

AIG-101 Series User Manual

Version 2.3, November 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

AIG-101 Series User Manual

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

Copyright Notice

© 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 the Serial Devices	5
Connecting to a Network	5
Access to the Web Console	6
3. Web Console	8
Overview	8
System Overview	8
Network Overview	9
System Configuration	10
System Settings—General	10
System Settings—IP Address	11
System Settings—Cellular	12
System Settings—Serial	14
Moxa Device Extension—ioLogik.....	15
Moxa Device Extension—UPort.....	18
Southbound Protocol	20
Modbus Master.....	20
Tag Hub	37
Tag List.....	37
Tag Management	37
Tag Data Processing	39
Northbound Protocol	42
Azure IoT Device.....	42
AWS IoT Core	46
Generic MQTT Client	50
Modbus TCP Slave	54
Security.....	59
Service Enablement.....	59
HTTP/HTTPS	60
Firewall	60
Certificate Center	61
OpenVPN Client.....	61
Account Management.....	63
Maintenance	66
Protocol Status	66
System Log	68
Event Log	69
General Operation—Reboot.....	71
General Operation - Config. Import/Export	72
General Operation—Firmware Upgrade.....	72
General Operation—Reset to Default.....	73
Device Management.....	73
Moxa DLM Service	73
Sign Up DLM Account.....	75
4. Security Hardening Guide	76
A. Appendix	79
Publish Mode.....	79
B. Additional Documentation	80
Software Downloads	80
Technical Documentation	80
OpenAPI Documentation	80

1. Introduction

Overview

The AIG-101 is an entry IIoT gateway that connects Modbus RTU/ASCII/TCP to the Azure, AWS, and MQTT cloud platforms. To integrate existing Modbus devices onto the cloud platform, use the AIG-101 as a Modbus master to collect data and transmit the data to the cloud. The MQTT standard with supported cloud solutions on the AIG-101 leverages advanced security, configuration, and diagnostics for troubleshooting to deliver scalable and extensible solutions that are suitable for remote monitoring applications such as energy management and assets management.

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

The unit can be powered by connecting a power source to the terminal block:

1. Loosen or remove the screws on the terminal block.
2. Turn off the power source and then connect a 9–36 VDC power line to the terminal block.
3. Tighten the connections, using the screws on the terminal block.
4. Turn on the power source.

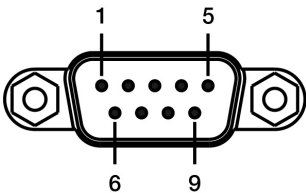
Note that the unit does not have an on/off switch. It automatically turns on when it receives power. It takes a couple of seconds for the system to boot up. Once the system is ready, the SYS LED will light up. Power terminal block pin assignments are shown below:



 **V- V+**
9-36 VDC

Connecting the Serial Devices

The AIG device supports connecting to Modbus serial devices. The serial port uses the DB9 male connector. It can be configured by software for the RS-232, RS-422, or RS-485 mode. The pin assignment of the port is shown below:



Pin	RS-232	RS-422	RS-485
1	DCD	TxD-(A)	–
2	RxD	TxD+(B)	–
3	TxD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	–	–	–

Connecting to a Network

Connect one end of the Ethernet cable to the AIG's 10/100M Ethernet port and the other end of the cable to the Ethernet network. The AIG will show a valid connection to the Ethernet by LAN1/LAN2 maintaining solid green color.

Access to the Web Console

Access to the web console to configure the AIG by just inputting the default IP address (default LAN1: 192.168.126.100; default LAN2: 192.168.127.100) or use AIG QuickON to scan the AIG in the network.

When you use default IP to access, do the following:

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

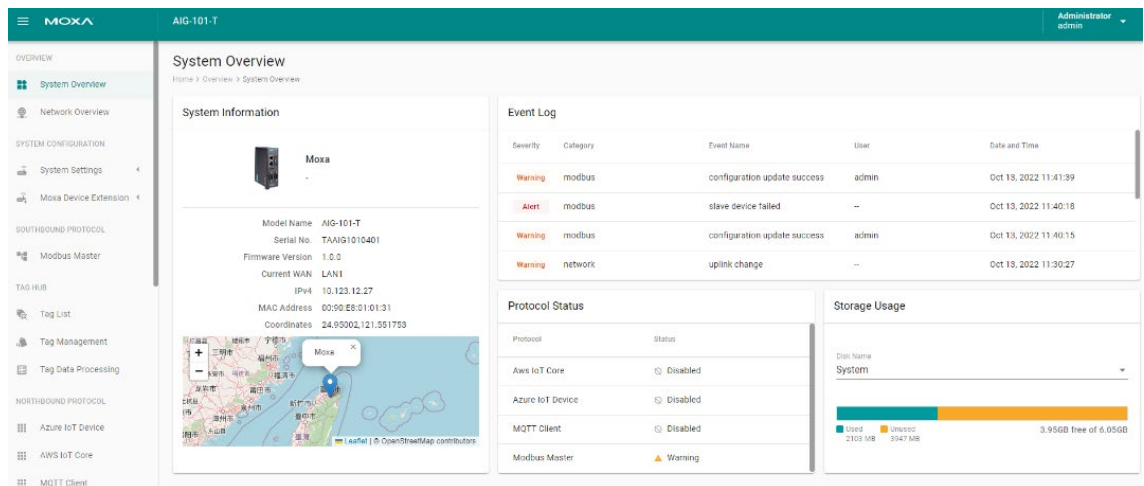
Default account: **admin**

Password: **admin@123**



The login page for the Moxa AIG-101-T web console. It features the Moxa logo at the top, followed by the text 'Sign in to AIG-101-T'. Below this are two input fields: 'Account' with the value 'admin' and 'Password' with the value 'admin@123'. A toggle icon for password visibility is located to the right of the password field. At the bottom right is a green 'SIGN IN' button.

4. Login successful



The dashboard for the Moxa AIG-101-T web console, showing the 'System Overview' page. The left sidebar contains a navigation menu with sections: OVERVIEW, SYSTEM CONFIGURATION, SOUTHBOUND PROTOCOL, TAG HUB, and NORTHBOUND PROTOCOL. The main content area is divided into several panels:

- System Information:** Displays device details including Model Name (AIG-101-T), Serial No. (TAAIG1010401), Firmware Version (1.0.0), Current WAN (LAN1), IPv4 (10.123.12.27), MAC Address (00:00:E8:01:01:31), and Coordinates (24.95002, 121.551753). It also includes a map of the device's location.
- Event Log:** A table showing recent events with columns for Severity, Category, Event Name, User, and Date and Time.
- Protocol Status:** A table showing the status of various protocols.
- Storage Usage:** A bar chart showing disk usage and free space.

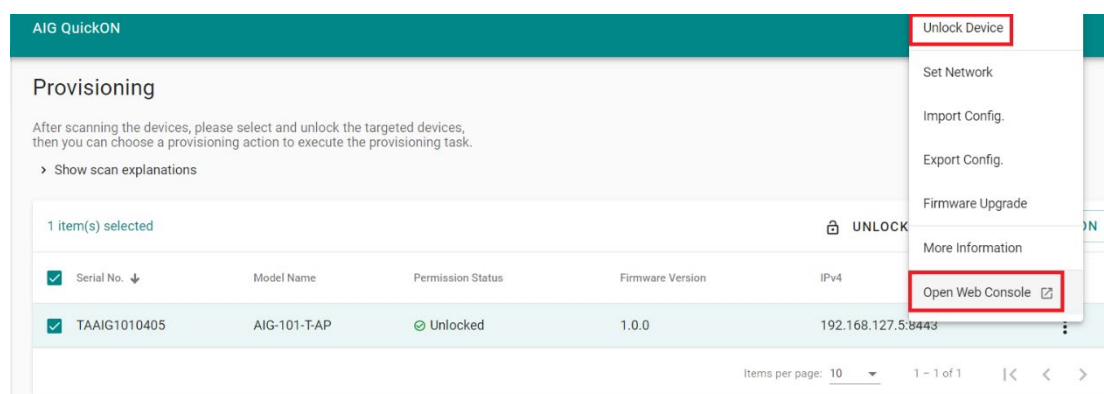
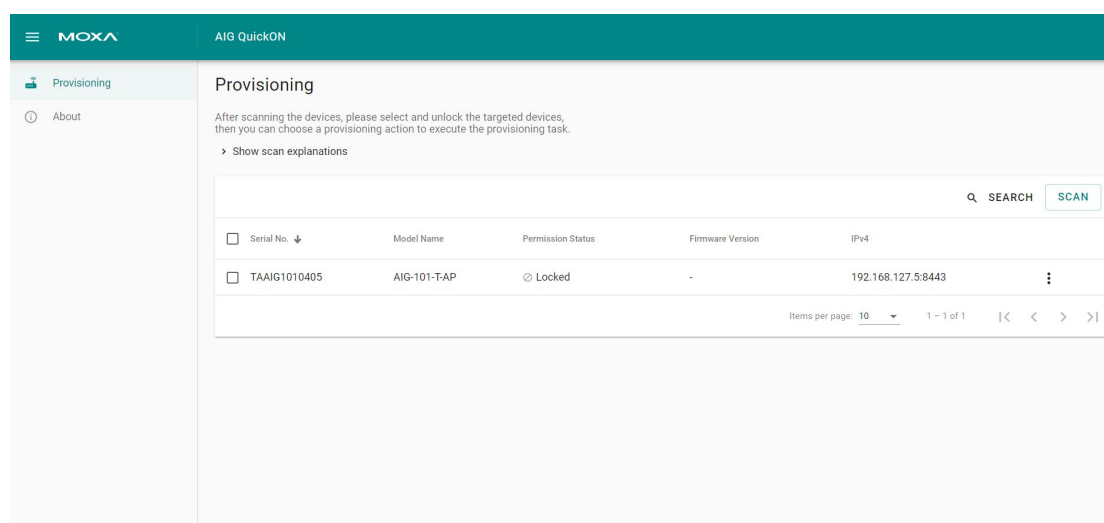
Severity	Category	Event Name	User	Date and Time
Warning	modbus	configuration update success	admin	Oct 13, 2022 11:41:39
Alert	modbus	slave device failed	--	Oct 13, 2022 11:40:18
Warning	modbus	configuration update success	admin	Oct 13, 2022 11:40:15
Warning	network	uplink change	--	Oct 13, 2022 11:30:27

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

Storage Usage: 3.95GB free of 6.05GB

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

1. Run the **AIG-QuickON-x.x.x-xxxxxxxxxxxxx.exe** to install the tool.
2. At the **Welcome** screen, click **Next** to continue.
3. At the **Select Destination Location** window, click **Next** to continue.
You can change the destination directory by first clicking on **Browse...**
4. At the **Select Additional Tasks** window, click **Next** to continue.
5. Click **Install** to copy the software files.
A progress bar will appear. The procedure should take only a couple of seconds to complete. A message will show to indicate that the AIG QuickON has been successfully installed.
6. Go to **Start > Program > AIG QuickON folder > AIG QuickON** and run the tool to automatically scan for AIG devices.
7. If a device is locked, click **Unlock Device** and use the login Account and Password. (Default Account: **admin**, Password: **admin@123**).
8. To access the device, click **Open Web Console**.



3. Web Console

Overview

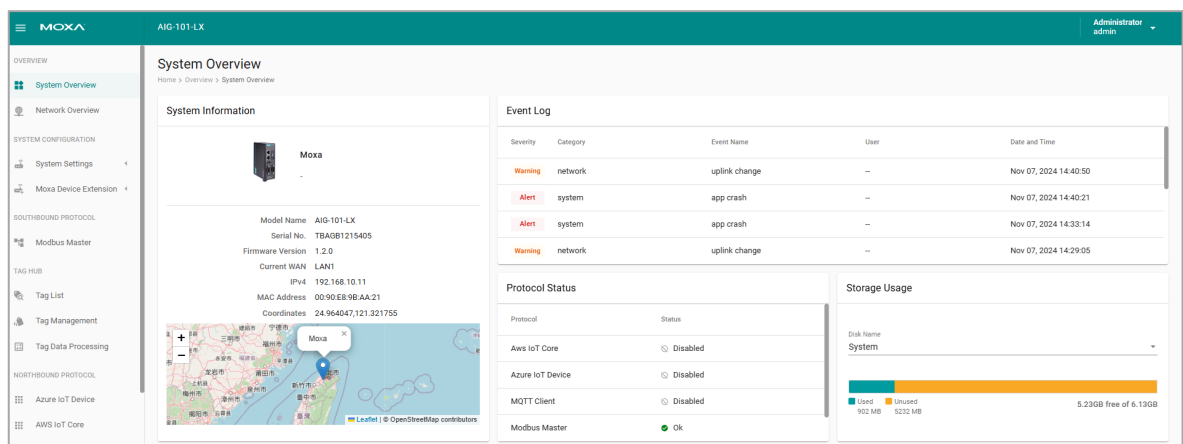
System Overview

This page gives you an overview of the gateway's status.

System information provides basic information such as model name, serial No., and firmware version.

Event logs and protocols status provide useful information for troubleshooting purposes.

Storage usage provides the remaining storage for the system or SD card.



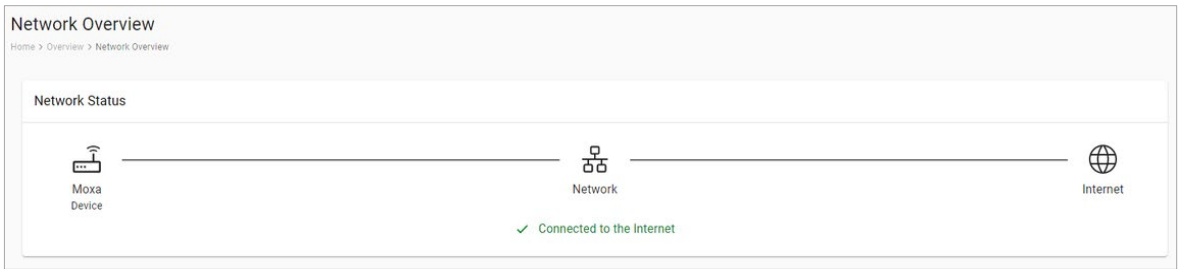
CAUTION

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 Overview

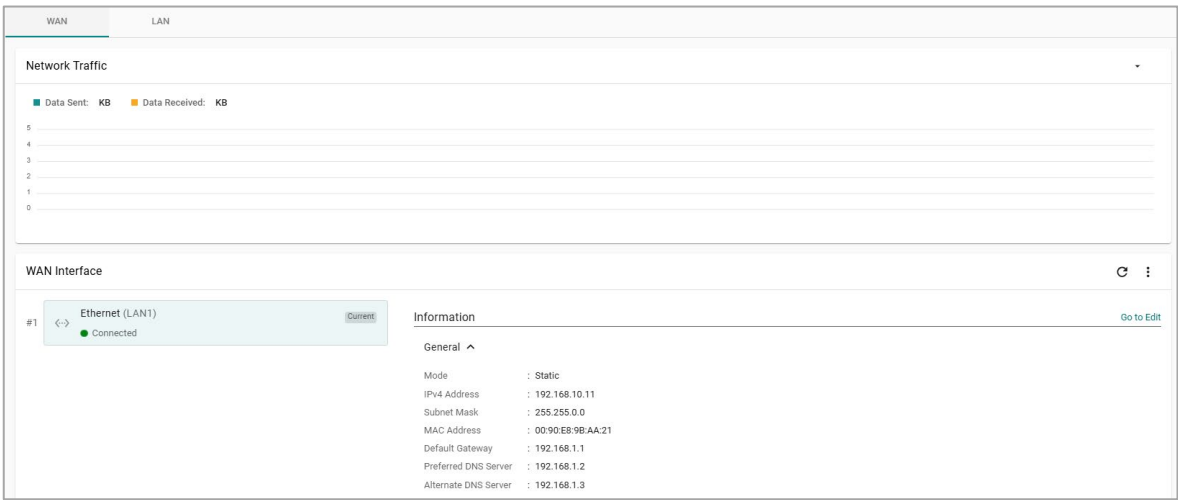
This dashboard displays information on the WAN and LAN interfaces and the network traffic passing through the interfaces.

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



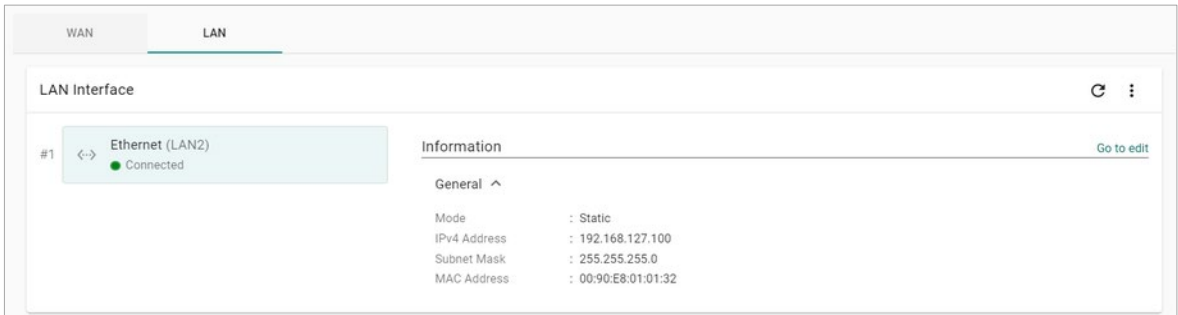
WAN

WAN displays information of the data sent and received through the WAN interfaces. You can select the interface that you want to monitor. In addition, other details on the usage of the WAN interfaces are displayed on the page. The information is refreshed every 10 seconds.



LAN

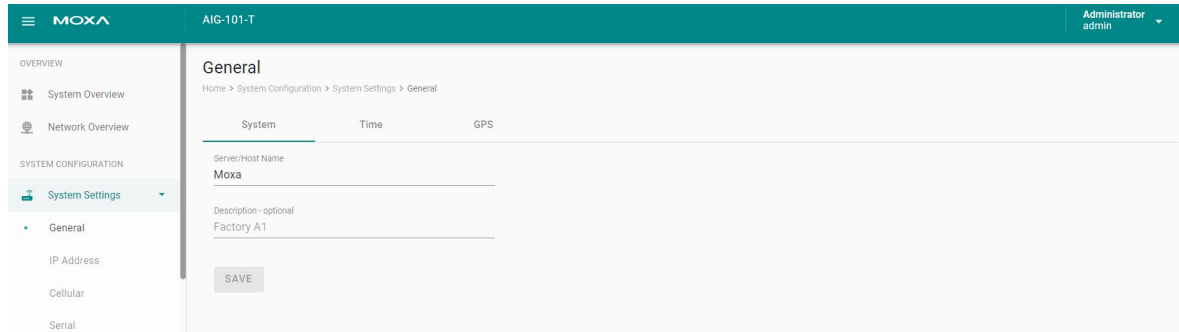
Information on the LAN interfaces is organized under the **LAN** tab and includes information on the usage of the interfaces and the traffic passing through them.



System Configuration

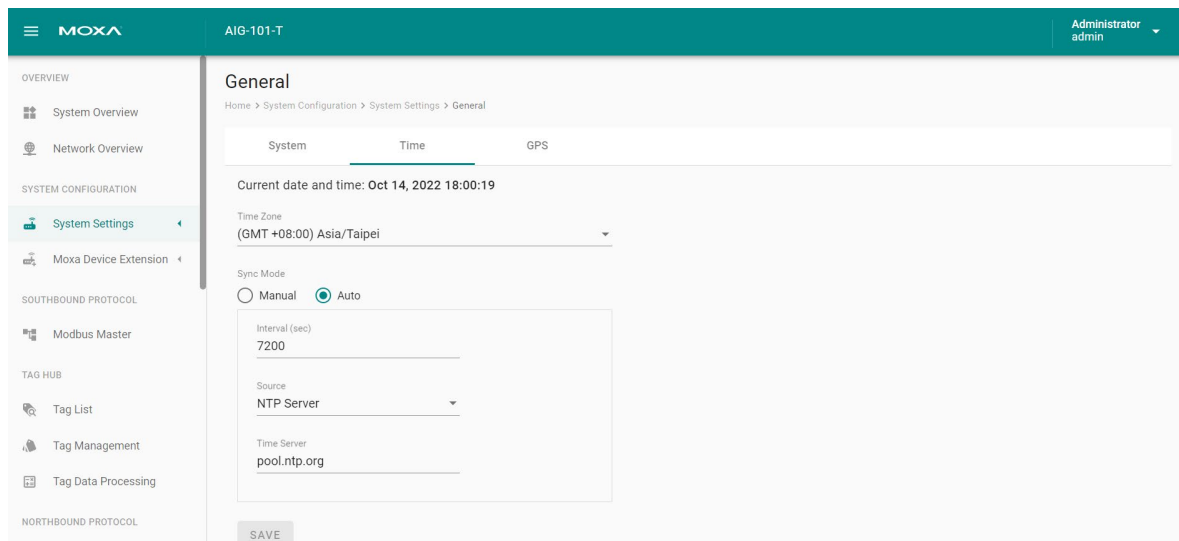
System Settings—General

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



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

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



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

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

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

System Settings—IP Address

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

To configure the network, do the following:

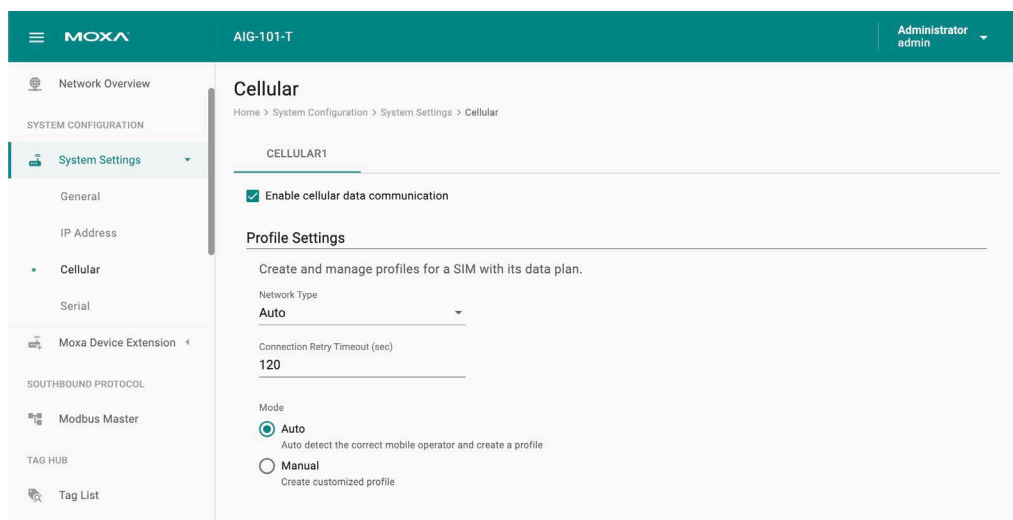
1. Choose **LAN1** or **LAN2** for configuration.
2. Select the **WAN (Wide Area Networks)** or **LAN (Local Area Networks)**.
3. Select **DHCP** or **Static** mode.
4. Configure **IP address**, **Subnet mask**, **Gateway**, and **DNS**.

Parameter	Value	Description
Types of connectivity	WAN LAN Note: LAN2 only supports LAN and not 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: 192.168.126.100 LAN2 default: 192.168.127.100(or other 32-bit number)	The IP (Internet Protocol) address identifies the server on the TCP/IP network
Subnet Mask	Default: 255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
Gateway—optional	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server—optional	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
Alternate DNS Server— optional	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

System Settings—Cellular

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

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.



First, you must select a network type Auto, 3G, or 4G.



NOTE

If you are not sure about the type of network, select Auto (default)

To connect a mobile operator, you can either select **Auto** mode to create a customized profile automatically, or **Manual** mode to create customized cellular profiles. **Create**, **Edit**, or **Delete** cellular profiles here.

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

1. Click **+ CREATE**.
2. Specify a unique **Profile Name**.

3. Specify the target **SIM** card.
4. Enter the **PIN Code** if your SIM card requires it. **NOTE:** Three wrong attempts will lock the SIM card.
5. Choose a **Carrier**. (**NOTE:** This option is displayed only if the cellular module supports carrier switching.)
6. Refer to instructions from your cellular carrier to select **Static** or **Dynamic** APN and configure the corresponding settings.

Create New Profile

Profile Name

SIM
SIM1

Pin Code - optional

Carrier
NTT

PDP CID
1

APN Type
Static

APN

CANCEL DONE

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

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

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

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

☒ Enable check-alive

Target Host: 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—Serial

Go to **System Settings > Serial** to view and configure serial parameters. (Once you connect the UPort 1100/1200 Series into the gateway, the extended serial ports will be shown here.)

To configure serial setting, do the following:

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

Port	Source	Interface	Baud Rate	Parity, Data Bits, Stop Bits	Flow Control
#1 COM1	System	rs422	4800	odd, 8, 1	none
#2 COM2	System	rs422	4800	odd, 8, 1	none
#3 COM3	Uport	rs485-2w	4800	odd, 8, 1	none

Parameter	Value
Interface	rs422
Baud Rate	4800
Parity	odd
Data Bits	8
Stop Bits	1
Flow Control	none

Parameter	Value	Description
Interface	rs-232 rs-422 rs-485-2w	
Baud Rate	300 to 921600	
Parity	none, odd, even, space, mark	
Data Bits	5, 6, 7, 8	
Stop Bits	1, 2	
Flow Control	none hardware software	Hardware: Flow control by RTS/CTS (for RS-232) Software: Flow control by XON/XOFF (for RS-232/422)

Moxa Device Extension—ioLogik

The AIG device can easily extend I/O interfaces by connecting to ioLogik devices. Here are the supported models:

- ioLogik E1210, ioLogik E1210-T
- ioLogik E1212, ioLogik E1212-T
- ioLogik E1214, ioLogik E1214-T
- ioLogik E1211, ioLogikE1211-T
- ioLogik E1213, ioLogikE1213-T
- ioLogik E1240, ioLogikE1240-T
- ioLogik E1241, ioLogikE1241-T
- ioLogik E1242, ioLogikE1242-T



NOTE

A maximum of 4 ioLogik devices can be connected to the AIG.

Before configuration the ioLogik, connect it to **LAN2** of this device, and then go to **Moxa Device Extension > ioLogik**. To extend I/O interfaces, do the following:

1. Click **+ ADD** and go to the wizard setting page.

2. Click the icon to click **Network Settings**, input **Password "moxa"**, change network settings, and click **DONE**.

Edit Network Settings

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

LAN2 IP Address : 192.168.127.100
 LAN2 Subnet Mask: 255.255.255.0

ioLogik

IP Address

192 . 168 . 127 . 253

Subnet Mark

255 . 255 . 255 . 0

CANCEL DONE

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Editing Tag Names

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

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

SCAN

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

CANCEL NEXT >

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

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

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

Password

....

CONFIRM

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

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

Device Name
my_first_io

Poll Interval (Sec)
1

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

7. (Optional) Edit Alias Name.

← Add Remote I/O Device

1 Device Selection 2 Basic Settings 3 Tag Name Editing

Tag Information

Device		
Tag Name	Tag Type	Read/Write
Device_Status	INT32	Read

DI			
Channel	Mode	Alias Name	Tag
DI-0	DI	DI-000000	DI-000000_DL_Status
DI-1	DI	DI-0111111	DI-0111111_DL_Status
DI-2	DI	DI-02345888	DI-02345888_DL_Status

Edit Alias Name

8. Click **DONE**.

ioLogik

Home > System Configuration > Moxa Device Extension > ioLogik

ioLogik

Linked I/O Devices + ADD

my_first_io
Connected

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

MANAGE



NOTE

*Ensure that both devices are under the same subnet mask.

Once you manage the ioLogik, meaning that all the I/O data has been sent to tag hub, you can check the corresponding tags in the **Tag List**.

Tag List				
Home > Tag Hub > Tag List				
Type to search Name + Add a filter				
Provider	Source	Name		
modbus_serial_master	ddd	status	int32	Read
modbus_tcp_master	test	status	int32	Read
remoteio	my_first_io	DI-08_DI_Status	boolean	Read
remoteio	my_first_io	DI-14_DI_Status	boolean	Read
remoteio	my_first_io	DI-13_DI_Status	boolean	Read
remoteio	my_first_io	DI-12_DI_Status	boolean	Read
remoteio	my_first_io	DI-11_DI_Status	boolean	Read
remoteio	my_first_io	DI-10_DI_Status	boolean	Read
remoteio	my_first_io	DI-09_DI_Status	boolean	Read
remoteio	my_first_io	DI-15_DI_Status	boolean	Read

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

ioLogik

Home > System Configuration > Moxa Device Extension > ioLogik

ioLogik

+

ADD

Linked I/O Devices

my_first_io

Connected

Model Name: E1210

Interface: 16xDI

Firmware Version: V3.2

IP Address: 192.168.127.127

Subnet Mask: 255.255.255.0

MAC Address: 00:90:e8:a4:36:e1

Poll Interval (sec): 1

View Tag Information

MANAGE

Edit Poll Interval

Device Authentication

Open Web Console ☒

Remove Device

NOTE

The maximum number of ioLogik units supported is 4. The performance of tag acquisition, processing, and transmission depends on overall system usage, including Modbus, cloud services, and tag processing.

Moxa Device Extension—UPort

The device easily extends serial ports by connecting the UPort 1100/1200 Series to a USB interface on the front panel. These UPort models are supported:

1. UPort 1100
2. UPort 1130, UPort 1130I
3. UPort 1150, UPort 1150I
4. UPort 1250, UPort 1250I*

NOTE

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

AIG-101 Series User Manual

18

After connecting the UPort to this device, go to **Moxa Device Extension > UPort** to view whether the UPort has been detected.

- Once this UPort has been detected, it will show the UPort model name and status in the list.
- If this UPort is not detected, unplug and plug in the UPort, then click **REFRESH**.

UPort

Home > System Configuration > Moxa Device Extension > UPort

Managed UPort Device REFRESH

UPort_1130

Connected

COM Port: 1

REMOVE

When the UPort has been detected, you can go to **System Settings > Serial** to see the new COM port shown as below. The user experience is just like the native COM ports. You can change the serial parameters and configure Modbus settings on the COM port.

Serial

Home > System Configuration > System Settings > Serial

SEARCH REFRESH

Port	Source	Interface	Baud Rate	Parity, Data Bits, Stop Bits	Flow Control	
#1 COM1	System	rs422	4800	odd, 8,1	none	⋮
#2 COM2	System	rs422	4800	odd, 8,1	none	⋮
#3 COM3	Uport	rs485-2w	4800	odd, 8,1	none	⋮

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

Modbus Master

Home > Southbound Protocol > Modbus Master

Modbus Master

Version: 1.5.0

Device Event: Enable

Command Event: Enable

MANAGE

Modbus TCP

TCP

1 Device , 2 Commands

Modbus RTU/ASCII

COM1 (RTU)

1 Device, 3 Commands

COM2 (RTU)

Not configured

COM3 (RTU)

Not configured

If we want to change to another UPort, do the following:

1. Backup Modbus configuration file that is based on UPort's COM port.
2. Unplug **UPort** from the device.
3. Click **REMOVE**.
4. **Plug** in another new UPort.
5. Press **REFRESH**, then the new UPort should be detected.



NOTE

The configuration of serial parameters and Modbus settings on the COM could be deleted. Ensure to do the configuration backup before replacing it with a new one.

Southbound Protocol

Modbus Master

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

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

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

Modbus Master

Home > Protocol > Modbus Master

⚙️

Modbus Master

Version: 1.4.1

Device Event: Enable

Command Event: Enable

MANAGE ▾

Modbus TCP

TCP

Not configured

Modbus RTU/ASCII

COM1 (RTU)

1 Device, 1 Command

COM2 (RTU)

Not configured

DISCARD

APPLY

Modbus TCP

Basic Settings

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

The screenshot shows the 'Basic Settings' dialog box for Modbus TCP. The dialog has three input fields: 'Initial Delay (ms)' with a value of 0, 'Maximum Retry' with a value of 3, and 'Response Timeout (ms)' with a value of 1000. At the bottom right of the dialog are 'CANCEL' and 'SAVE' buttons. In the background, the 'Operation Mode: TCP' is selected, indicated by a red box around the selection icon.

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

Modbus Device Settings

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

The screenshot shows the main configuration page for Modbus TCP. It features a breadcrumb trail: 'Home > Southbound Protocol > Modbus Master > Modbus TCP > TCP'. Below this, 'Operation Mode TCP' is selected. There is a search bar labeled 'Search Command Name'. A prominent 'ADD DEVICE' button is visible. The main area contains a large grey box with a router icon and the text '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

+ ADD COMMAND

Poll Interval (ms) Enable

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

CANCEL

NEXT >

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

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

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 whether the information of the settings is correct.

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

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

Device Name: SE_Meter

Slave ID: 1

Slave IP: 192.168.127.50

Slave Port: 502

Status: Enable

Number of Commands: 1

← BACK

CANCEL

DONE

Then, you will see the setting results.

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

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

Search command name...

ADD DEVICE

SE_Meter
Enable

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

SE_Meter

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

Items per page: 10 1 - 1 of 1

Editing

GO TO APPLY SETTINGS

← TCP ▾

Home > Protocol > Modbus Master > Modbus TCP > TCP

Operation Mode: TCP

Search command name...

ADD DEVICE

SE_Meter
Enable

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

Import Command Configuration

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

Command Configuration

BROWSE...

CANCEL DONE

Editing

GO TO APPLY SETTINGS

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

Modbus Master

Home > Protocol > Modbus Master

Modbus Master
Version: 1.4.1

Device Event: Enable
Command Event: Enable

MANAGE ▾

Modbus TCP

TCP
1 Device, 1 Command

Modbus RTU/ASCII

COM1 (RTU)
1 Device, 1 Command

COM2 (RTU)
Not configured

Editing

DISCARD **APPLY**

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

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

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

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

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

Modbus RTU/ASCII

Basic Settings

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

Serial Basic Settings

Mode
☒ RTU ☐ ASCII

Initial Delay (ms)
0

Maximum Retry
3

Response Timeout (ms)
1000

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

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

CANCEL SAVE

GO TO APPLY SETTINGS

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

Modbus Device Settings

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

← 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

CANCEL NEXT >

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

Step 2. Command

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

The command settings will pop up.

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

Parameter	Value	Default	Description
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	None: not to swap Byte: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. Byte and Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in the tag hub.

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

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

Mode

☐ Manual
☒ Import Configuration

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

Command Configuration

BROWSE...

< BACK

CANCEL

NEXT >

Step 3. Confirm

Review whether the information of the settings is correct.

← Create New Device

✓ Basic Settings

✓ Command Optional

3 Confirm

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

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

← BACK

CANCEL

DONE

Then, you will see the setting results.

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

← COM2 ▾

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

Operation Mode: RTU

🔍 Search command name...

ADD DEVICE

SE_Meter

Enable

Slave ID: 1

SE_Meter

+ ADD COMMAND

IMPORT

EXPORT

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

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

Editing

GO TO APPLY SETTINGS

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

Modbus Master

Home > Protocol > Modbus Master

★ Modbus Master

Version: 1.4.1

Device Event: Enable

Command Event: Enable

MANAGE ▾

Modbus TCP

TCP

1 Device, 1 Command

Modbus RTU/ASCII

COM1 (RTU)

1 Device, 1 Command

COM2 (RTU)

Not configured

Editing

DISCARD

APPLY

Management

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

Modbus Master

Home > Protocol > Modbus Master

★ Modbus Master

Version: 1.4.1

Device Event: Enable

Command Event: Enable

MANAGE ▾

Edit General Settings

Import Configuration

Export Configuration

Modbus TCP

TCP

Not configured

Modbus RTU/ASCII

COM1 (RTU)

1 Device, 1 Command

COM2 (RTU)

1 Device, 1 Command

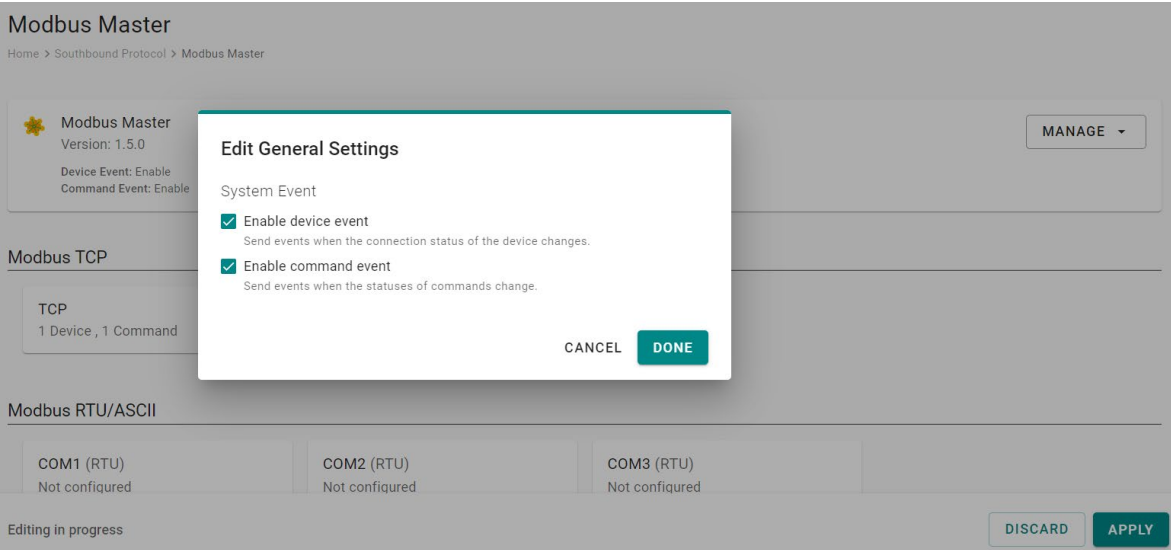
Editing

DISCARD

APPLY

Edit General Settings

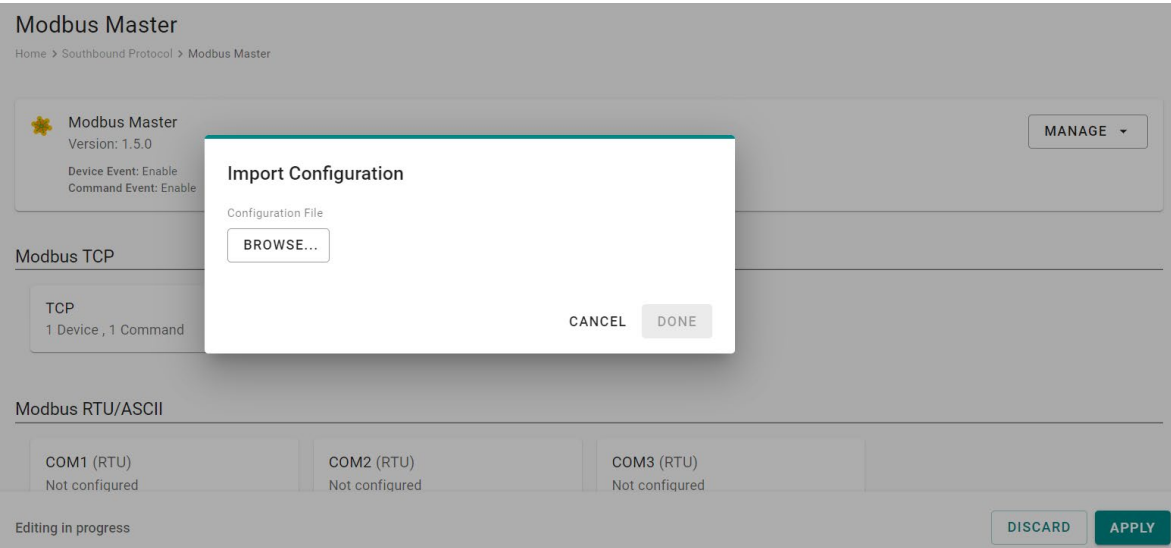
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	Check: If the Modbus communication fails, such as the TCP connection gets disconnected, the Modbus response timeout, the value of the status tag in the tag hub, will change to 1. Uncheck: Disable the function
Enable command event	Check uncheck	Check	Check: If the Modbus command fails, e.g., Modbus exception code is received, the Modbus response timeout, the value of the status tag in the tag hub, will change to 1. Uncheck: Disable the function

Import/Export Configuration

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



master-tcp-faces]																								
@masterTcpMaster	initialDel	retryCour	responseTou																					
1	1	0	3	1000																				
ser-masters]																								
@serMas	confidg	name																						
1	1	modbus_serial_master																						
master-ser-faces]																								
@masterSerMaster	portValue	format	initialDel	retryCour	responseT	frameIn	charInterval																	
1	1	0	0	0	3	1000	0	0																
2	1	1	0	0	3	1000	0	0																
remote-devs]																								
@remoteMasterSer	masterTcp	name	enable	slaveld	slavelpad	slaveTcpPort																		
1	1	1232	1	1	0	0	502																	
2	2	SE_Meter	1	1	0	0	502																	
3		1 GE_Meter	1	1	1	1	502																	
mcmds]																								
@remoteMaster	enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollInterval	swap	fpFunc	fpTou	fpData	scalingFu	intercept	intercept	pointSou	pointSou	pointTarg	pointTarg	tagName	dataType	dataUnit	access	dataSize
1	231	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	231 raw	r		20	
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600	0	1	0	0	1	0	1	Voltage_11	int16	r		
																				Voltage_12	int16	r		
																				Voltage_13	int16	r		
																				Voltage_14	int16	r		
																				Voltage_15	int16	r		
																				Voltage_16	int16	r		
																				Voltage_17	int16	r		
																				Voltage_18	int16	r		

Tag List

Since it shows all the tags in all the devices, use **SEARCH** to review easily.

MOXA

AIG-101-T

Administrator admin

MOXA Device Extension

SOUTHBOUND PROTOCOL

Modbus Master

TAG HUB

Tag List

Tag Management

Tag Data Processing

NORTHBOUND PROTOCOL

Azure IoT Device

AWS IoT Core

MQTT Client

Tag List

Home > Tag Hub > Tag List

SEARCH

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

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

1. Click **+ EDIT TAGS**.

MOXA

AIQ-101-T

Administrator admin

Moxa Device Extension

SOUTHBOUND PROTOCOL

Modbus Master

TAG HUB

Tag List

Tag Management

Tag Data Processing

NORTHBOUND PROTOCOL

Azure IoT Device

AWS IoT Core

MQTT Client

Tag Management

Home > Tag Hub > Tag Management

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

SEARCH

EDIT TAGS

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

Items per page: 100 of 0< < > >

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

83 item(s) selected

CLEAR

SEARCH

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

Items per page: 5

1 - 5 of 83

<<

<

>

>>

CANCEL

SAVE

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

Tag Management

Home > Tag Hub > Tag Management

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

Monitoring tags ⋮

SEARCH

+ EDIT TAGS

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

4. Click **SAVE**.

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

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

Tag Management

Home > Tag Hub > Tag Management

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

Monitoring tags ⋮

SEARCH

+ EDIT TAGS

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

Items per page: 10

1 - 1 of 1

<<

<

>

>>

CANCEL

SAVE

Write value

Provider

modbus_serial_master

Source

123

Name

DO

Type

boolean

Value *

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

CANCEL

SAVE

CANCEL

NEXT >

AIG-101 Series User Manual

38

Tag Data Processing

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

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

1. Click **+ ADD TAG**.

Tag Data Processing

Home > Tag Hub > Tag Data Processing

+ ADD TAG

No.	Tag Name	Sample Rate (sec)	Initial Value	Max Value	Min Value	Description
There is no tag. Click + ADD TAG to create first calculation tag.						

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

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

Add New Tag

1 Basic Setting 2 Sampling Setting 3 Tag Selecting 4 Formula Setting

Tag Name

Initial Value

0

Max Value - optional ?

Min Value - optional ?

Description - optional

CANCEL NEXT >

3. Select a sampling mode and click **NEXT**.

Add New Tag

✓ Basic Setting 2 Sampling Setting ✓ Tag Selecting 4 Formula Setting

Sampling Mode

Sample rate

Interval Setting

Interval (sec)

10

< BACK CANCEL NEXT >

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

Add New Tag

☒ Basic Setting
 ☒ Sampling Setting
 ☒ 3 Tag Selecting
 ☐ 4 Formula Setting

Select a max of 8 parameters (tags) along with the assigned code (A, B, C, ...). You can edit the formula using the code in the next step.

prvd1 (1)

src1 (9)

☒ tag1
 ☒ tag10
 ☐ tag11
 ☐ tag110

A	prvd1/src1/tag1
B	prvd1/src1/tag10
C	--
D	--
E	--

< BACK
 CANCEL
 NEXT >

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

Add New Tag

☒ Basic Setting
 ☒ Sampling Setting
 ☒ Tag Selecting
 ☒ 4 Formula Setting

Math
 Lists
 Tag

Demo = A 'value' + B 'value'

A	prvd1/src1/tag1
B	prvd1/src1/tag10
C	--
D	--
E	--
F	--
G	--

< BACK
 CANCEL
 SAVE

- Click **SAVE** and you will see the new tag in the list.

Tag Data Processing

Home > Tag Hub > Tag Data Processing

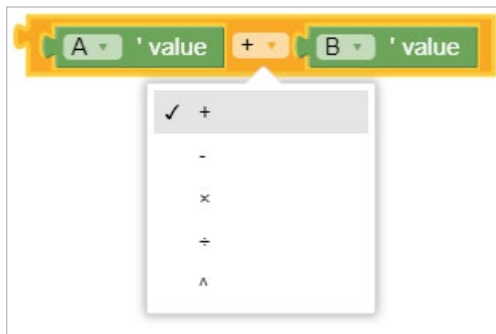
+ ADD TAG

No.	Tag Name	Sample Mode	Initial Value	Max Value	Min Value	Description
1	Demo	Sample rate	0	--	--	--

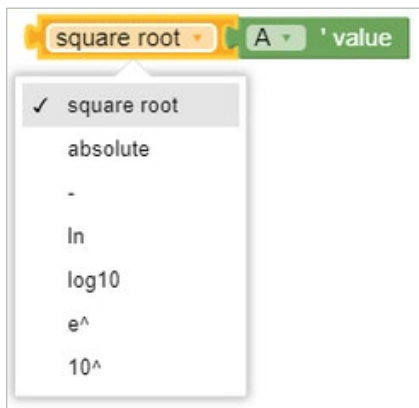
Items per page: 10 1 - 1 of 1

The supported formulas are:

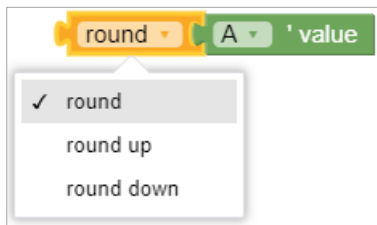
- **addition(+), subtraction(-), multiplication(x), division(/), and power(^)**



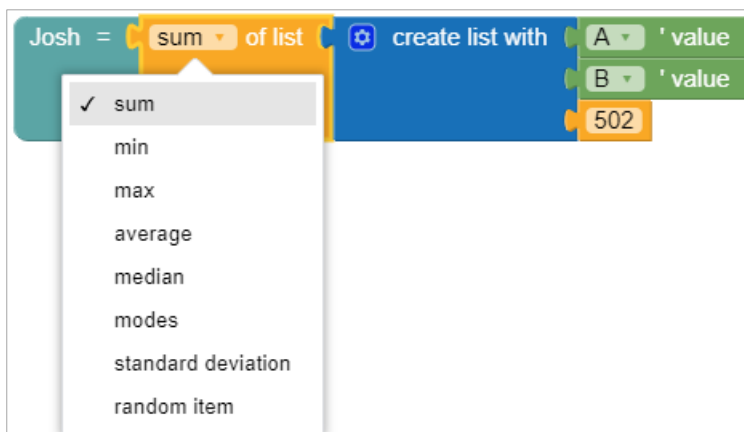
- **square root, absolute, negative(-), natural logarithm(ln), 10 logarithm(log10), power by Euler's number(e^), power by 10(10^)**



- **round, round up, round down**



- **sum, minimum, maximum, average, median, modes, standard deviation, random items**





NOTE

A maximum of 32 tags can be processed at once.
Each tag processing operation can handle up to 8 tags for calculations.

Northbound Protocol

Azure IoT Device

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

Note that you will need to register an Azure account to manage the Azure IoT Device service for your IIoT application.

To create the Azure IoT Device connectivity, follow the steps below:

1. Click  to set up the connection.
2. Enter **Connection String**.
3. Select a **Connection Protocol**.
4. Select an **Authentication Type**.

When using the X.509 authentication type, you only need to enter the HostName (FQDN) in the **Connection String**. TPE will automatically complete the connection string based on the following format:

HostName={iothub name}.azure-devices.net;DeviceId={device ID};x509=true

{iothub name}: The connection string parameter that you provide
{device ID}: Abstracted from the cn of the subject in X.509 certificate.

5. (optional) Upload X.509 Certificate and Private Key.
6. (optional) Upload a trusted root CA to connect to a transparent gateway (e.g., Azure IoT Edge).
7. Click **SUBMIT**.

Connection Settings

INFO: You must configure the provisioning settings for your device before you start the Azure IoT Device service.

Device Connection

Connection String

HostName=thingspro-IoTHub-newTwin.azure-devices.net;DeviceId=TingAID;SharedAccessKey=Vq2qbpoo7I/PUFt0s

Connection Protocol

mqtt (Port: 8883)

Authentication Type

☒ Symmetric Key ☐ X.509 Certificate

Trusted Root CA - optional

BROWSE...

CANCEL

SAVE

Telemetry Message

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

1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.

The screenshot shows the 'Create New Telemetry Message' dialog with four steps: 1. Basic Settings, 2. Message Tags, 3. Custom Payload Optional, and 4. Properties Optional. Step 1 is active. It includes a checkbox for 'Enable Telemetry Message' which is checked. Below it is the 'Output Topic' field with the value 'Demo'. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. Below these are two input fields: 'Publish Interval (sec)' with the value '60' and 'Sampling Mode' with a dropdown menu showing '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.

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 includes an 'Info' box stating 'Select one or more tag providers and select tags to map data.' Below this is a 'Providers' dropdown menu showing 'modbus_serial_master, modbus_tcp_master'. A modal window is open showing a list of tags with checkboxes: 'Power2' and 'Power1' are checked, while 'device_info_t27' and 'device_info_t26' are unchecked. The modal has 'SELECT ALL' and 'CLEAR' buttons. At the bottom of the modal, it says 'Total: 41, Selected: 2' and a 'DONE' button. The main dialog has 'CANCEL' and 'NEXT >' buttons at the bottom right.

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 Message Tags **3 Custom Payload** 4 Properties

Optional Optional

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

☒ Basic Editing ☐ Advanced Editing

Tag Pre-merge Format

Message Result

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

< BACK CANCEL NEXT >

8. Click **NEXT**.

9. (Optional) Enter Property Key and Value.

Create New Telemetry Message

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

Optional Optional

Property Key Property Value

+ Add another

< BACK CANCEL SAVE

10. Click **SAVE**.



NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.



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

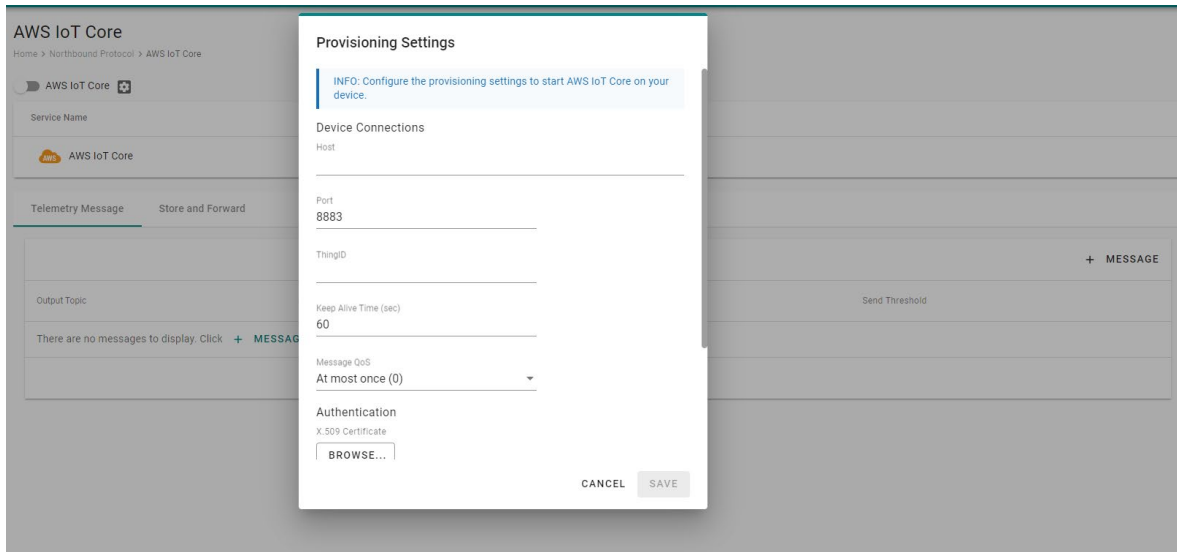
Storage Full Policy ⓘ
☒ Drop Oldest ☐ Drop Newest

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

AWS IoT Core

Go to **AWS IoT Core** and enable or disable the AWS IoT Core. To create the AWS IoT Core connectivity, follow the steps below:

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



Telemetry Message

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

1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.

The screenshot shows the 'Create New Telemetry Message' interface with three steps: 1. Basic Settings, 2. Message Tags, and 3. Custom Payload Optional. Step 1 is active. It includes a checkbox for 'Enable Telemetry Message' which is checked. Below it is the 'Output Topic' field with the value 'Demo'. A progress indicator shows '4/128'. The 'Publish Mode' section has three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. Below this is a 'Publish Interval (sec)' input field with the value '60'. There is a 'Sampling Mode' dropdown menu currently set to 'All Changed Values'. At the bottom of this section is a checkbox for 'Custom sampling rate from acquired data' which is unchecked. At the bottom right of the form are 'CANCEL' and 'NEXT >' buttons.

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

The screenshot shows the 'Create New Telemetry Message' interface with three steps: 1. Basic Settings, 2. Message Tags, and 3. Custom Payload Optional. Step 2 is active. It includes a 'Select Tags' section with an info message: 'INFO: Select one or more tag providers and select tags to map data.' Below this is a 'Providers' dropdown menu with the value 'events, modbus_serial_master, modbus_tcp_master'. To the right of this dropdown is a label '86 Tags'. Below the providers is a 'Selected Tags' dropdown menu with the value '123_12 (+10 others)'. At the bottom left of the form is a '< BACK' button. At the bottom right are 'CANCEL' and 'NEXT >' buttons.

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

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

Create New Telemetry Message

Basic Settings Message Tags Custom Payload Optional

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

☒ Basic Editing ☐ Advanced Editing

Tag Pre-merge Format

Message Result

```
1 {
2   "tags": {
3     "modbus_tcp_master": {
4       "SE_meter": {
5         "t1": {
6           "values": [
7             {
8               "updateTimeStamp": "2020-02-14T05:53:23Z",
9               "value": 11
10            }
11          ]
12        },
13        "t2": {
14          "values": [
15            {
16              "updateTimeStamp": "2020-02-14T05:53:23Z",
17              "value": 11
18            }
19          ]
20        },
21        "t3": {
22          "values": [
```

< BACK CANCEL SAVE

8. Click **SAVE**.



NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.



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

Generic MQTT Client

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



NOTE

You must create a connection first and then 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 'General' tab is also visible. The 'SSL/TLS' section has a checkbox 'Enable SSL/TLS' which is checked. Below it, there is a 'TLS Version' section with three radio buttons: '1.2' (selected), '1.1', and '1.0'. There are three 'BROWSE...' buttons for 'Client Certificate - optional', 'Client Key - optional', and 'Trusted Root CA - optional'. At the bottom, there is an 'Ignore Server Certificate' checkbox which is unchecked. The 'CANCEL' and 'SAVE' buttons are at the bottom right.

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

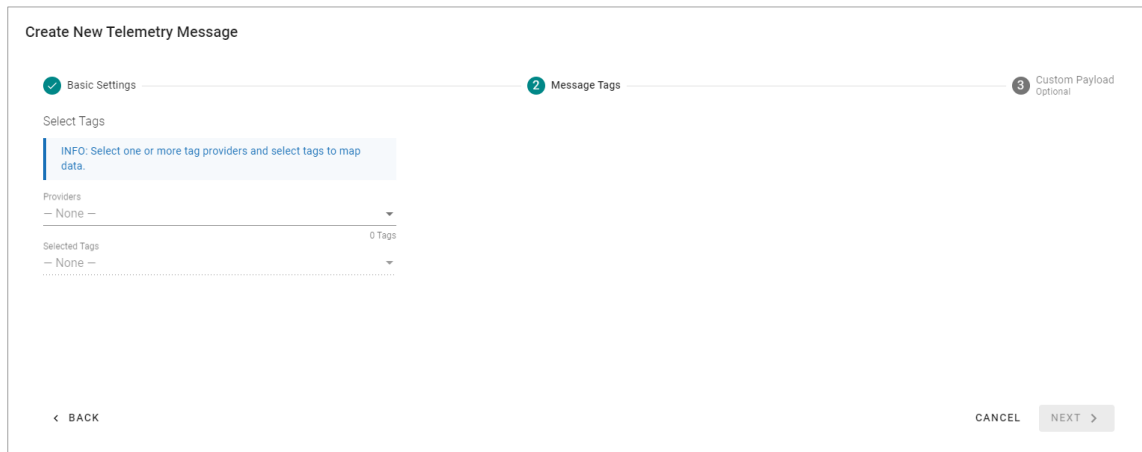
Once an MQTT Broker has been created, create a new telemetry message by following the steps below:

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

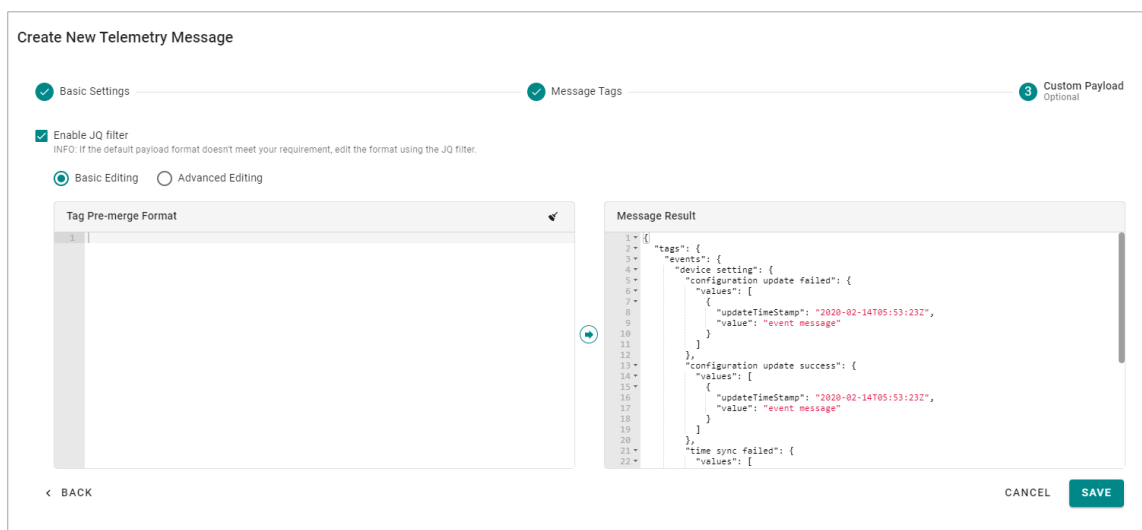
The screenshot shows the 'Create New Telemetry Message' dialog. It has a progress bar at the top with four steps: '1 Basic Settings', '2 Message Tags', '3 Custom Payload Optional', and '4 Properties Optional'. The 'Basic Settings' step is active. There is a checkbox 'Enable Telemetry Message' which is checked. Below it, the 'Output Topic' is 'Demo'. There is a 'Publish Mode' section with three radio buttons: 'By Interval' (selected), 'Immediately', and 'By Size'. Below that, there is a 'Publish Interval (sec)' input field with the value '60'. There is a 'Sampling Mode' dropdown menu with the value 'All Changed Values'. There is a checkbox 'Custom sampling rate from acquired data' which is unchecked. The 'CANCEL' and 'NEXT >' buttons are at the bottom right.

3. Select a Publish Mode (for details, see Publish Mode).
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.

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



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



8. Click **SAVE**.

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: <https://stedolan.github.io/jq/manual/>.



NOTE

The initial message generated may not include all the tags that you select. However, the subsequent messages will include all the selected tags. This is because the system requires an additional process to be completed for the initial message, which may result in some tags not being included in the first message.



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.

ADD CONNECTION

test.mosquitto.org
● Connected

Telemetry Message

Store and Forward

Remote API Invocation

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

☒ Enable Store and Forward

Storage Setting

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

Target Disk
System (3.59GB free of 6.05 GB)

Maximum Storage Cache (MB) ⓘ
10

Storage Full Policy ⓘ
☒ Drop Oldest ☐ Drop Newest

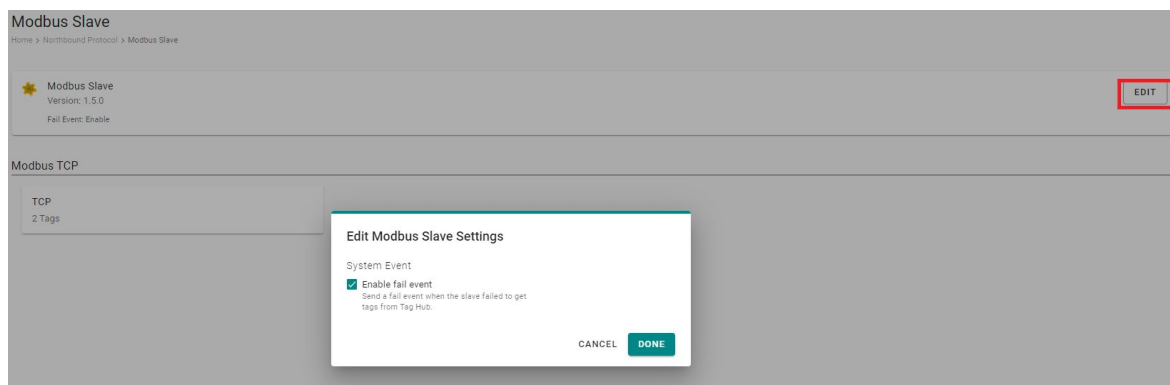
Advanced Storage Limitation

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

SAVE

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.

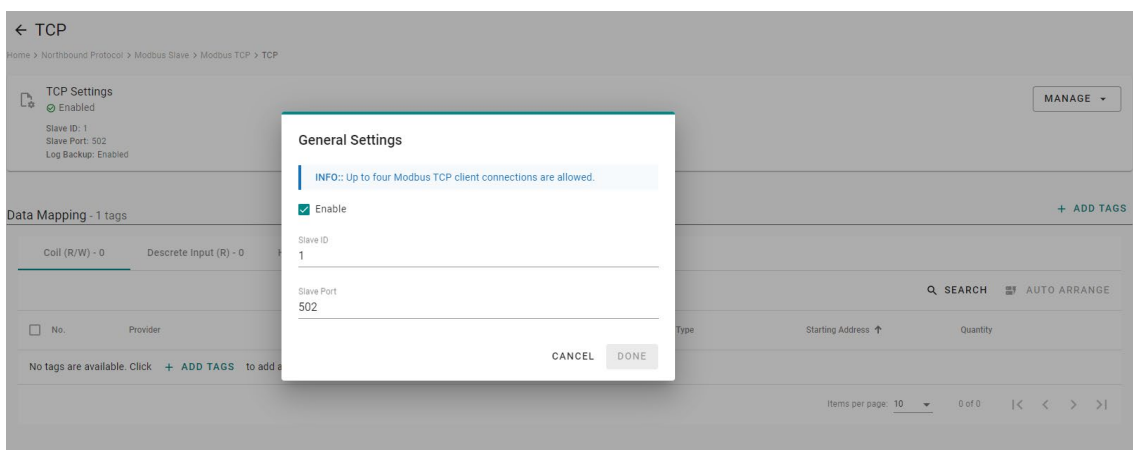


To create a Modbus TCP server (slave), following the steps below:

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).

← TCP

Home > Northbound Protocol > Modbus Slave > Modbus TCP > TCP

TCP Settings

Enable

MANAGE

Slave ID: 1

Slave Port: 502

Backup Logging: Disable

Data Mapping - 2 Tag(s)

+ ADD TAGS

Coil (R/W) - 0

Discrete Input (R) - 0

Holding Register (R/W) - 0

Input Register (R) - 2

SEARCH

AUTO ARRANGE

No.

Provider

Source

Tag Name

Tag Data Type

Start Address ↑

Quantity

No tags yet. Click + ADD TAGS button to add the first tag.

Items per page: 10

0 of 0

|<

>|

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

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

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

Data Mapping - 4 Tag(s)

+ ADD TAGS

Coil (R/W) - 0

Discrete Input (R) - 0

Holding Register (R/W) - 0

Input Register (R) - 4

SEARCH

AUTO ARRANGE

No.

Provider

Source

Tag Name

Tag Data Type

Start Address ↑

Quantity

☐

1

modbus_serial_master

ddd

device_info_12

int16

00000

1

⋮

☐

2

modbus_serial_master

ddd

Power1

int16

00001

1

⋮

☐

3

modbus_serial_master

ddd

Power2

int16

00002

1

⋮

☐

4

modbus_serial_master

ddd

status

int32

00003

2

⋮

Items per page: 10

1 - 4 of 4

|<

>|

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

Auto Arrange

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

Item Sorting Priority

☒ Provider → Source → Tag Name

☐ Provider → Tag Name → Source

Sort Order

Ascending

CANCEL

DONE

Backup Logging

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



NOTE

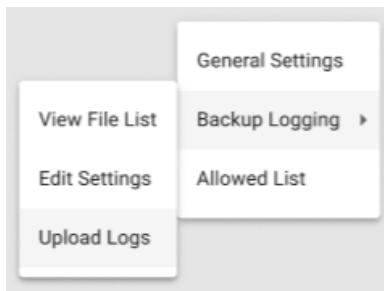
If the data is stored in an SD card, ensure that the SD card is installed before enabling this function. If you replace the SD card, reboot your device and confirm that the backup function is working properly. The SD card should have at least 1 GB free space.

To enable log backups, do that following:

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

To upload log files via FTP, do the following:

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



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

Upload Logs

☐ Enable FTP/SFTP log upload

Upload Method

☒ FTP ☐ SFTP

Upload Information

Server

Port

22

1 ~ 65535

Path

/

Username

Password

Upload Interval (min)

10

Upload interval can be 10 ~ 1440

CHECK CONNECTION

Info

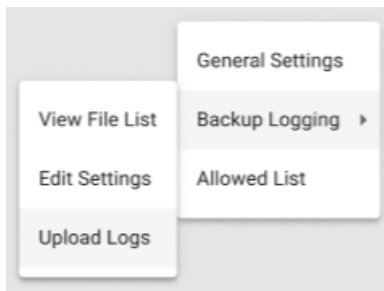
Click the "CHECK CONNECTION" to check connectivity to the remote server and ensure your connector is properly configured.

CANCEL

SAVE

To upload files via SFTP, do the following:

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



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

Upload Logs

☒ Enable FTP/SFTP log upload

Upload Method

☐ FTP ☒ SFTP

Upload Information

Server	Port
111.11.11.11	22

Path

/home/stfpuser/stage

Username

sftpuser

Authentication Method

Upload SSH key

SSH Key

5bb65fe6266bd6b6
8f71cb897b90d4b7

Upload Interval (min)

10

CHECK CONNECTION

Info

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

CANCEL SAVE

Modbus Capability:

Max. # of Serial Slave Device 31

Max. # of TCP Slave Device 64

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

Max. # of Tags for Modbus Master 1500

Max. # of Tags for Modbus Slave 2048

Max. # of Commands for a Slave Device 256

Max. # of Commands for a TCP Slave Device 2048



NOTE

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

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

Security

Service Enablement

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

Service Enablement

Home > Security > Service Enablement

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

System

Event Log

HTTP Service

HTTPS Service

Internet Check Alive Service ?

Login Policy

NAT Service ?

NTP Service

SD Card

System Log

Network

Cellular1

LAN1

LAN2

Provision Service

AIG QuickON

HTTP/HTTPS

To ensure secure access to the web console of the device, we strongly recommend you **disable HTTP** and **enable HTTPS**. To do this, go to **Security > HTTP/HTTPS**.

The default setting for **HTTP redirect to HTTPS** is **Enabled** (starting with firmware version v1.3.0) to enhance security capabilities. To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority. If there are no imported certificates, the AIG Series can generate the "AIG Series Root CA for HTTPS" certificate instead.

HTTP/HTTPS

Home > Security > HTTP/HTTPS

HTTP Service

☐ Enable HTTP Service

HTTPS Service

☒ Enable HTTPS Service

Port Number
8443

Import TLS/SSL Certificate

Certificate
 default.crt

Private Key
 default.key

Firewall

If we want to see the ports, protocols, and services that are used to communicate between the AIG Series and other devices, go to **Security > Firewall** to view all the information.

Firewall

Home > Security > Firewall

Inbound

System

SEARCH

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

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

Certificate Center

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

rootCA.cer is used to sign the HTTP SSL X.509 certificate, default.crt. You can download this root CA and import it to your client devices to enable trust for the HTTPS connection between clients and the AIG. To import to Google Chrome, you can refer to the below link:

https://docs.moxa.online/tpe/users-manual/security/certificate_center/#import-rootcacer-to-google-chrome

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

<

<

>

>

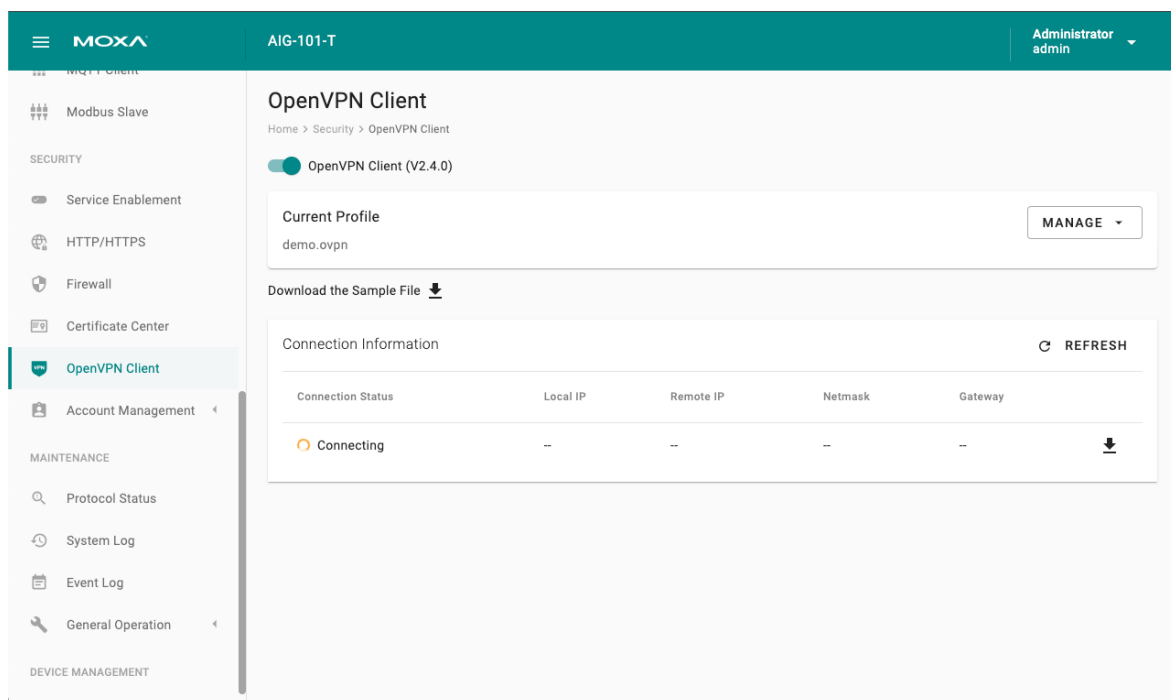
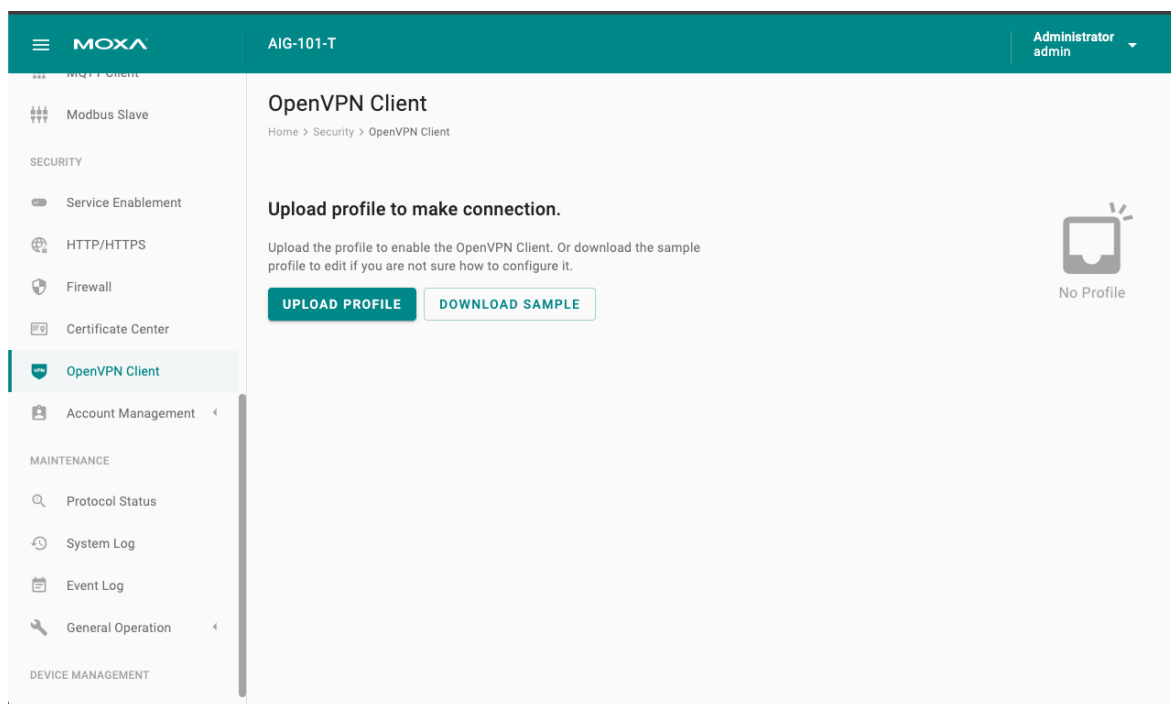
OpenVPN Client

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.
2. Import the OpenVPN profile.
You should see it listed in the OpenVPN client.
3. Click the button to enable OpenVPN client to connect.

If the connection is successful, you will be connected to the VPN network, and your internet traffic will be encrypted and routed through the VPN server.

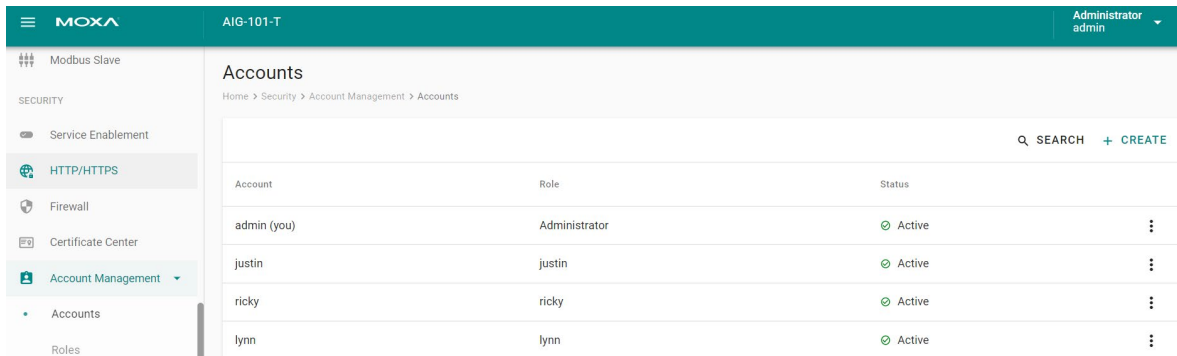


Account Management

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

Accounts

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



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

Creating a New User Account

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



NOTE

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

Password Policy	Valid Password
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
ricky	ricky	Active

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



NOTE

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

User Roles

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

MOXA	AIG-101-T	Administrator admin
Modbus Slave	Roles	
SECURITY	Home > Security > Account Management > Roles	
Service Enablement	Q SEARCH + CREATE	
HTTP/HTTPS	Role Name	
Firewall	Administrator (built-in) Users of this role have full permissions. This is a built-in role and can't be modify or delete.	
Certificate Center	justin	1 account
Account Management	ricky	1 account
Accounts	lynn	1 account
Roles	albert	1 account
MAINTENANCE	Items per page: 10 1 ~ 5 of 5	
Protocol Status		

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

justin

6 / 30

Description - optional

0 / 100

Access Permissions

You must grant at least one privilege to this role.

☐ AWS IoT Core

☐ Azure IoT Device

☐ Moxa Service

☐ Modbus Master

☐ Modbus Slave

☐ MQTT Client

☐ Maintenance

☐ System Configuration

☐ Security

☐ Tag Hub

CANCEL

SAVE

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

Roles		
Home > Security > Account Management > Roles		
		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	⋮

Taking into consideration the security requirements of the AIG-101, 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

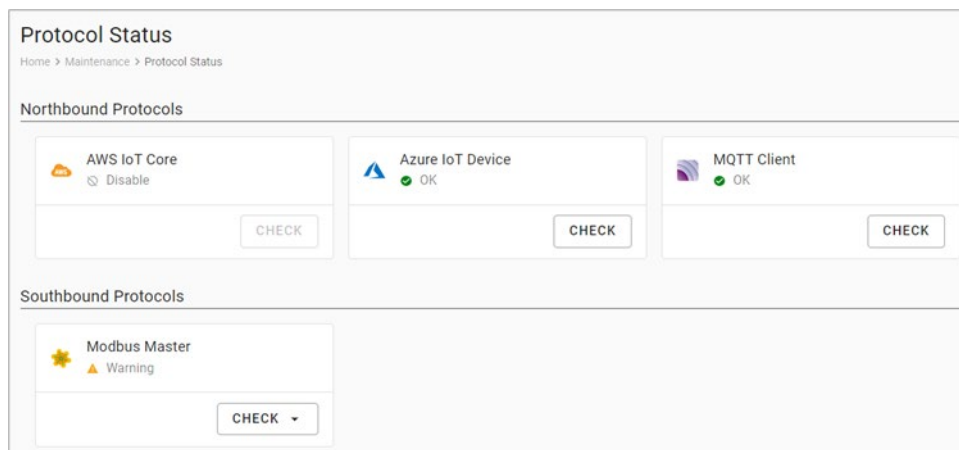
Protocol Status

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

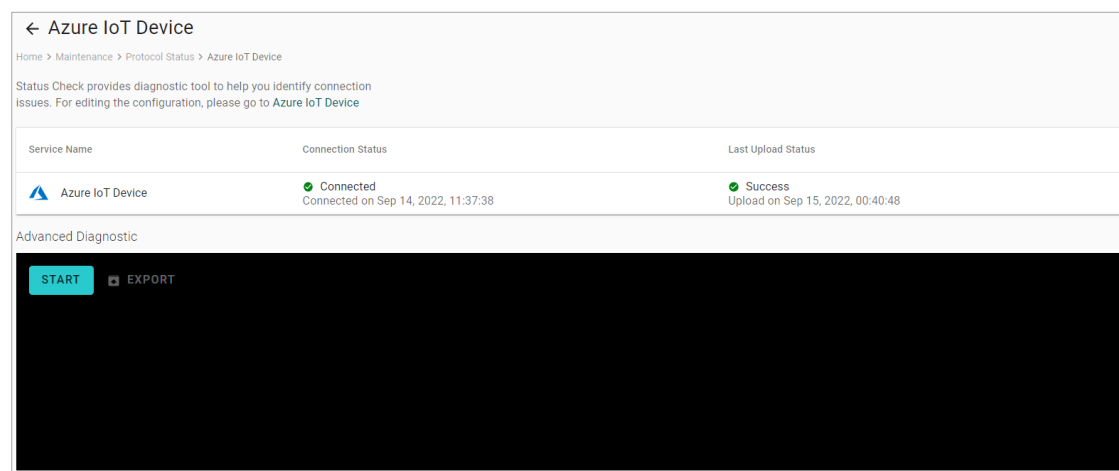
When you access the page, you can see an overview of the status for Northbound Protocols and Southbound Protocols.

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

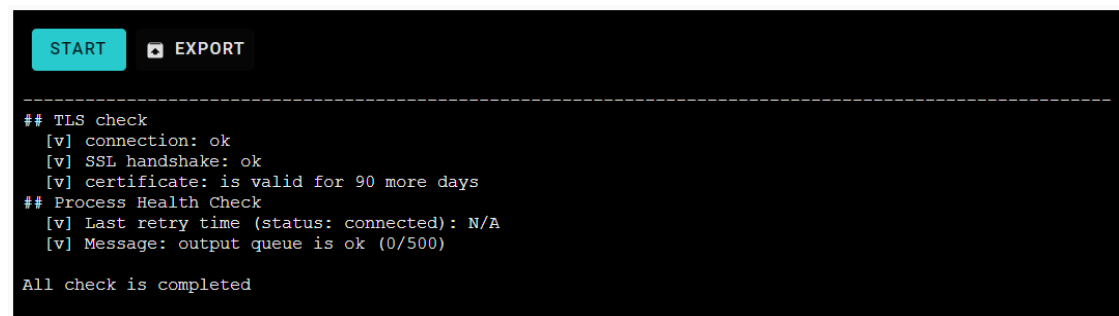
1. Click **CHECK**.



2. Click **START**.



3. View the logs to identify the issue.

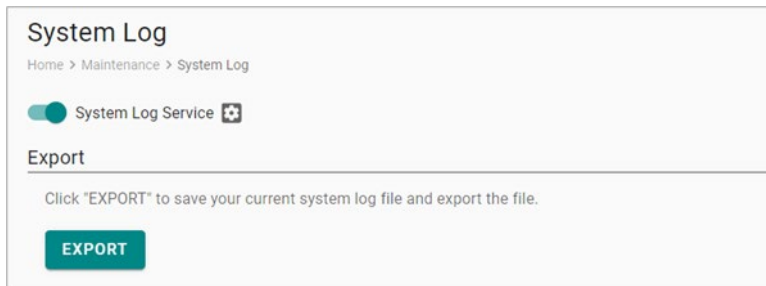


4. (Optional) **Export** the logs.

System Log

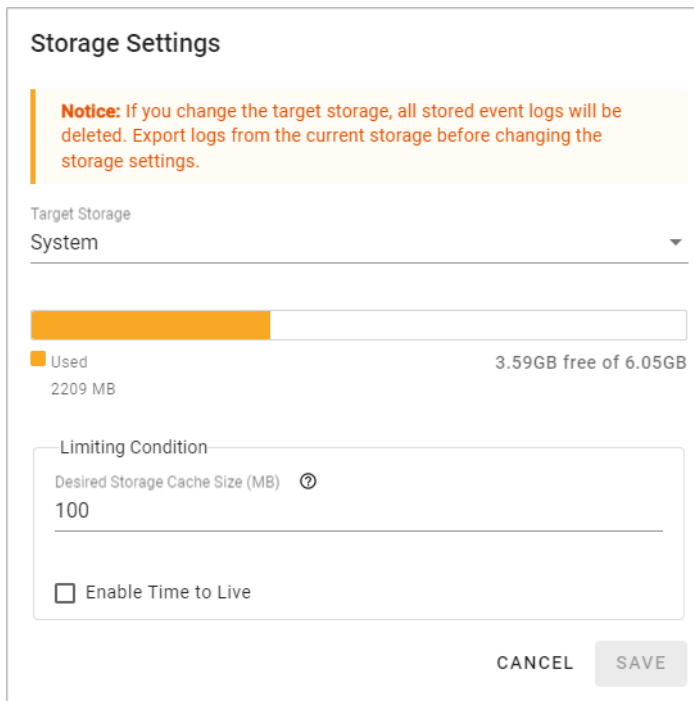
The main purpose of system log is to help Moxa engineers with troubleshooting. When you encounter an issue that you are not able to solve by yourself, export the log file and send it to Moxa TS for analysis.

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



The screenshot shows the 'System Log' page. At the top, there is a breadcrumb trail: 'Home > Maintenance > System Log'. Below this, a toggle switch for 'System Log Service' is turned on, accompanied by a gear icon. Under the 'Export' section, a text instruction reads: 'Click "EXPORT" to save your current system log file and export the file.' A green 'EXPORT' button is positioned below the text.

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.

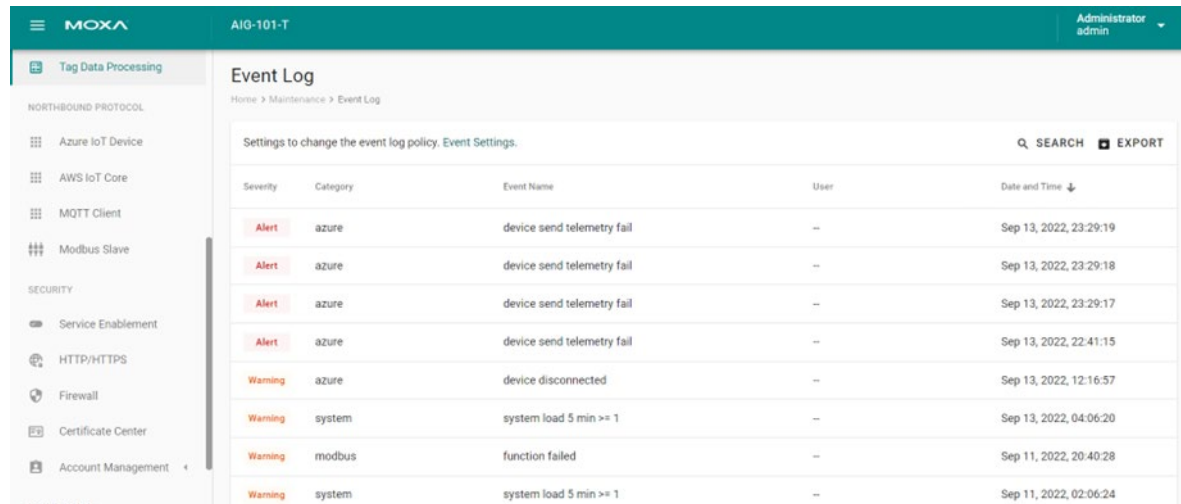


The screenshot displays the 'Storage Settings' dialog. A yellow notice box at the top states: 'Notice: If you change the target storage, all stored event logs will be deleted. Export logs from the current storage before changing the storage settings.' Below the notice, the 'Target Storage' dropdown menu is set to 'System'. A progress bar shows the storage usage, with a label 'Used 2209 MB' and '3.59GB free of 6.05GB'. Under the 'Limiting Condition' section, there is a text input field for 'Desired Storage Cache Size (MB)' with a value of '100' and a help icon. At the bottom, there is an unchecked checkbox labeled 'Enable Time to Live'. The dialog concludes with 'CANCEL' and 'SAVE' buttons.

Event Log

When you face issues, you can check the event logs for recorded events that help you to narrow down the problems. If there are a large number of event logs, you can export the log to read easily.

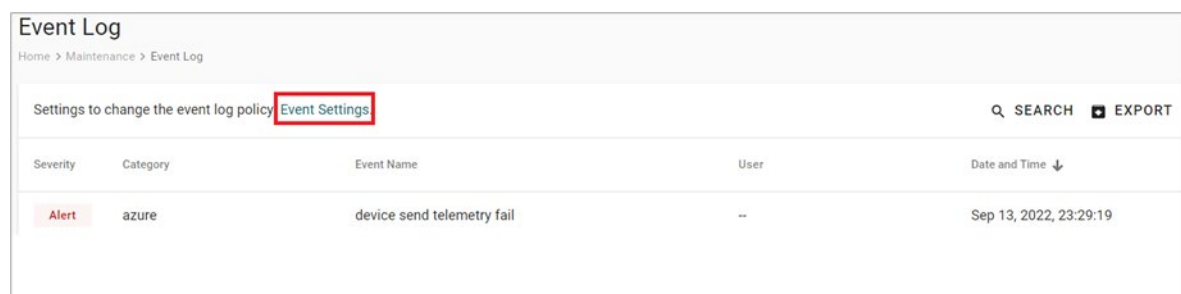
Go to **Event Logs** to view all event logs categorized by **Severity**, **Event Name**, and **Category**. You can use the **SEARCH** function to filter the Event logs to find a specific event. The Event Logs can be exported as a *.zip file and downloaded on to your computer.



Severity	Category	Event Name	User	Date and Time
Alert	azure	device send telemetry fail	--	Sep 13, 2022, 23:29:19
Alert	azure	device send telemetry fail	--	Sep 13, 2022, 23:29:18
Alert	azure	device send telemetry fail	--	Sep 13, 2022, 23:29:17
Alert	azure	device send telemetry fail	--	Sep 13, 2022, 22:41:15
Warning	azure	device disconnected	--	Sep 13, 2022, 12:16:57
Warning	system	system load 5 min >= 1	--	Sep 13, 2022, 04:06:20
Warning	modbus	function failed	--	Sep 11, 2022, 20:40:28
Warning	system	system load 5 min >= 1	--	Sep 11, 2022, 02:06:24

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.



Severity	Category	Event Name	User	Date and Time
Alert	azure	device send telemetry fail	--	Sep 13, 2022, 23:29:19

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

← Event Settings

Home > Maintenance > Event Log > event settings

Event Log Service

Event Index

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

All events

Severity: Alert

Severity: Warning

Severity: Info

aws

device connected

device connection failed

device disconnected

device send telemetry

azure

1 - 73 of 73 , Selected: 44

SAVE

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

Storage Settings

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

Target Storage

System

Used

2209 MB

3.59GB free of 6.05GB

Limiting Condition

Desired Storage Cache Size (MB) 

100

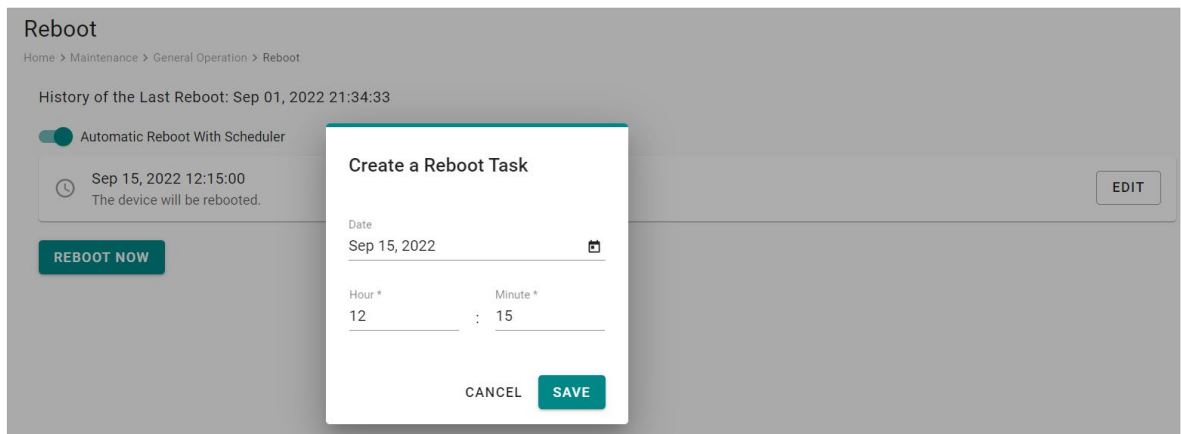
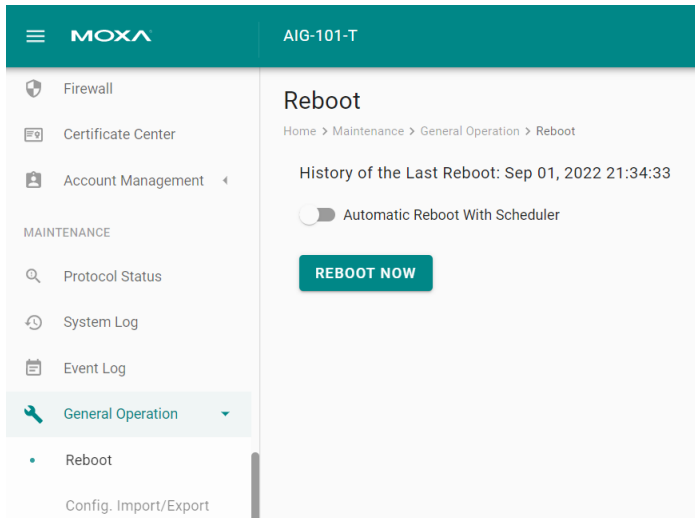
Enable Time to Live

CANCEL

SAVE

General Operation—Reboot

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



General Operation - Config. Import/Export

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

The screenshot shows the Moxa AIG-101-T web interface. The top navigation bar includes the Moxa logo, the device name 'AIG-101-T', and a user dropdown menu showing 'Administrator admin'. The left sidebar contains a menu with categories: 'Firewall', 'Certificate Center', 'Account Management', 'MAINTENANCE', and 'DEVICE MANAGEMENT'. Under 'MAINTENANCE', 'General Operation' is selected, showing sub-items like 'Reboot', 'Config. Import/Export', 'Software Upgrade', and 'Reset to Default'. The main content area is titled 'Config. Import/Export' with a breadcrumb 'Home > Maintenance > General Operation > Config. Import/Export'. It features two sections: 'Export' and 'Import'. The 'Export' section instructs the user to encrypt the file for security and click 'EXPORT' to export the current system configuration as a configuration file. It includes password fields for 'Password' and 'Confirm Password', each with a strength indicator bar and an eye icon for toggling visibility. A green 'EXPORT' button is present. The 'Import' section instructs the user to click 'BROWSE' to select a previously exported configuration file and enter the password to upload the file. It includes a 'Configuration File' label and a 'BROWSE...' button.

General Operation—Firmware Upgrade

Go to **General Operation > Firmware Upgrade** to upgrade this device with Moxa's software packages.

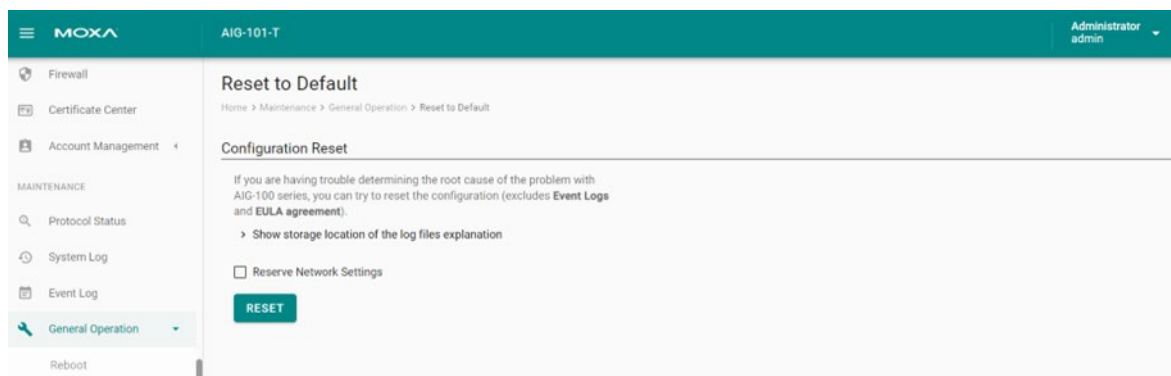
Click **BROWSER** and select the software package file in *.deb file format on your computer, then click **UPLOAD**.

The screenshot shows the Moxa AIG-101-T web interface for the Firmware Upgrade page. The top navigation bar is the same as the previous screenshot. The left sidebar shows 'General Operation' selected, with 'Firmware Upgrade' highlighted under the 'MAINTENANCE' category. The main content area is titled 'Firmware Upgrade' with a breadcrumb 'Home > Maintenance > General Operation > Firmware Upgrade'. It features an 'Upgrade' section with instructions: 'You may upload the upgrade pack from your local drive. Upgrade Settings'. There are two radio button options: 'Upgrade From the Local Drive' (which is selected) and 'Upgrade From the Cloud'. Below the instructions, it says 'Choose the upgrade pack (*.deb) from your local drive and upload it to your IloT gateway. The installation process will start automatically after the upload is complete.' There is a 'Firmware Upgrade File' label and a 'BROWSE...' button. Below that is an 'UPLOAD' button.

General Operation—Reset to Default

If you want to clear all the settings to configuration default, there are two ways:

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



2. Press and hold the Reset button on the device till the SYS LED blinks (approximately seven seconds).

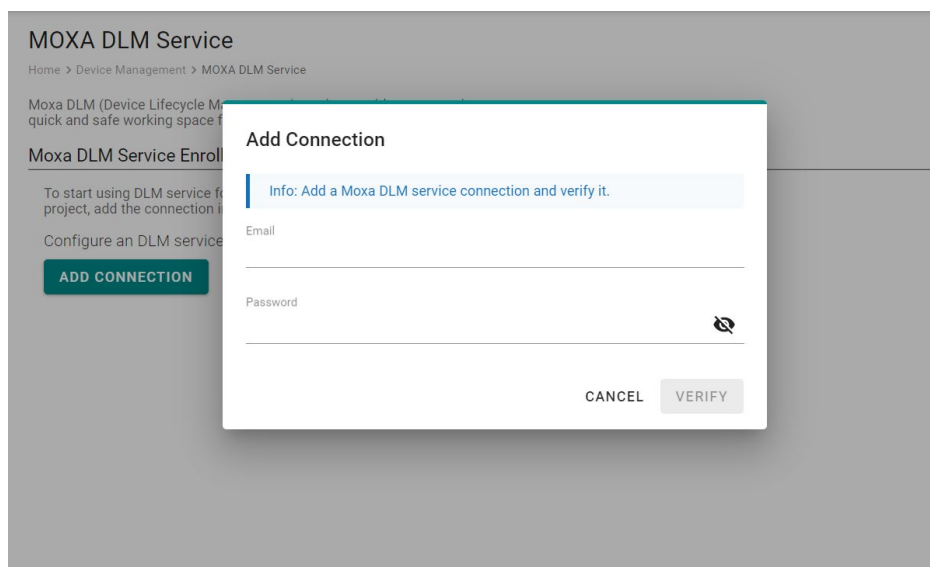
Device Management

Moxa DLM Service

Moxa DLM (device lifecycle management) service is used for management of the AIG Series. Imagine sitting in your office and using this service to remotely manage a large number of devices distributed around the world. You can monitor the device's health status, upgrade firmware, import/export configuration, and remotely log into the device's web console. If you want to apply for this service, contact the product manager, Joshua Lin, at joshua.lin@moxa.com.

Once you get the service, go to **Moxa DLM Service** to register the product online. Follow these steps:

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



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

MOXA DLM Service

Home > Device Management > MOXA DLM Service

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

MOXA DLM Service Enrollment

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

Configure an DLM service connection

Moxa DLM service connection

Verified

Email: ichbinjoshua@gmail.com

Password:

EDIT

Enrollment setting

Project Name

Test

ENROLL

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

MOXA DLM Service

Home > Device Management > MOXA DLM Service

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

MOXA DLM Service Enrollment

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

Configure an DLM service connection

Moxa DLM service connection

Verified

Email: ichbinjoshua@gmail.com

Password:

EDIT

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 > Device Management > MOXA DLM Service

Moxa DLM service

Project Name	Status
Test	Connected Connect on Oct 16, 2024, 17:06:11

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 16, 2027 09:05:46

Organization: Moxa Inc.

Model Name: AIG-101-T-EU

MAC Address: 0090E8B4F4D2

Serial Number: TBC8B1037026

AIG-101 Series User Manual

74

5. Log in to the Moxa DLM Service to check if the AIG device is online.

All Devices					
Home > Projects > All Devices					
SEARCH REFRESH					
☐ Serial Number	Model Name	Host Name	Connection Status	Firmware Version	Labels
☐ TBCB1037026	AIG-101-T-EU	Moxa	Online Connected on Oct 16, 2024 17:06:09	1.1.0	-
Items per page: 10 1 - 1 of 1 < > >>					

Sign Up DLM Account

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

MOXA

Sign in Moxa DLM Service

Account

Password

[Forgot password?](#)
[Sign up](#)

SIGN IN

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.

MOXA

Welcome to Moxa DLM Service.

Company Name

Moxa Inc.

Email

entity_owner_email@moxa.com

✓

I'm not a robot

reCAPTCHA

Privacy · Terms

[Back to login](#)

SIGN UP

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

MOXA

Sign Up Successful

We have sent the confirmation letter to your email account. Please verify it and follow the instructions provided in the letter.

GO TO LOGIN

4. Security Hardening Guide

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

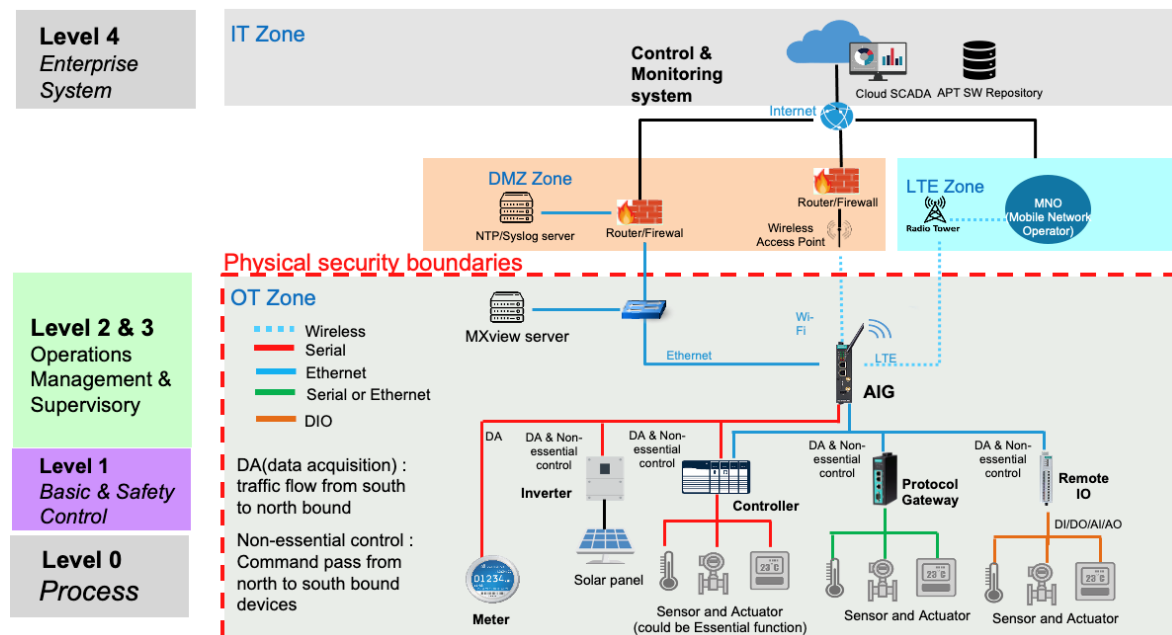
Communication Integrity and Authentication

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

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

Potential Threats and Corresponding Security Measures

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



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

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

Installation

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

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

Publish Mode

Publish Mode	Parameters	Value	Description
By Interval	Publish Intervals (sec)	0 - 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. Additional Documentation

Software Downloads

Upgrade Packs:

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

Utility (QuickON):

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

Technical Documentation

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

OpenAPI Documentation

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