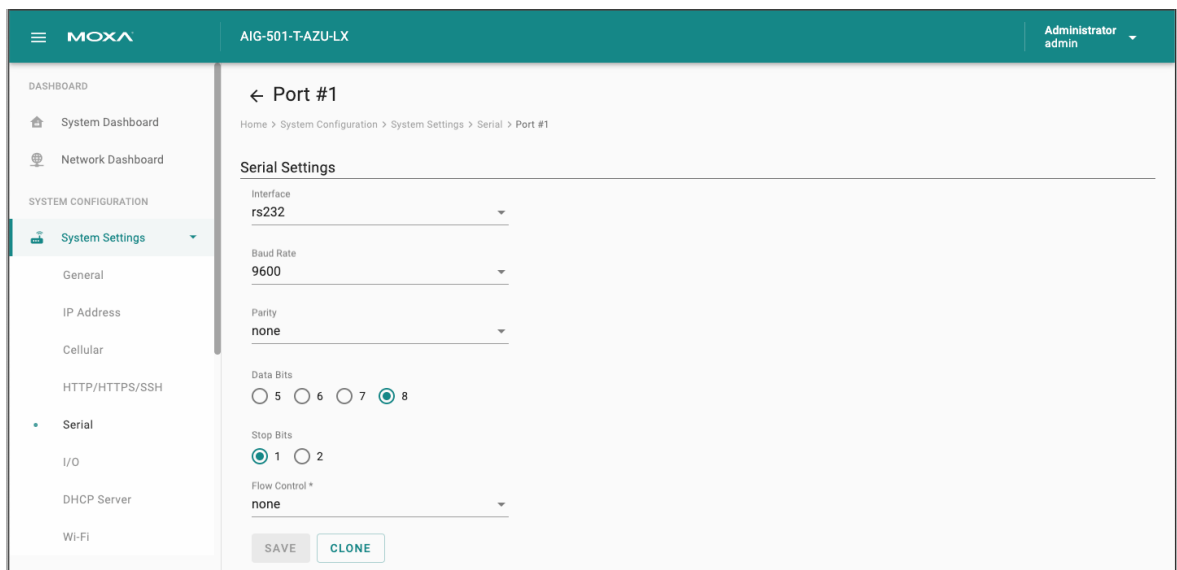
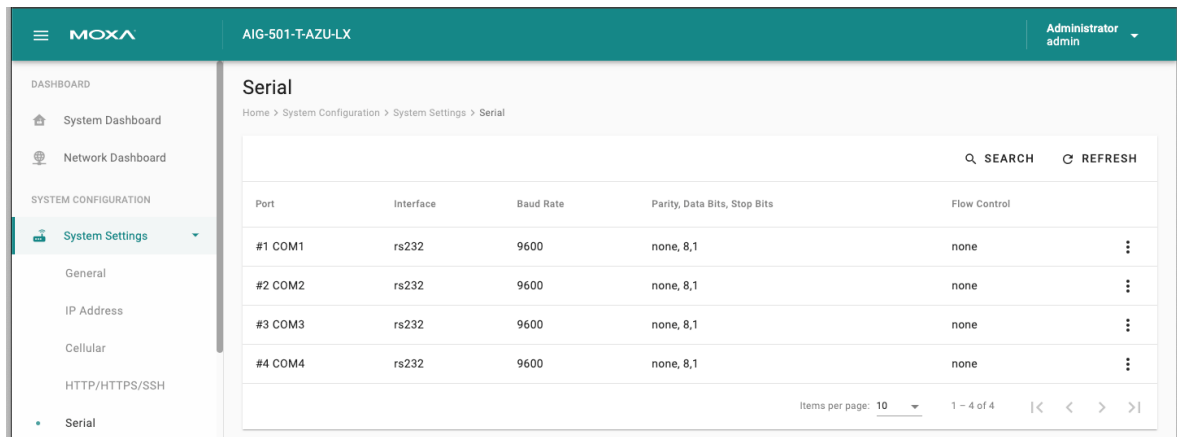
After the first SSH login, we force a password change to comply with general security policies and practices and to increase the security of your device.

System Settings—Serial

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

To configure serial setting, do the following:

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

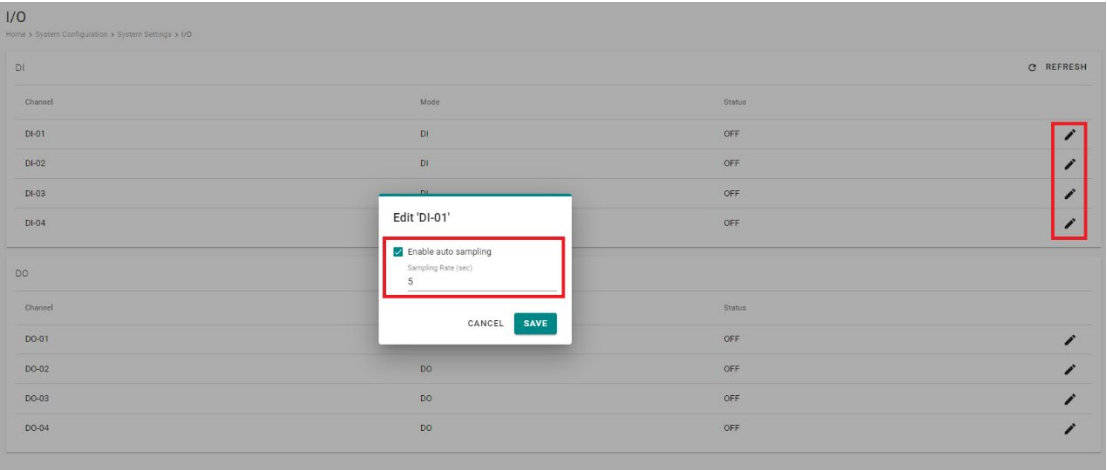


Parameter	Value	Description
Interface	rs232 rs422 rs485-2w rs-485-4w	
Baud Rate	300 to 115200	
Parity	none, odd, even, space, mark	
Data Bits	5, 6, 7, 8	
Stop Bits	1, 2	
Flow Control	none hardware software	Hardware: flow control by RTS/CTS (for RS-232) Software: flow control by XON/XOFF (for RS-232/422/485-4W)

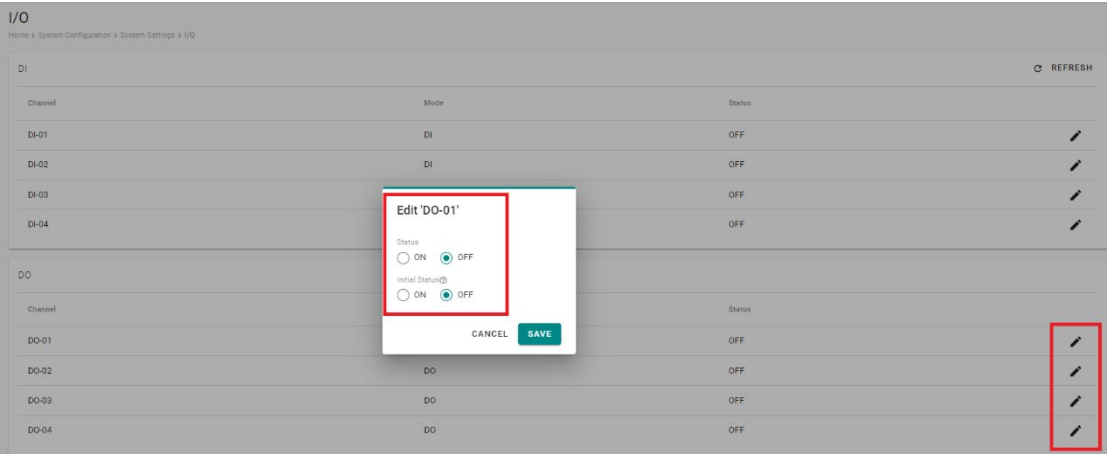
System Settings—I/O

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 management interface for the AIG-501-T-AZU-LX device. The left sidebar contains a navigation menu with sections: 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 'DHCP Server' option is selected. The main content area is titled 'DHCP Server' and shows tabs for LAN1, LAN2, LAN3, and LAN4. The 'Server Status' is 'Stopped'. There is a checkbox to 'Enable DHCP Server'. An info box states: 'Info: The DHCP Server setting is only for LAN and static IP interfaces. You can change the settings using IP settings'. The 'IP Address Range' section shows 'Start IP' as 192.168.3.200, 'End IP' as 192.168.3.250, and 'Netmask' as 255.255.255.0. The 'DNS' section shows 'Primary DNS - optional' as 8.8.8.8 and 'Secondary DNS - optional' as 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**.

The screenshot shows the 'Wi-Fi' settings page. At the top, there's a breadcrumb trail: 'Home > System Configuration > System Settings > Wi-Fi'. Below this, the 'Wi-Fi1' section is highlighted. It contains a checkbox for 'Enable Wi-Fi' which is currently unchecked. Below the checkbox is a dropdown menu for 'Wi-Fi Mode' with 'Wi-Fi AP' selected. The page is divided into three sections: 'General Settings', 'Advanced Settings', and 'Wi-Fi Mode'. In 'General Settings', there is a checkbox for 'Broadcast SSID' which is checked. Below it, the 'SSID' field is filled with 'moxa-sample-ap'. The 'Password (WPA2-PSK)' field is masked with asterisks. In 'Advanced Settings', there are three dropdown menus: 'Band' is set to '2.4GHz (802.11 b/g/n)', 'Region' is set to 'Taiwan', and 'Channel' is set to '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**.

Add by SSID

SSID

Security Mode

WPA/WPA2 Personal

Password

CANCEL ADD

Add by Scan Results

1 Select AP 2 View Details

Info: Please choose the Wi-Fi network that you want to add from the list. Note that only WPA and WPA2 Personal are supported.

SQA3_WiFi6		
sqa-iiot-lan-50G		
SQA2-TestBed-AWK3131A		
SQA-LAB-TV		
.M-Guest		

CANCEL NEXT >

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

Wi-Fi

Home > System Configuration > System Settings > Wi-Fi

Wi-Fi1

☐ Enable Wi-Fi

Wi-Fi Mode
Wi-Fi Client

AP List + CREATE

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

Mode

☒ DHCP: Obtain an IP address automatically

☐ Static: Assign IP address by manual configuration

Check-alive

☐ Enable check-alive

SAVE

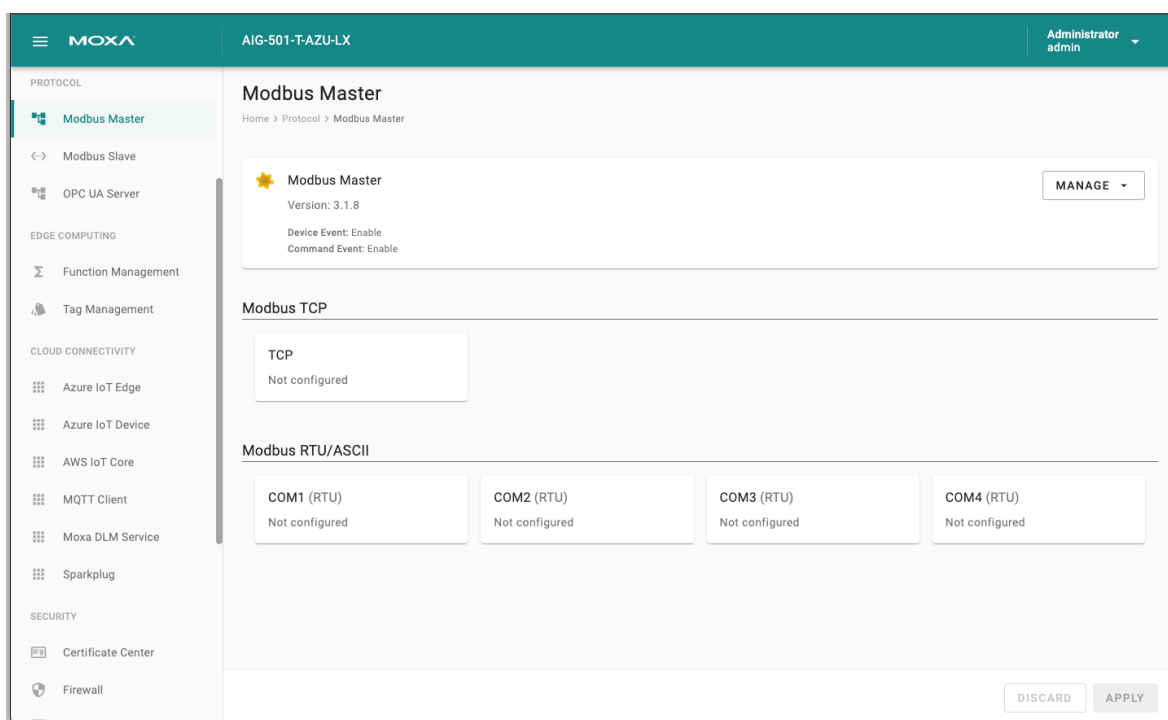
Protocol

Modbus Master

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

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

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



Modbus TCP

Basic Settings

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

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

Search command name.

ADD DEVICE

Basic Settings

Initial Delay (ms)
0

Maximum Retry
3

Response Timeout (ms)
1000

CANCEL SAVE

Parameter	Value	Default	Description
Initial Delay (ms)	0 to 30000	0	Some Modbus slaves may take more time to boot up than other devices. In some environments, this may cause the entire system to suffer from repeated exceptions during the initial bootup. After booting up, you can force the AIG to wait some time before sending the first request by setting a value for this parameter.
Maximum Retry	0 to 5	3	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.

← TCP ▾

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

Operation Mode: TCP

Search Command Name

ADD DEVICE

Select a device to view its details.

Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

☒ Enable This Device

Device Name
SE_Meter

Slave IP
192 . 168 . 127 . 50

Slave Port
502

Slave ID
1

CANCEL

NEXT >

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

Step 2. Command

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

The command settings will pop up.

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

☒ Enable this command

Basic

Command Name

Function
03 - Read Holding Registers

Read Holding Registers

Read Starting Address
0

Read Quantity
10

Trigger
Cyclic

Poll Interval (ms)
1000

CANCEL

DONE

SE_Meter

No. Command Name

There are no commands

Mode
☒ Manual ☐ Import

+ ADD COMMAND

Poll Interval (ms) Enable

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

CANCEL

NEXT >

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

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

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

← 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

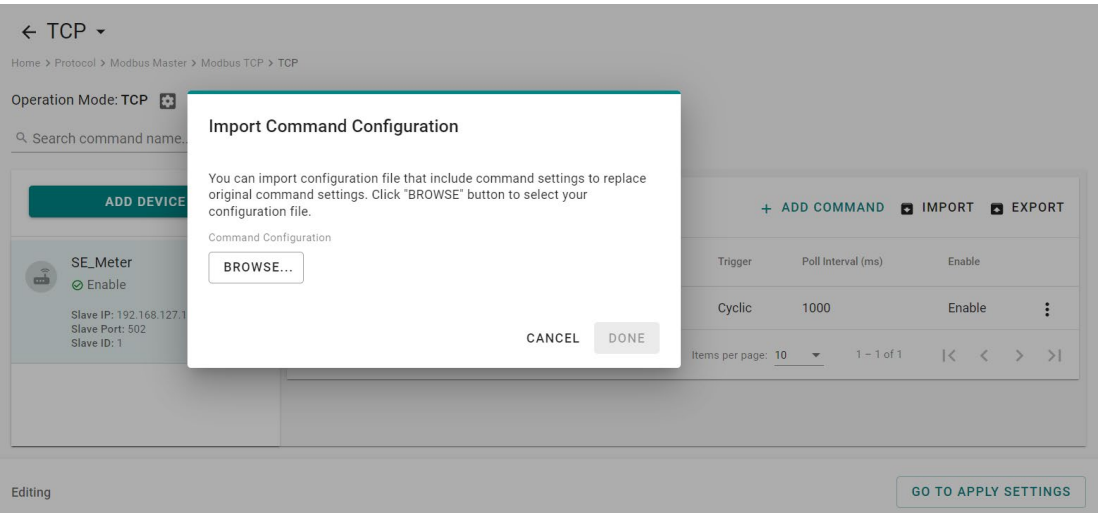
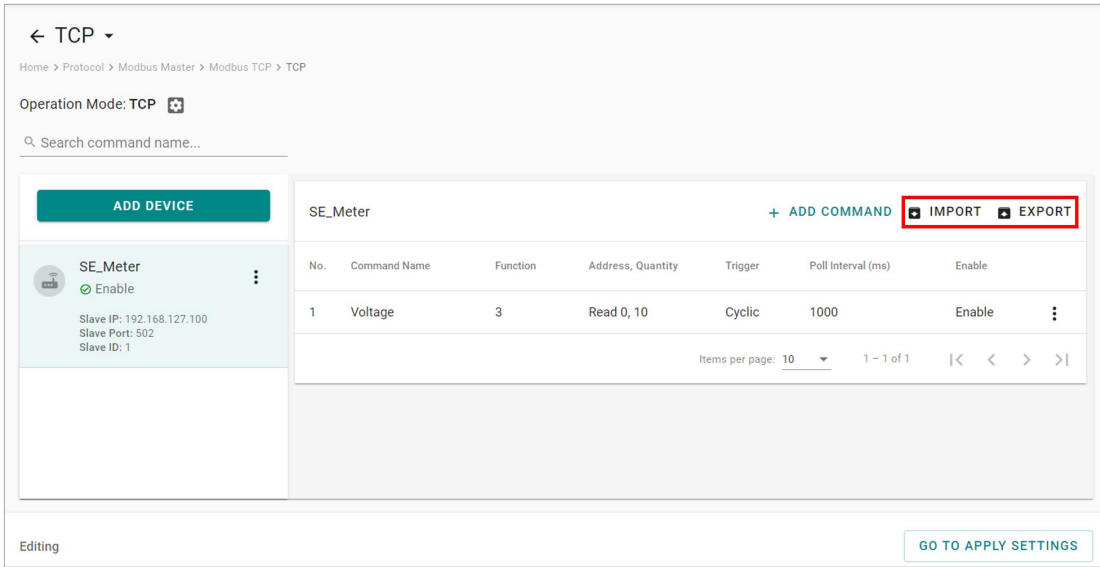
Number of Commands: 1

< BACK

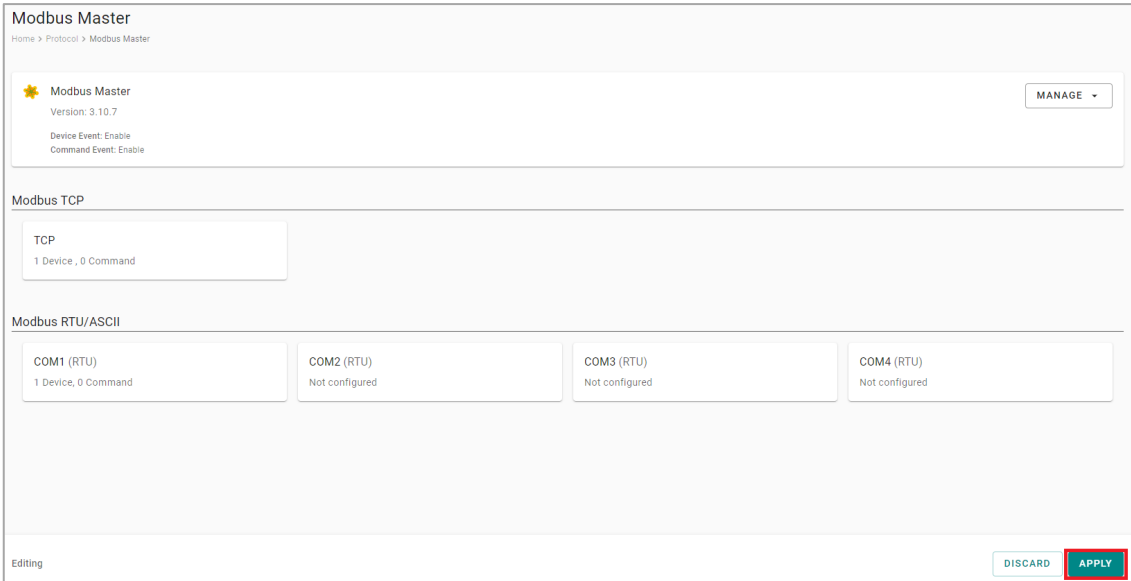
CANCEL

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.



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



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

Parameter	Value	Default	Description
name	Alphanumeric string	–	Name the command
enable	0: disable command 1: enable command		Enable/ Disable the command
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Function	01 – Read Coils 02 – Read Discrete Inputs 03 – Read Holding Registers 04 – Read Inputs Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 23 – Read/Write Multiple Registers	–	How to collect data from the Modbus device
readAddress	0 to 65535	–	Modbus registers the address for the collected data Note: Not applicable for write commands.
readQuantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	–	How much data to read. Note: Not applicable for write commands.
writeAddress	0 to 65535	–	Modbus registers the address for the written data. Note: Not applicable for read commands.
writeQuantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	–	How much data to write. Note: Not applicable for read commands.
pollInterval	100 to 86400000	–	Polling intervals are in milliseconds. Since the module sends all requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters.
swap	0: Big-endian (None, conversion AB CD → AB CD) 1: Big-endian byte swap (Byte, conversion AB CD → BA DC) 4: Little-endian (conversion AB CD → DC BA) 5: Little-endian byte swap (conversion AB CD → CD AB)	–	Byte swap mode

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

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

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

Modbus RTU/ASCII

Basic Settings

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

The screenshot shows the 'Serial Basic Settings' dialog box. The 'Mode' is set to 'RTU'. The 'Initial Delay (ms)' is 0. The 'Maximum Retry' is 3. The 'Response Timeout (ms)' is 1000. There are two checked options: 'Automatically determine the Inter-frame delay' and 'Automatically determine the Inter-character timeout'. The background shows the 'Operation Mode: RTU' button highlighted with a red box.

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 unchecked: 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 unchecked: 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.

← COM2 ▾

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

Operation Mode: RTU

🔍 Search command name...

ADD DEVICE

Select a device to view its details.

Editing

GO TO APPLY SETTINGS

Step 1. Basic Settings

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

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

☒ Enable this device

Device Name
SE_Meter

Slave ID
1

CANCELNEXT >

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

Step 2. Command

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

The command settings will pop up.

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

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 requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	None: not to swap Byte: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. Byte and Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	pause	The defined value of the Status Term will be effective when the read command encounters an error or times out.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in the tag hub.

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

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

Mode

☐ Manual
☒ Import Configuration

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

Command Configuration

BROWSE...

< BACK

CANCEL

NEXT >

Step 3. Confirm

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

← Create New Device

✓ 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

✓ Enable

Slave ID: 1

+ ADD COMMAND

IMPORT

EXPORT

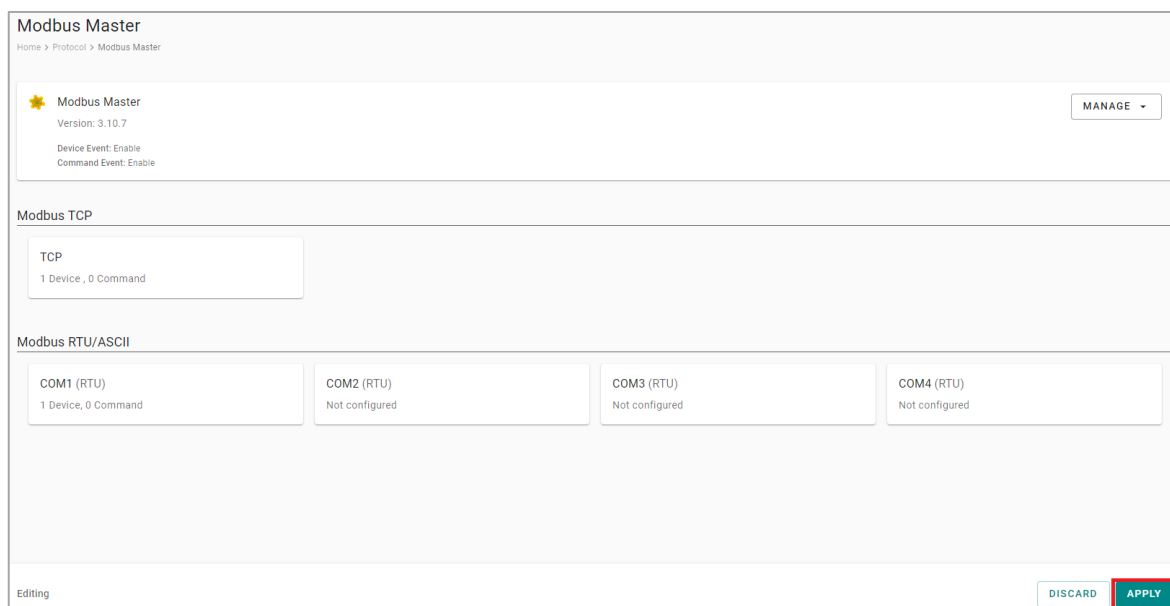
No.	Command Name	Function	Address, Quantity	Trigger	Poll Interval (ms)	Enable
1	Voltage	3	Read 0, 10	Cyclic	1000	Enable

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

GO TO APPLY SETTINGS

Editing

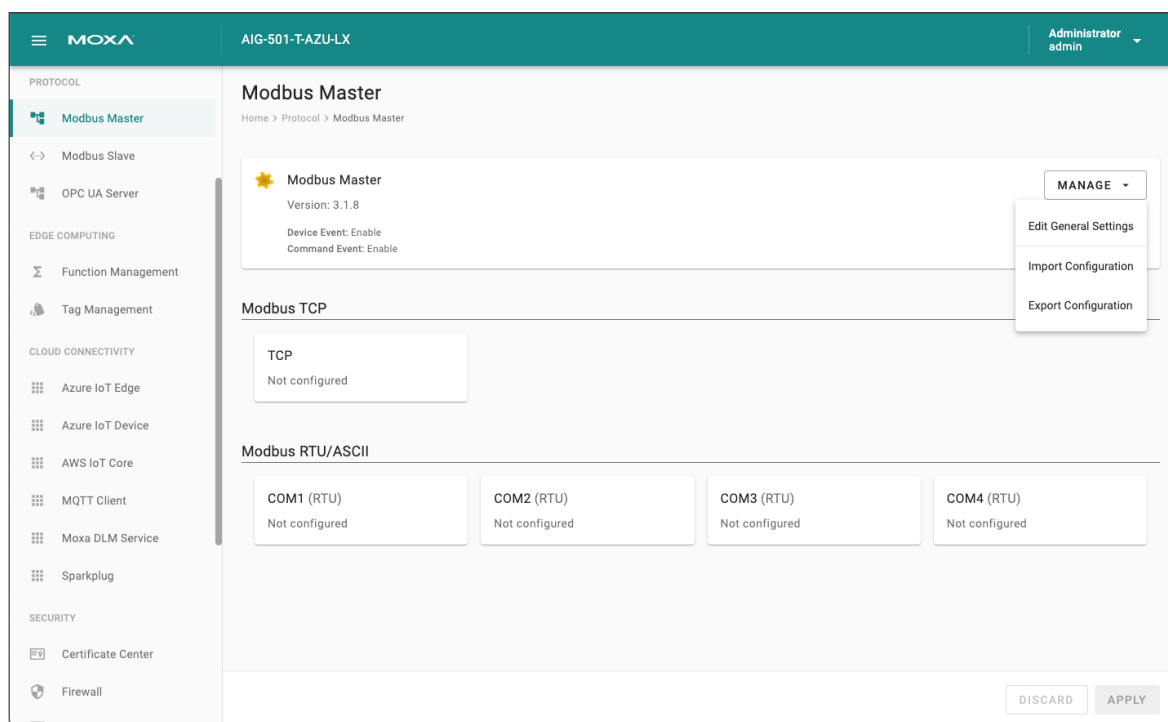
After finishing all the settings, press **GO TO APPLY SETTINGS** and click **APPLY** for the settings to take effect.



The image shows a web interface for configuring a Modbus Master. The page has a breadcrumb trail: Home > Protocol > Modbus Master. At the top, there is a 'Modbus Master' section with a star icon, version 3.10.7, and status 'Device Event: Enable' and 'Command Event: Enable'. A 'MANAGE' button is in the top right. Below this is the 'Modbus TCP' section with a 'TCP' box showing '1 Device, 0 Command'. The 'Modbus RTU/ASCII' section contains four boxes for COM1 (RTU), COM2 (RTU), COM3 (RTU), and COM4 (RTU), all showing 'Not configured'. At the bottom right, there are 'DISCARD' and 'APPLY' buttons. The 'APPLY' button is highlighted with a red border.

Management

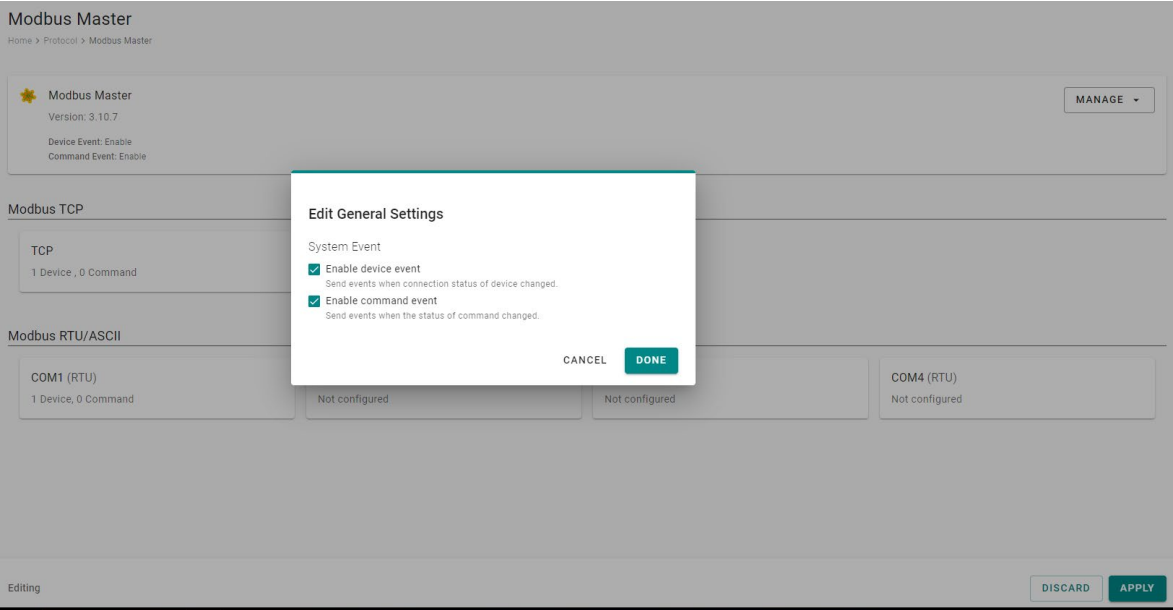
The AIG provides advanced features that help you save installation time and maintenance effort.



The image shows a more comprehensive web interface for configuring a Modbus Master. The page has a breadcrumb trail: Home > Protocol > Modbus Master. At the top, there is a 'Modbus Master' section with a star icon, version 3.1.8, and status 'Device Event: Enable' and 'Command Event: Enable'. A 'MANAGE' button is in the top right. Below this is the 'Modbus TCP' section with a 'TCP' box showing 'Not configured'. The 'Modbus RTU/ASCII' section contains four boxes for COM1 (RTU), COM2 (RTU), COM3 (RTU), and COM4 (RTU), all showing 'Not configured'. At the bottom right, there are 'DISCARD' and 'APPLY' buttons. The 'APPLY' button is highlighted with a red border. On the left side, there is a sidebar with a menu. The menu has sections: PROTOCOL (Modbus Master, Modbus Slave, OPC UA Server), EDGE COMPUTING (Function Management, Tag Management), CLOUD CONNECTIVITY (Azure IoT Edge, Azure IoT Device, AWS IoT Core, MQTT Client, Moxa DLM Service, Sparkplug), and SECURITY (Certificate Center, Firewall). The 'Modbus Master' item is selected and highlighted. The top right of the page shows the user 'Administrator admin'.

Edit General Settings

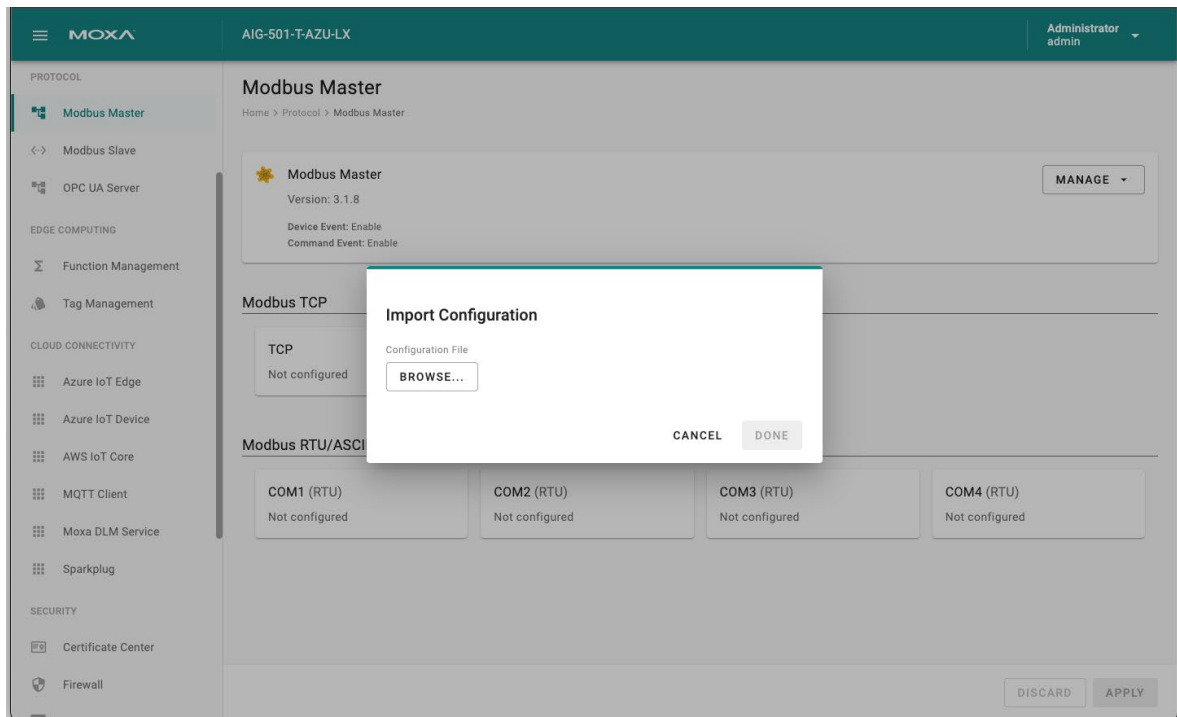
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	Check: If the Modbus communication fails, e.g., Modbus exception code is received The Modbus response timeout and the value of the status tag in the tag hub will change to 1. Uncheck: Disable the function
Enable command event	Check uncheck	Check	Check: If the Modbus command fails, e.g., Modbus exception code is received or Modbus response times out, the value of the status tag in the tag hub will change to 1. Uncheck: Disable the function.

Import/Export Configuration

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

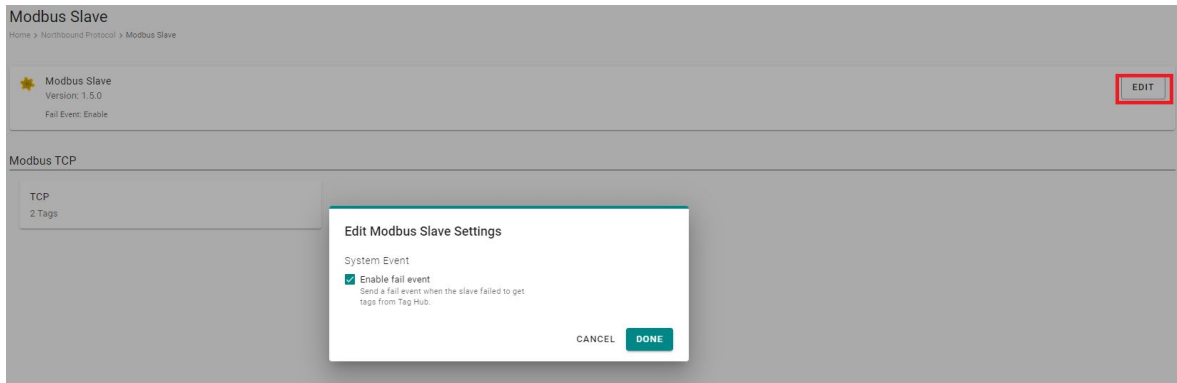


An example of an exported file that can be viewed/edited by EXCEL.

master-tcp- <i>ifaces</i>																								
@master	tcpMaster	initialDel	retry	Cour	response	Tout																		
1	1	0	3	1000																				
ser-masters																								
@serMas	configId	name																						
1	1	modbus_serial_master																						
master-ser- <i>ifaces</i>																								
@master	serMaster	port	Value	format	initialDel	retry	Cour	response	frame	inte	char	interval												
1	1	1	0	0	0	3	1000	0	0															
2	1	1	0	0	3	1000	0	0																
remote-devs																								
@remote	masterSer	masterTcr	name	enable	slaveld	slavelpad	slaveTcr	Port																
1	1	1232	1	1	0	0	0	502																
2	2	SE_Meter	1	1	0	0	0	502																
3	1	GE_Meter	1	1	1	1	1	502																
mcmds																								
@remote	name	enable	mode	func	readAddr	readQuai	poll	interval	swap	fpFunc	fpTout	fpData	scalingFu	intercept	pointSou	pointSou	pointTarg	pointTarg	name	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	231.raw	int16	r		20
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	Voltage_t1	int16	r		
																			1	Voltage_t2	int16	r		
																			1	Voltage_t3	int16	r		
																			1	Voltage_t4	int16	r		
																			1	Voltage_t5	int16	r		
																			1	Voltage_t6	int16	r		
																			1	Voltage_t7	int16	r		
																			1	Voltage_t8	int16	r		

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.

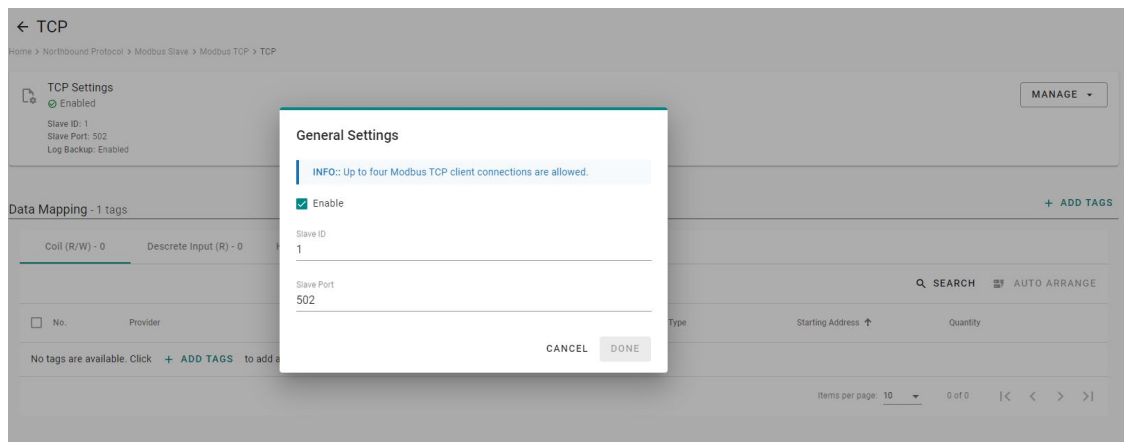


To create a Modbus TCP server (slave), following the steps below:

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

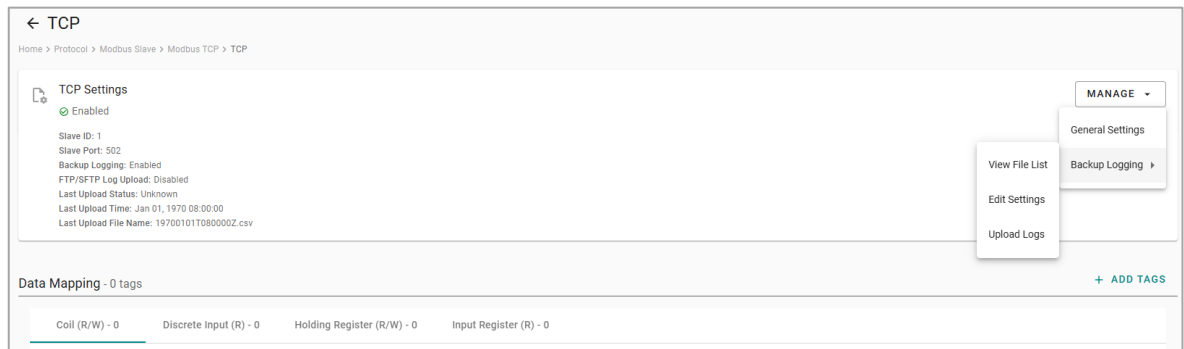
Under Data Mapping, you can view all the selected tags, which will be divided into Coil, Discrete Input, Holding Register, and Input Register. The rule is based on the tag's attribute stored in the tab hub. For example, if the tag type is Boolean and Tag Access permissions are Read, the tag will be mapped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

Backup Logging

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



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

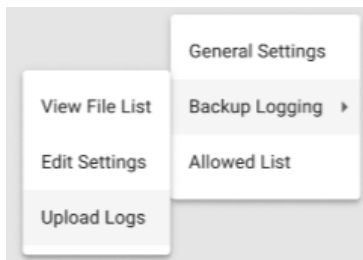
File Split Mode
☒ By Time ☐ By Size

Time Interval (min)
1440

CANCEL DONE

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

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

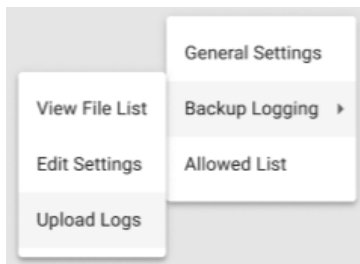


2. Enable the FTP/SFTP uploader.
3. Select FTP as upload Method.
4. Configure the necessary parameters, such as server, port, path, username, and password.
5. Configure the upload interval.
6. (Option) Click "Check Connection" to verify that the communication is functioning correctly.
7. Click "Save"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

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

Upload Logs

☒ Enable FTP/SFTP log upload

Upload Method

☐ FTP ☒ SFTP

Upload Information

Server	Port
111.11.11.11	22

Path
/home/stfpuser/stage

Username
stfpuser

Authentication Method
Upload SSH key

SSH Key
5bb65fe6266bd6b6
8f71cb897b90d4b7

Upload Interval (min)
10

CHECK CONNECTION

Info

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

CANCEL

SAVE

Modbus Capability:

Max. # of Serial Slave Device 31

Max. # of TCP Slave Device 64

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

Max. # of Tags for Modbus Master 4500

Max. # of Tags for Modbus Slave 6000

Max. # of Commands for a Slave Device 256

Max. # of Commands for a TCP Slave Device 2048



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

← Account Management

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

CREATE

No.	Account	
1	admin	⋮

BACK

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

← Certificate Management

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

Server Certificate

My Certificates

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

Client Certificate

Trusted Certificates

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

Download Certificate

Update - Manually Upload

Update - Regenerate by ThingsPro

← Certificate Management

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

Server Certificate

My Certificates

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

Client Certificate

Trusted Certificates

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

Upload Client Certificate

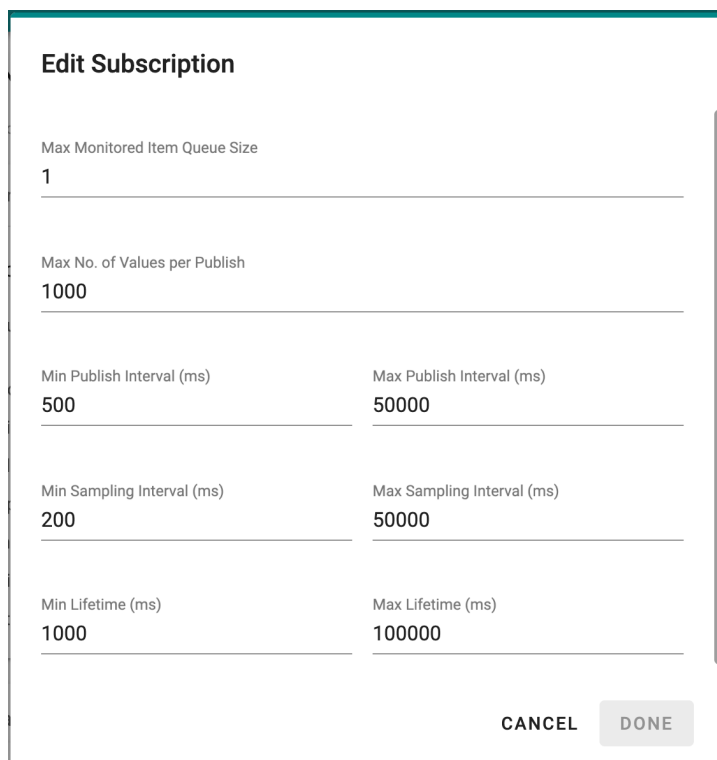
Certificate File

BROWSE...

CANCEL DONE

UPLOAD

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



Edit Subscription

Max Monitored Item Queue Size
1

Max No. of Values per Publish
1000

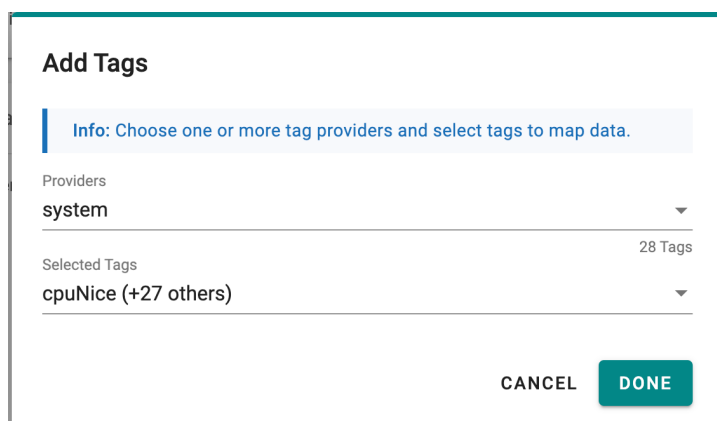
Min Publish Interval (ms) 500 Max Publish Interval (ms) 50000

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

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

CANCEL DONE

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



Add Tags

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

Providers
system

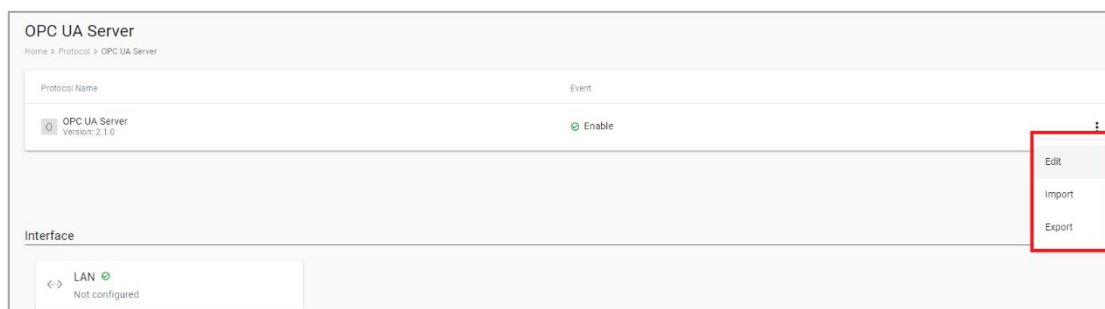
Selected Tags
cpuNice (+27 others)

28 Tags

CANCEL DONE

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

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



OPC UA Server

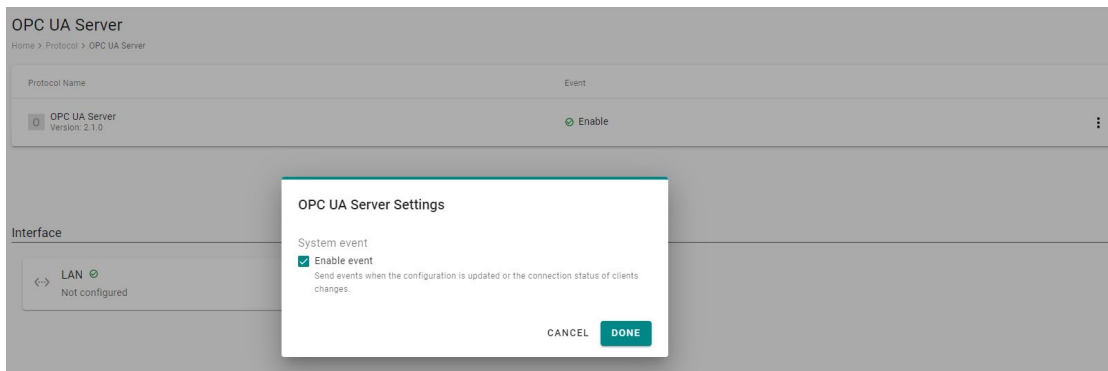
Home > Protocol > OPC UA Server

Protocol Name	Event
OPC UA Server Version: 2.1.0	Enable

Interface

LAN Not configured

Edit
Import
Export



Edge Computing

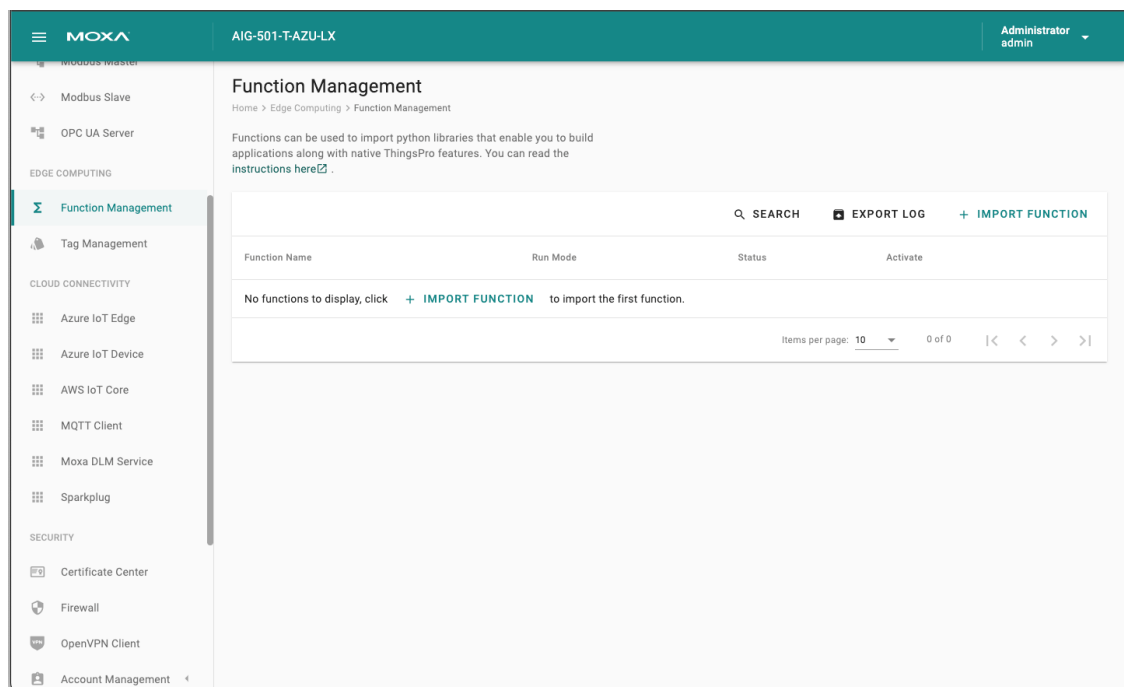
Function Management

AIG-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**.

Import Function

Compress the function source code into a tar.gz file and upload it here.
Ensure that the file contains a package.json file and at least one exe file.

Function File

BROWSE...

CANCEL

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](#).

Q SEARCH

EXPORT LOG

+ IMPORT FUNCTION

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

```

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

	Run Mode
1	Boot
2	Cron job

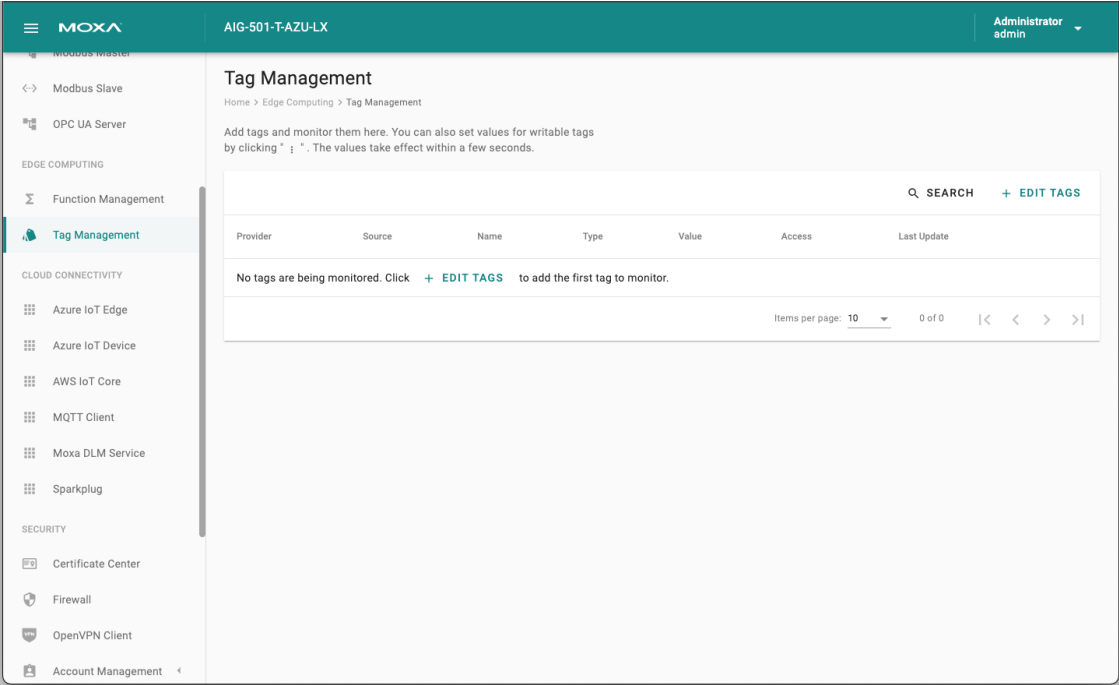
Status	Description
Running	The function is running
Retrying	Retrying a failed function every 5 seconds (unlimited tries)
Failure	The function failed during a retry. The correspondent error message will be displayed in the table. You can click EXPORT LOG to check the logs.
Inactive	The function is disabled.

Tag Management

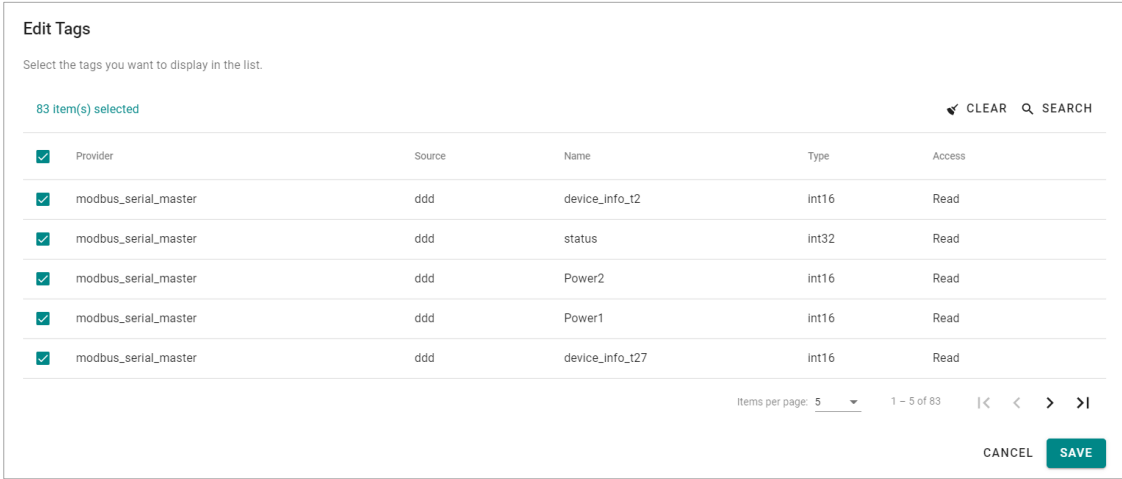
Go to **Tag Management**, where you can create and monitor the real-time tag value for troubleshooting purposes.

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

1. Click **+ EDIT TAGS**.



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. 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	123	DO	boolean		Write	-	⋮

Items per page: 10 1 - 1 of 1 [< < > >]

Write value

Provider
modbus_serial_master

Source
123

Name
DO

Type
boolean

Value *

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

CANCEL SAVE

CANCEL

NEXT >



NOTE

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

Cloud Connectivity

Azure IoT Edge

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

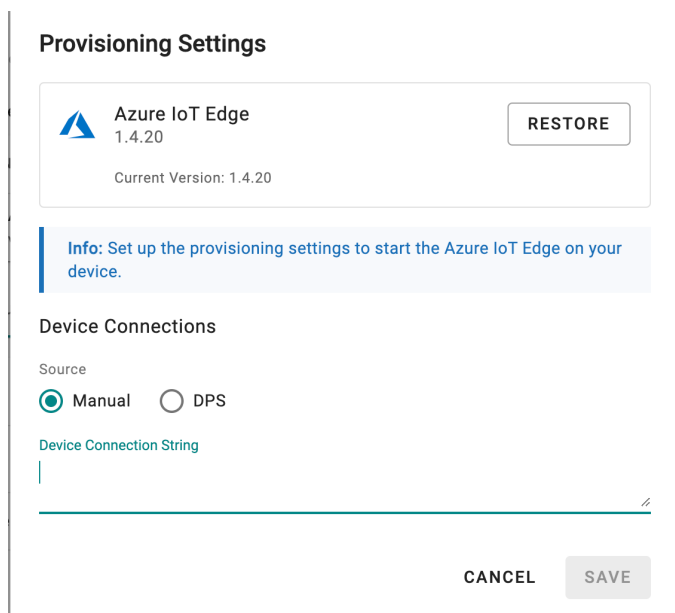


NOTE

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

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

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



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

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



NOTE

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

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

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 Modes](#).

The screenshot shows the 'Create New Telemetry Message' dialog with three steps: 1. Basic Settings, 2. Message Tags, and 3. Properties Optional. Step 1 is active. It includes a checkbox for 'Enable Telemetry Message' which is checked. Below it is an 'Output Topic' field. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. A 'Publish Interval (sec)' input field is set to 60. A '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 right are 'CANCEL' and 'NEXT >' buttons.

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

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

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

Create New Telemetry Message

Basic Settings

2 Message Tags

3 Properties Optional

Select Tags

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

Providers

IO

Selected Tags

DI-01 (+3 others)

8 Tags

jq Filter

TEST

Custom Payload Result

Enable custom payload

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

< BACK

CANCEL

NEXT >

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

Create New Telemetry Message

Basic Settings

2 Message Tags

3 Properties Optional

Property Key

Property Value

+ Add another

< BACK

CANCEL

SAVE



NOTE

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



NOTE

If you cannot receive D2C messages, check and ensure that a default route of the modules is added. You can add routes in Azure IoT Hub. 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.

The screenshot shows the 'Azure IoT Edge' configuration page. At the top, there's a breadcrumb trail: 'Home > Cloud Connectivity > Azure IoT Edge'. Below this is a toggle switch for 'Azure IoT Edge' which is currently turned on. A table lists the service with columns 'Service Name' and 'Status'. The entry shows 'Azure IoT Edge' with 'Version: 1.4.10' and a status of 'Exited'. Below the table are tabs for 'Module List', 'Device Management' (which is selected), 'Telemetry Message', 'Downstream Certificate', and 'AIE Checks'. A message states: 'Allow managing this device from Azure IoT Hub via a Module Twin and Direct Methods technology.' Below this is a checkbox for 'Allow Device Management' which is checked, with a note: 'This feature requires the ThingsProAgent module installed.' At the bottom is a 'SAVE' button.



NOTE

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

Downstream Certificate

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

The screenshot shows the Moxa AIG-501-T-AZU-LX web interface. The left sidebar contains navigation menus for 'EDGE COMPUTING', 'CLOUD CONNECTIVITY', 'SECURITY', and 'MAINTENANCE'. The 'CLOUD CONNECTIVITY' menu is expanded, showing 'Azure IoT Edge' as the selected option. The main panel displays the 'Azure IoT Edge' configuration page, which is identical to the one in the previous screenshot. Overlaid on this is a modal window titled 'Upload Downstream Certificate'. The modal has three sections: 'X.509 Certificate' with a 'BROWSE...' button, 'Private Key' with a 'BROWSE...' button, and 'Trusted CA Certificate' with a 'BROWSE...' button. At the bottom of the modal are 'CANCEL' and 'SUBMIT' buttons.

Azure IoT Edge

Home > Cloud Connectivity > Azure IoT Edge

Azure IoT Edge

Service Name

Status

Azure IoT Edge

Version: 1.4.10

Running

Module List

Device Management

Telemetry Message

Downstream Certificate

AIE Checks

This identity check prevents your devices from connecting to potentially malicious gateways.

aziot-edge CA marco-301-connect

Verified

Issued On: aziot-edge CA marco-301-connect

Valid Until: Jan 14 09:02:40 2024 GMT

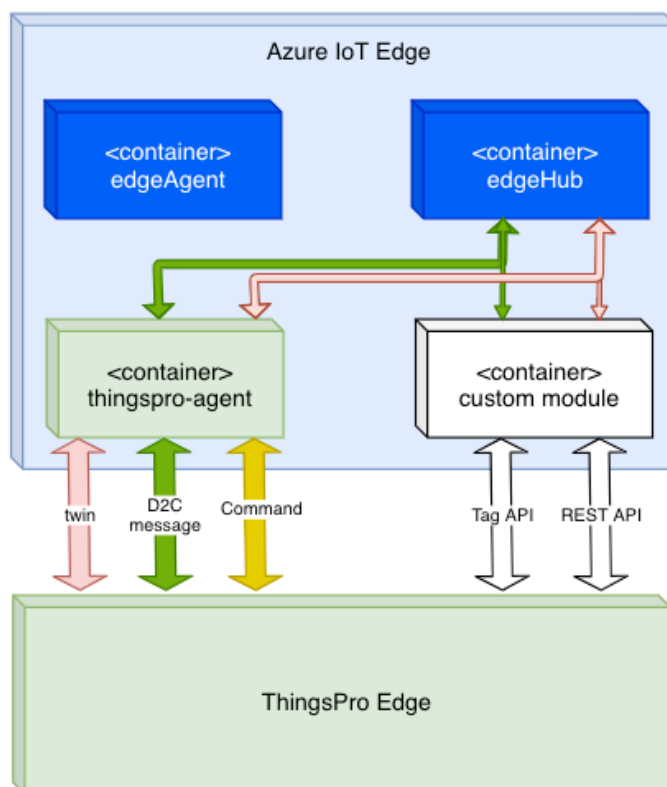


NOTE

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

3. 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 *

thingspro-api-v1

Payload

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

Response timeout 30 seconds

Connection timeout Module must already be connected

[Invoke method](#)

4. system-reboot

Method Name:

```
system--reboot
```

Request Payload:

```
{}
```

Response:

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

5. 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.

6. Thingspro-software-upgrade

Method Name:

```
thingspro-software-upgrade
```

Request Payload:

```
{
  "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.

Method name * ⓘ

thingspro-software-upgrade

Payload ⓘ

{}

Response timeout ⓘ Connection timeout ⓘ

1 minute Module must already be connected ▾

Invoke method

Result

```
{
  "status": 200,
  "payload": {
    "data": [
      "moxa-aig-502-tpe"
    ],
    "message": "Successfully trigger"
  }
}
```

7. 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.
sendOutThreshold	Type: object Define conditions to send out messages to Azure Edge Hub based on: - 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	Type: integer Unit: second Description: A fixed interval between the two immediately mode publish
samplingMode	Type: string Enum: allValues, latestValues, allChangedValues, latestChangedValues
customSampling	Type: boolean Description: Enable will use the pollingInterval that user input.
pollingInterval	Type: integer Description: The interval at which to poll tag data. For example, - value 10 : Every 10 second - value 0 : when the data is pushed into the tag (almost real time)

8. 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.

The screenshot shows the 'Create New D2C Message' interface with three steps: Basic Settings, Message Tags (active), and Properties (optional). In the 'Message Tags' step, there are three dropdown menus for 'System Tags', 'IO Tags', and 'Virtual Tags'. The 'System Tags' dropdown is set to 'cpuUsage'. Below these is a checkbox for 'Enable custom payload'. To the right, the 'Custom Payload Result' panel displays a JSON object:

```
{
  "messageTimeStamp": "2019-11-15T15:53:47Z",
  "tags": {
    "system": {
      "cpuUsage": {
        "values": [
          {
            "updateTimeStamp": "2019-08-07T09:05:28Z",
            "value": 86
          }
        ]
      }
    }
  }
}
```

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

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

Create New D2C Message

1 Basic Settings 2 Message Tags 3 Properties (optional)

Learn how to [edit message tags](#).

Select Tags ☒ Enable custom payload

System Tags
cpuUsage

IO Tags
— None —

Virtual Tags
— None —

jq Filter
{device:(.srcName),timestamp:(now|todateiso8601),TagName:(.tagName), Value:.dataValue} **TEST**

Custom Payload Result

```
{
  "TagName": "cpuUsage",
  "Value": 30,
  "device": "system",
  "timestamp": "2019-11-15T15:55:10Z"
}
```

< BACK CANCEL NEXT >

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|todateiso8601),(.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.

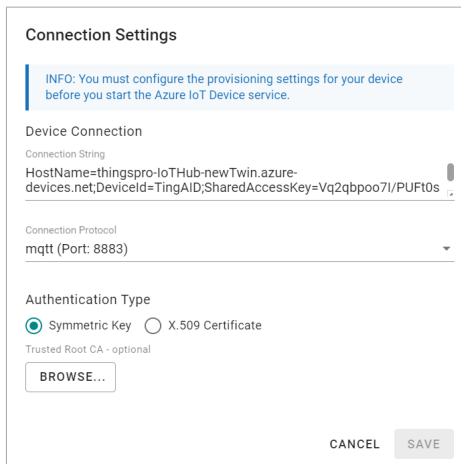


NOTE

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
BROWSE...

CANCEL SAVE

Telemetry Message

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

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

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

The screenshot shows the 'Create New Telemetry Message' dialog with three steps: 1. Basic Settings, 2. Message Tags, and 3. Properties Optional. In Step 1, the 'Enable Telemetry Message' checkbox is checked. Below it is an 'Output Topic' text field. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. Below these is a 'Publish Interval (sec)' text field with 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 are 'CANCEL' and 'NEXT >' buttons.

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

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

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

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

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

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

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

8. Click **NEXT**.

9. (Optional) Enter Property Key and Value.

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

10. Click **SAVE**.

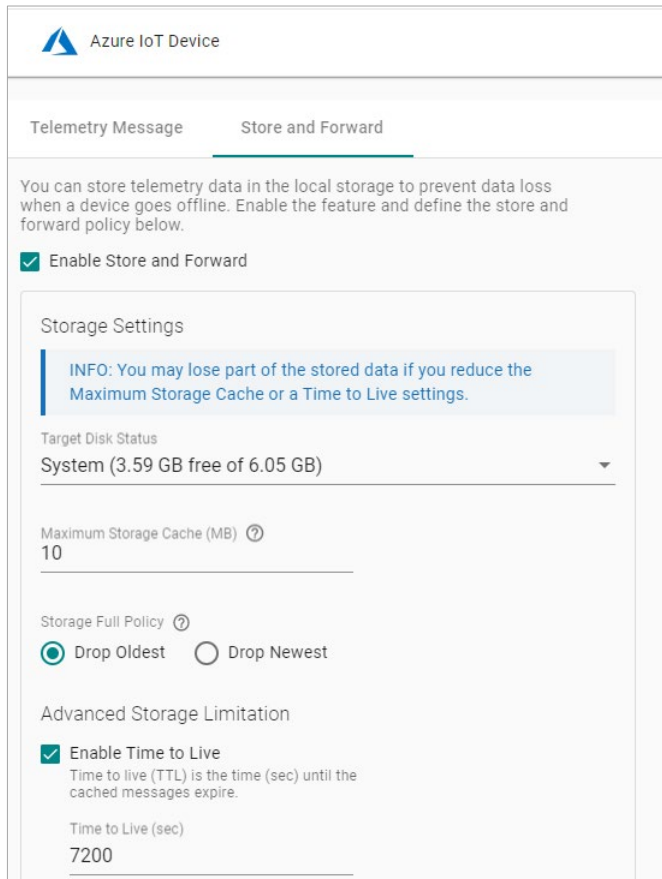


NOTE

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

Store and Forward

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



Azure IoT Device

Telemetry Message **Store and Forward**

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

☒ Enable Store and Forward

Storage Settings

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

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

Maximum Storage Cache (MB) ?
10

Storage Full Policy ?
☒ Drop Oldest ☐ Drop Newest

Advanced Storage Limitation

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

Time to Live (sec)
7200

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.



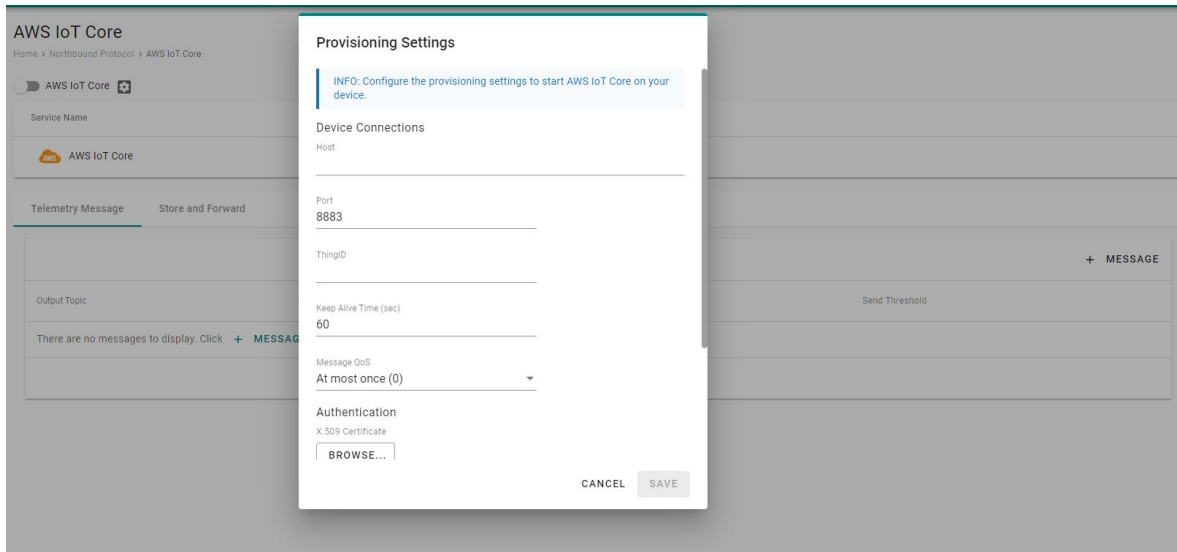
NOTE

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 Modes](#).
4. Input corresponding parameters such as publish interval, sampling mode, and publish size.
5. Click **NEXT**.

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

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

The screenshot shows the 'Create New Telemetry Message' dialog with the 'Message Tags' tab selected. The 'Basic Setting' tab is marked as completed. The 'Select Tags' section shows a list of providers with 'IO' selected. A search bar is present. The 'Default Payload' is set to 'null'. There is a checkbox for 'Enable custom payload' which is unchecked. At the bottom right, there are 'CANCEL' and 'SAVE' buttons. A 'DONE' button is also visible at the bottom of the 'Select Tags' panel.

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

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

Create New Telemetry Message

✓ Basic Setting 2 Message Tags

Select Tags

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

Providers

IO

Selected Tags

DI-01 (+3 others)

8 Tags

Default Payload

☐ Enable custom payload

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

```

< BACK CANCEL SAVE

8. Click **SAVE**.



NOTE

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

Store and Forward

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

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

☒ Enable Store and Forward

Storage Setting

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

Target Disk

System (3.59GB free of 6.05GB) ▼

Maximum Storage Cache (MB) ?

10

Storage Full Policy ?

☒ Drop Oldest ☐ Drop Newest

Advanced Storage Limitation

☒ Enable Time to Live

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

Time to Live (sec)

7200

SAVE

Device Management

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



NOTE

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

Generic MQTT Client

Go to **Cloud Connectivity > MQTT Client**, 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 the 'Connect to New MQTT Broker' dialog with the 'SSL/TLS' tab selected. The 'Enable SSL/TLS' checkbox is checked. Under 'TLS Version', '1.2' is selected with a radio button. There are three 'BROWSE...' buttons for 'Client Certificate - optional', 'Client Key - optional', and 'Trusted Root CA - optional'. An 'Ignore Server Certificate' checkbox is unchecked. '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 the 'Create New Telemetry Message' dialog with the 'Basic Setting' tab selected. The 'Enable Telemetry Message' checkbox is checked. The 'Output Topic' field contains '123'. Under 'Publish Mode', 'By Interval' is selected with a radio button. The 'Publish Interval (sec)' field contains '60'. The 'Sampling Mode' dropdown is 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 Modes](#).
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

Select Tags

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

☐ Enable custom payload

CANCEL SAVE

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

Create New Telemetry Message

Basic Setting

Select Tags

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

Providers

IO

Selected Tags

DI-01 (+3 others)

8 Tags

Default Payload

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

```

☒ Enable custom payload

CANCEL SAVE

< BACK

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 a connection list showing 'test.mosquitto.org' as 'Connected'. The main panel has three tabs: 'Telemetry Message', 'Store and Forward' (selected), and 'Remote API Invocation'. The 'Store and Forward' tab contains the following settings:

- Enable Store and Forward:** A checkbox that is checked.
- Storage Setting:**
 - INFO:** You may lose part of stored data stored if you reduce the maximum Disk Size or Time to Live settings.
 - Target Disk:** A dropdown menu showing 'System (3.59GB free of 6.05 GB)'.
 - Maximum Storage Cache (MB):** A text input field with the value '10'.
 - Storage Full Policy:** Two radio buttons: 'Drop Oldest' (selected) and 'Drop Newest'.
 - Advanced Storage Limitation:**
 - Enable Time to Live:** A checkbox that is checked.
 - Time to live (TTL) is the time (sec) until the cache messages expire.**
 - Time to Live (sec):** A text input field with the value '7200'.

A 'SAVE' button is located at the bottom right of the configuration panel.

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' (selected). The page contains the following settings:

- Enable Invoking of Device Restful APIs from MQTT Server:** A checkbox that is checked.
- Input Topic to Subscribe:** A text input field with a help icon.
- Output Topic to Subscribe:** A text input field with a help icon.

A 'SAVE' button is located at the bottom left of the configuration panel.



NOTE

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

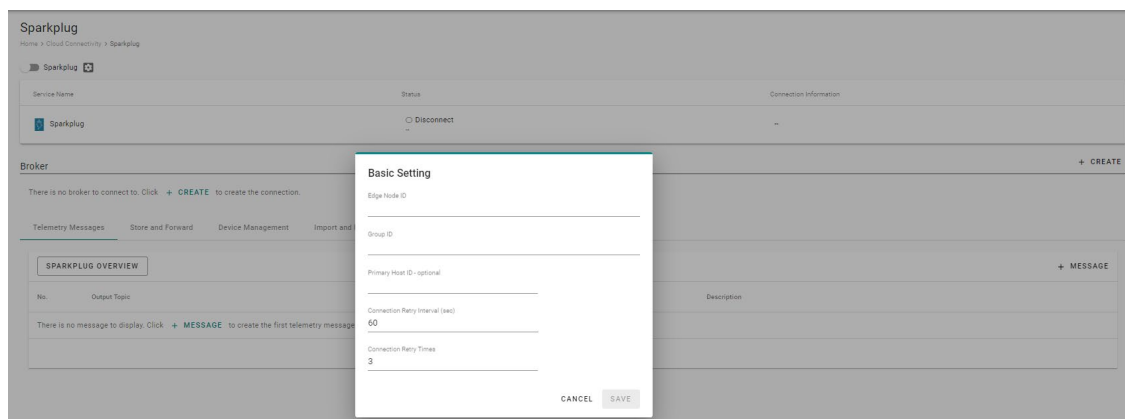
Sparkplug

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:

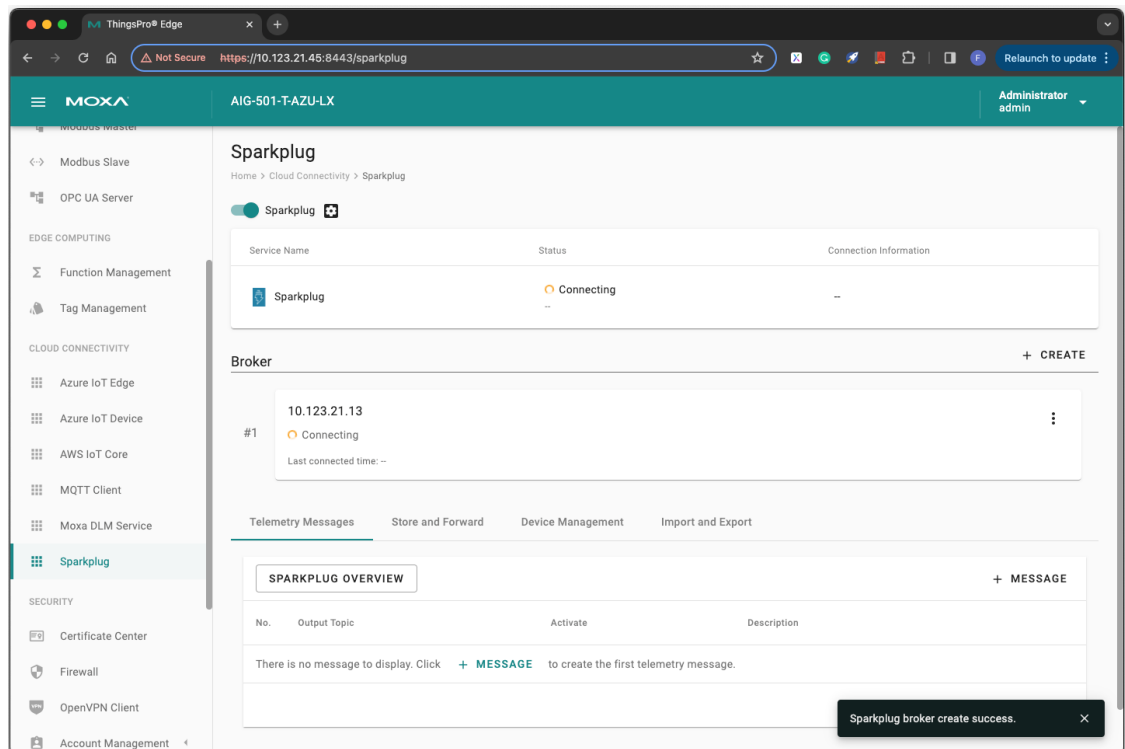
- Enabling Sparkplug
- Configuring a Broker
- Configuring a Telemetry Message

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.

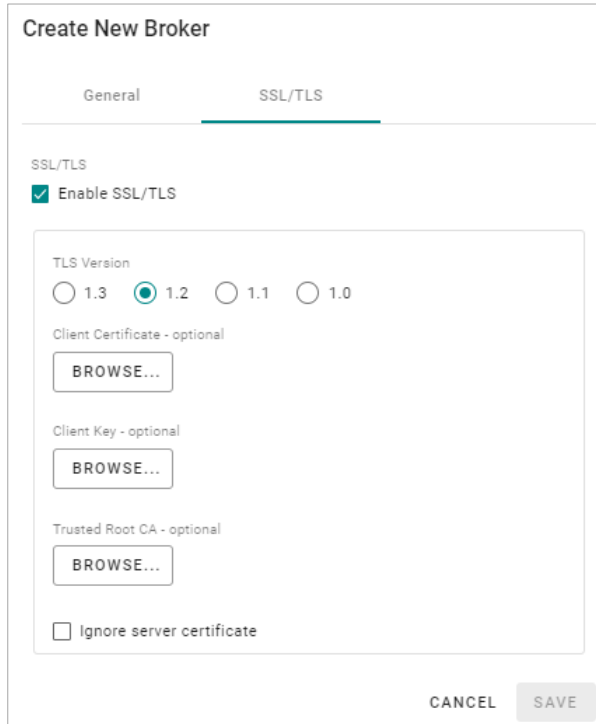


5. Click **SAVE**.



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

6. Click **SAVE**.



NOTE

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

Configuring a Telemetry Message

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

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

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

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

8. (optional) Specify a description.

9. Click **SUBMIT**.

Create New Telemetry Message

✓ Select Tags

✓ Set Up Transmission Setting

3 Confirm

[modbus_tcp_master] Test

c1

Message Transmission Setting

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

Message Group Description

Description

0 / 1024

☐ Enable this message group later

< BACK

CANCEL SUBMIT



NOTE

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

Store and Forward

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

☒ Enable Store and Forward

Storage Setting

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

Target Disk
System (6.92GB free of 15.41GB)

Maximum Storage Cache (MB) ?
10

Storage Full Policy ?
☒ Drop Oldest ☐ Drop Newest

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

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

SAVE

Device Management

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

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



NOTE

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

Import & Export

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

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



NOTE

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

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

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**.

The screenshot shows the 'MOXA DLM Service' page with a modal dialog titled 'Add Connection'. The dialog contains an information message: 'Info: Add a Moxa DLM service connection and verify it.' Below this are input fields for 'Email' and 'Password'. The 'Password' field has a toggle icon to show or hide the password. At the bottom of the dialog are 'CANCEL' and 'VERIFY' buttons. The background page shows a breadcrumb 'Home > Device Management > MOXA DLM Service' and a section titled 'Moxa DLM Service Enrollment' with an 'ADD CONNECTION' button.

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

The screenshot shows the 'Moxa DLM Service' page with a section titled 'Moxa DLM Service Enrollment'. This section is highlighted with a red box. It contains the text: 'To start using Moxa DLM service for the device and connect to the Moxa DLM service project, add the connection in the device and select a project to enroll.' Below this is a heading 'Configure an Moxa DLM service connection' and a list item 'Moxa DLM service connection' with a green checkmark and the word 'Verified'. Below the list item are the details: 'Email: ichbinjoshua@gmail.com' and 'Password: *****'. To the right of the list item is an 'EDIT' button. Below the enrollment section is an 'Enrollment setting' section with a 'Project Name' dropdown menu set to 'Test' and an 'ENROLL' button.

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

Moxa DLM Service

Home > Cloud Connectivity > Moxa DLM Service

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

Moxa DLM Service Enrollment

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

Configure an Moxa DLM service connection

↔

Moxa DLM service connection
✓ Verified
Email: ichbinjoshua@gmail.com
Password:

Enrollment setting

Project Name

Test

ENROLL

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



NOTE

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

Moxa DLM Service

Home > Cloud Connectivity > Moxa DLM Service

Moxa DLM service

Project Name	Status
Test	✓ Connected Connect on Oct 14, 2024, 12:14:01

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-T-AP-AZU-LX
MAC Address: 0090E88F9A95
Serial Number: TBZJE1013036

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

All Devices

Home > Projects > All Devices

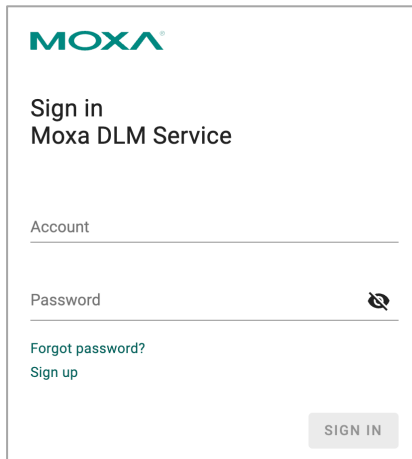
Connected Status:online REFRESH

☐	Serial Number	Model Name	Host Name	Connection Status	Firmware Version	Labels	
☐	TBZJE1013036	AIG-501-T-AP-AZU-LX	Moxa	Online Connected on Oct 14, 2024 12:01	1.3	-	⋮

Items per page: 10 1 - 1 of 1

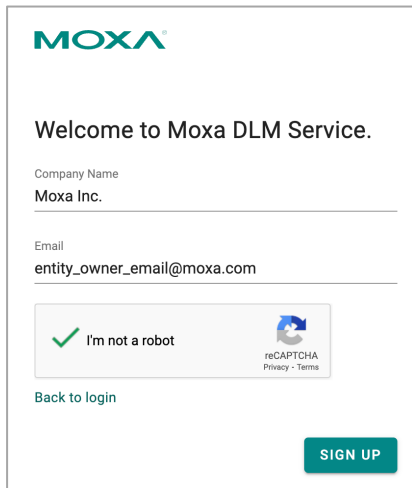
Sign Up DLM Account

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



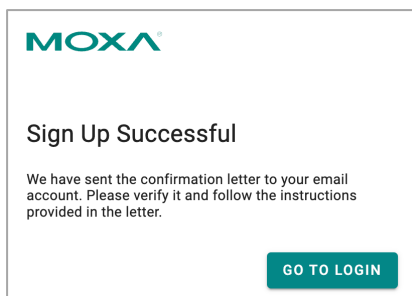
The image shows the 'Sign in Moxa DLM Service' page. At the top is the MOXA logo. Below it, the text 'Sign in Moxa DLM Service' is displayed. There are two input fields: 'Account' and 'Password'. The 'Password' field has a toggle icon for visibility. Below the 'Password' field are two links: 'Forgot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

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



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

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



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

Security

Certificate Center

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

Certificate Center

Home > Security > Certificate Center

My Certificates

Trusted Root CA

Q SEARCH

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

Items per page: 10 1 - 2 of 2 |< < > >|

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.

1. Download the rootCA.cer from **Certificate Center > Trusted Root CA**, and extract the download file (i.e. rootCA.cer).
2. Launch Google Chrome. Click **Settings > Privacy and security > Security > Manage certificates**. Normally, a Certificate dialog will be popped up.
3. Go to **Trusted Publishers**, and click **Import** button to trigger **Certificate Import Wizard** to import rootCA 2.cer.
4. 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**.

Firewall

Home > Security > Firewall

Inbound

System Default

Q SEARCH

Action	Priority ↑	Rule Name	Gateway Port	Protocol	Source IP	Destination IP
Deny	1	default deny all	--	Any	Any	Localhost
Allow	1	https service	8443	TCP	Any	Localhost
Allow	1	ssh service	22	TCP	Any	Localhost
Forward	5	app(opcuaserver) forward port	4840	TCP	Any	172.31.9.7

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

Allowed List

Allowed List

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

Firewall

Home > Security > Firewall

Inbound

System Default

Allowed List

Q SEARCH + ADD RULE

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

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

To create firewall rules, do the following:

Create Allow Rule:

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

Add Rule

Priority
1001

Protocol
☐ Any
☒ TCP
☐ UDP
☐ ICMP

Gateway Port

Rule Name
Port_

Description - optional

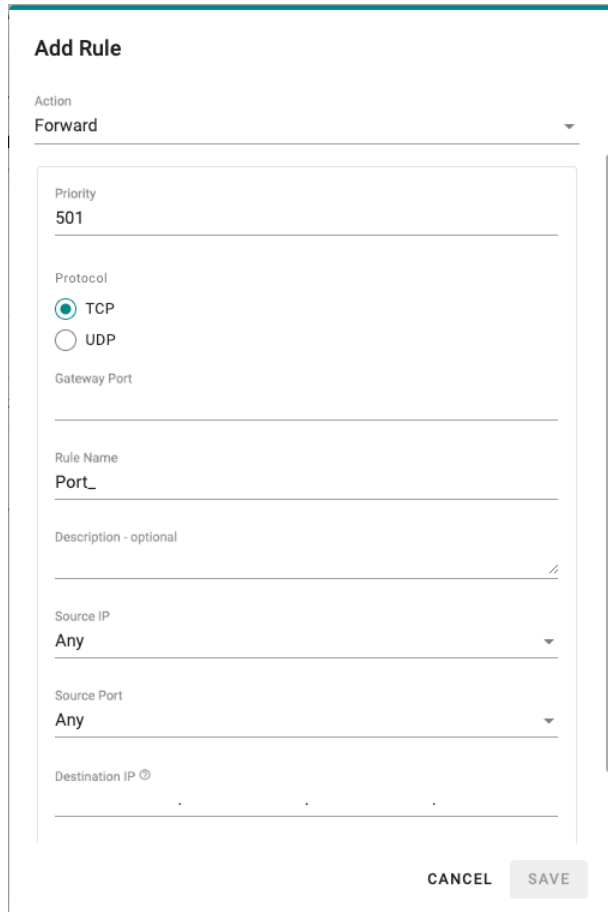
Source IP
Any

Source Port
Any

CANCEL SAVE

Create Forward Rule:

1. Click **+ ADD RULE**.
2. Select action **Forward**.
3. Specify 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.

The top screenshot shows the 'OpenVPN Client' page with the 'Upload profile to make connection.' section. It includes instructions to upload a profile or download a sample, and two buttons: 'UPLOAD PROFILE' and 'DOWNLOAD SAMPLE', which are highlighted by a red box.

The bottom screenshot shows the 'OpenVPN Client' page with the 'OpenVPN Client (V2.4.0)' toggle switch highlighted by a red box. Below the toggle, it shows the 'Current Profile' as 'QA-test-1 (1) (1).ovpn' and a 'MANAGE' button. There is a 'Download the Sample File' link. Below that is a 'Connection Information' section with a 'REFRESH' button. A table shows the connection status as 'Connecting'.

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



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.

Accounts

Home > Security > Account Management > Accounts

Q SEARCH

+ CREATE

Account	Role	Status	
admin (you)	Administrator	🟢 Active	⋮
Josh	Administrator	🟢 Active	⋮
Justin	Administrator	🟢 Active	⋮
Items per page: 10 1 - 3 of 3 < >			

Creating a New User Account

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



NOTE

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

Password Policy	Valid Password
Create New Account Account Josh 4/16 Role Administrator Password ***** Contains at least 8 characters Contains at least 1 number Confirm Password ***** Email - optional CANCEL SAVE	Create New Account Account Josh 4/16 Role Administrator Password ***** Confirm Password ***** Email - optional CANCEL SAVE

Managing Existing User Accounts

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

Accounts

Home > Security > Account Management > Accounts

Q SEARCH + CREATE

Account	Role	Status	
admin (you)	Administrator	Active	
justin	justin	Active	Edit
ricky	ricky	Active	Change Password

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



NOTE

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

Roles

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

MOXA

AIG-101-T

Administrator admin

Modbus Slave

SECURITY

Service Enablement

HTTP/HTTPS

Firewall

Certificate Center

Account Management

Accounts

Roles

MAINTENANCE

Protocol Status

Roles

Home > Security > Account Management > Roles

Q SEARCH + CREATE

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

Items per page: 10 1 ~ 5 of 5

Click **+ CREATE** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions. When you are done, click 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		
		Q SEARCH + CREATE
Role Name		
Administrator (built-in)	1 account	⋮
Users of this role have full permissions. This is a built-in role and can't be modify or delete.		
justin	1 account	⋮
...		

Taking into consideration the security requirements of the AIG-501, we recommend creating these roles with the specified permissions.

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

Maintenance

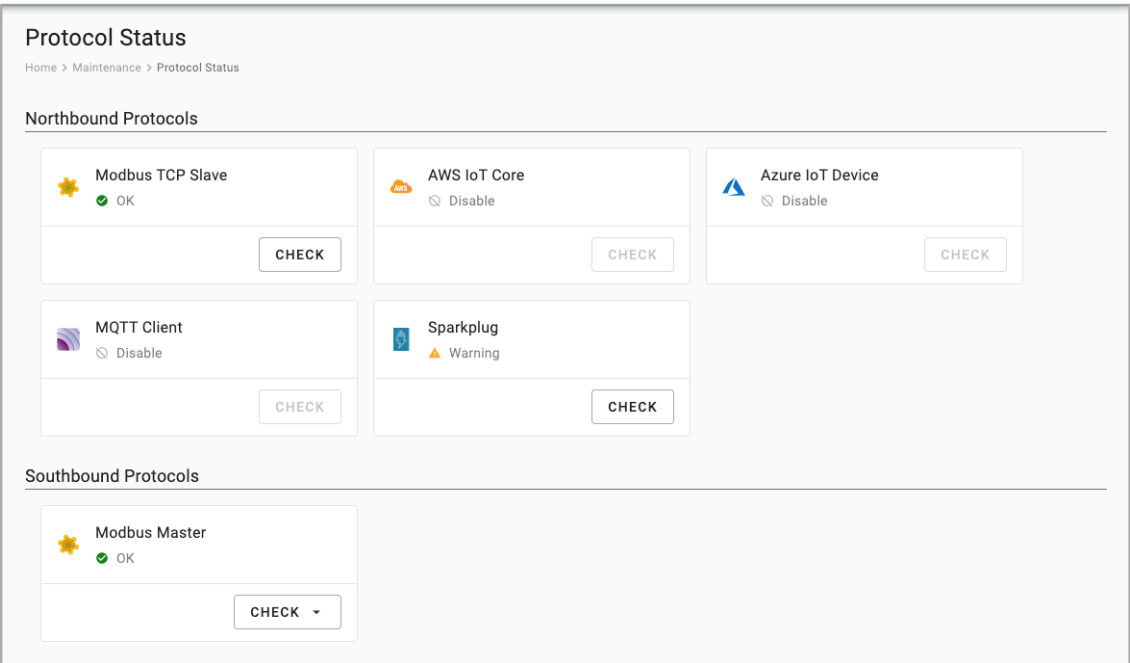
Protocol Status

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

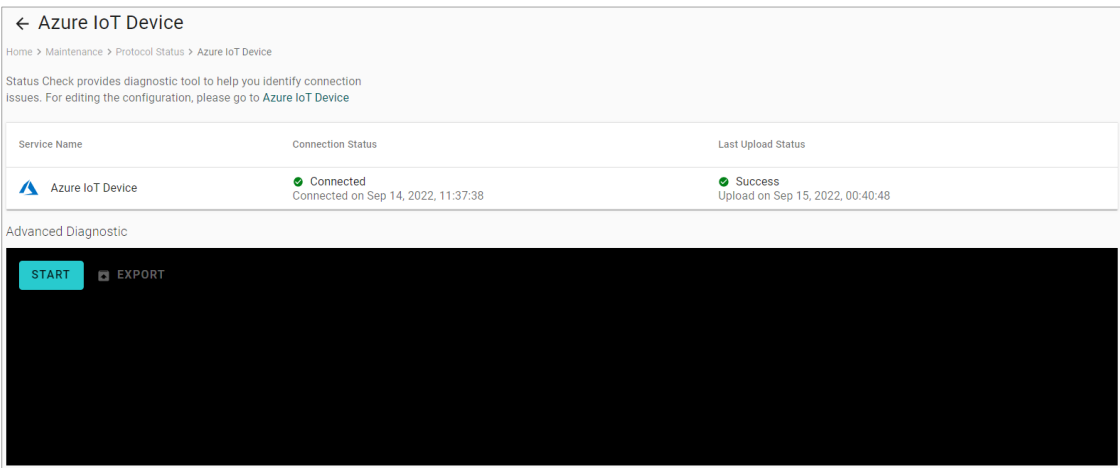
When you access the page, you can see an overview of the status for Northbound Protocols and Southbound Protocols.

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

1. Click **CHECK**.



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



3. View the logs to identify the issue.



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

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

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

General Operation

Reboot

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

Reboot

Home > Maintenance > General Operation > Reboot

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

Automatic Reboot With Scheduler

REBOOT NOW

Reboot

Home > Maintenance > General Operation > Reboot

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

Automatic Reboot With Scheduler

Sep 15, 2022 12:15:00

The device will be rebooted.

REBOOT NOW

EDIT

Create a Reboot Task

Date

Sep 15, 2022

Hour *

12

:

Minute *

15

CANCEL

SAVE

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 screenshot shows the Moxa web interface for the AIG-501-T-AZU-LX device. The page title is "Config. Import/Export". The left sidebar contains a navigation menu with categories: SECURITY (Certificate Center, Firewall, OpenVPN Client, Account Management) and MAINTENANCE (Protocol Status, General Operation, Reboot, Config. Import/Export, Software Upgrade, Reset to Default, Enablement). The "General Operation" menu is expanded, and "Config. Import/Export" is selected. The main content area has two sections: "Export" and "Import". The "Export" section includes a text prompt to encrypt the file, a "Password" field, a "Confirm New Password" field, and an "EXPORT" button. The "Import" section includes a text prompt to click "BROWSE" to select a file, a "BROWSE..." button, a "Password" field, and an "UPLOAD" button.

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

BROWSE...

UPLOAD

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

Software Upgrade

Home > Maintenance > General Operation > Software Upgrade

Upgrade

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

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

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

Upgrade File URL

DOWNLOAD



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 ?

DHCP Server - LAN2

DHCP Server - LAN3

DHCP Server - LAN4

Event Log

HTTP Service

HTTPS Service

Internet Check Alive Service ?

Local Console

Login Policy

NAT Service ?

NTP Service

SD Card

SSH Server

System Log

Network

Cellular1

LAN1

LAN2

LAN3

LAN4

Wi-Fi1

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

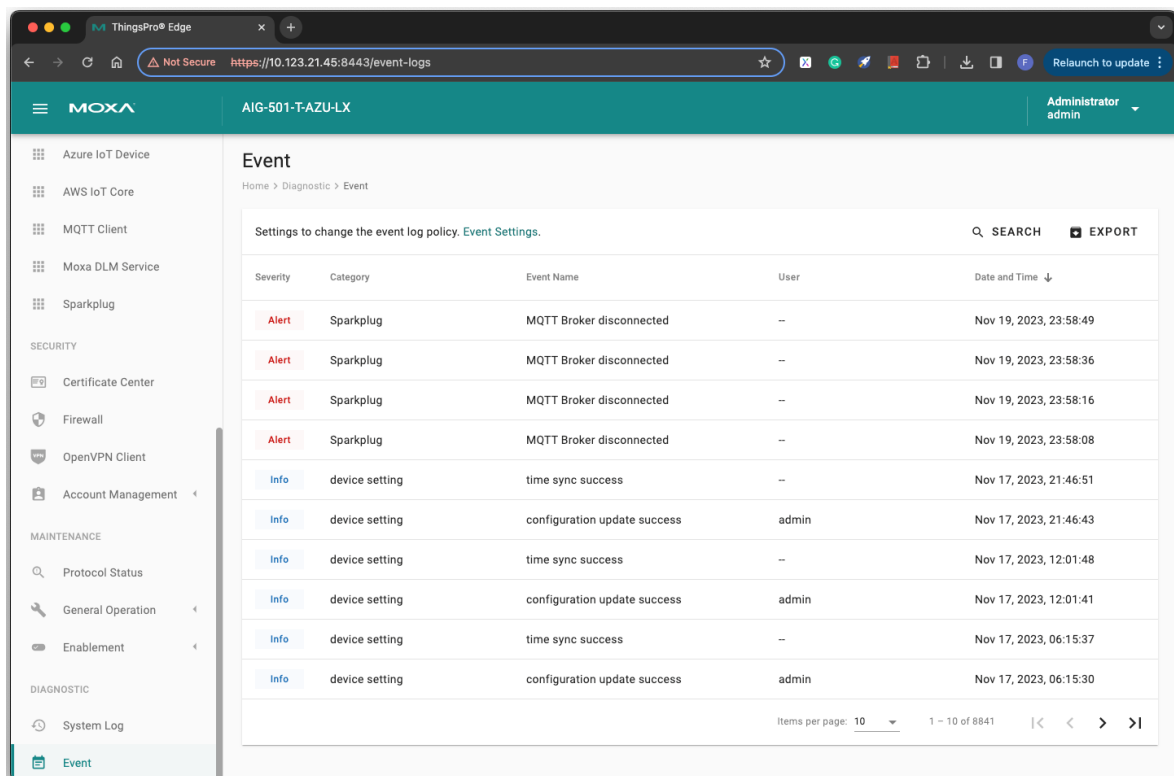
☐ Enable Time to Live

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.

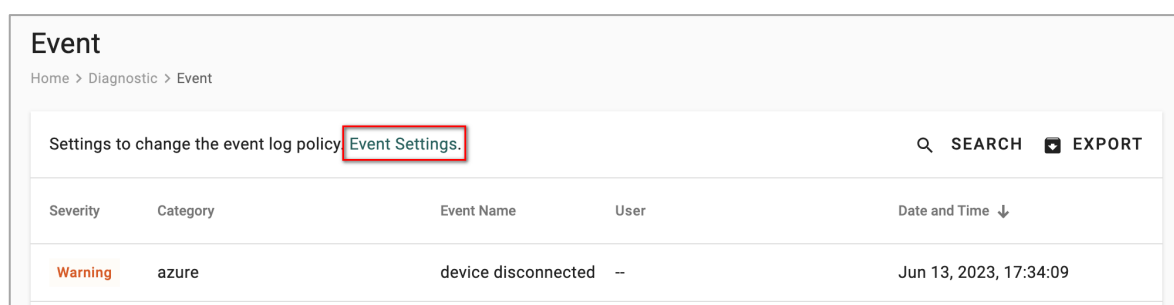


The screenshot shows the Moxa AIG-501-T-AZU-LX Event Logs page. The page has a sidebar with navigation options: Azure IoT Device, AWS IoT Core, MQTT Client, Moxa DLM Service, Sparkplug, SECURITY (Certificate Center, Firewall, OpenVPN Client, Account Management), MAINTENANCE (Protocol Status, General Operation, Enablement), and DIAGNOSTIC (System Log, Event). The main content area is titled 'Event' and shows a list of events. The events are categorized by Sparkplug and device setting. The Sparkplug events are marked as Alert, and the device setting events are marked as Info. The page also includes a search bar and an export button.

Severity	Category	Event Name	User	Date and Time ↓
Alert	Sparkplug	MQTT Broker disconnected	--	Nov 19, 2023, 23:58:49
Alert	Sparkplug	MQTT Broker disconnected	--	Nov 19, 2023, 23:58:36
Alert	Sparkplug	MQTT Broker disconnected	--	Nov 19, 2023, 23:58:16
Alert	Sparkplug	MQTT Broker disconnected	--	Nov 19, 2023, 23:58:08
Info	device setting	time sync success	--	Nov 17, 2023, 21:46:51
Info	device setting	configuration update success	admin	Nov 17, 2023, 21:46:43
Info	device setting	time sync success	--	Nov 17, 2023, 12:01:48
Info	device setting	configuration update success	admin	Nov 17, 2023, 12:01:41
Info	device setting	time sync success	--	Nov 17, 2023, 06:15:37
Info	device setting	configuration update success	admin	Nov 17, 2023, 06:15:30

Configuring Event Log Settings

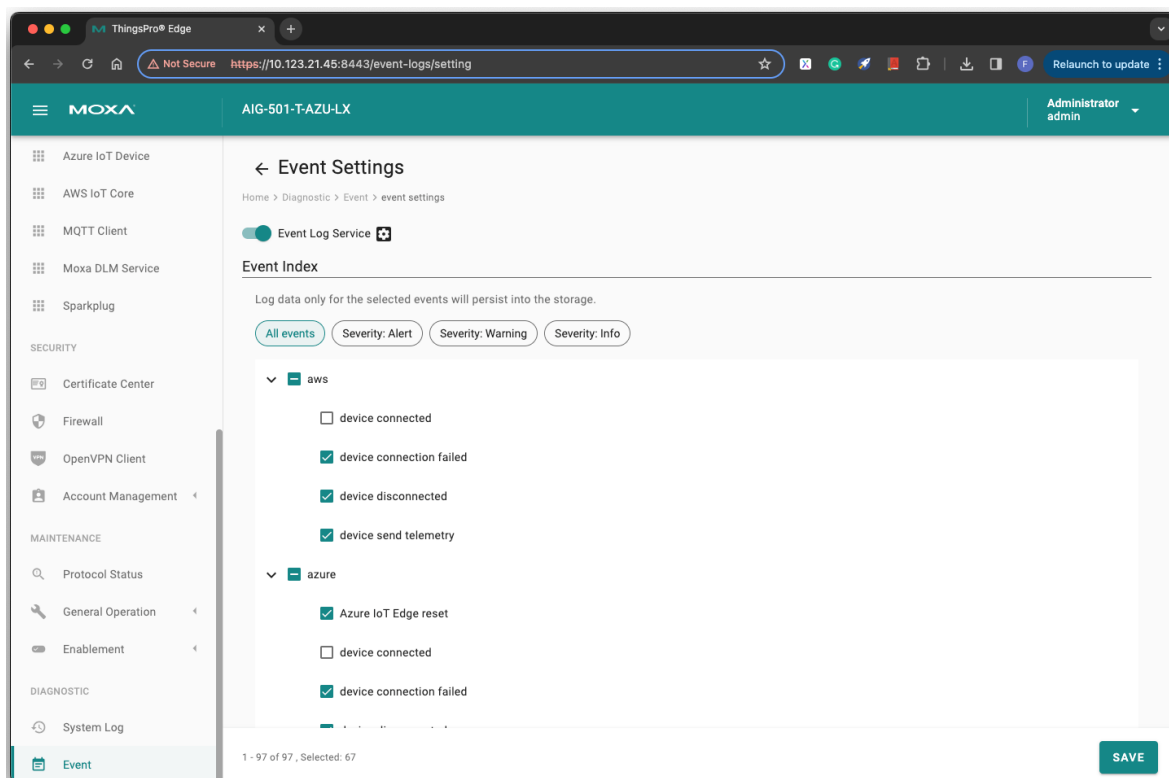
Choose the type of events to be stored, specify where to keep the logs, and the maximum storage size to use. Click the **Event Settings** to access these settings.



The screenshot shows the Moxa AIG-501-T-AZU-LX Event Settings page. The page has a sidebar with navigation options: Azure IoT Device, AWS IoT Core, MQTT Client, Moxa DLM Service, Sparkplug, SECURITY (Certificate Center, Firewall, OpenVPN Client, Account Management), MAINTENANCE (Protocol Status, General Operation, Enablement), and DIAGNOSTIC (System Log, Event). The main content area is titled 'Event' and shows a table with columns for Severity, Category, Event Name, User, and Date and Time. The table contains one event: Warning, azure, device disconnected, --, Jun 13, 2023, 17:34:09. The 'Event Settings' link is highlighted with a red box.

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

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



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

Storage Settings

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

Target Storage

System

Used

2209 MB

3.59GB free of 6.05GB

Limiting Condition

Desired Storage Cache Size (MB) 

100

☐ Enable Time to Live

CANCEL

SAVE

4. Security Hardening Guide

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

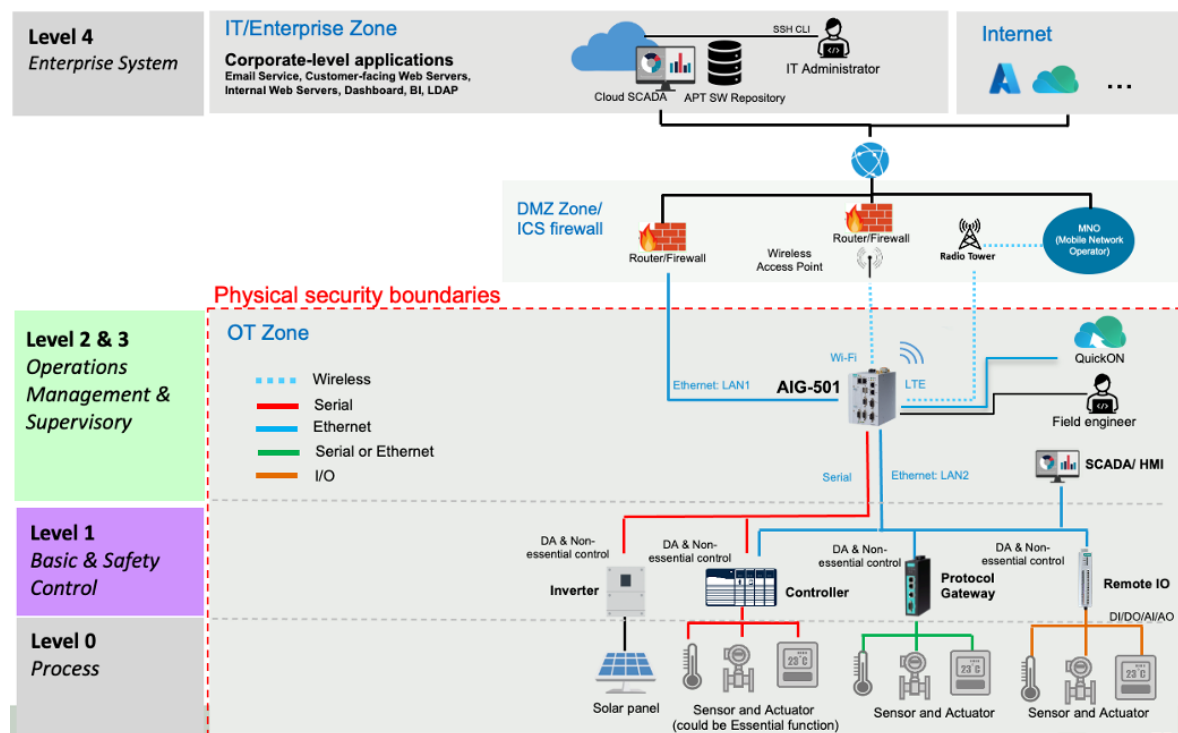
Communication Integrity and Authentication

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

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

Potential Threats and Corresponding Security Measures

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



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

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

Installation

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

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

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

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>
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>
serials	<pre>{ "serials": { "0": { "baudRate": 9600, "dataBits": 8, "device": "/dev/ttyM0", "displayName": "PORT 1", "flowControl": "none", </pre>

Properties	Sample
	<pre> "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>
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>
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", </pre>

Properties	Sample
	<pre> "interface": "", "location": { "lat": 24.984129, "lng": 121.551753 } } </pre>
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": "", "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, } } } </pre>

Properties	Sample
	<pre> "cellId": "", "displayName": "Cellular1", "dns": { "arraySize": 0 }, "enable": false, "status": "sim_pin_locked", "signalStrength": 0, "capabilities": { "sim": 2 }, "iccId": "", "ip": "", "mode": "unknown", "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": "", "simSlot": 2 }, "arraySize": 1 }, "currentProfileName": "Profile-1", "imsi": "", "keepalive": { "enable": true, "intervalSec": 60, </pre>

Properties	Sample
	<pre> "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", "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": "", "simSlot": 2 } } } } } </pre>

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

Desired Properties

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

Properties	Sample
serials	<pre> { "desired": { "serials": { "0": { "mode": "rs232", "stopBits": 1, "baudRate": 9600, "dataBits": 8, "parity": "none", "flowControl": "none", "id": 1 }, "arraySize": 1 } } }</pre>
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>
general	<pre> Update gateway host name: { "desired": { "general": { "hostName": "MyHost" } } } Update gateway description: { "desired": { "general": { "description": "MyDevice" } } }</pre>

Properties	Sample
route	<pre>{ "route": { "priorityList": { "0": "Cellular1", "1": "LAN1", } } }</pre>
gps	Update GPS latitude and longitude by manual mode: <pre>{ "desired": { "gps": { "mode": "manual", "location": { "lat": 11, "lng": 12 } } } }</pre> Update GPS by auto mode: <pre>{ "desired": { "gps": { "mode": "auto", "interface": "GPS1" } } }</pre>
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>
SoftwareUpgrade	<pre>{ "desired": { "softwareUpgrade": { "allowUpdate": true, "allowOverCellular": false, "snapshotBeforeUpdate": true, "autoScan": false, "autoScanExpression": "0 3 * * 1-5" } } }</pre>

Properties	Sample
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 }, "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>