AIG-301 Series User Manual

Version 2.3, November 2025

www.moxa.com/products

AIG-301 Series User Manual

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

Copyright Notice

Trademarks

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

Overview

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

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

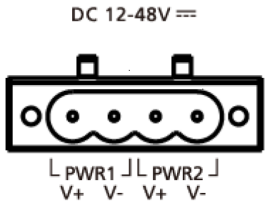
NOTE

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

2. Getting Started

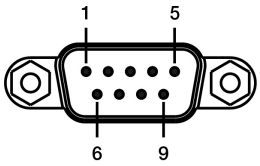
Connecting the Power

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



Connecting Serial Devices

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



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

Connecting to a Network

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

Access to the Web Console

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

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

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

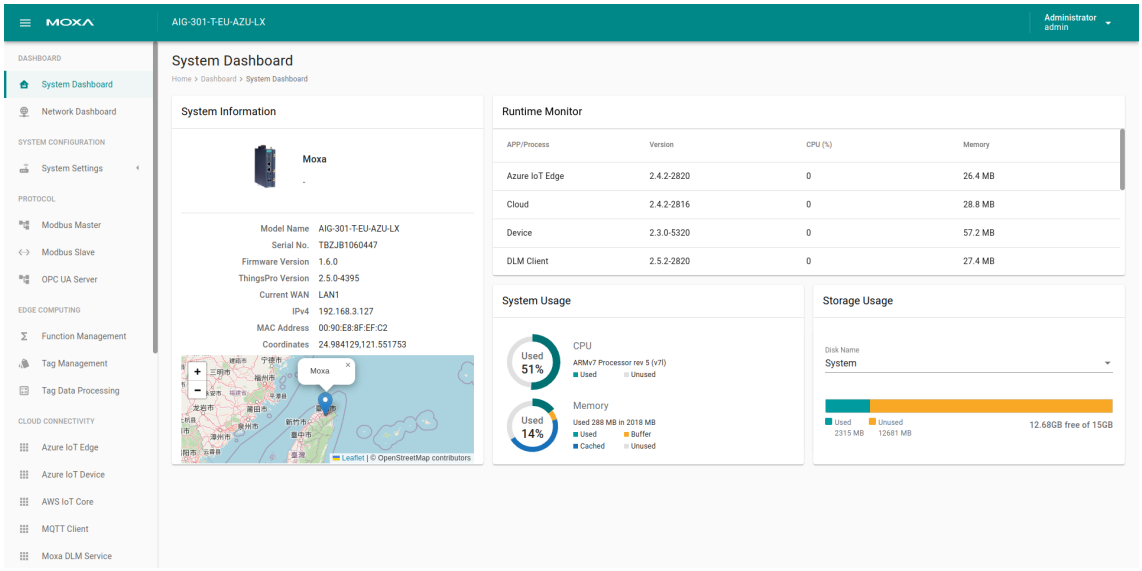
   Default account: **admin**

   Password: **admin@123**

NOTE

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

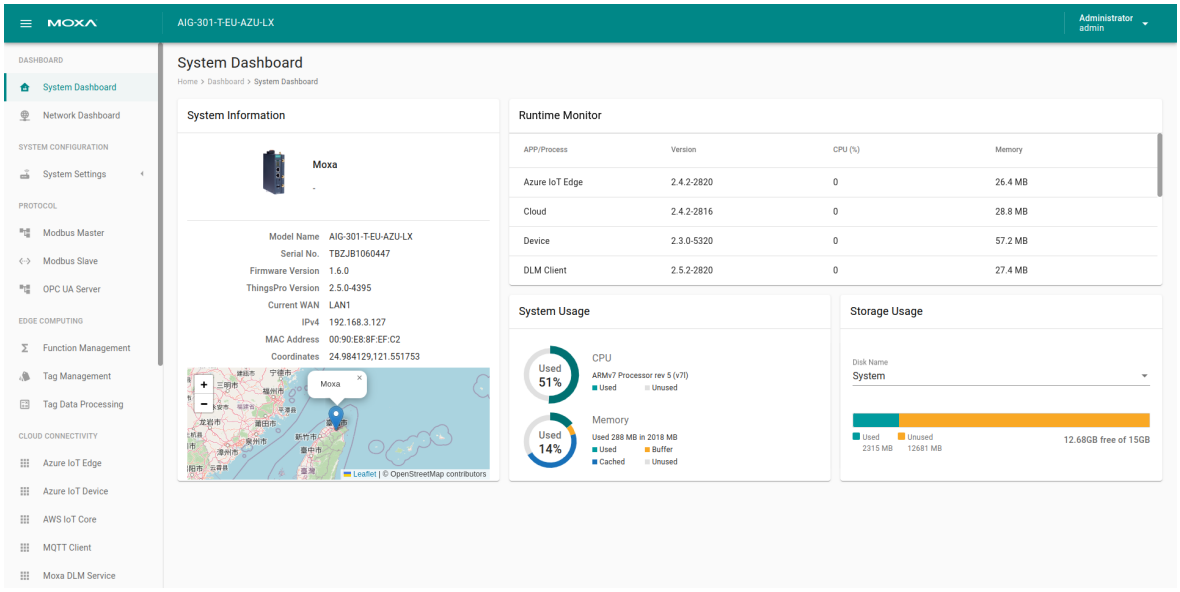
You will see the following homepage after logging in successfully.



Dashboard

System Dashboard

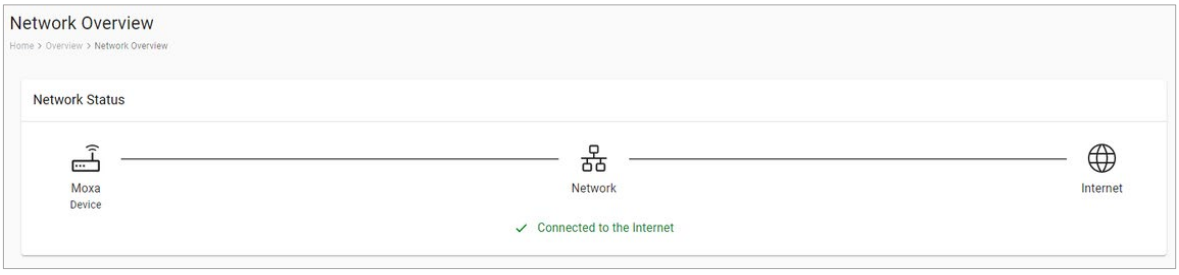
This page gives you an overview of the gateway's system status. Basic system information such as model name, serial No., and firmware version are displayed. In addition, Storage Usage provides information on the unused storage on the system or on the SD card. Ensure that you provide accurate information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



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

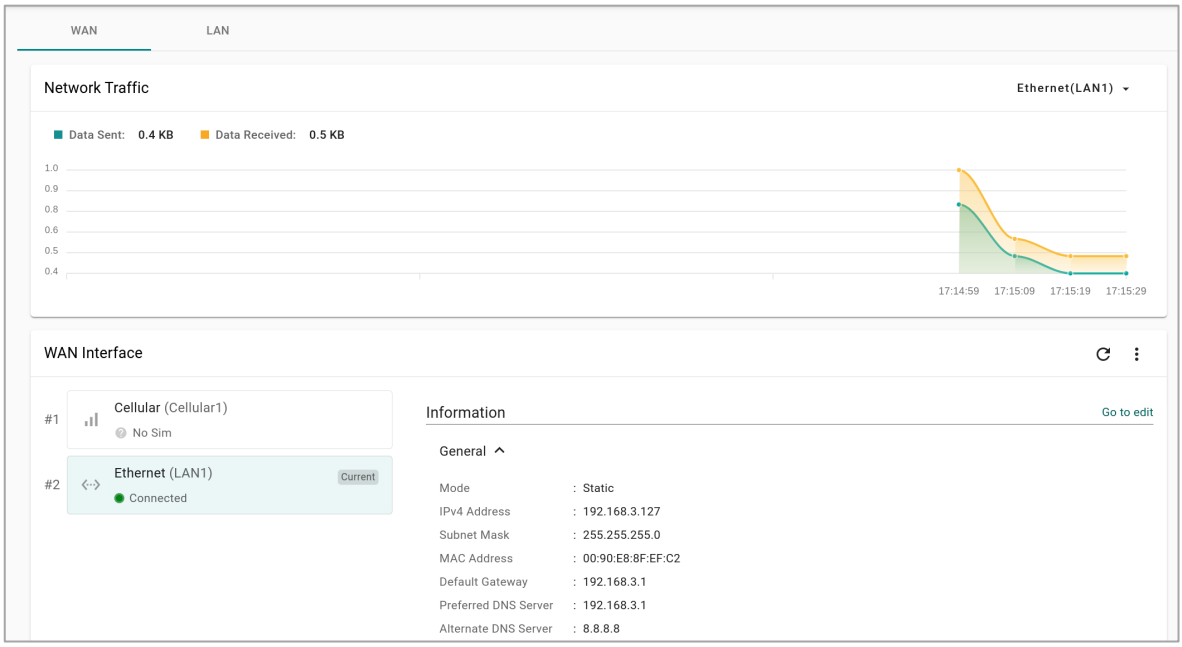
Network Dashboard

This dashboard displays information on the WAN and LAN interfaces and the network traffic passing through the interfaces. Network Status shows whether the gateway can connect to the Internet.



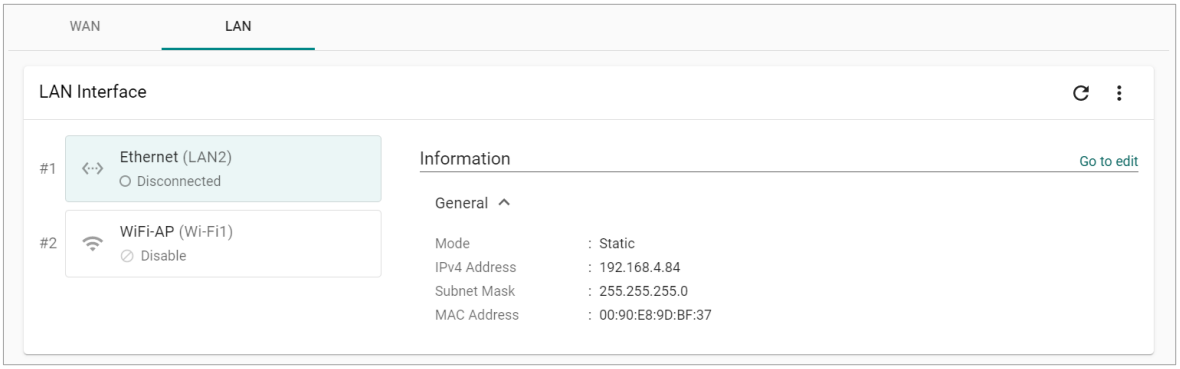
WAN

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



LAN

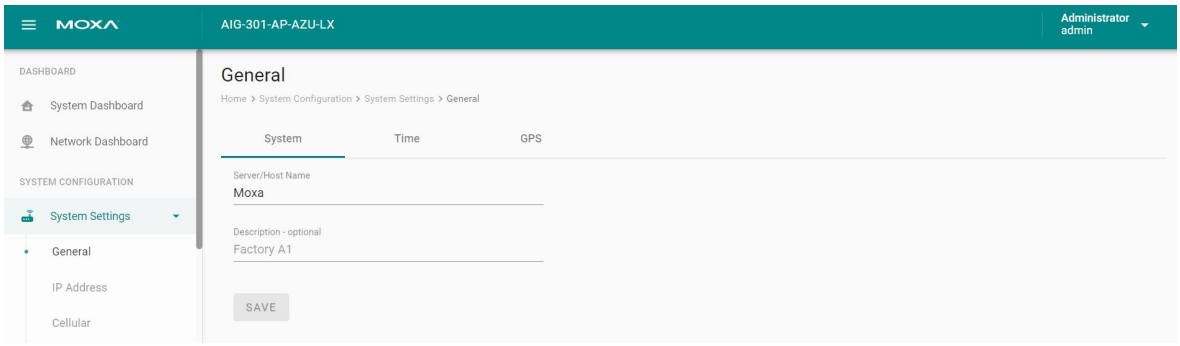
Information on the LAN interfaces is organized under the **LAN** tab and includes information on the usage of the interfaces and the traffic passing through them.



System Configuration

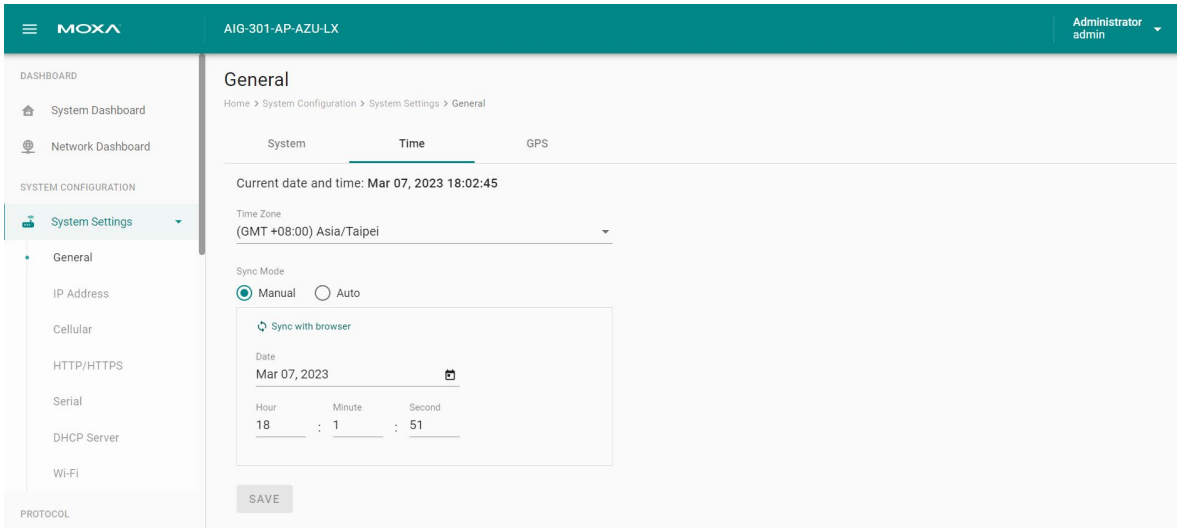
System Settings—General

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



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

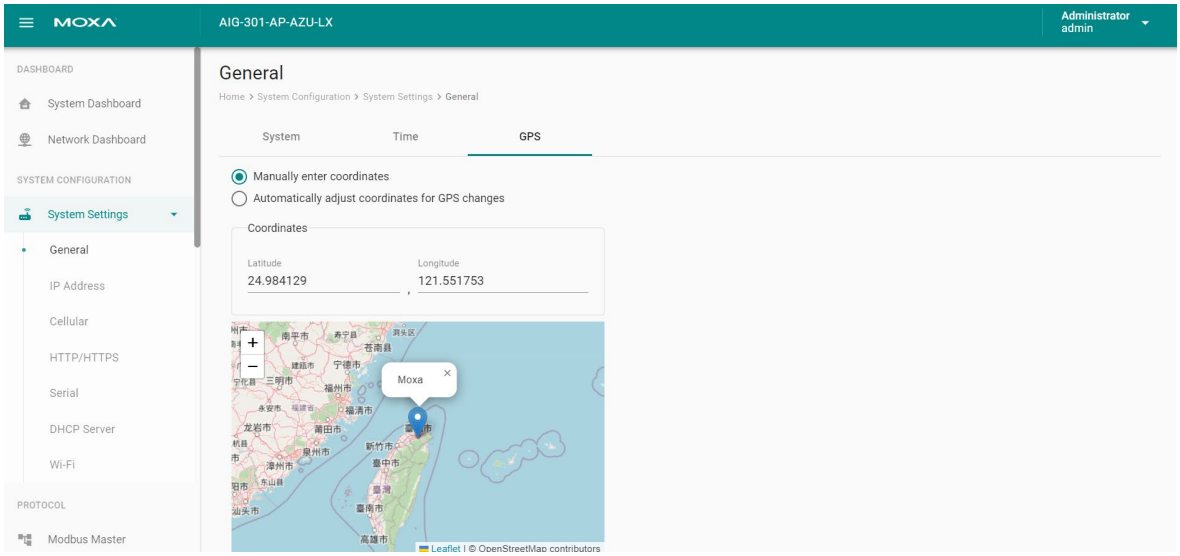
Go to **System Settings > General > Time** to select a time zone. Choose between the Manual or Auto option to update the system time.



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

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

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

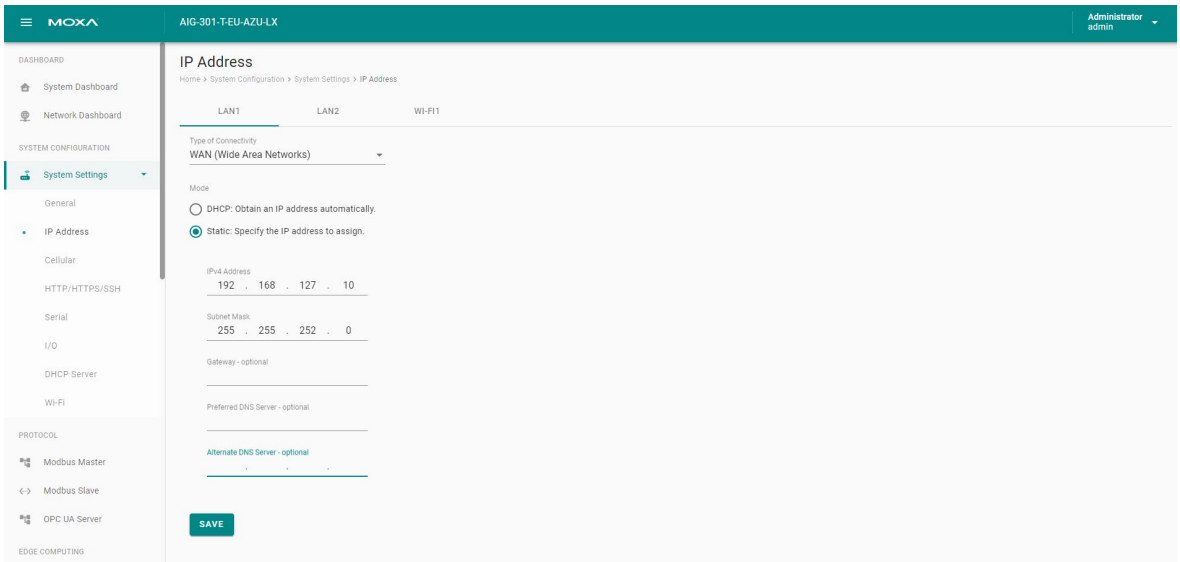


System Settings—IP Address

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

To configure the network, do the following:

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

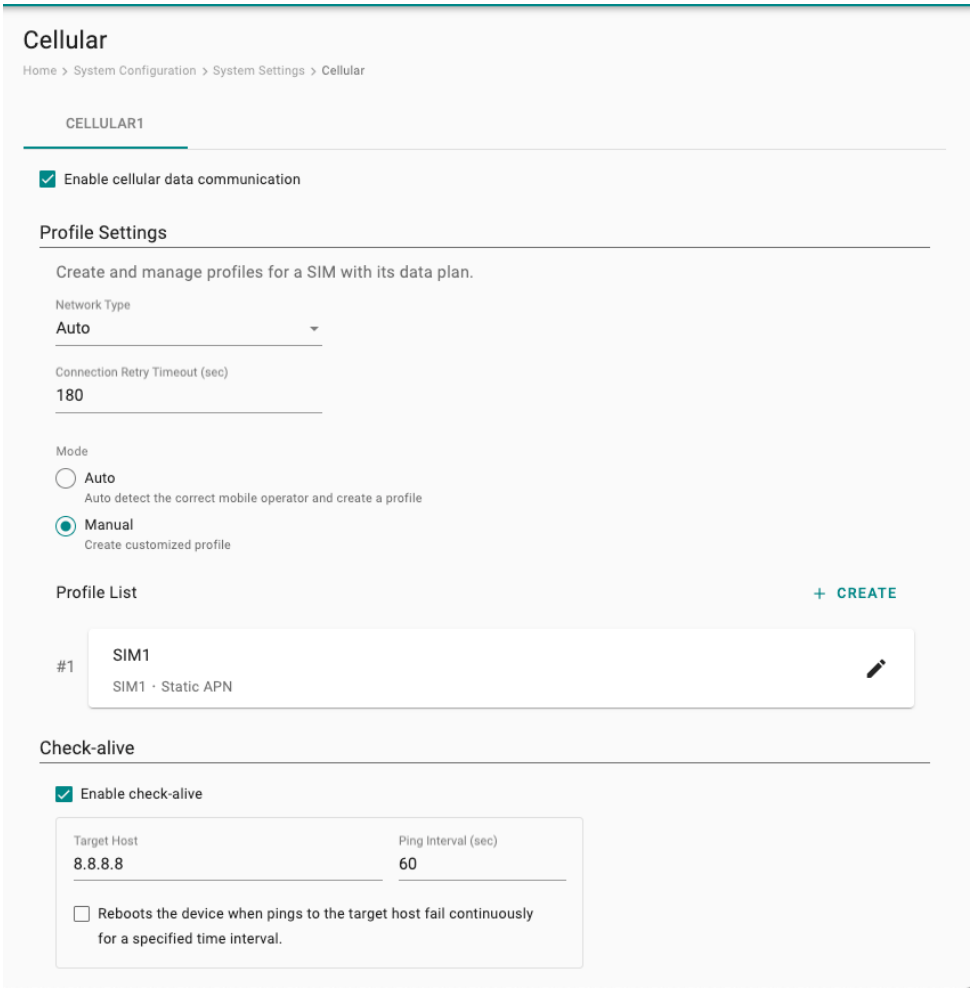


Parameter	Value	Description
Types of connectivity	WAN LAN NOTE: LAN2 does not support WAN.	WAN: Wide Area Networks LAN: Local Area Networks
Mode	DHCP Static	DHCP: Gets the IP address automatically. Static: Specify the IP address
IPv4 Address	LAN1 default: DHCP LAN2 default: 192.168.4.127 (or other 32-bit number)	The IP (Internet Protocol) address identifies the server on the TCP/IP network
Subnet Mask	Default: 255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
Gateway—optional	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server —optional	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
Alternate DNS Server— optional	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

System Settings—Cellular

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

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.



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

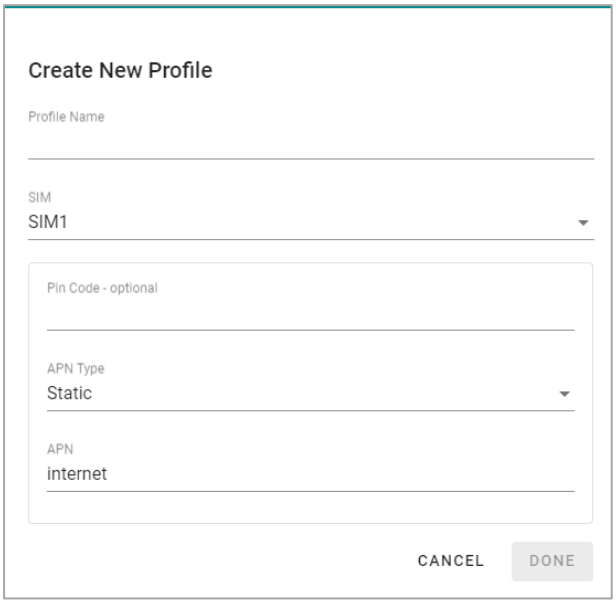
You also can create customized cellular profiles by choosing the **Manual** option in the **Profile Settings** section. A list of all the profiles in the system is displayed. **Create**, **Edit**, or **Delete** cellular profiles here.

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

1. Click **+ CREATE**.
2. Specify a unique **Profile Name**.
3. Specify the target **SIM** card.
4. Enter the **PIN Code** if your SIM card requires it. (**NOTE:** Three wrong attempts will lock the SIM card.)
5. Choose a **Carrier**.

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

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

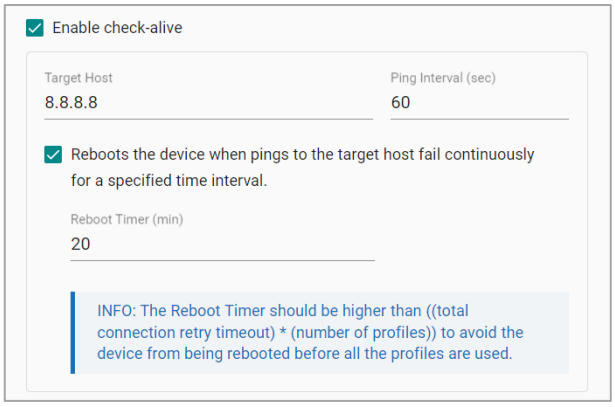


7. Click **DONE**.
8. On the **Cellular** setting page, click **SAVE**.

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

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

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



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

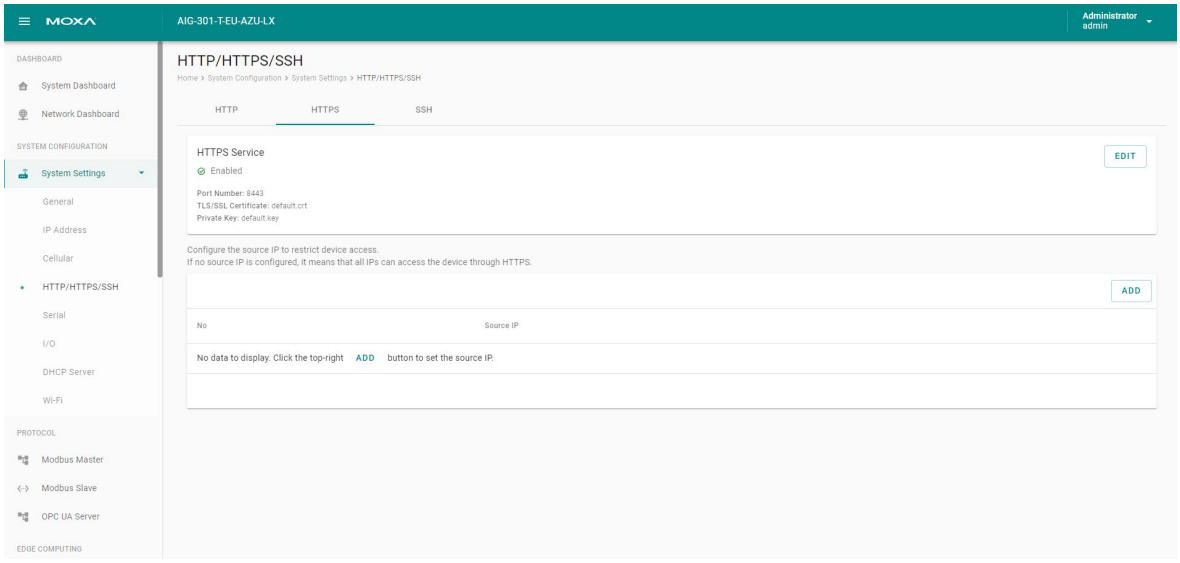
NOTE

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

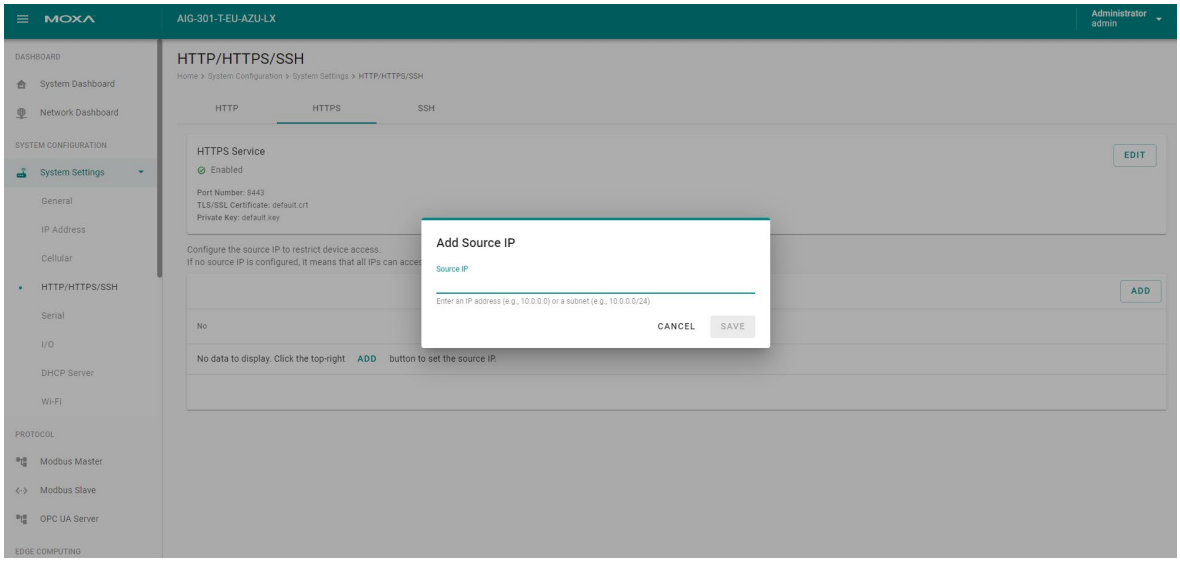
System Settings—HTTP/HTTPS

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

The default setting for **HTTP redirect to HTTPS** is **Enabled** (starting with firmware version v1.8.0) to enhance security capabilities. To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority. If there are no imported certificates, the AIG can generate a "AIG Series Root CA for HTTPS" certificate.



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



NOTE

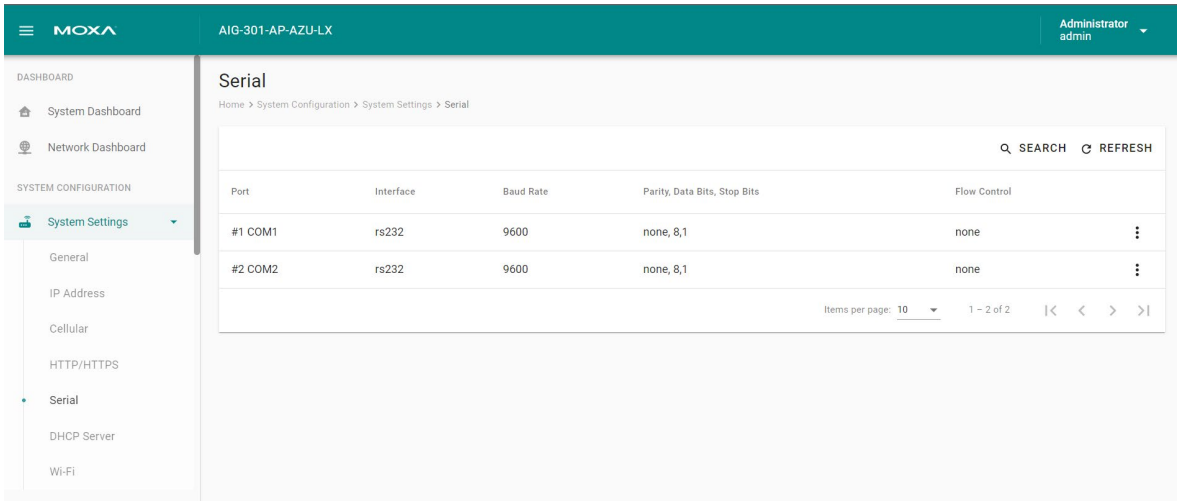
After the first SSH login, we force a password change to comply with general security policies and practices and to increase the security of your device.

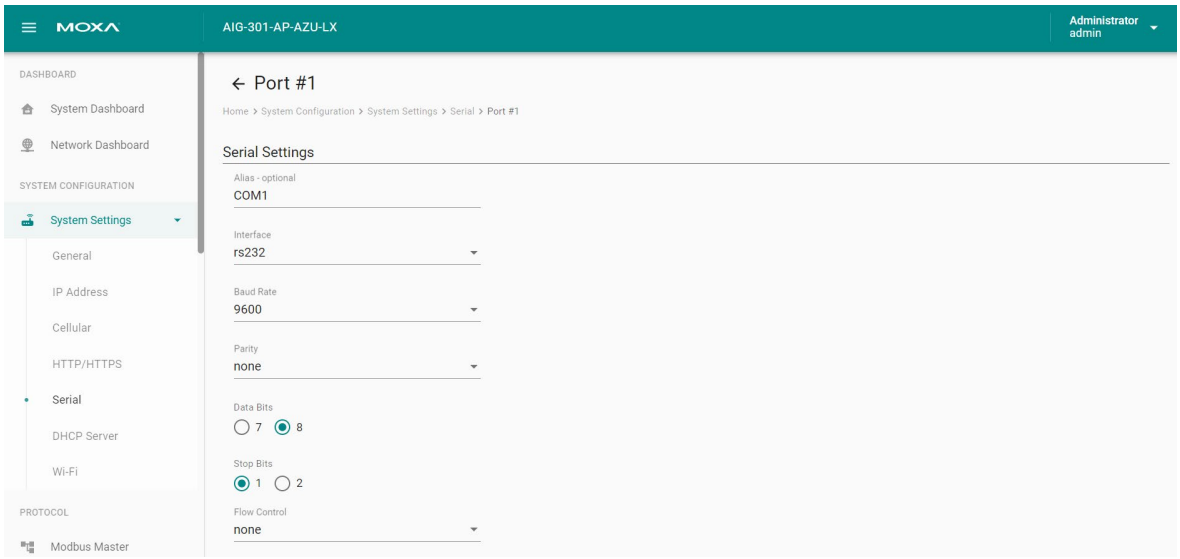
System Settings—Serial

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

To configure serial settings, do the following:

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



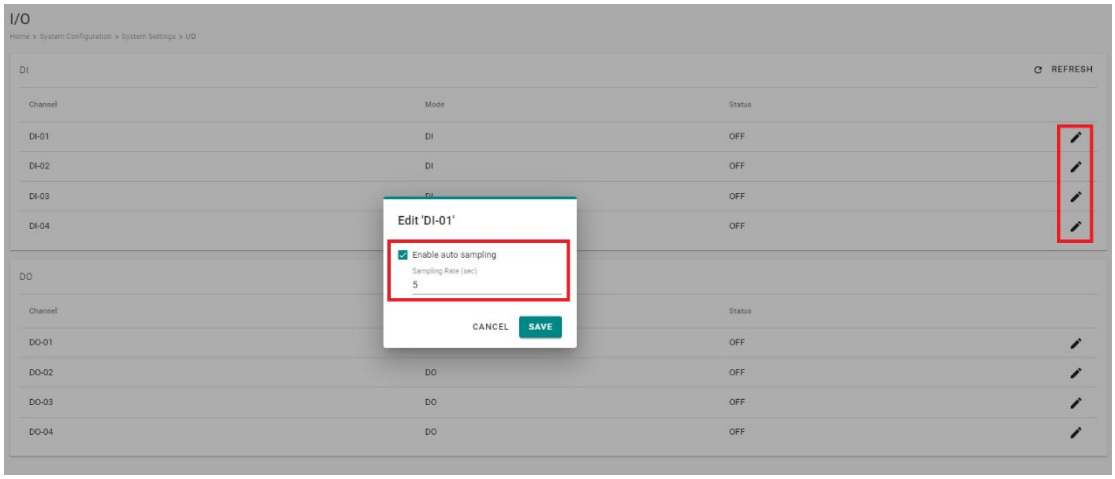


Parameter	Value	Description
Interface	rs232 rs422 rs485-2w rs-485 4w	
Baud Rate	300 to 921600	
Parity	none, odd, even, space, mark	
Data Bits	7, 8	
Stop Bits	1, 2	
Flow Control	none hardware software	Hardware: Flow control by RTS/CTS (for RS-232) Software: Flow control by XON/XOFF (for RS-232/422/485-4W)

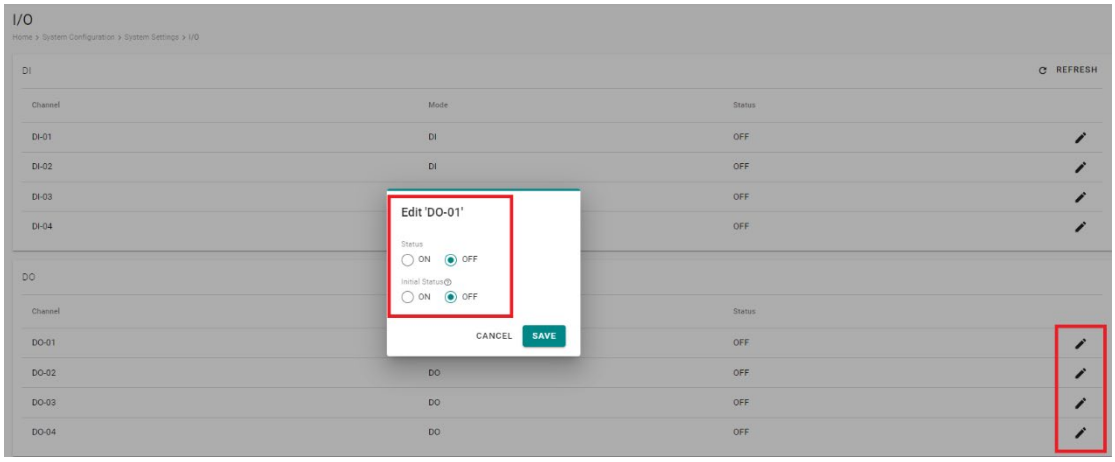
System Settings—I/O

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

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



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



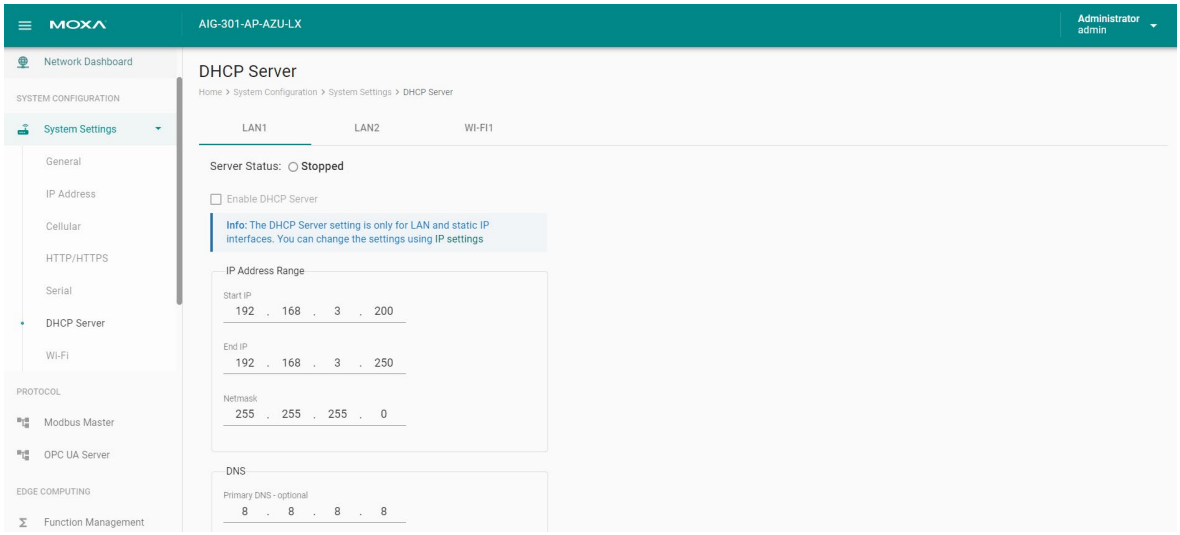
Parameter	Value	Description
Status	ON	High voltage
	OFF	Low voltage

System Settings—DHCP Server

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

To configure DHCP server settings, do the following:

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



NOTE

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

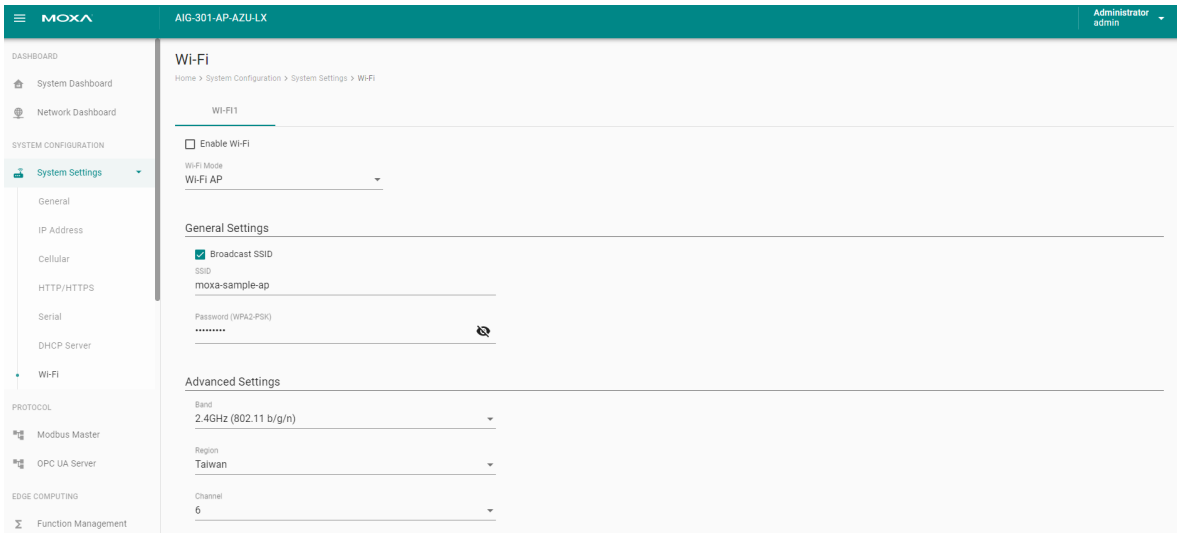
System Settings—Wi-Fi

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

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

If the Wi-Fi AP is Selected

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



NOTE

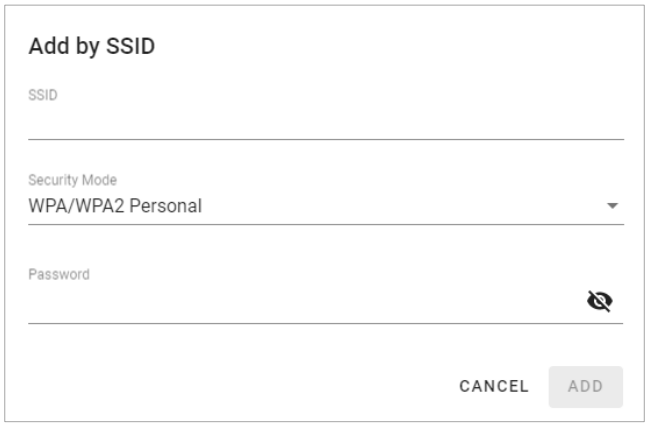
The maximum number of Wi-Fi clients allowed is 2.

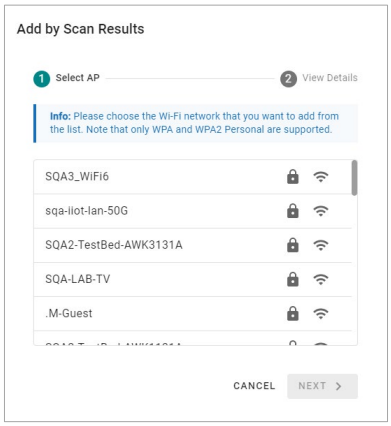
NOTE

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

If the Wi-Fi Client is Selected

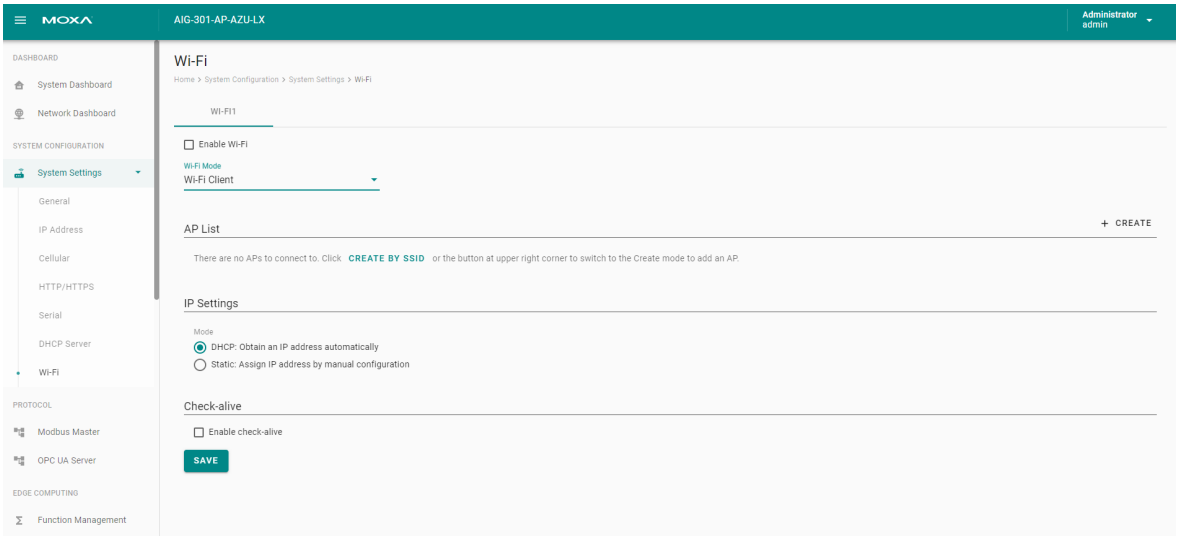
1. Click **+CREATE** to manually **Create by SSID** or be **Created by Scan Results**.





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

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



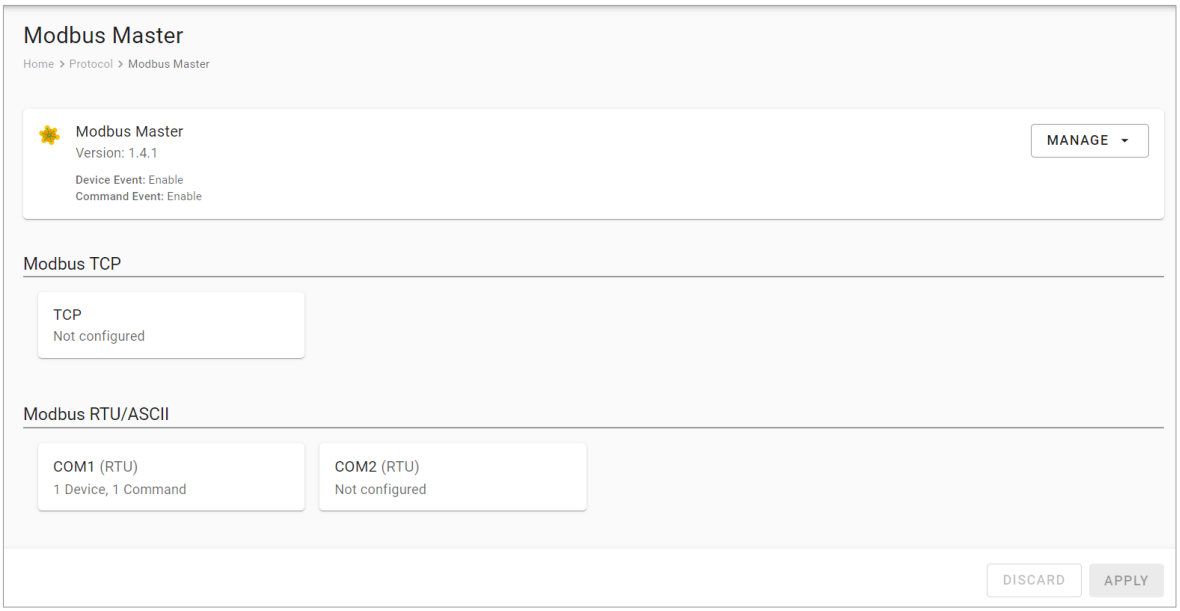
Protocol

Modbus Master

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

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

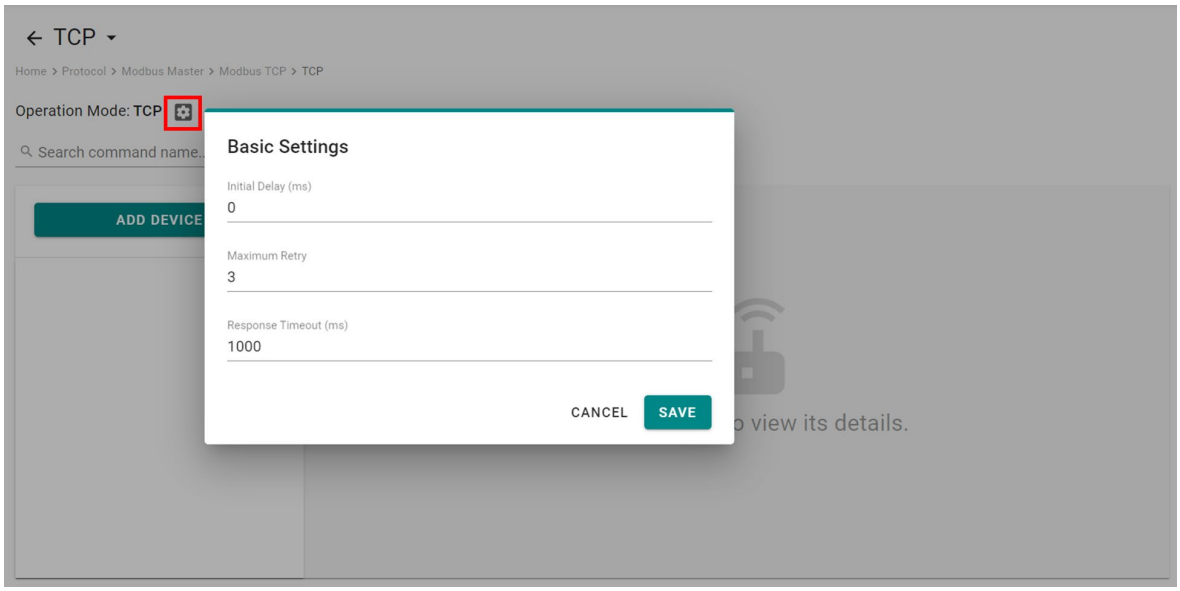
1. Click **TCP** under Modbus TCP or **COMx** under Modbus RTU/ASCII.
2. Click **ADD DEVICE** and go to the 3-step wizard page.
3. Input **device name**, **slave ID, IP Address,** and **TCP port**, then press **NEXT.**
4. Click **+ ADD COMMAND** to add Modbus commands to collect the data, then press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



Modbus TCP

Basic Settings

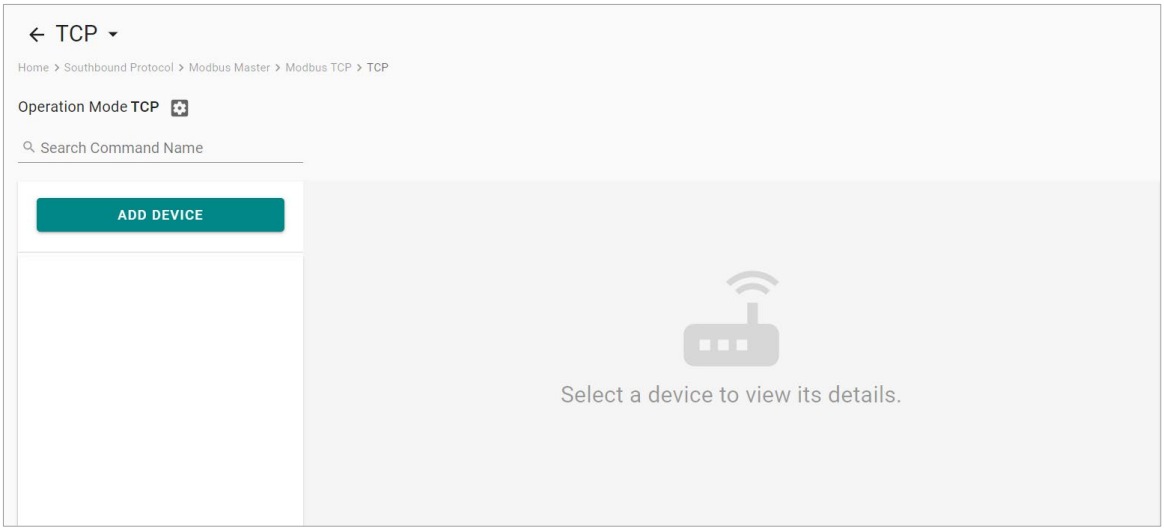
When you access the Modbus TCP setting page, you will first need to configure the basic settings.



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

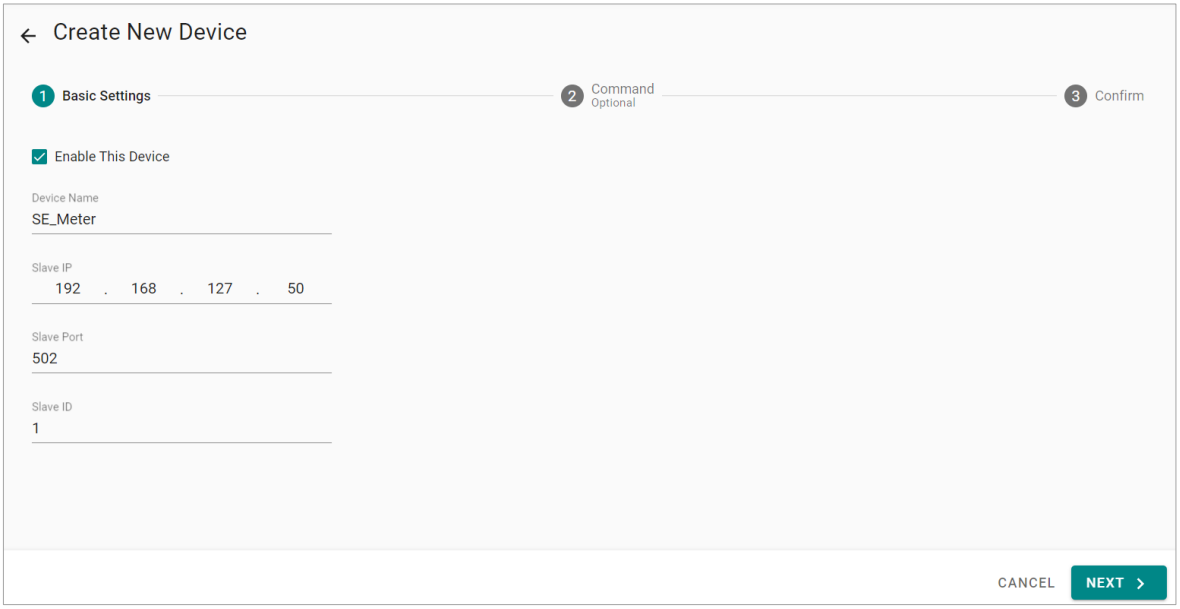
Modbus Device Settings

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



Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.

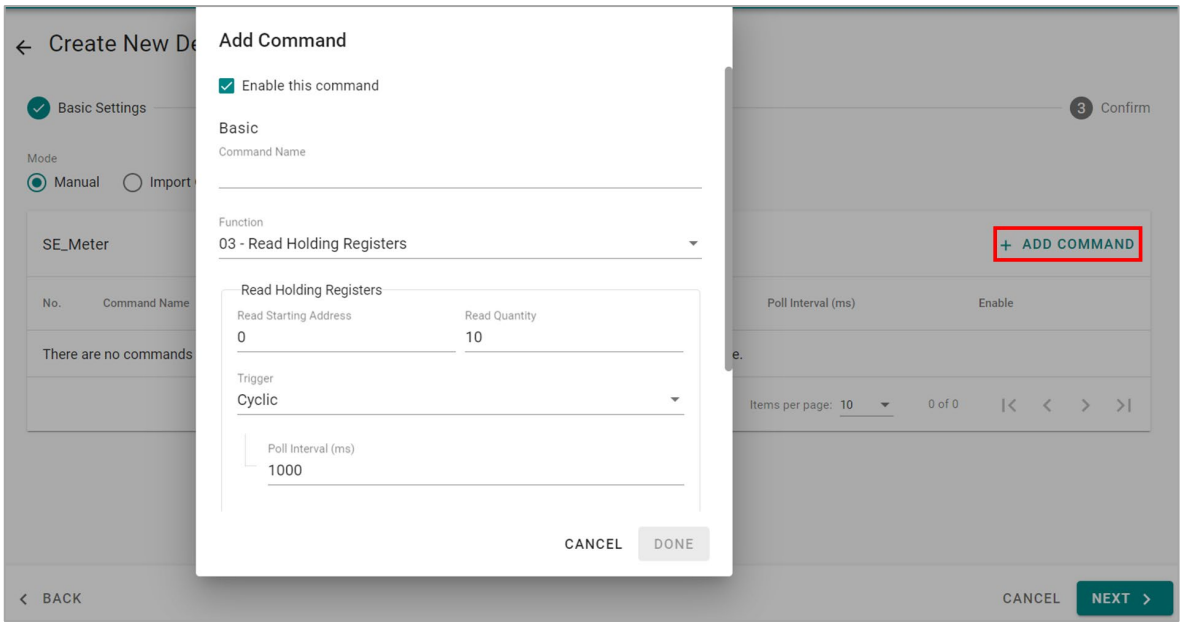


Parameter	Value	Default	Description
Device Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name your Modbus device
IP Address	0.0.0.0 to 255.255.255.255	–	The IP address of a remote slave device.
Slave Port	1 to 65535	502	The TCP port number of a remote slave device.
Slave ID	1 to 255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

Step 2. Command

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

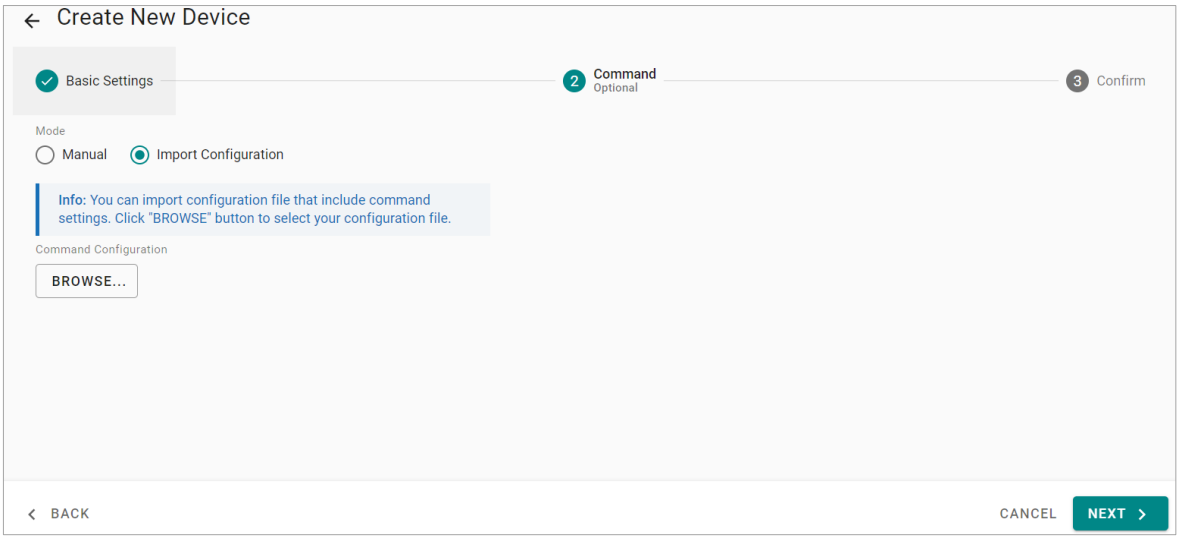
The command settings will pop up.



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

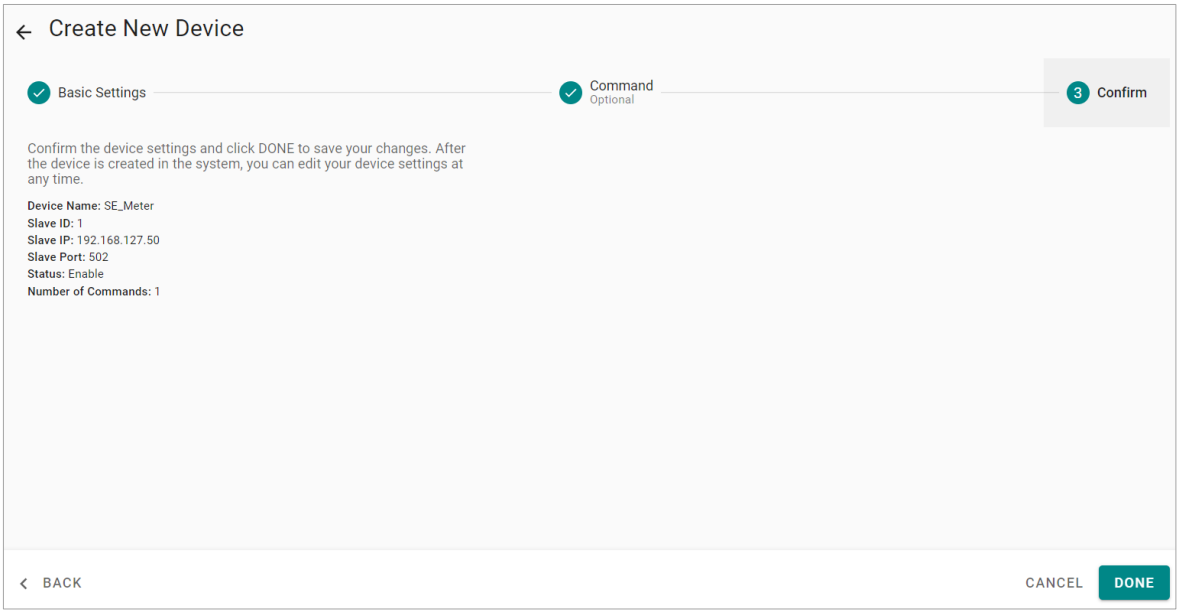
Parameter	Value	Default	Description
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	pause	The defined value of the Status Term will be effective when a read command encounters an error or times out.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in tag hub.

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

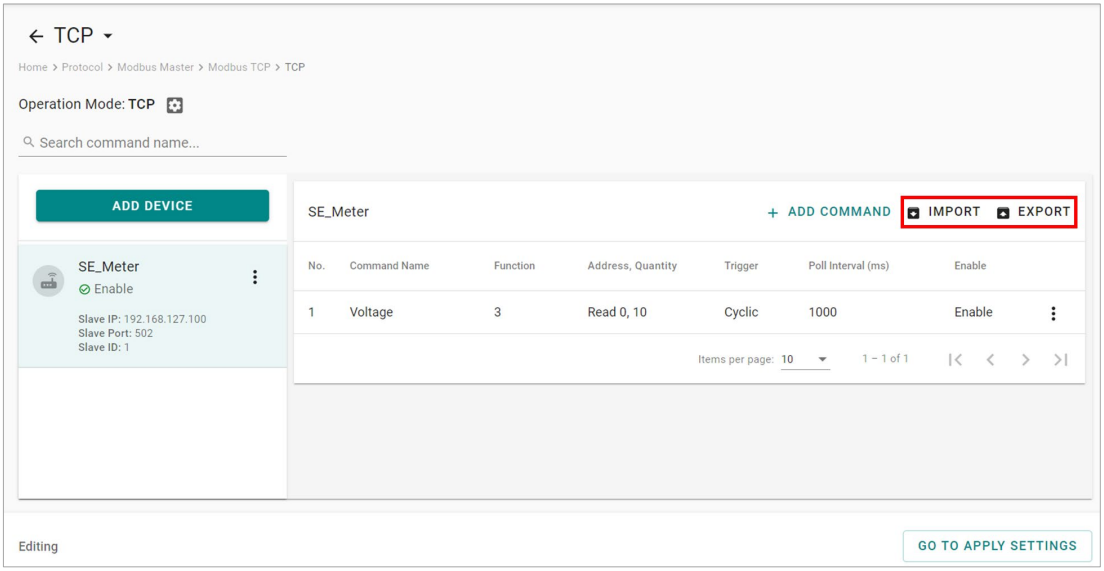


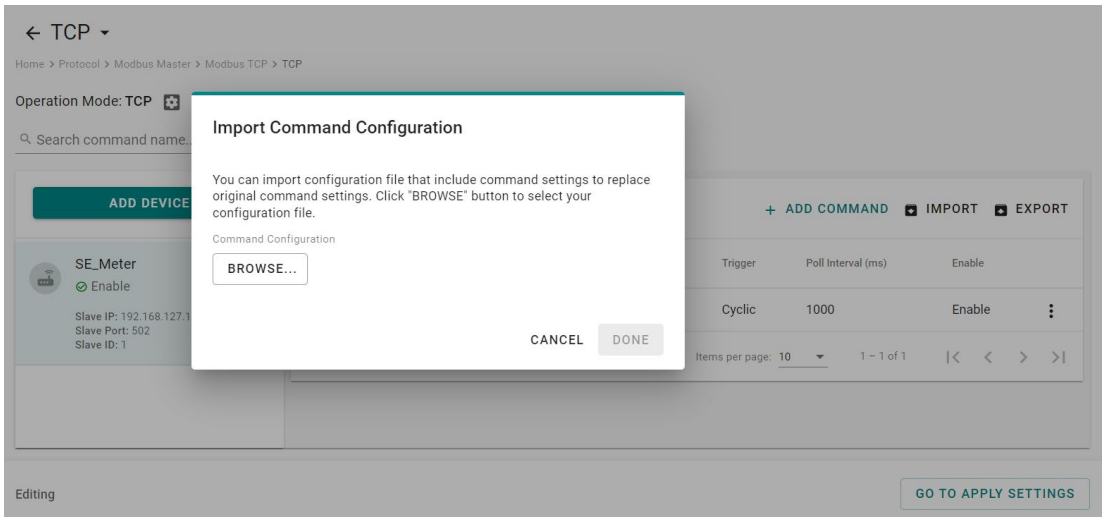
Step 3. Confirm

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

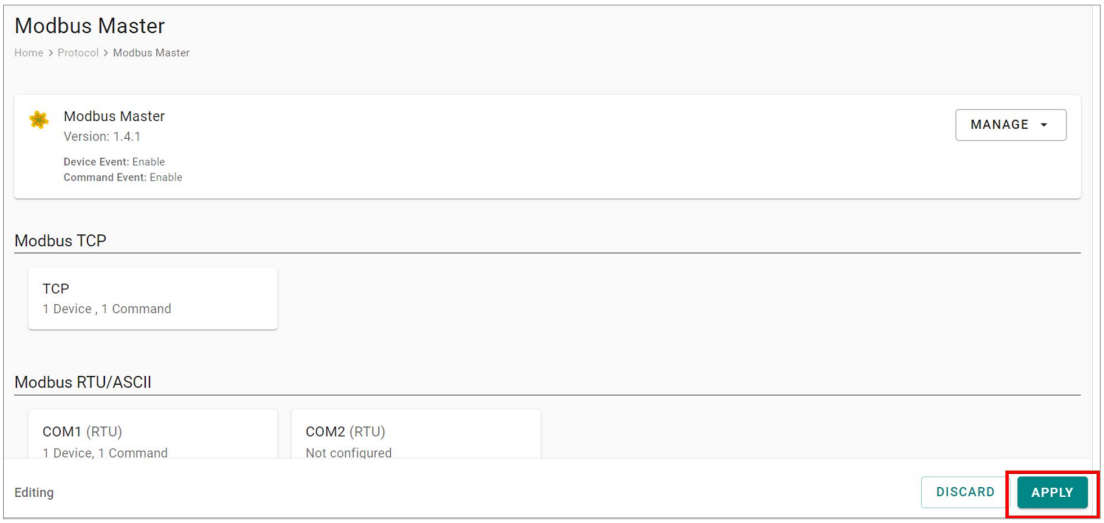


AIG provides an easier way for installation and maintenance. You can **EXPORT** all the Modbus commands into a file for backup purposes, or you can **IMPORT** a file (golden sample) to reduce configuration time.





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



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

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

Parameter	Value	Default	Description
fpFunc	Applicable only when the function code is **5, 6, 15, 16, or 23**. For other function codes, set this value to **0**. When the command trigger mode (**mode**) is **cyclic (0)**: **0**: Continue – retain the latest data **1**: Continue – clear data to zero **2**: Continue – set to user-defined value (**fpData**) When the command trigger mode (**mode**) is **data change (1)**: **0**: Pause **1**: Continue – clear data to zero **2**: Continue – set to user-defined value (**fpData**)		Fail-safe Mode Note: Not applicable for read commands.
fuTout	Applicable only when the function code is **5, 6, 15, 16, or 23**. Type: Integer Minimum: **1** Maximum: **86400**		Fail-safe Timeout (seconds) Note: Not applicable for read commands.
fpData	Applicable only when the function code is **5, 6, 15, 16, or 23**. Represented as a **hexadecimal string**, with bytes separated by spaces. For function codes **5, 15**: Byte count = ⌈(*writeQuantity* ÷ 8)⌉ 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 = *writeQuantity* × 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: ±1.79×10^(-308) ~ ±1.79×10^(+308) (IEEE 754 Double)		**Slope**
interceptOffset	Double precision floating-point number (double) Range: ±1.79×10^(-308) ~ ±1.79×10^(+308) (IEEE 754 Double)		Offset
pointSourceMin	Double precision floating-point number (double) Range: ±1.79×10^(-308) ~ ±1.79×10^(+308) (IEEE 754 Double)		Source data minimum value

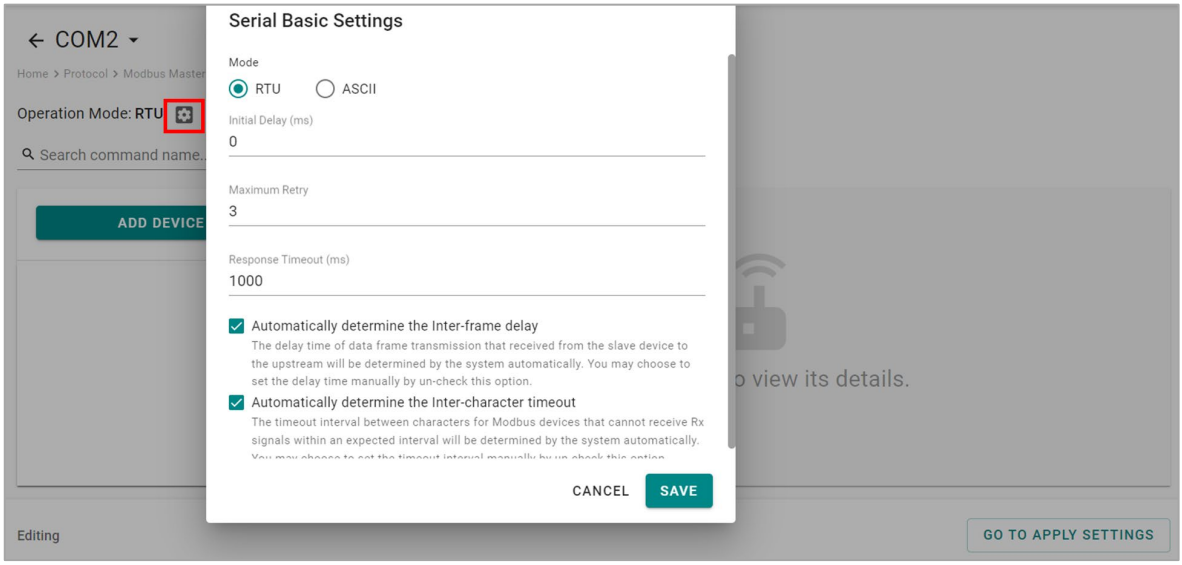
Parameter	Value	Default	Description
pointSourceMax	Double precision floating-point number (double) Range: ±1.79×10^(-308) ~ ±1.79×10^(+308) (IEEE 754 Double) Note: pointSourceMax cannot be the same as pointSourceMin		Source data maximum value
pointTargetMin	Double precision floating-point number (double) Range: ±1.79×10^(-308) ~ ±1.79×10^(+308) (IEEE 754 Double)		Target data minimum value
pointTargeMax	Double precision floating-point number (double) Range: ±1.79×10^(-308) ~ ±1.79×10^(+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 = ⌈(readQuantity)/8⌉ - 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 = readQuantity × 2 - Modbus addresses grouped by 1, mapped left to right in stData (two bytes per address)		Custom Status Value. Note: Not applicable for write commands.
tagName	String, length 1–128 characters. Allowed characters: uppercase/lowercase letters, digits, “.”, “_”, “~”, “-”. Must not duplicate other tag names in the device. Reserved name "status" cannot be used.		Tag Name

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

Modbus RTU/ASCII

Basic Settings

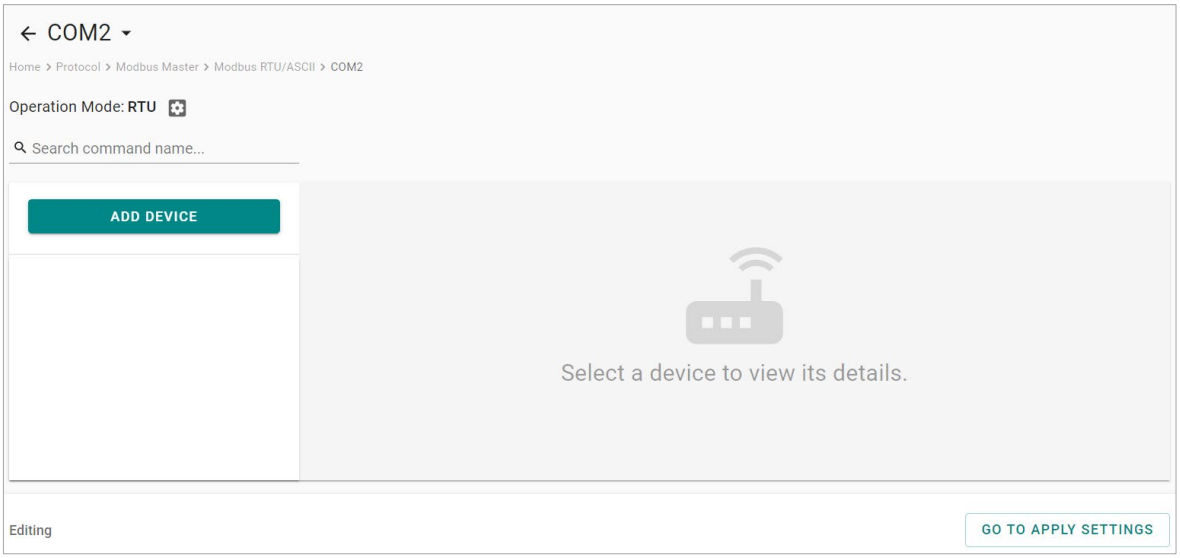
When you access the Modbus RTU/ASCII settings page, you will first need to configure the basic settings.



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

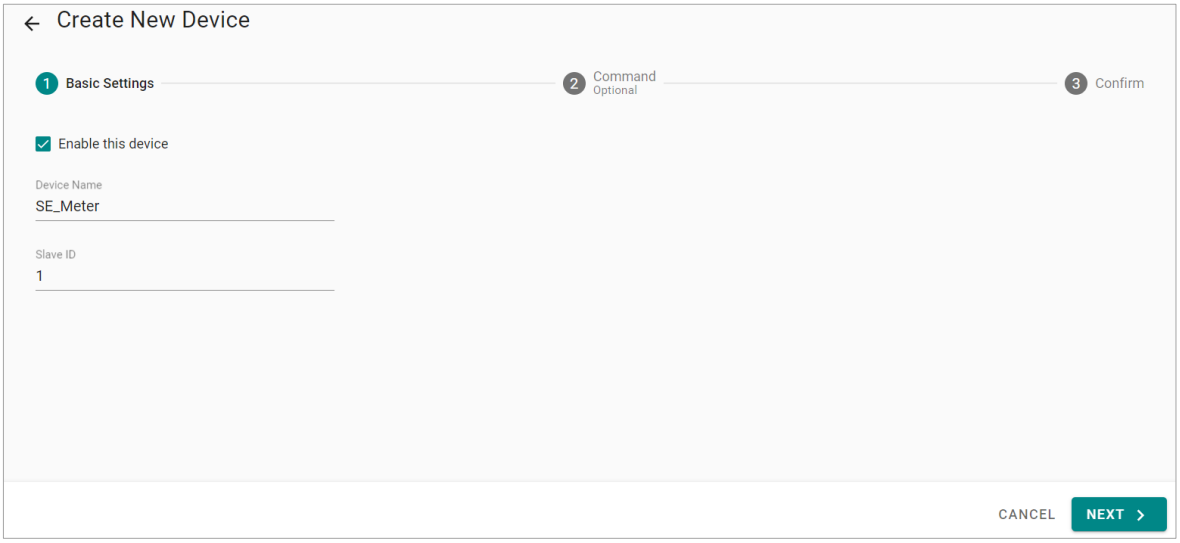
Modbus Device Settings

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



Step 1. Basic Settings

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

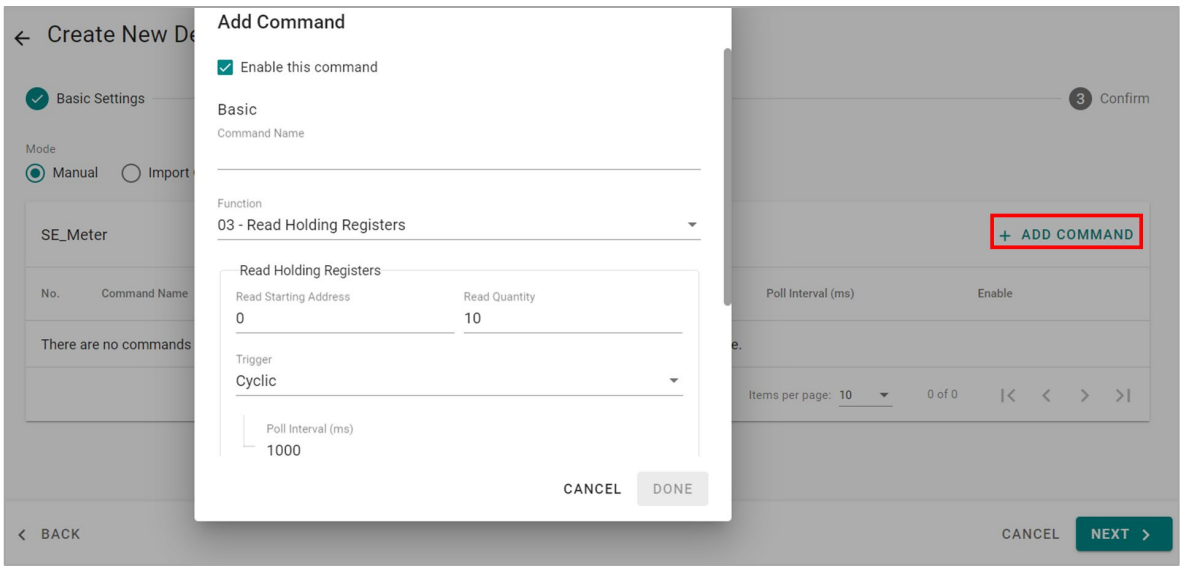


Parameter	Value	Default	Description
Device Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name your Modbus device
Slave ID	1 to 255	–	The slave ID of a remote slave device.

Step 2. Command

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

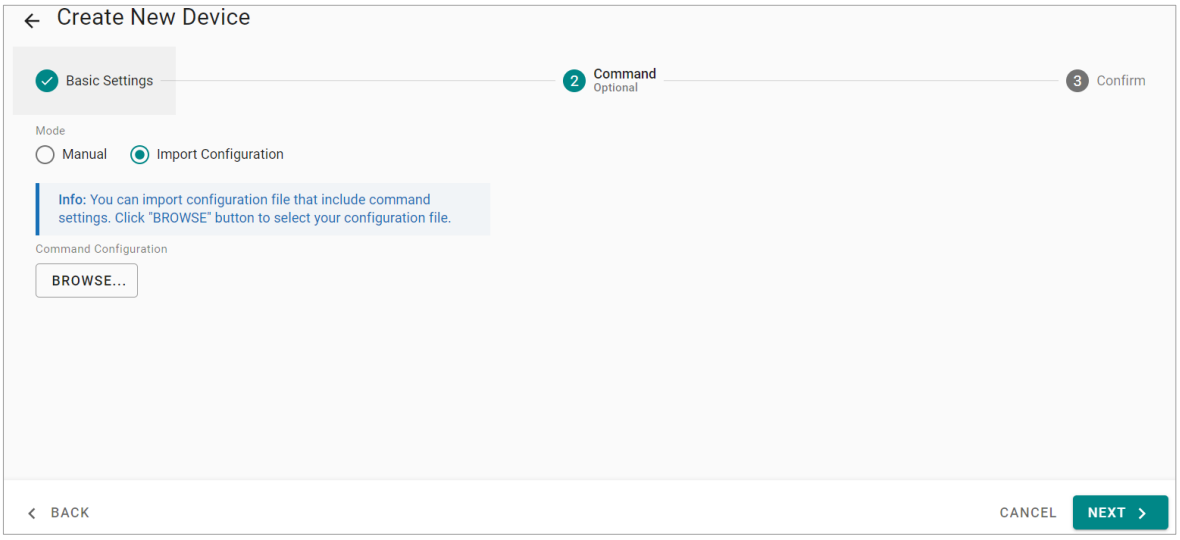
The command settings will pop up.



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

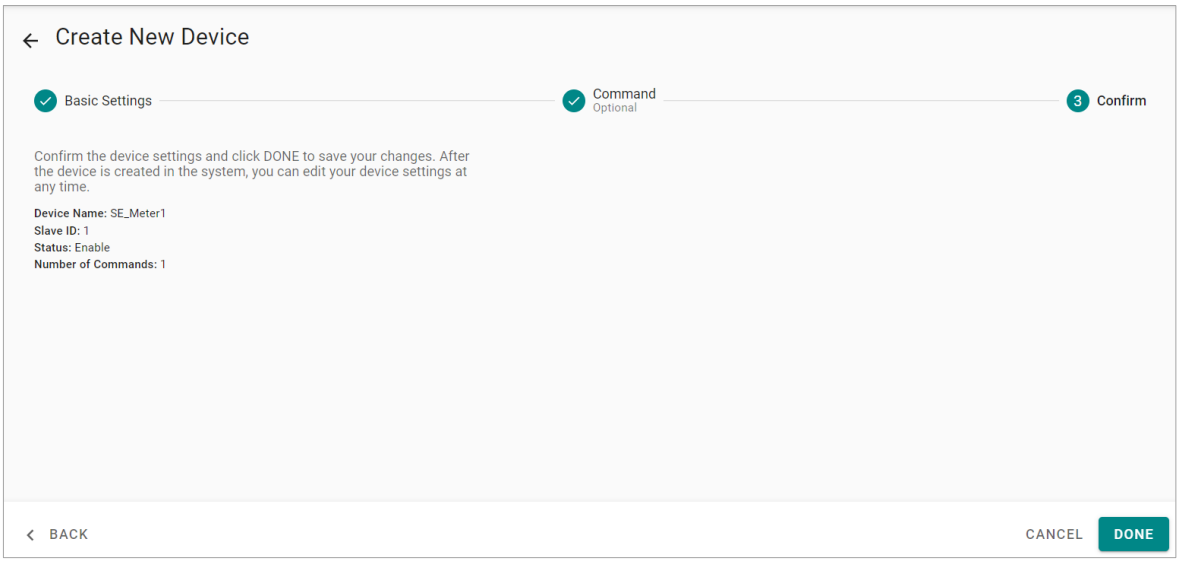
Parameter	Value	Default	Description
Read quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how much data to read
Write starting address	0 to 65535	0	Modbus registers the address for the written data
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	**None:** not to swap **Byte:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C **Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. **Byte and Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	pause	The defined value of the Status Term will be effective when the read command encounters an error or time out.
Tag Type	boolean int16 int32 int64 uint16 uint32 uint64 float double string	–	The command will be generated into a meaningful tag by tag type and stored in the tag hub.

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

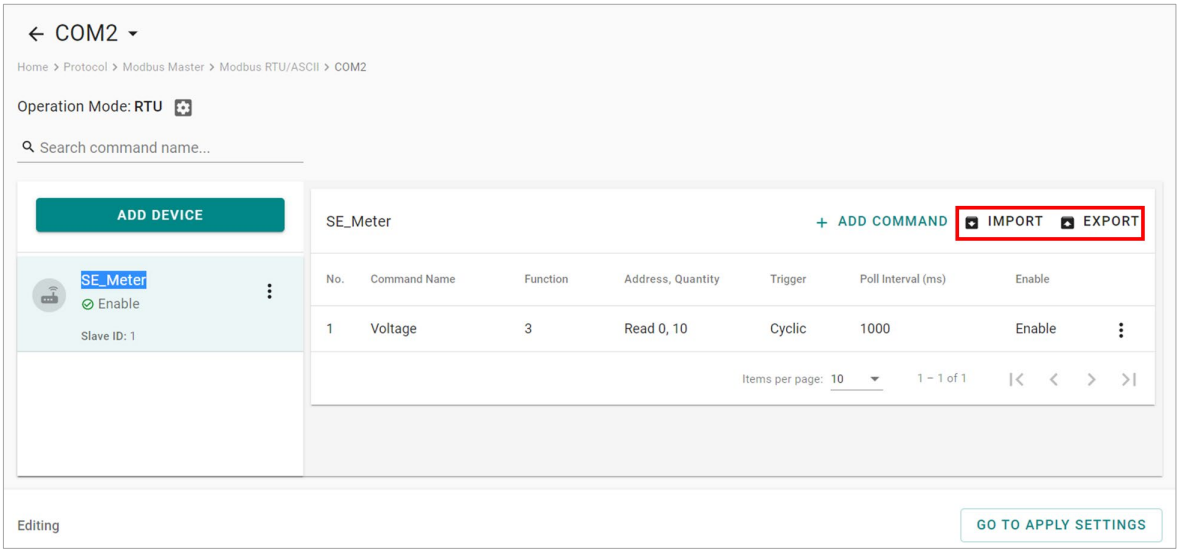


Step 3. Confirm

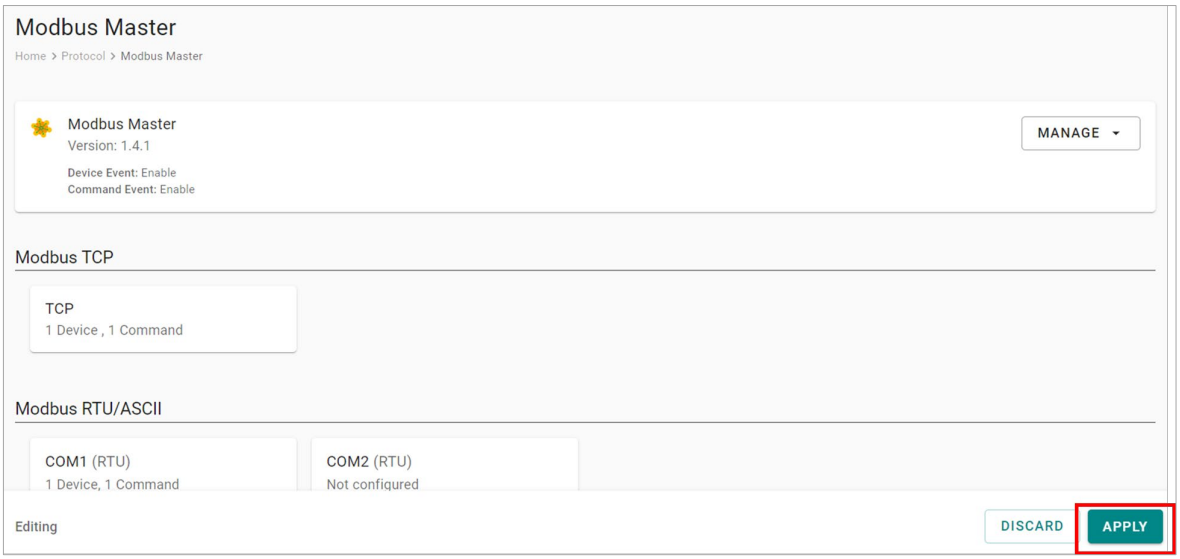
Review the settings and click **DONE** to apply them.



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

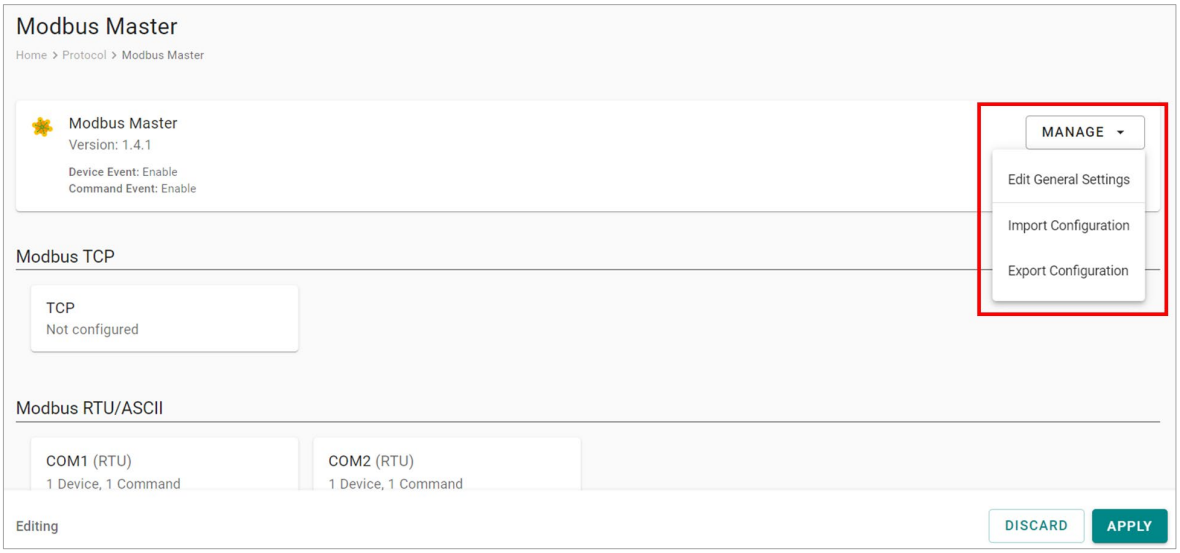


After finishing all the settings, press **GO TO APPLY SETTINGS** and click **APPLY** for the settings to take effect.



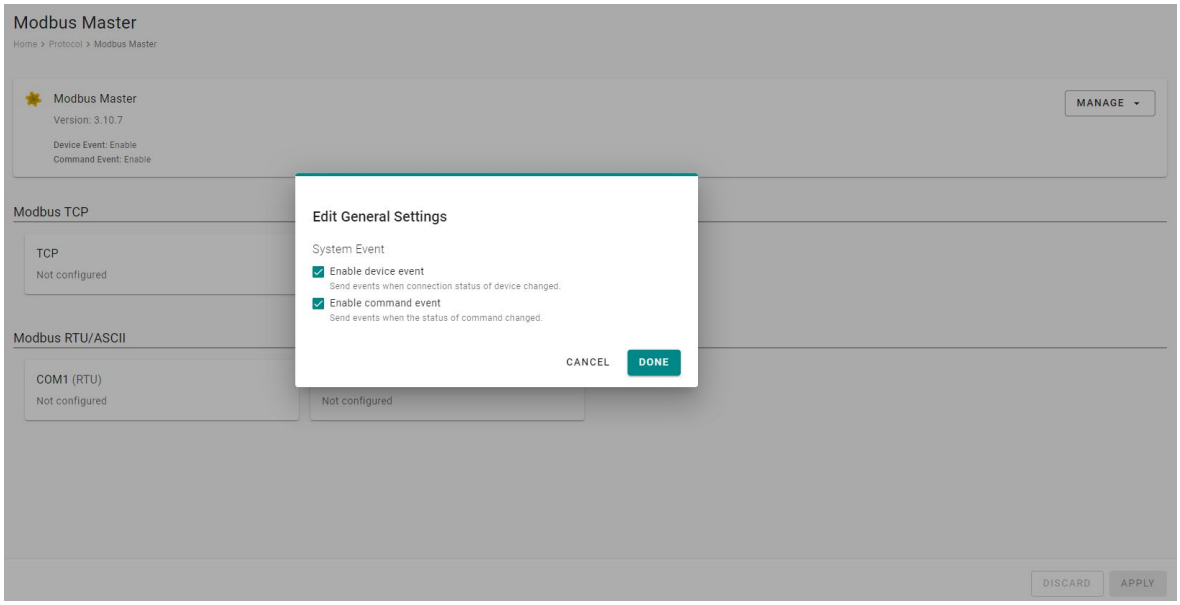
Management

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



Edit General Settings

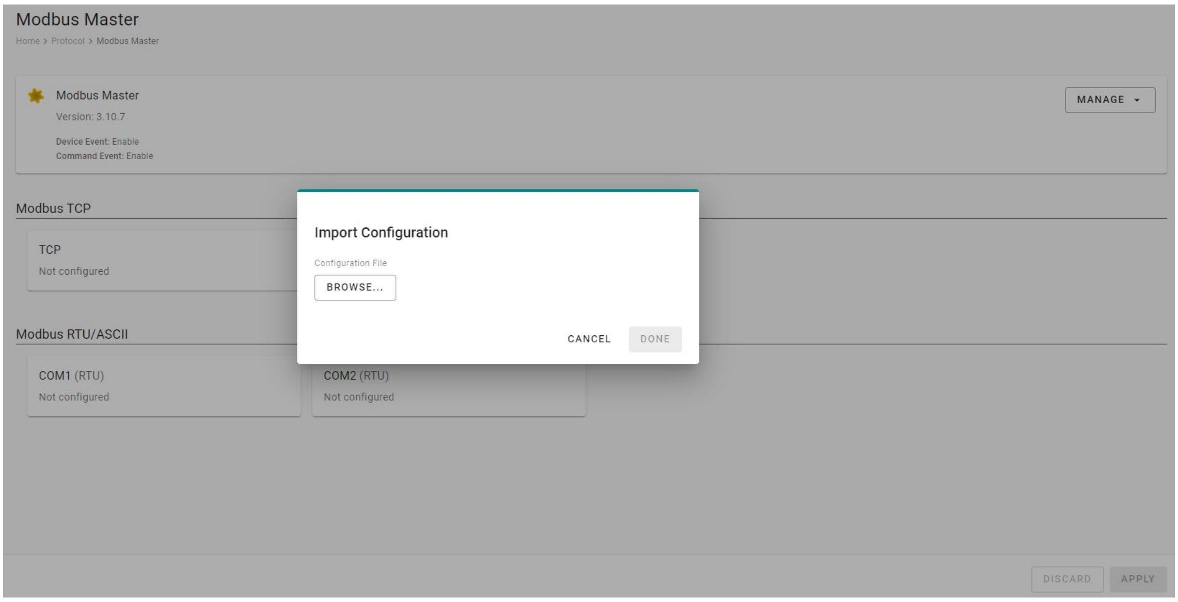
Once your northbound main system wants to monitor the Modbus communication status, you can enable this function.



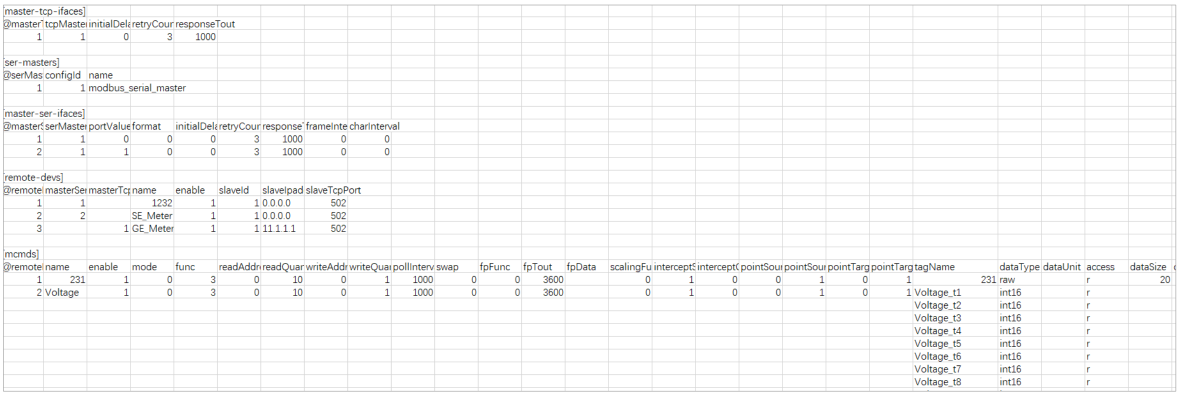
Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	**Check:** If the Modbus communication fails, e.g., Modbus exception code is received The Modbus response timeout and the value of the status tag in the tag hub will change to 1. **Uncheck:** Disable the function
Enable command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

Import/Export Configuration

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



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



[master-tcp-ifaces]

@master	tcpMaste	initialDela	retryCour	responseTout
1	1	0	3	1000

[ser-masters]

@serMas	configId	name
1	1	modbus_serial_master

[master-ser-ifaces]

@master	serMaste	portValue	format	initialDela	retryCour	response	frameInte	charInterval
1	1	0	0	0	3	1000	0	0
2	1	1	0	0	3	1000	0	0

[remote-devs]

@remote	masterSe	masterTc	name	enable	slaveId	slaveIpad	slaveTcpPort
1	1		1232	1	1	0.0.0.0	502
2	2		SE_Meter	1	1	0.0.0.0	502
3		1	GE_Meter	1	1	11.1.1.1	502

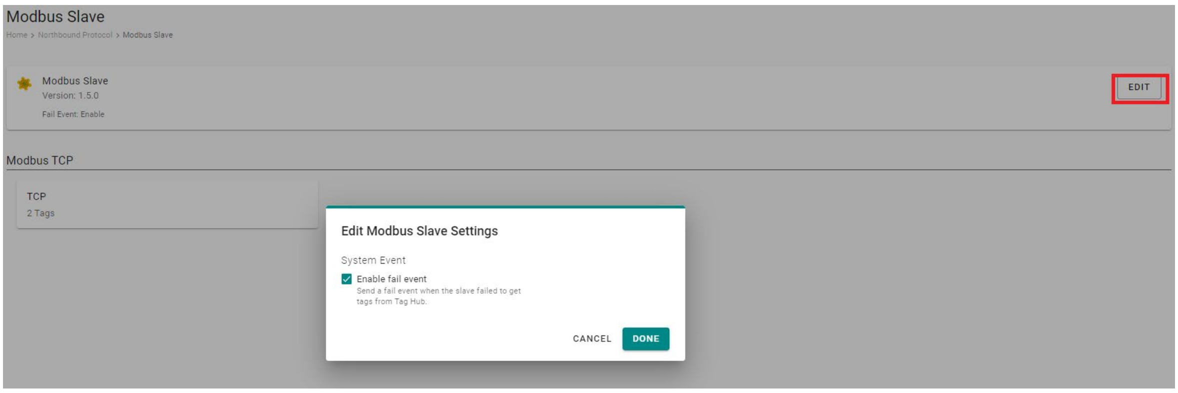
[mcmds]

@remote	name	enable	mode	func	readAddr	readQuar	writeAddr	writeQuar	pollInterv	swap	fpFunc	fpTout
1	231	1	0	3	0	10	0	1	1000	0	0	3600
2	Voltage	1	0	3	0	10	0	1	1000	0	0	3600

@remote	fpData	scalingFu	interceptS	interceptC	pointSour	pointSour	pointTarg	pointTarg	tagName	dataType	dataUnit	access	dataSize
1		0	1	0	0	1	0	1	231	raw		r	20
2		0	1	0	0	1	0	1	Voltage_t1	int16		r	
									Voltage_t2	int16		r	
									Voltage_t3	int16		r	
									Voltage_t4	int16		r	
									Voltage_t5	int16		r	
									Voltage_t6	int16		r	
									Voltage_t7	int16		r	
									Voltage_t8	int16		r	

Modbus TCP Slave

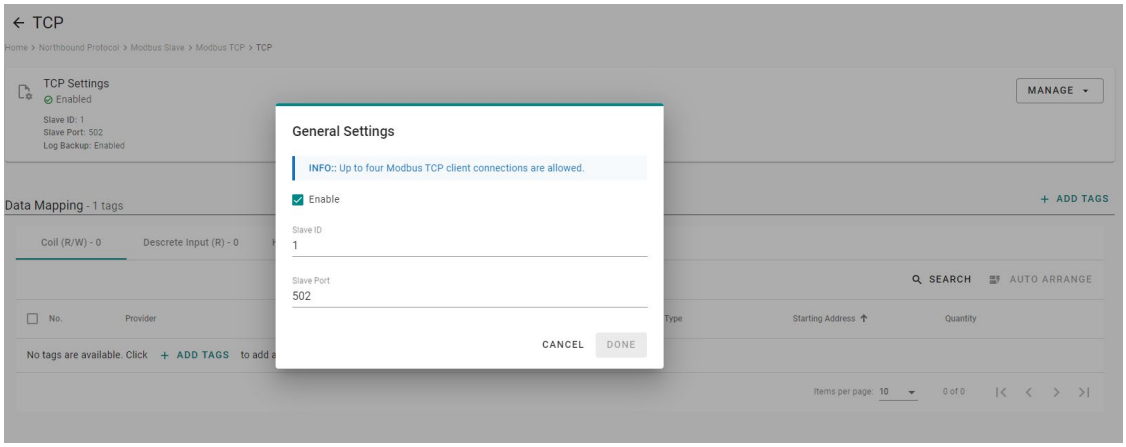
Go to **Modbus Slave** and click **EDIT** to modify the Modbus Slave advanced settings. You must enable the Modbus TCP server to communicate with SCADA as a Modbus TCP client. If you want an event added to the event log when the Modbus TCP connection gets disconnected, select **Enable fail event**.



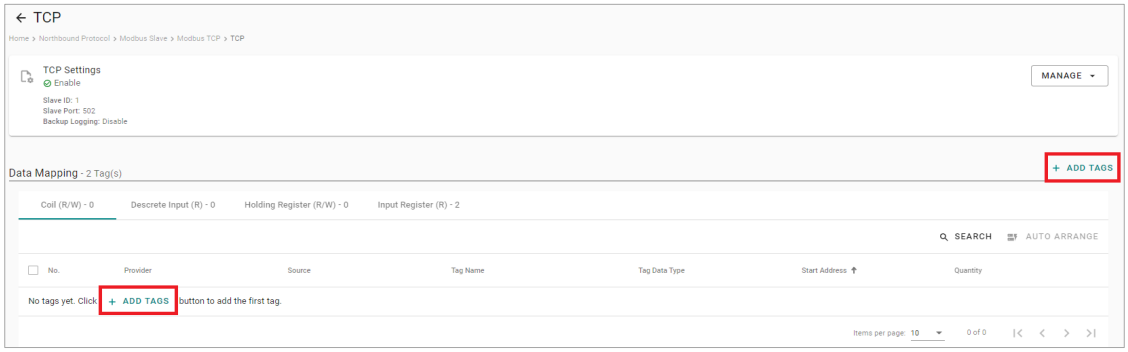
To create a Modbus TCP server (slave), do the following:

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

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



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

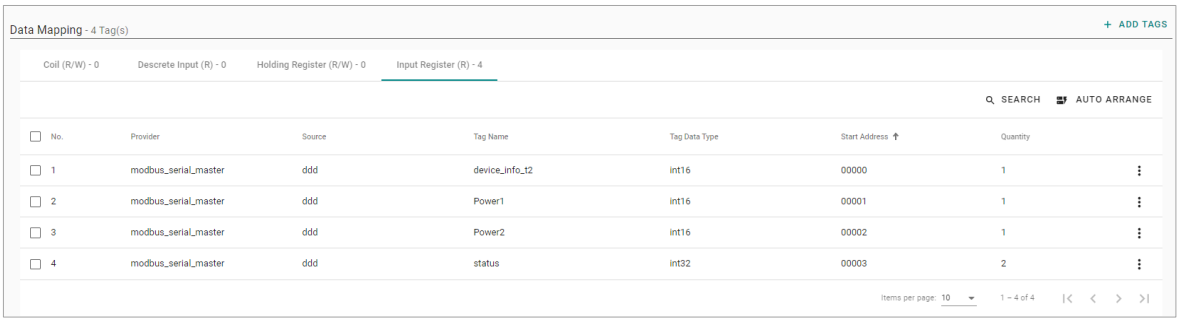


5. Click **DONE** to complete settings.

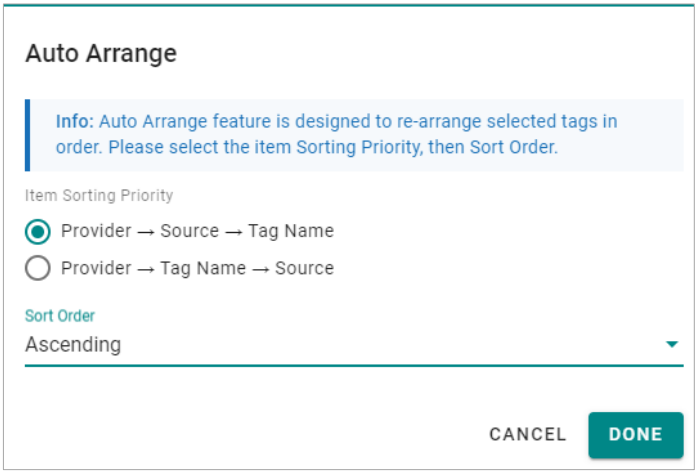
Data Mapping

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

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



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



Backup Logging

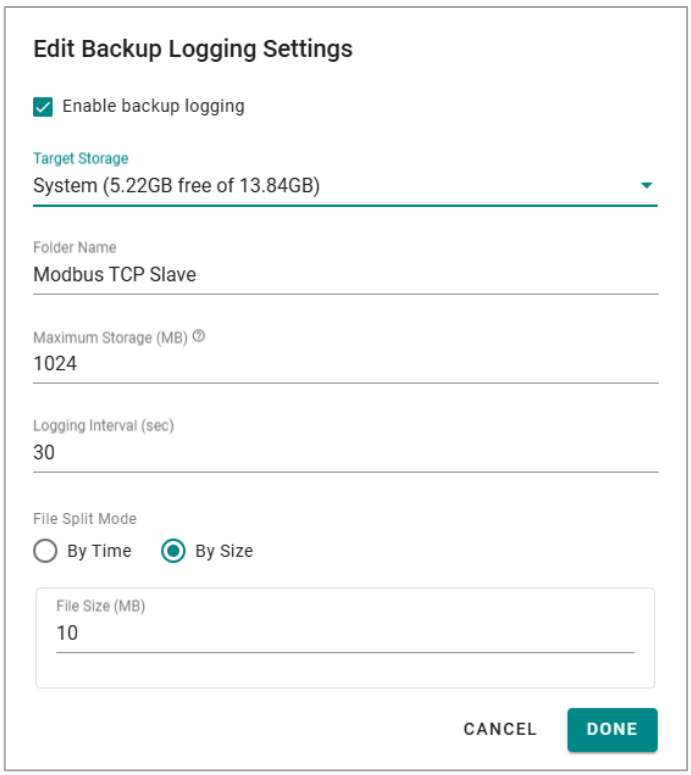
If you want to enable the data logger function, go to **MANAGE > Backup Logging > Edit Settings** to enable the feature.

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.

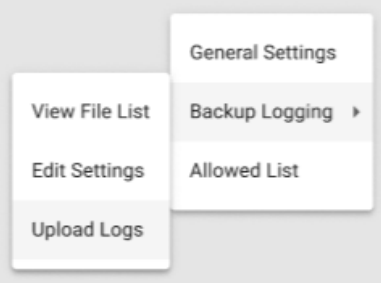
To enable log backups, do that following:

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.**

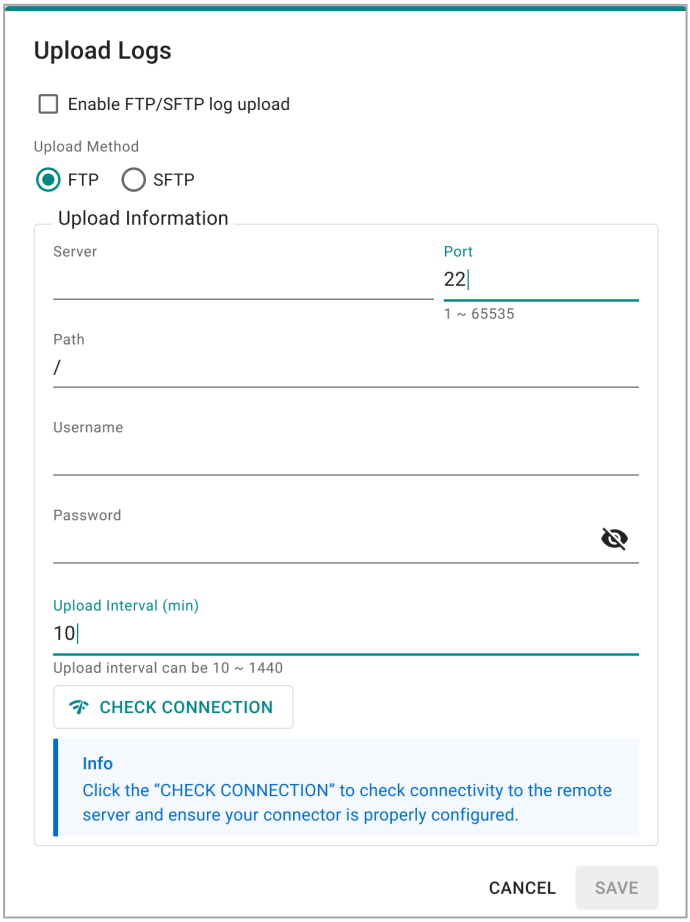


To upload log files via FTP, do the following:

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

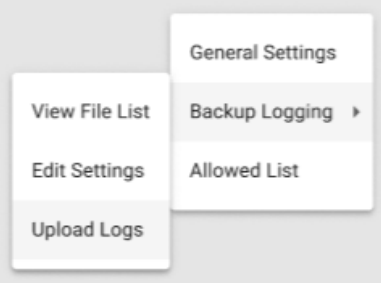


2. Select **Enable the FTP/SFTP uploader**.
3. Select **FTP** for **Upload Method**.
4. Enter the necessary parameters: **Server**, **Port**, **Path**, **Username**, and **Password**.
5. Set the **Upload Interval**.
6. (optional) Click **CHECK CONNECTION** to verify that the communication is working.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

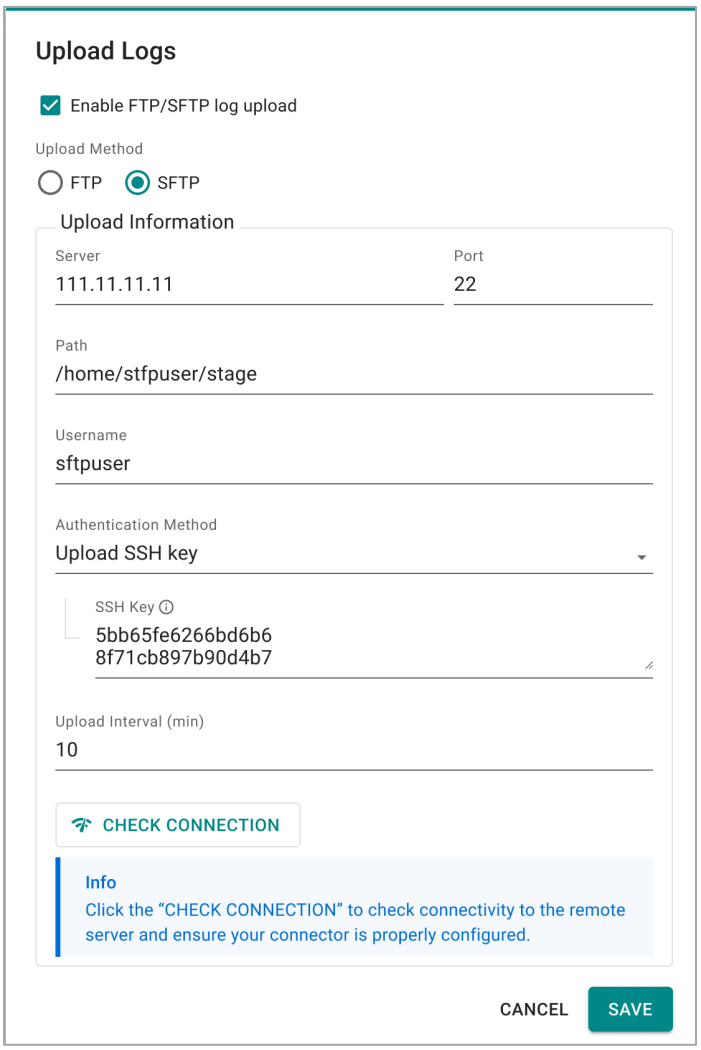


To upload files via SFTP, do the following:

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.



Modbus Capability:

Max. # of Serial Slave Device 31

Max. # of TCP Slave Device 64

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

Max. # of Tags for Modbus Master 3000

Max. # of Tags for Modbus Slave 4500

Max. # of Commands for a Slave Device 256

Max. # of Commands for a TCP Slave Device 2048

NOTE

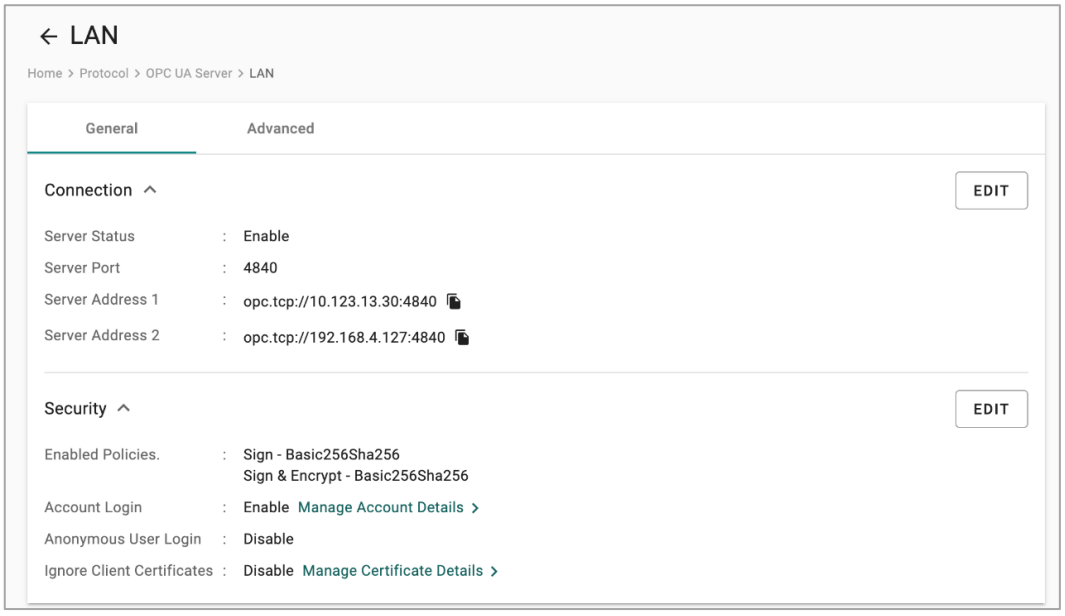
After using **CHECK CONNECTION**, if you observe a connection failure, or if you notice in the Event Log that data cannot be uploaded via FTP/SFTP, do one the following to troubleshoot the issue:

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

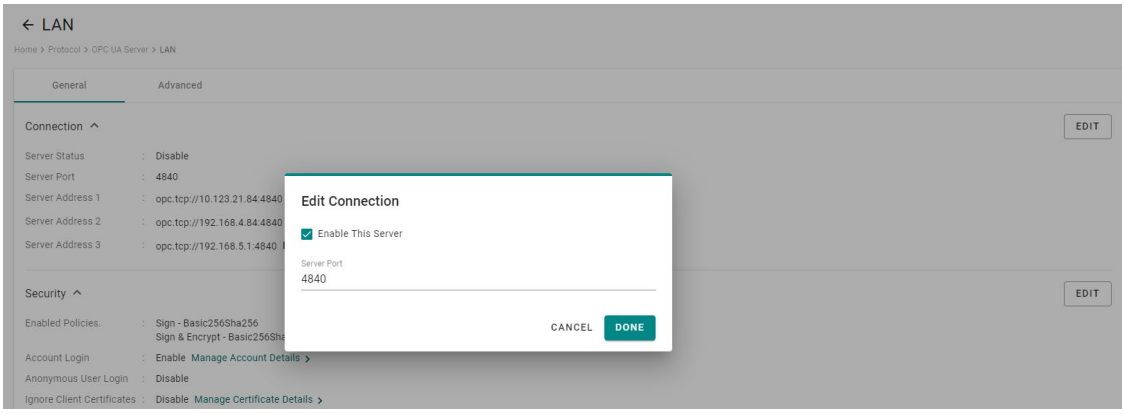
OPC UA Server

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

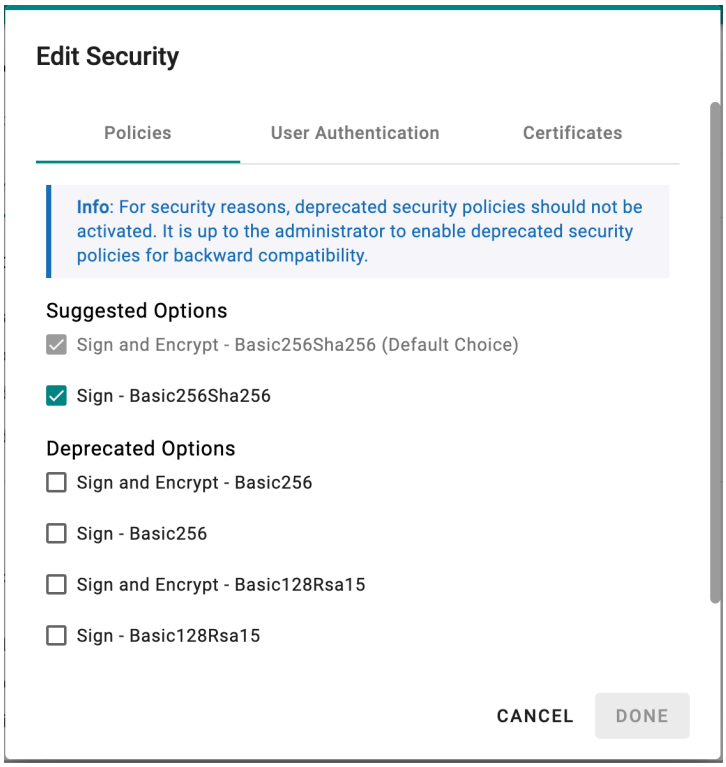
To enable the OPC UA Server, click **LAN** and do the following:



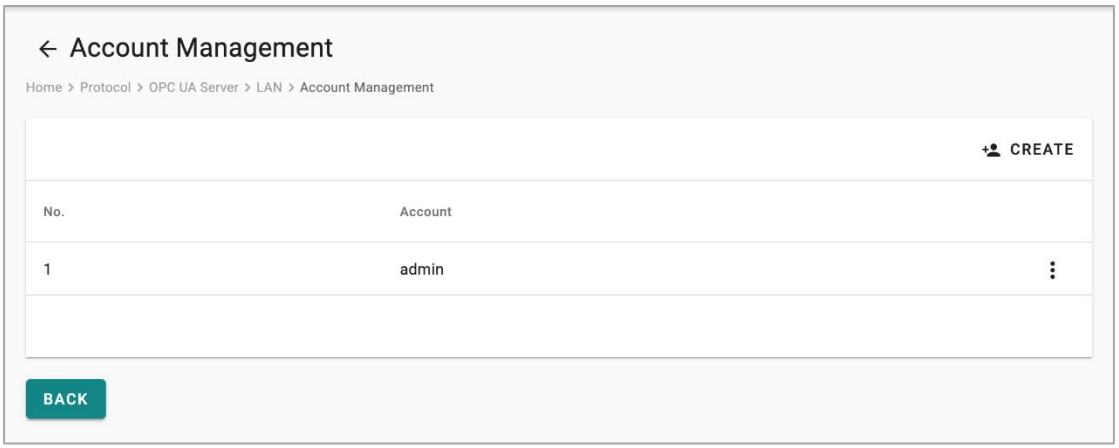
1. Click Connection **EDIT**, select **Enable This Server**, and click **DONE.**
   The service is enabled by default on port 4840.



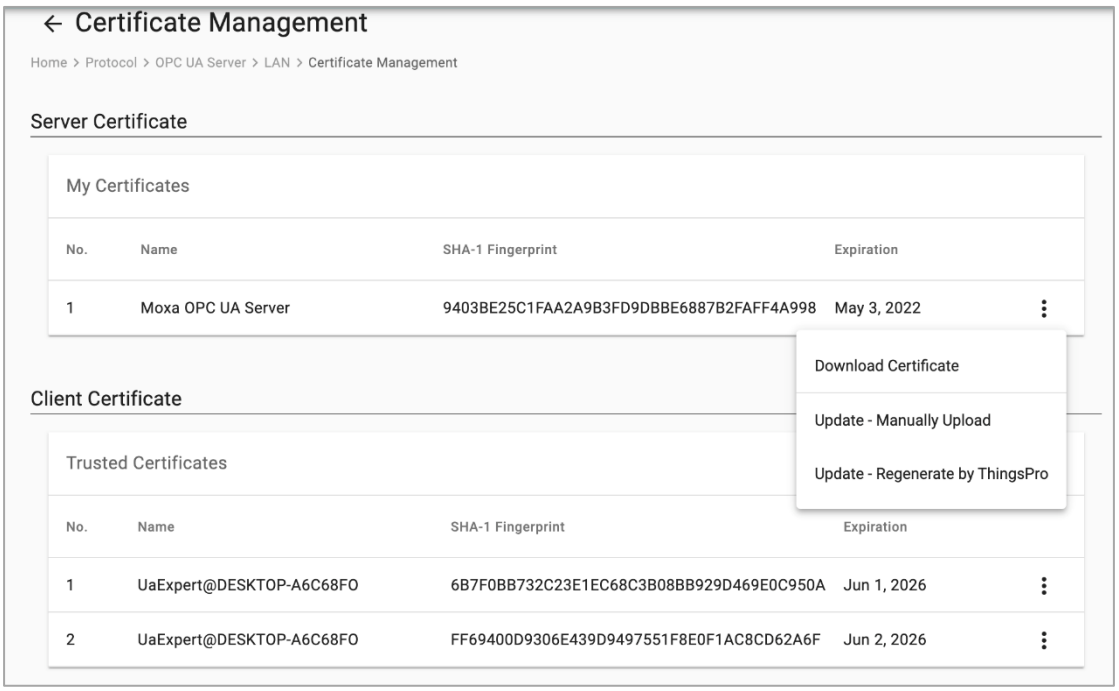
2. (Optional) Click Security **EDIT** to edit Policies, User Authentication, and Certificates.

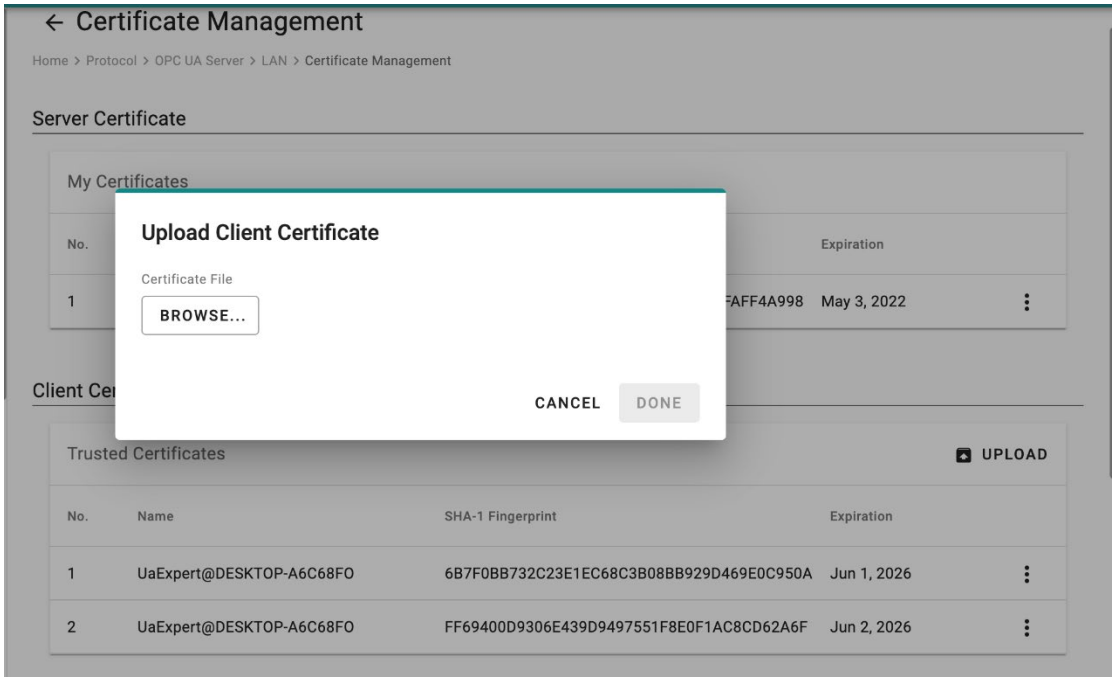


3. Click **Manage Account Details** to **CREATE** new accounts.
   The default account/password is **admin/moxa** (for firmware version of v1.7.0 and prior).
   a. Click **CREATE**.
   b. Specify an **Account** and **Password**.
   c. Click **DONE**.

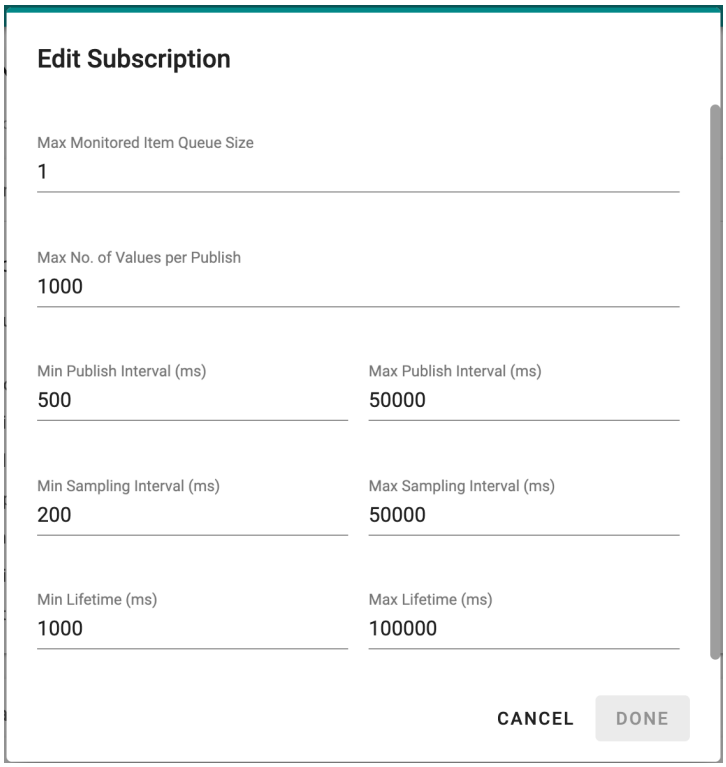


4. (Optional) Click **Manage Certificate Details** to download the server certificate or upload a client certificate.

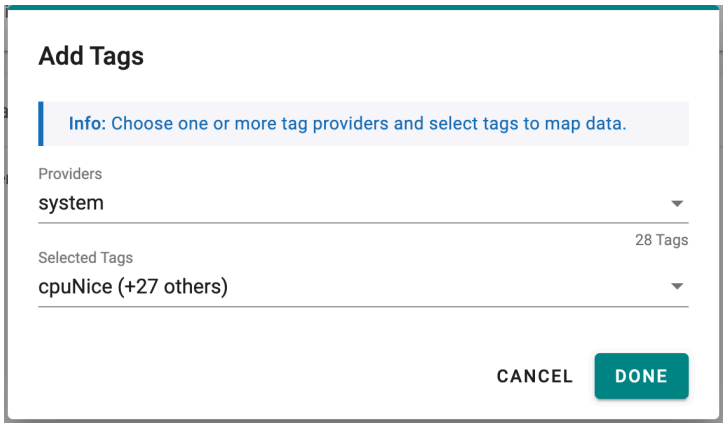




5. (Optional) Click **Advanced > EDIT** to configure the subscription settings here.

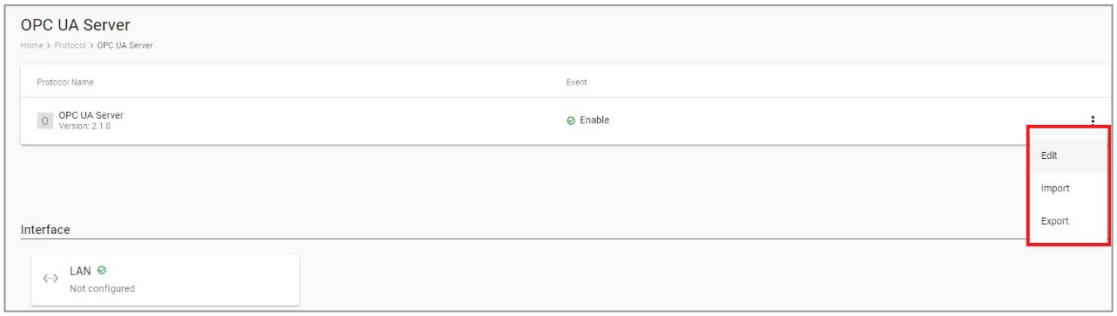


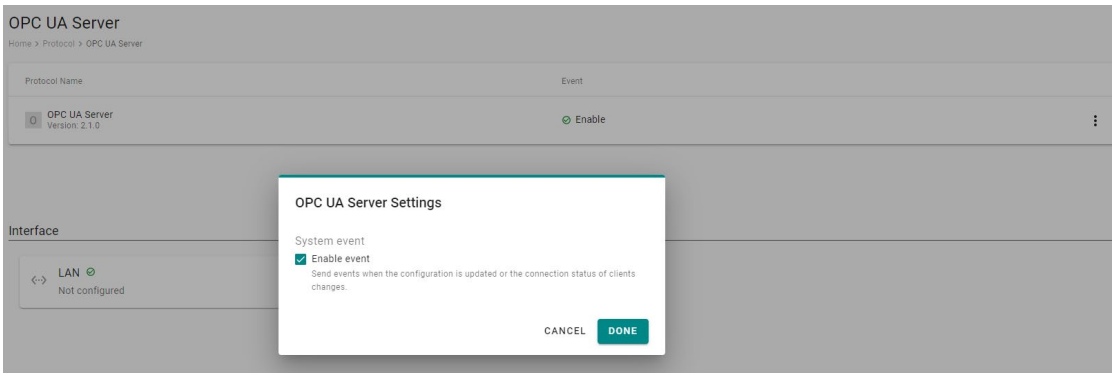
6. Click **ADD TAGS** and select providers and tags.



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

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





Edge Computing

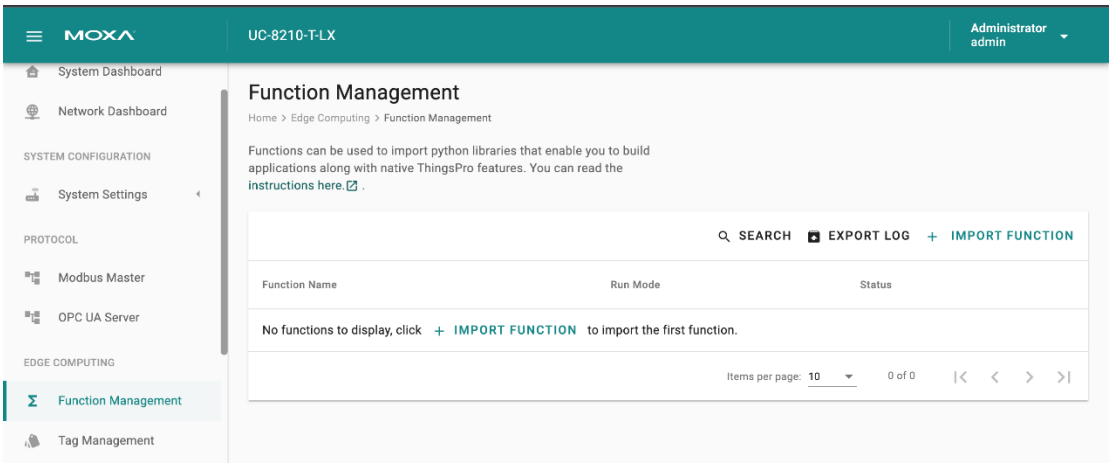
Function Management

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

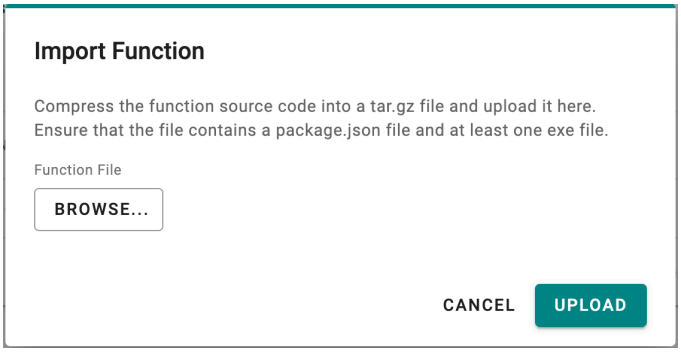
Go to **Edge Computing > Function Management** to import and manage functions. For additional information, see build your own functions.

To import functions, do the following:

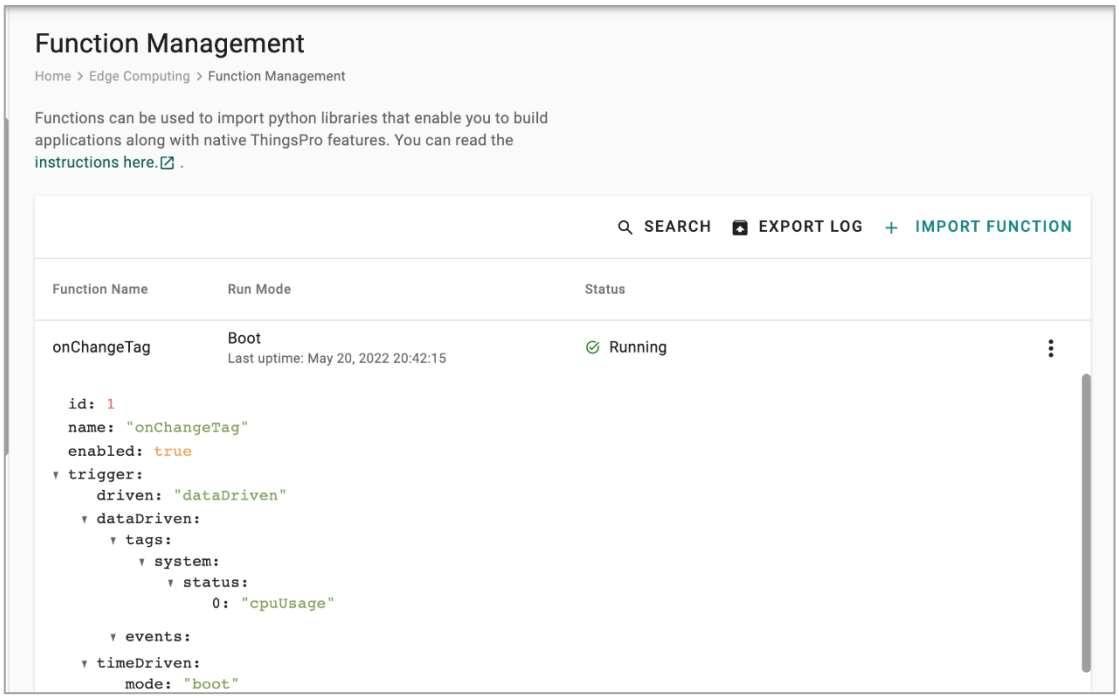
1. Click **IMPORT FUNCTION**.



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



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



	Run Mode
1	Boot
2	Cron job

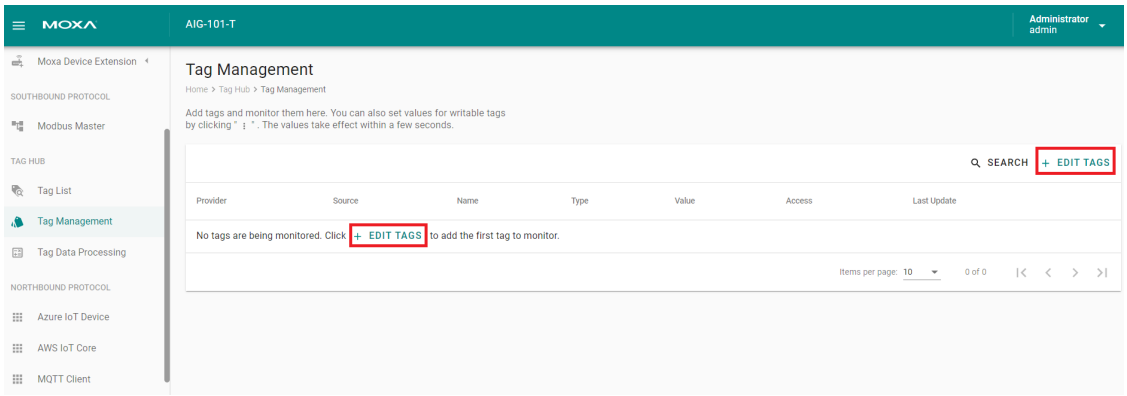
Status	Description
Running	The function is running
Retrying	Retrying a failed function every 5 seconds (unlimited tries)
Failure	The function failed during a retry. The correspondent error message will be displayed in the table. You can click **EXPORT LOG** to check the logs.
Inactive	The function is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

Tag Management

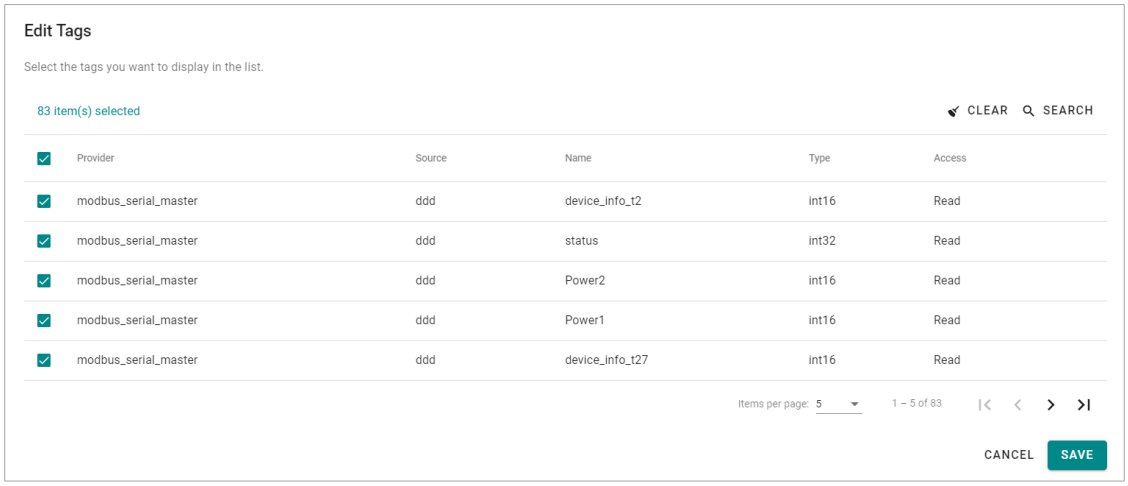
Go to **Tag Management,** where you can create and monitor the real-time tag value for troubleshooting purposes.

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

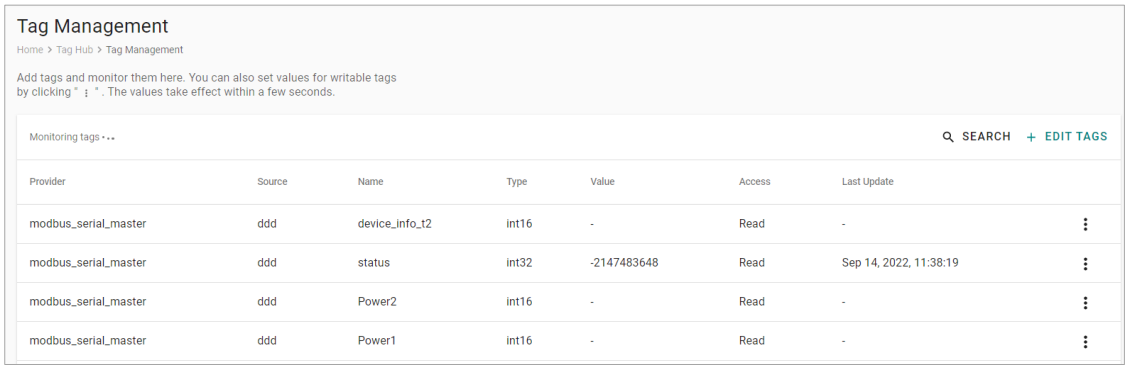
1. Click **+ EDIT TAGS**.



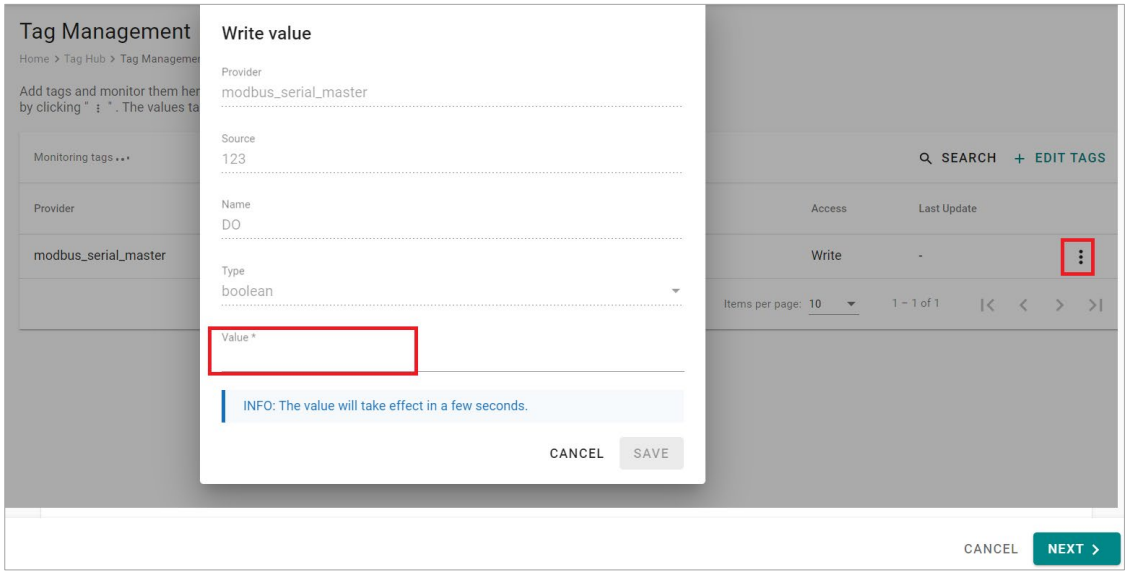
2. Select the **tags** to monitor in the list.



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



4. Click **SAVE**.
5. (Optional) Press the icon to deactivate the monitoring tags.
6. (Optional) Press the icon to write value for test purposes.



NOTE

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

Cloud Connectivity

Azure IoT Edge

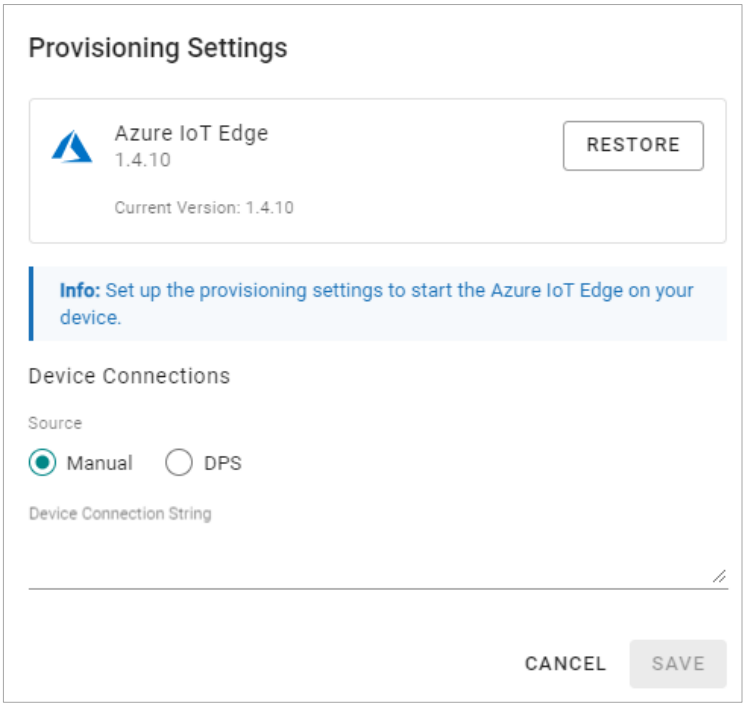
Go to **Cloud Connectivity > Azure IoT Edge** to configure the Azure IoT Edge settings. You can enable/disable the Azure IoT Edge service and enroll the device via manual setting or DPS (Device Provisioning Service) here.

NOTE

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

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

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

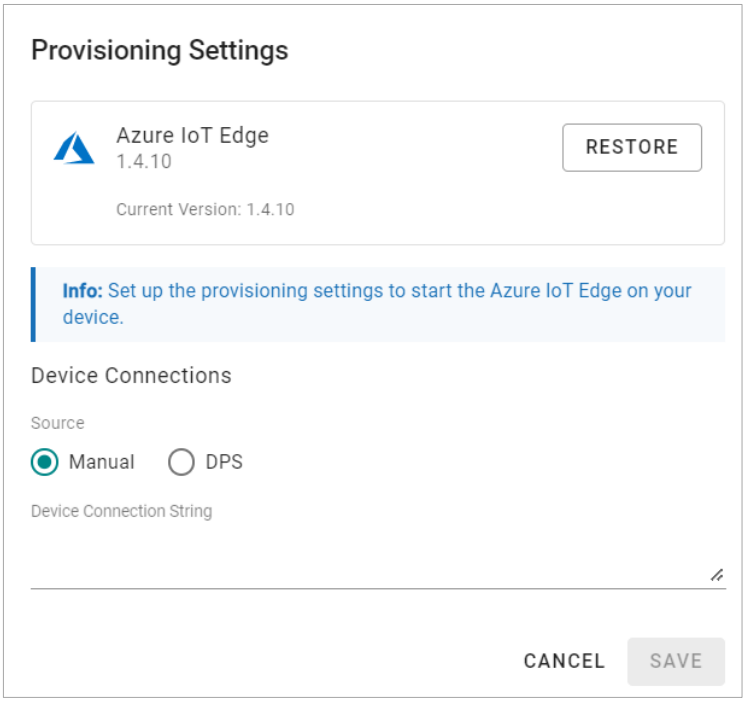


To create an Azure IoT Edge connection for your device via DPS, do the following:

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

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

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



More information about the Azure DPS configuration in the Azure IoT Hub at Set up a DPS.

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

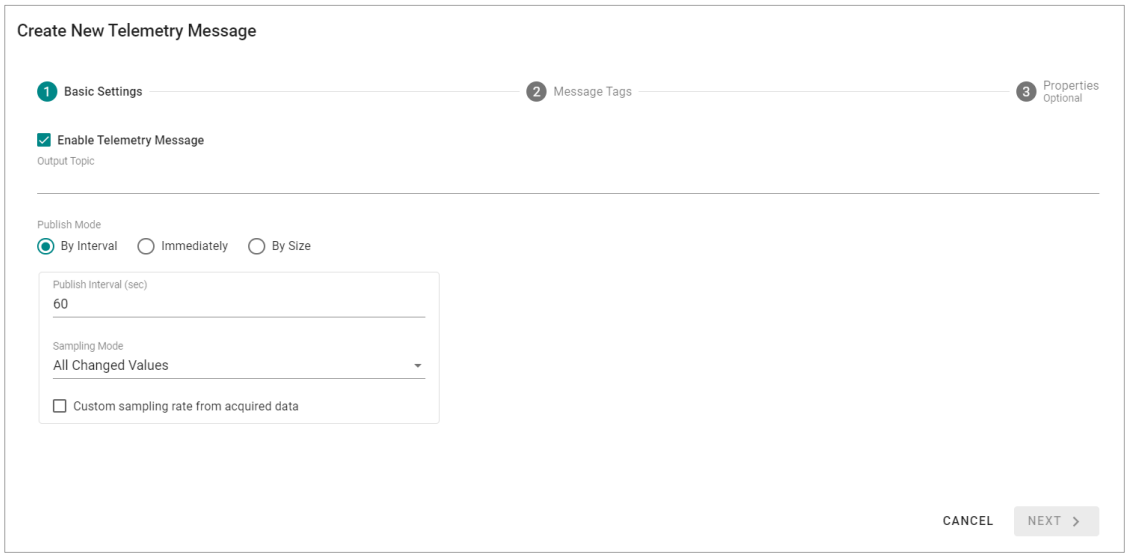
For additional information on AIE Checks, see https://github.com/Azure/iotedge/blob/master/doc/troubleshoot-checks.md.

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

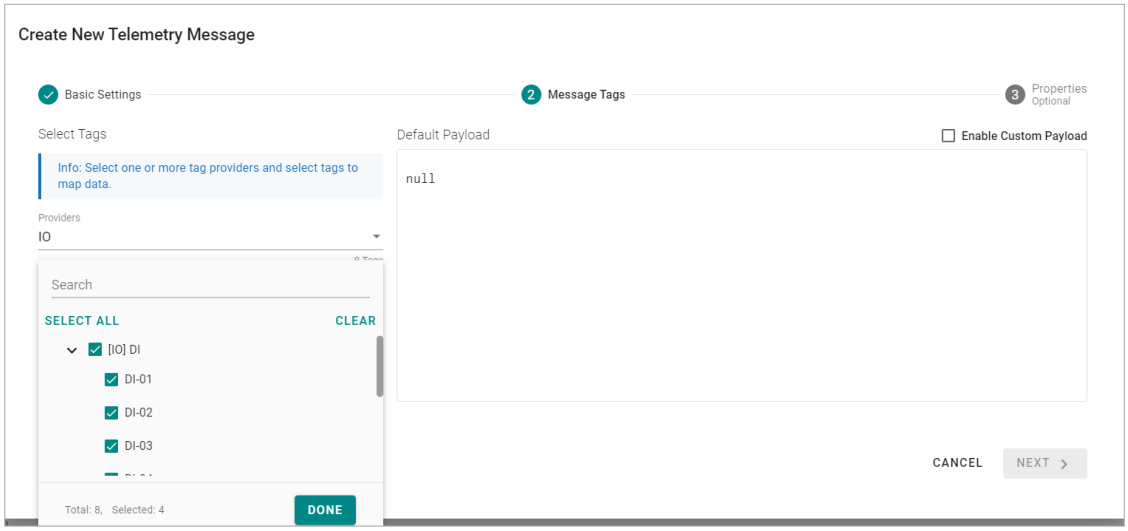
Telemetry Message Settings

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

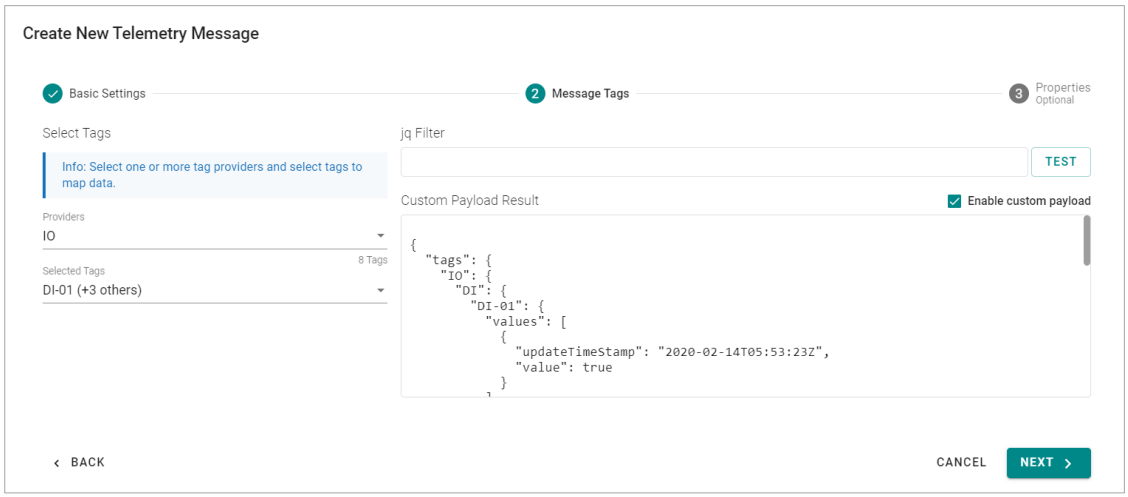
1. Click **+ MESSAGE** to create a new telemetry message.
2. Specify an **Output Topic** name.
3. Select a **Publish Mode**.
   For details, see Publish Mode.



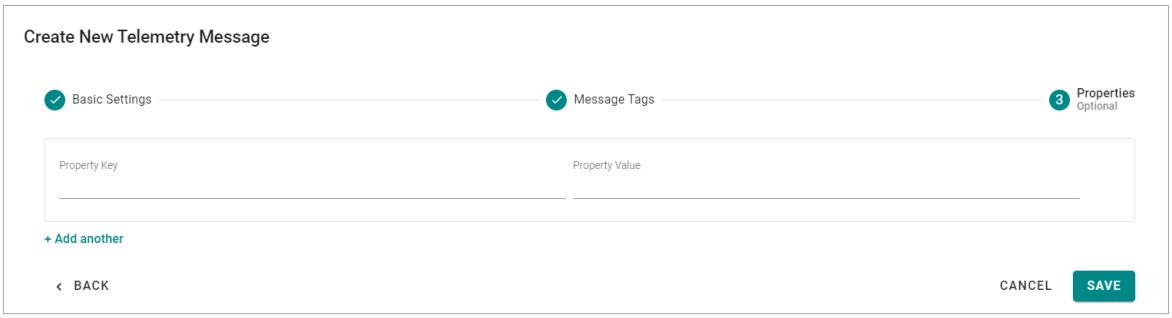
4. Input corresponding parameters such as publish interval, sampling mode, and publish size.
5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).



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/).



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

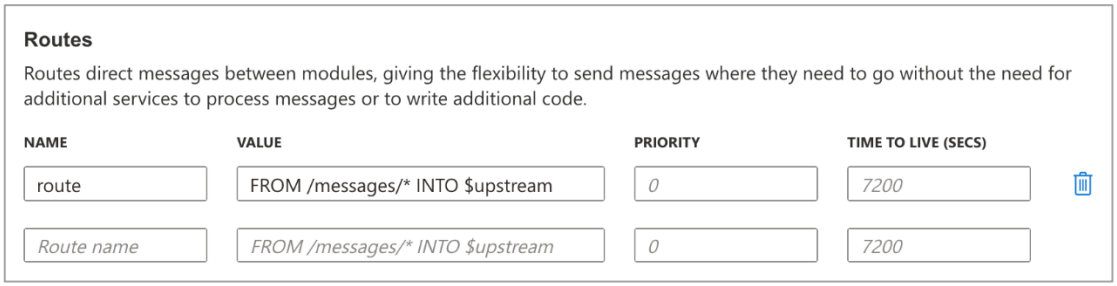


NOTE

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

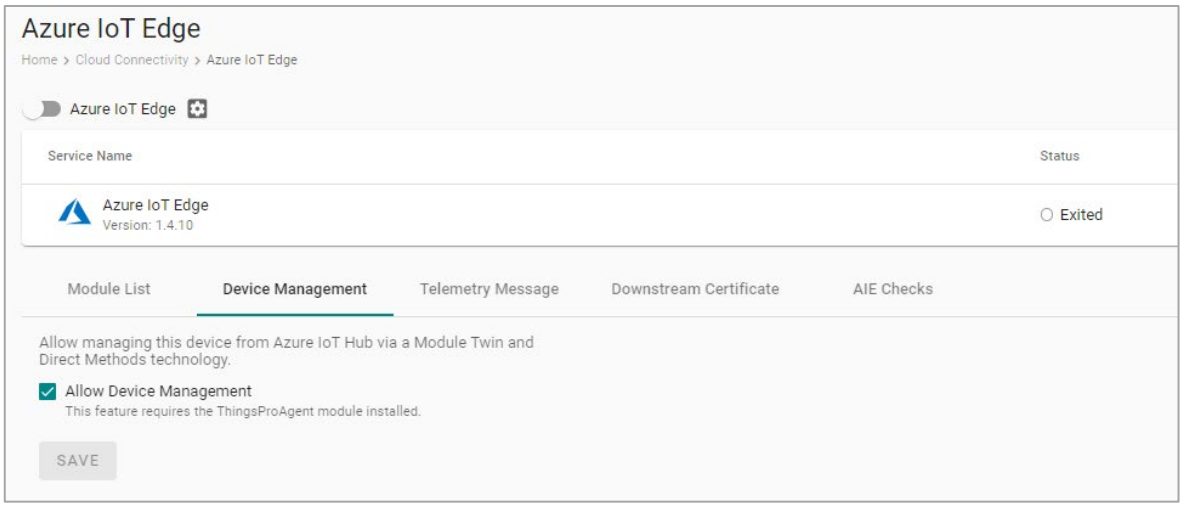
NOTE

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



Device Management Settings

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

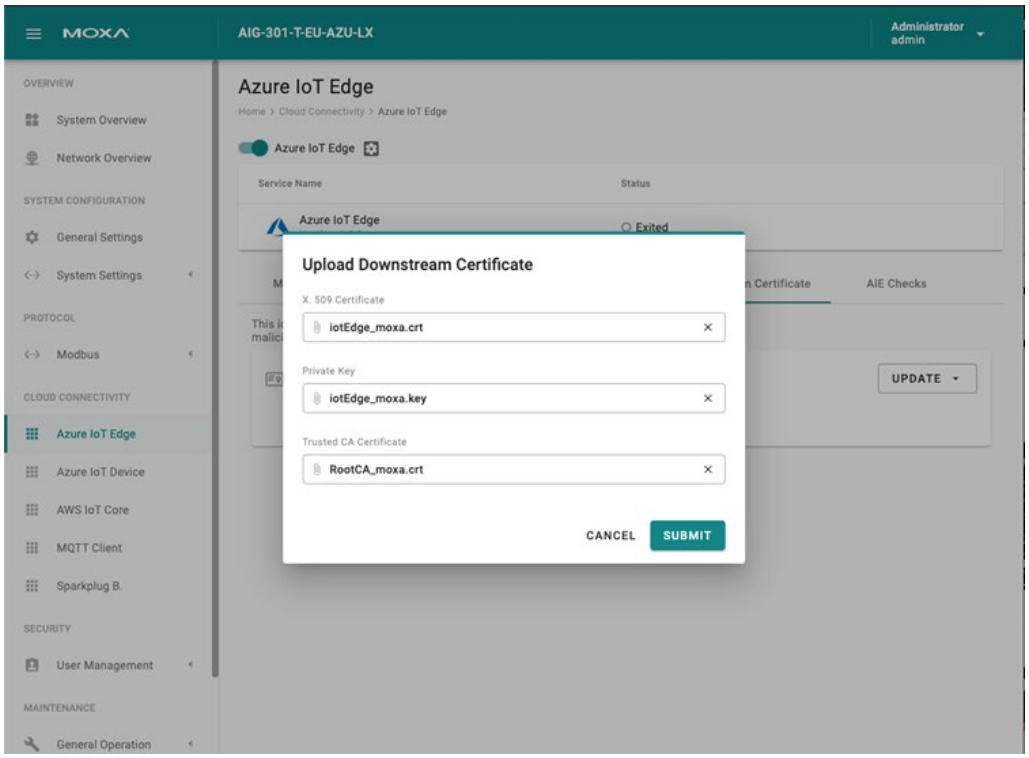


NOTE

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

Downstream Certificate

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



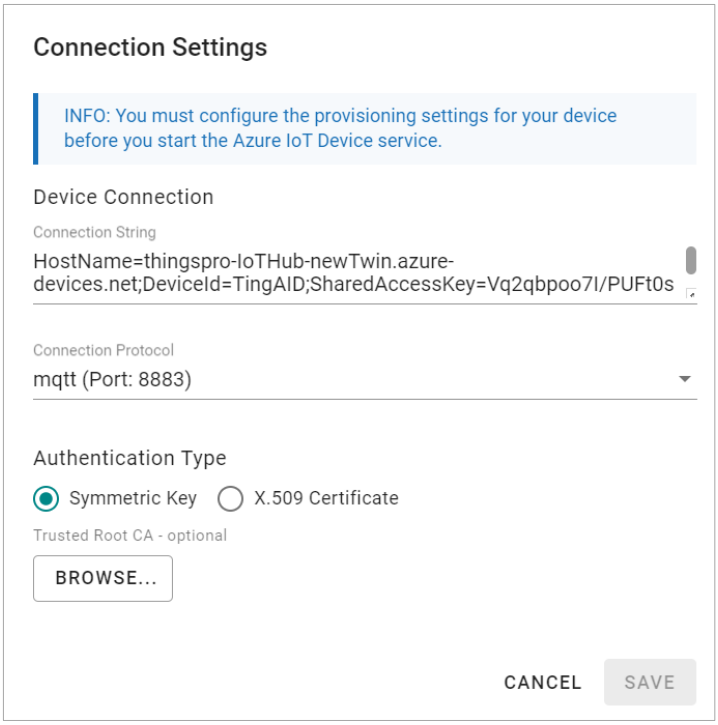
Azure IoT Device

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

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

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

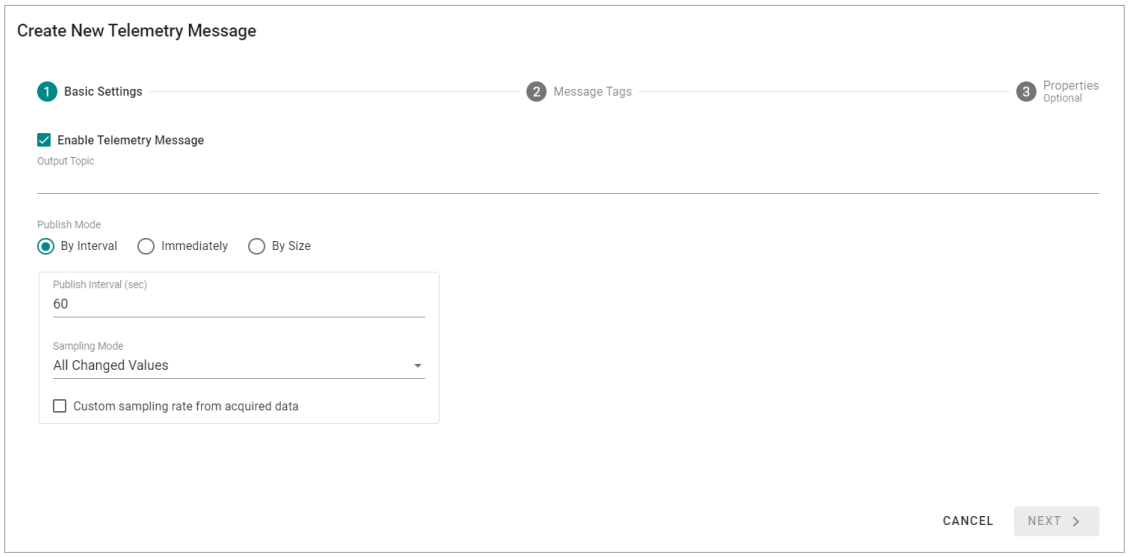
1. Click  to set connection.
2. Enter **Connection String.**
3. Select a **Connection Protocol.**
4. Select an **Authentication Type.**
5. (Optional) Upload X.509 Certificate and Private Key.
6. Click **SUBMIT**.



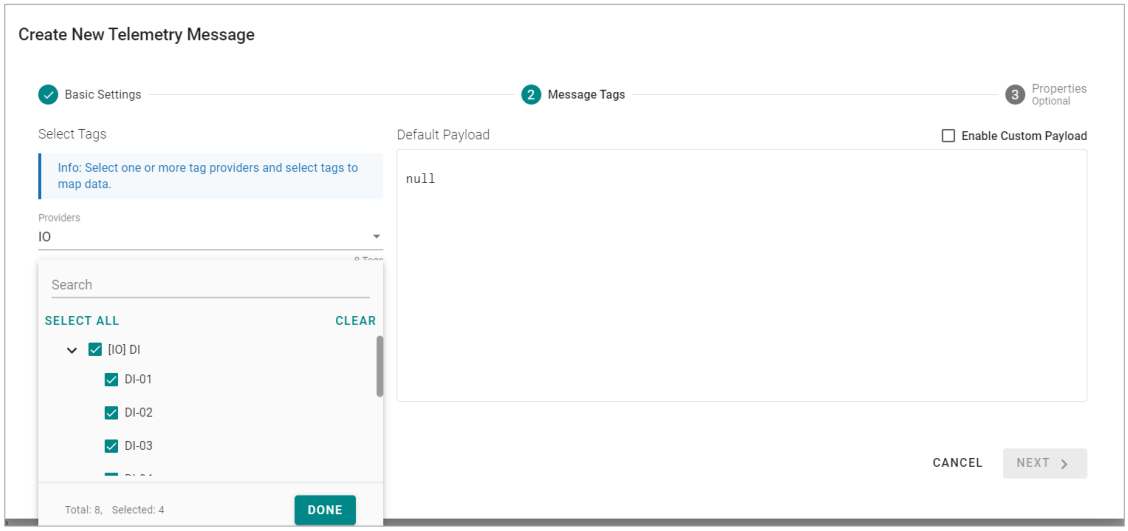
Telemetry Message

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.

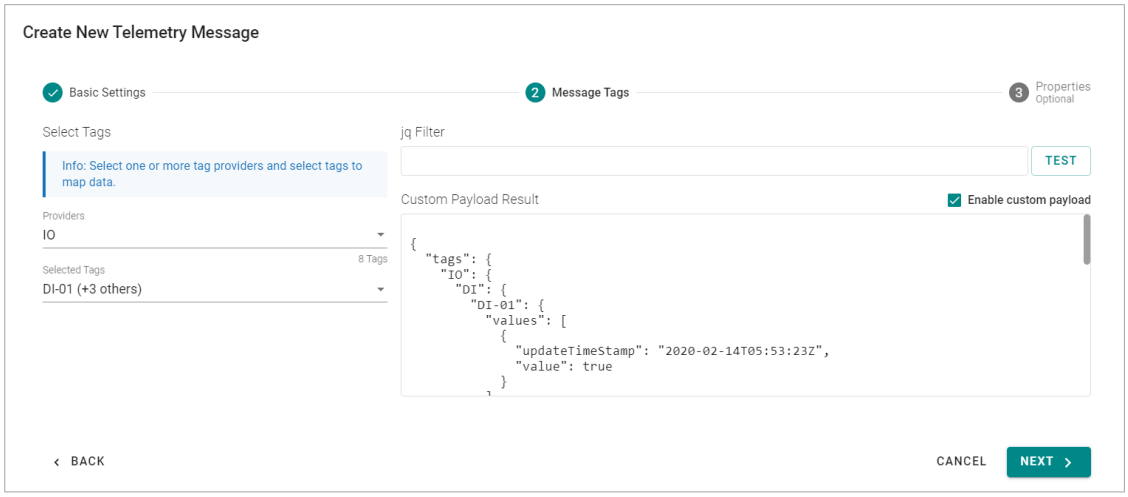


4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **NEXT**.
6. Select tags (e.g., Modbus Master).

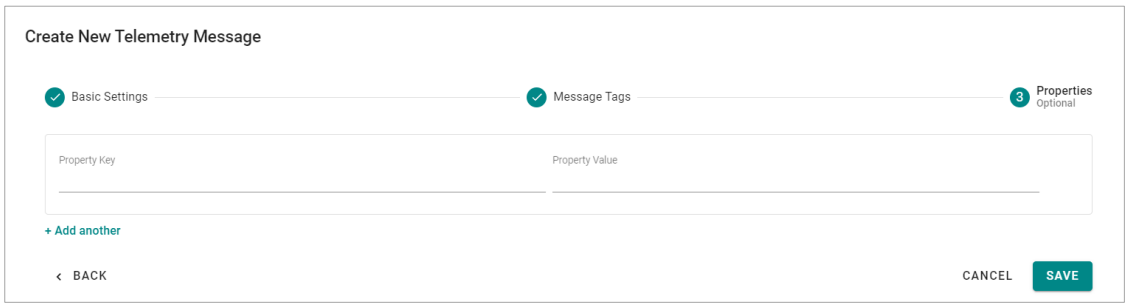


7. (Optional) Enable custom payload by using the **jq** filter.

   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/).



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



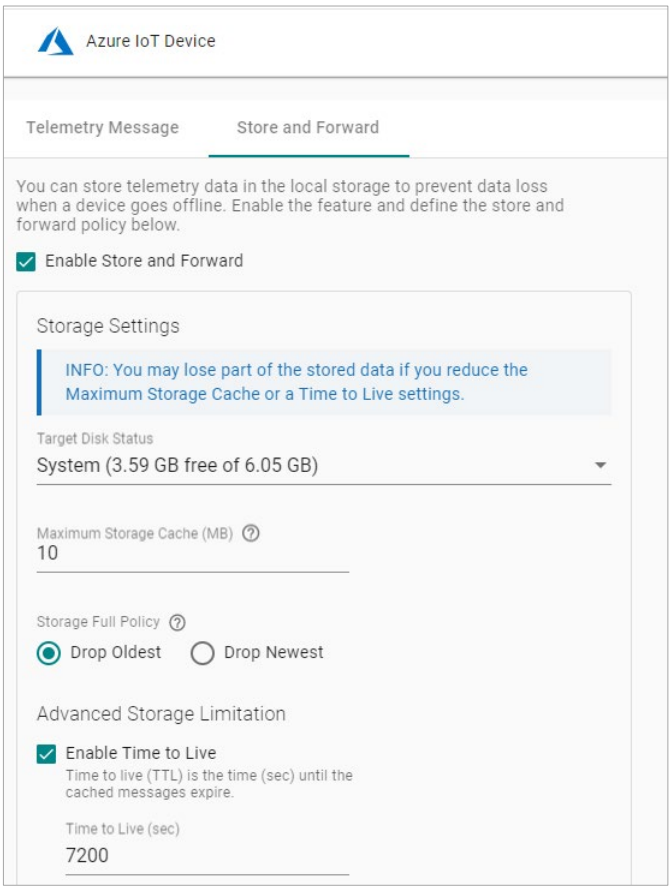
10. Click **SAVE**.

NOTE

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

Store and Forward

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



Device Management

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

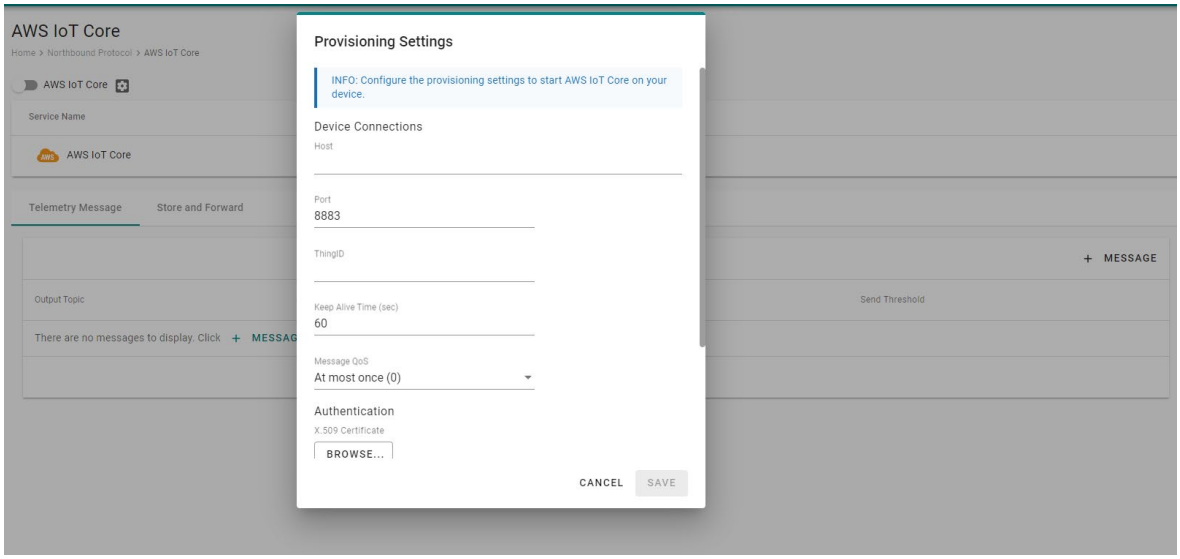
NOTE

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

AWS IoT Core

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

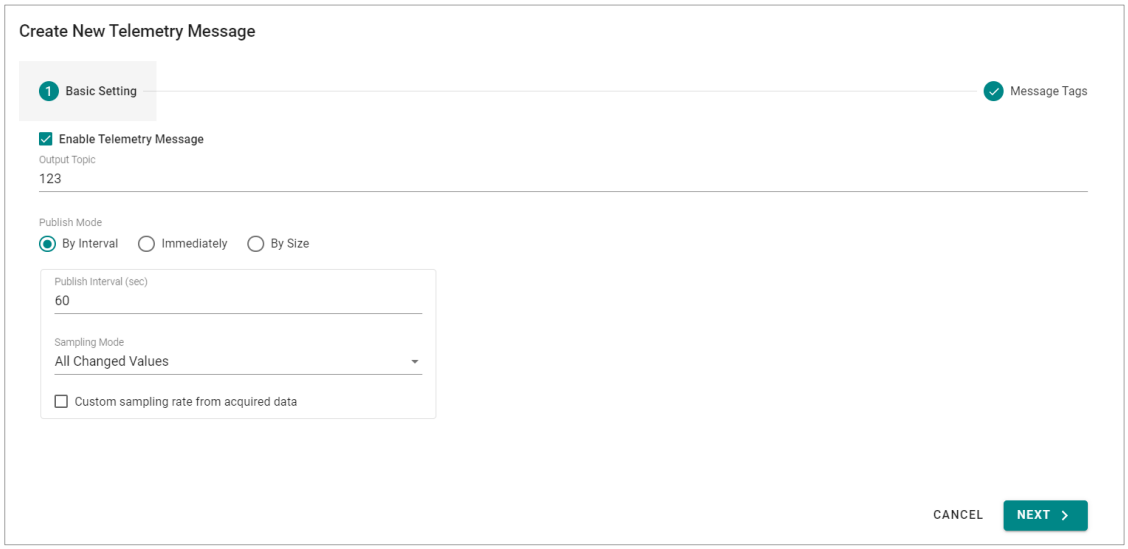
1. Click  to set connection.
2. Enter **Host (Endpoint)**. **Port** (default: 8883).
3. Enter **ThingID**.
4. Input **Keep Alive Time** (sec)
5. Select a way of message **QoS**.
6. Upload X.509 Certificate, Private Key, and (optional) Trusted Root CA.
7. Click **SAVE**.



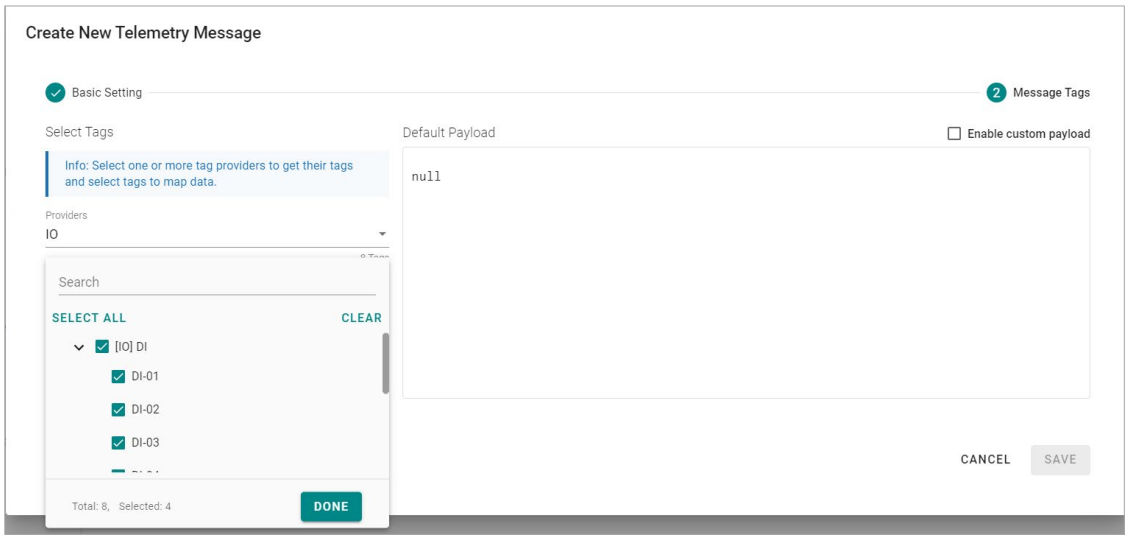
Telemetry Message

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

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

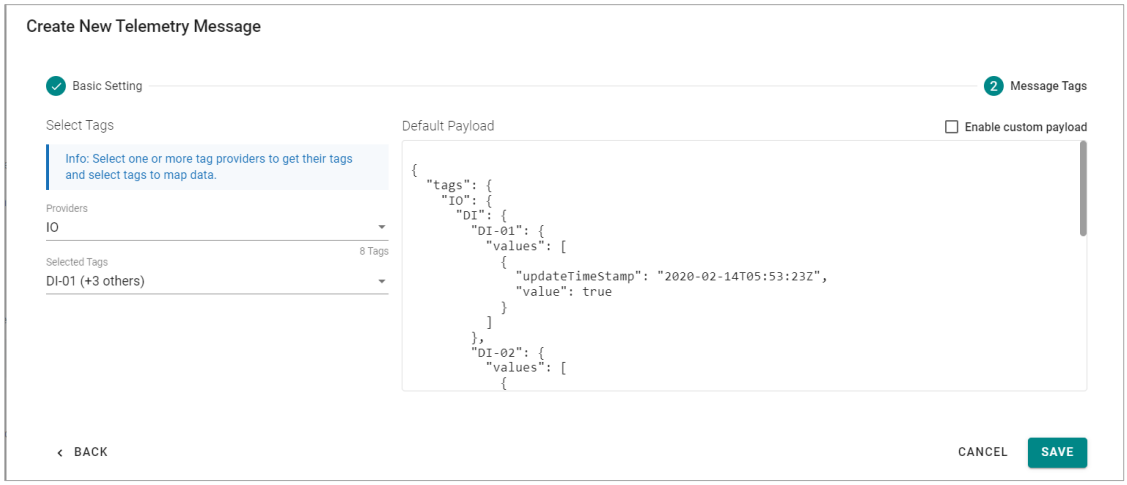


6. Select tags (e.g., Modbus Master).



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/).



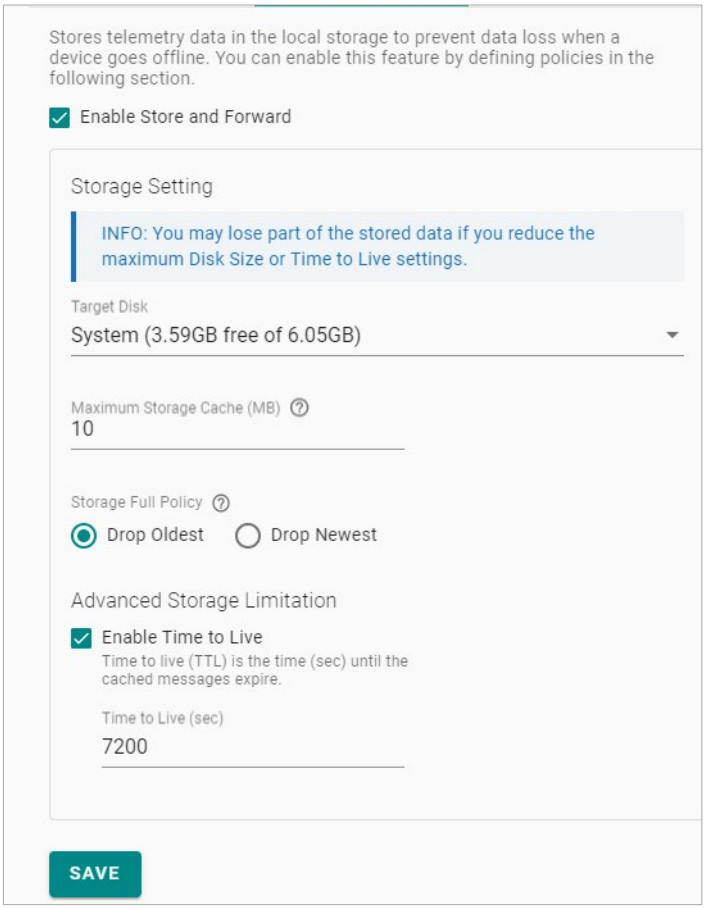
8. Click **SAVE.**

NOTE

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

Store and Forward

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



Device Management

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

NOTE

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

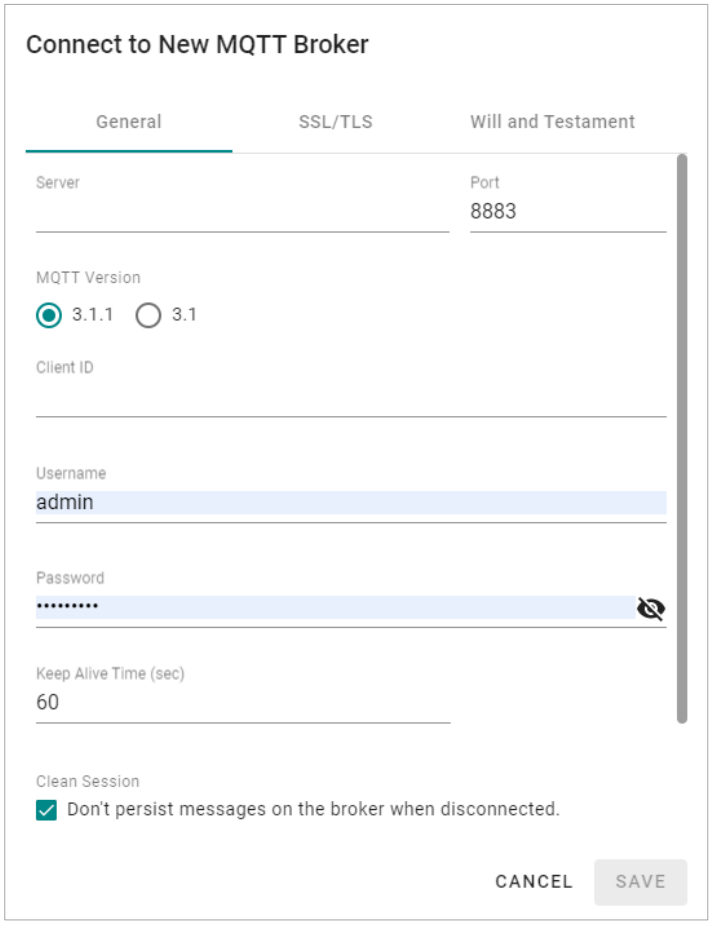
Generic MQTT Client

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

Note that you need to create a connection first and select D2C telemetry messages to an MQTT broker.

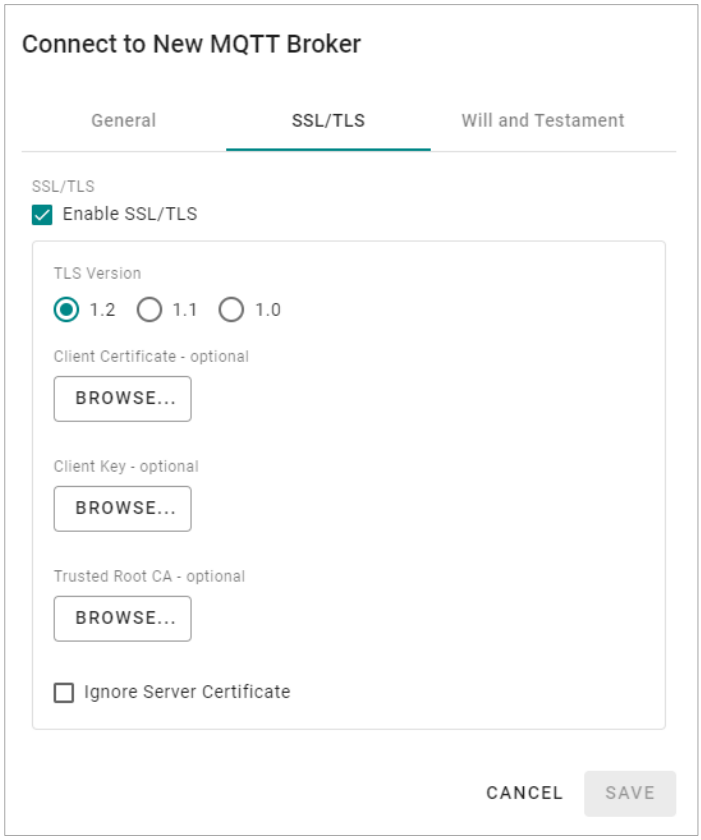
To create an MQTT Client, follow the steps below:

1. Click **ADD CONNECTION**.
2. Specify a **Server** (default port: 8883).



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**.

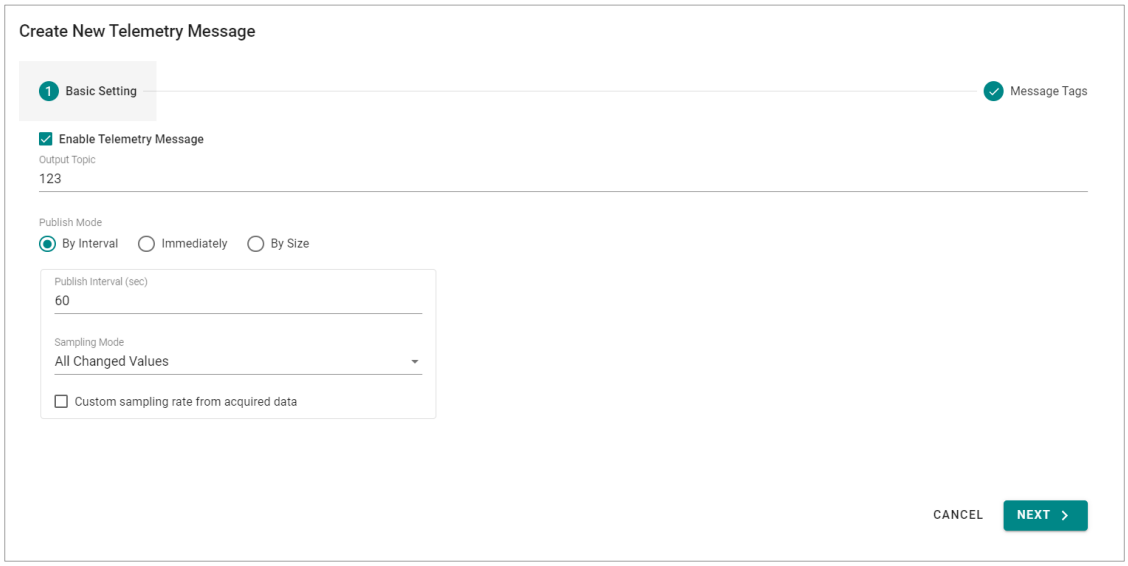
7. (Optional) Enable SSL/TLS, and upload Client Certificate, Client Key, Trusted Root CA.



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

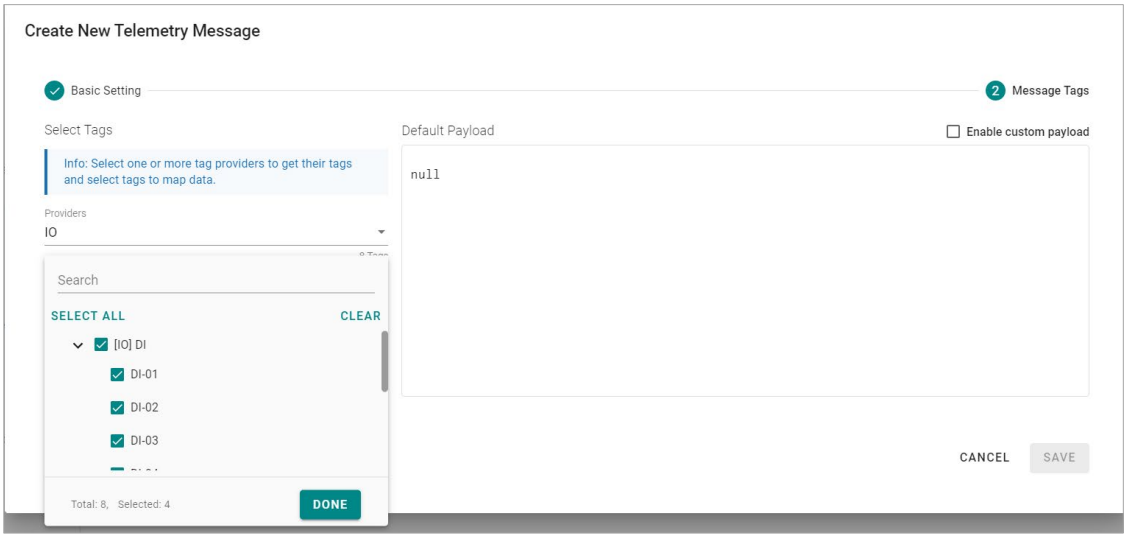
Once an MQTT Broker has been created, create a new telemetry message by following the steps below:

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

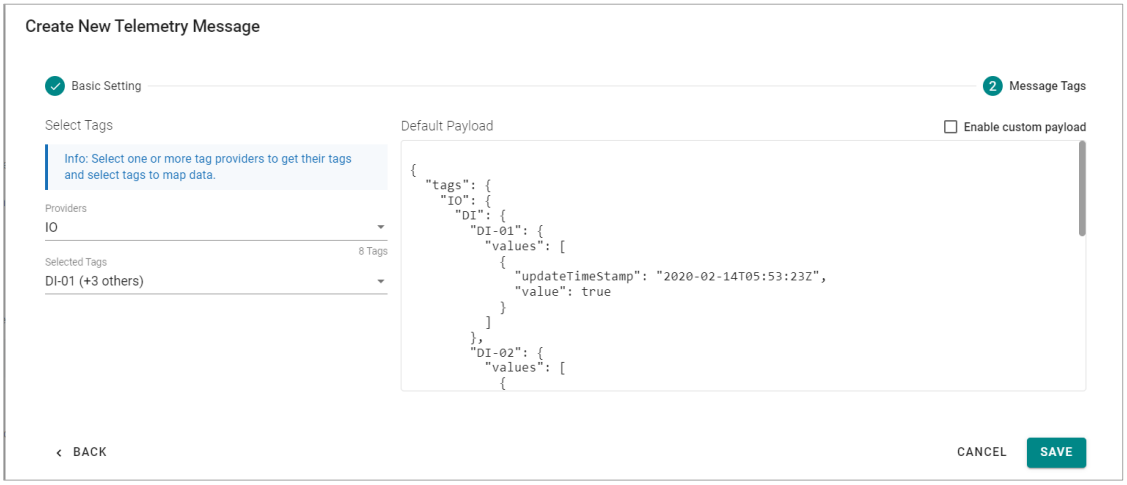


3. Select a **Publish Mode**.
   For details, see Publish Mode.

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



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



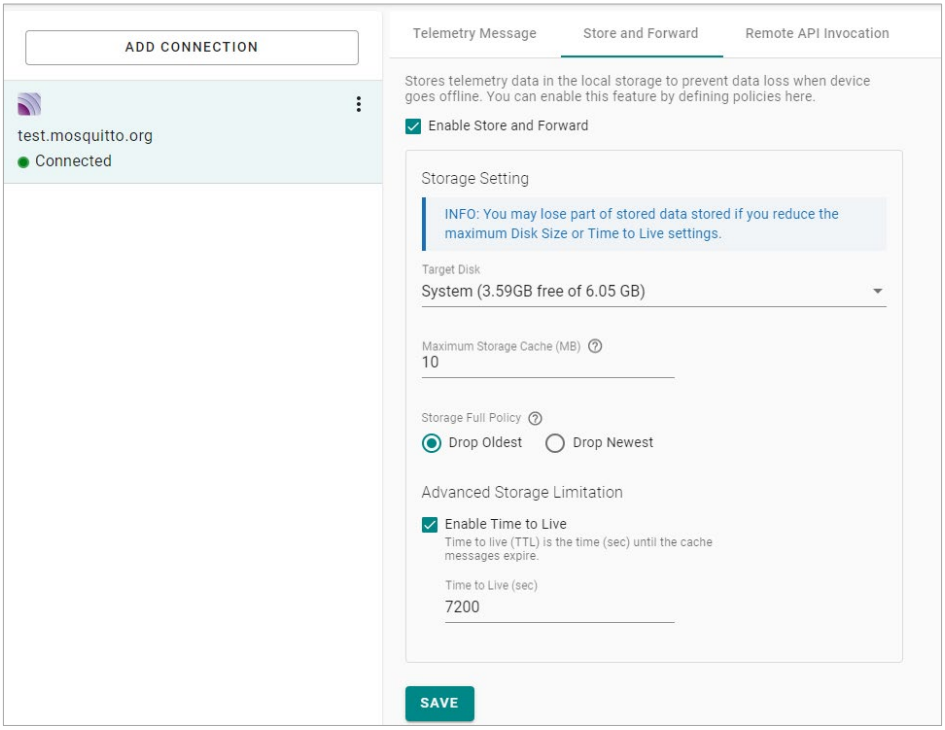
8. Click **SAVE**.

NOTE

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

Store and Forward

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

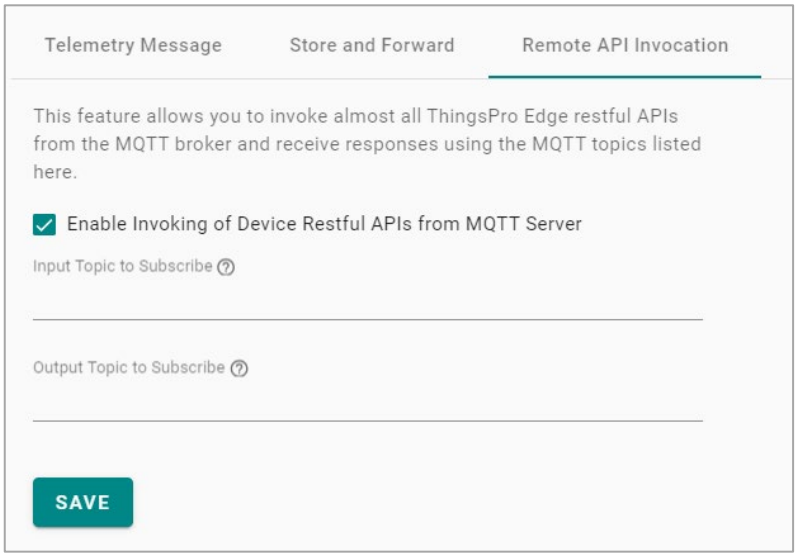


NOTE

if you want to use the direct method to write tags from the cloud, refer to https://github.com/TPE-TIGER/TPE-TIGER.github.io.

Remote API Invocation

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



NOTE

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

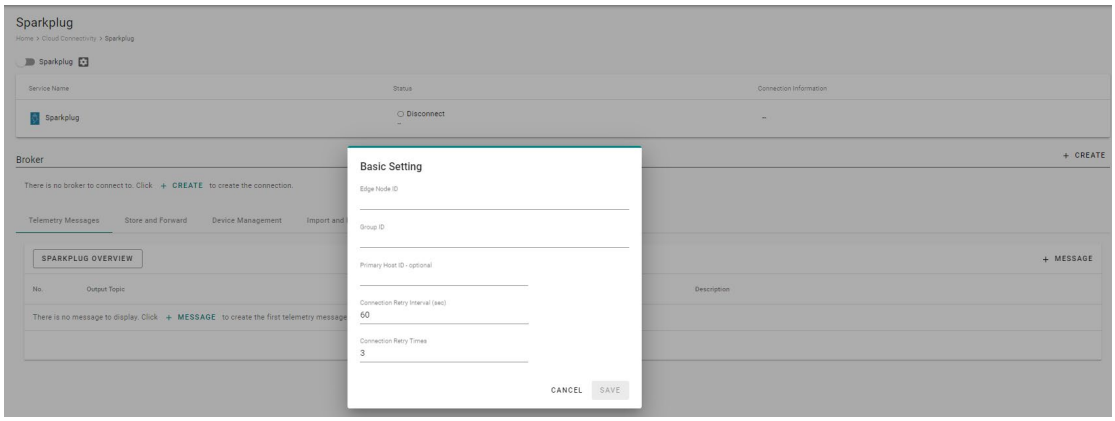
Sparkplug

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

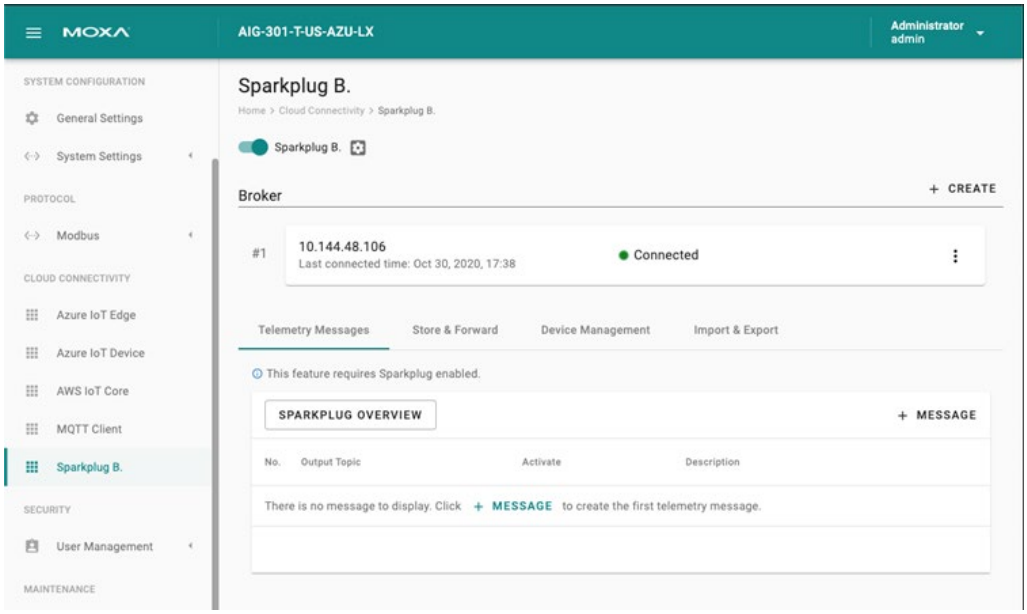
- Enabling Sparkplug
- Configuring a Broker
- Configuring a Telemetry Message

Enabling Sparkplug

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

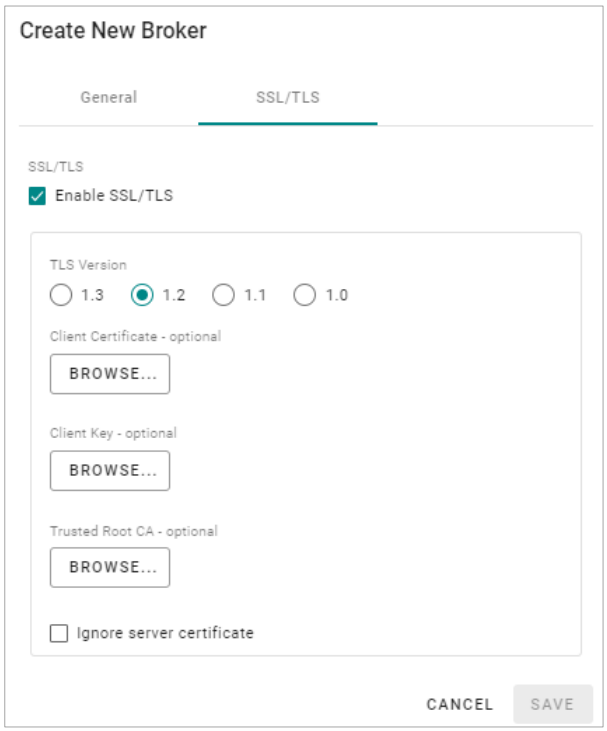


5. Click **SAVE**.



Configuring a Broker

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



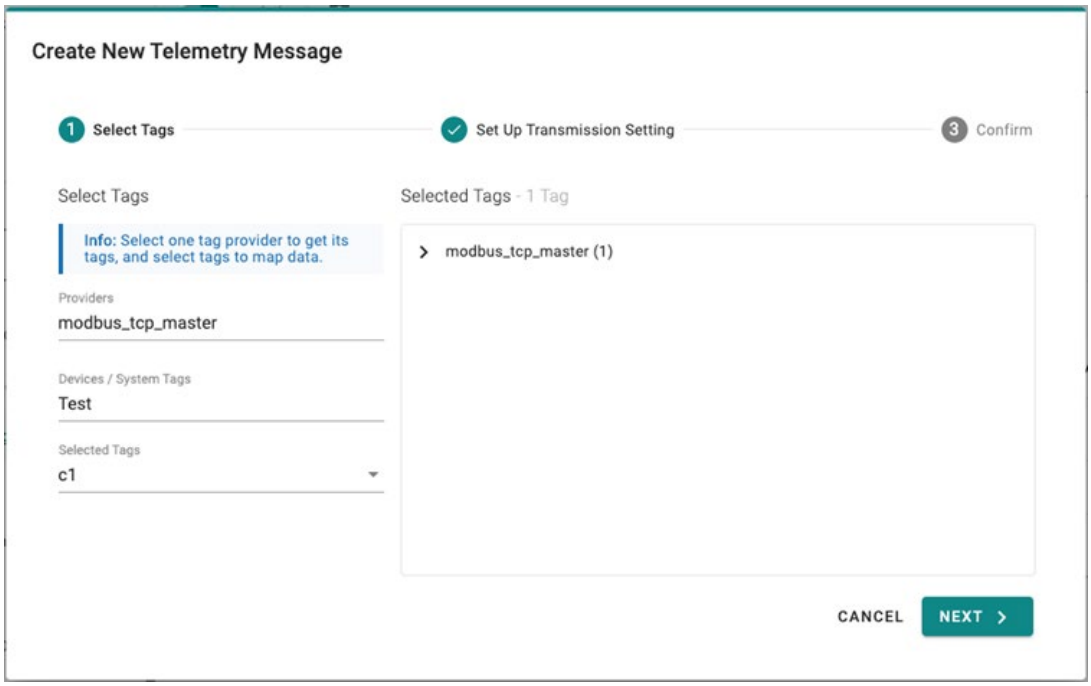
6. Click **SAVE**.

NOTE

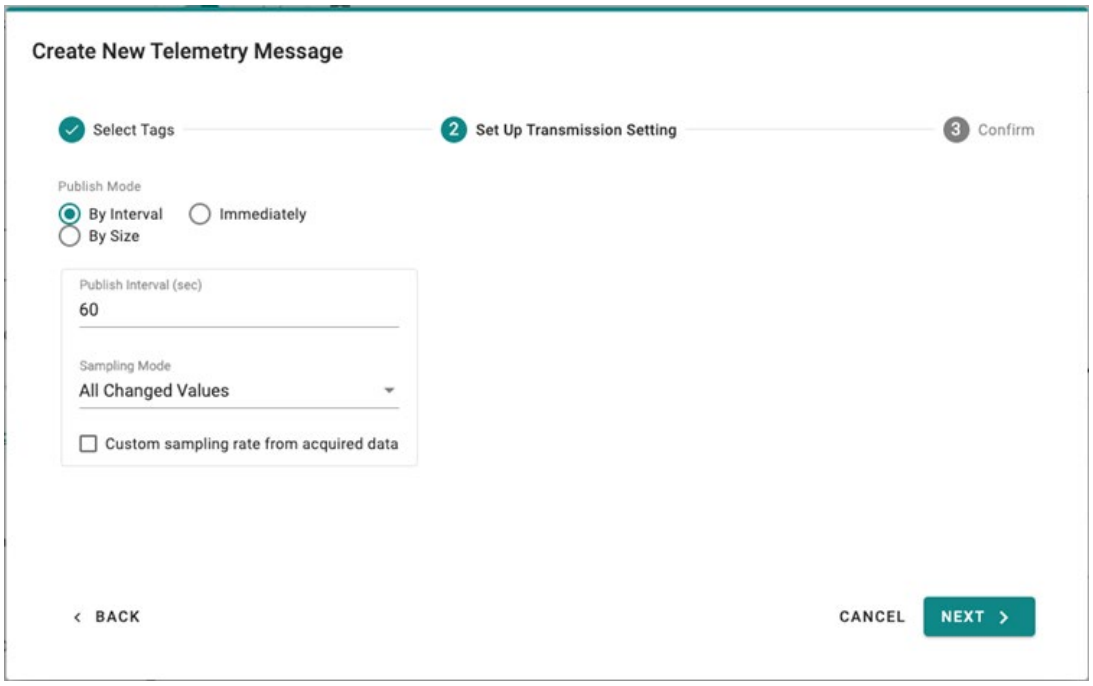
Data loss might occur during the period of connection interval prior to network connection check (Keep Alive Time). We suggest setting a shorter interval of Keep Alive Time (e.g., 10 seconds)

Configuring a Telemetry Message

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

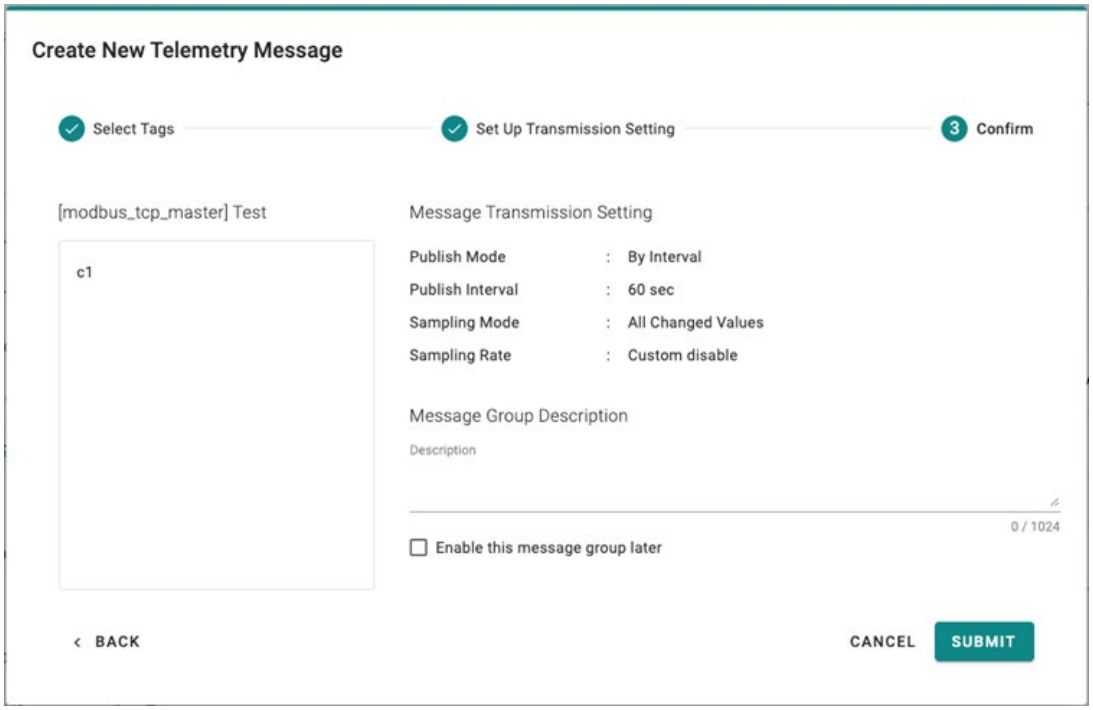


5. Select a publish mode.
   For details, see Publish Mode.
6. Select a sampling mode.
7. Click **NEXT**.



8. (optional) Specify a description.

9. Click **SUBMIT**.

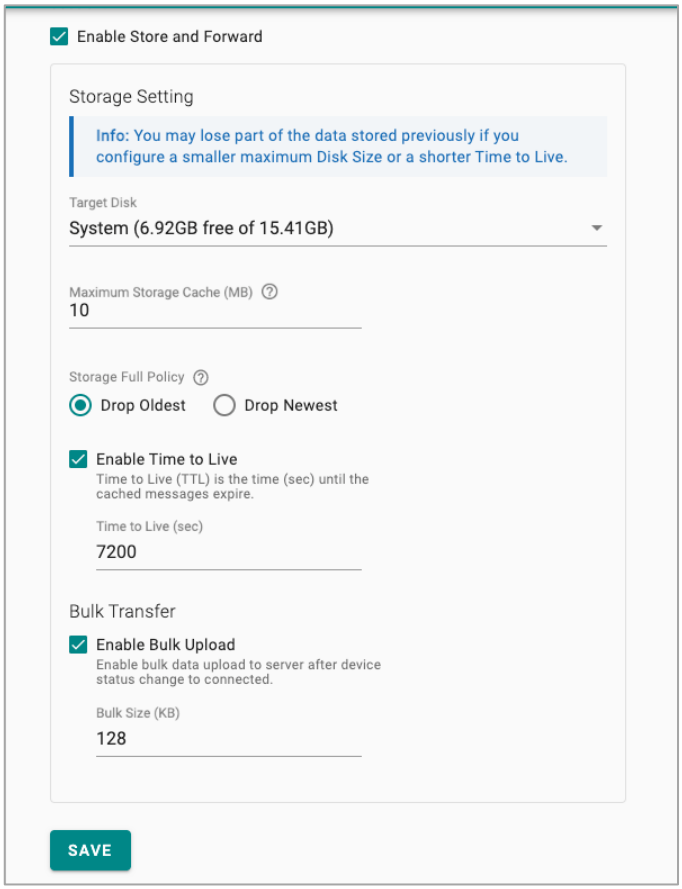


NOTE

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

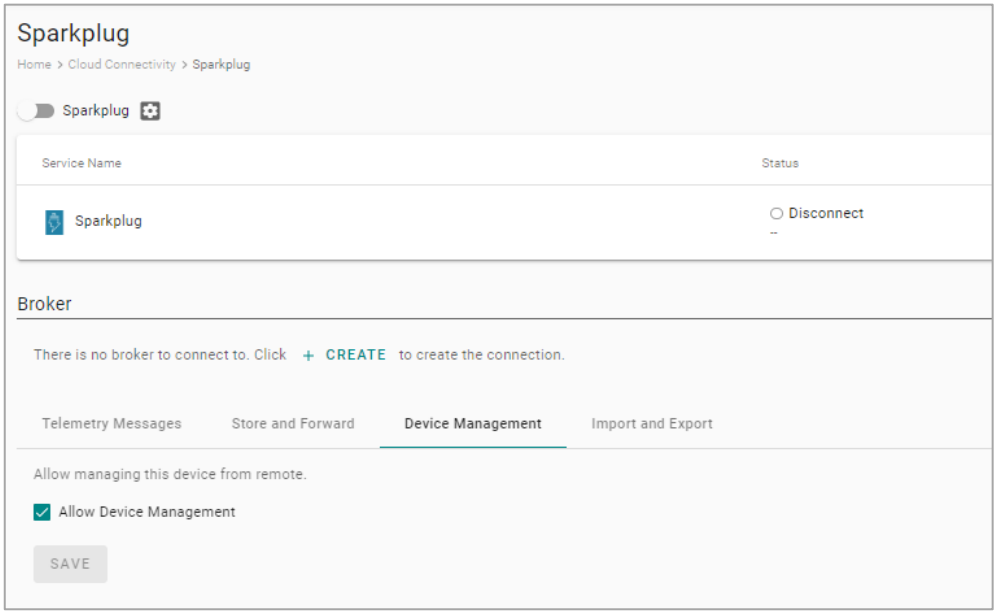
Store and Forward

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



Device Management

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



NOTE

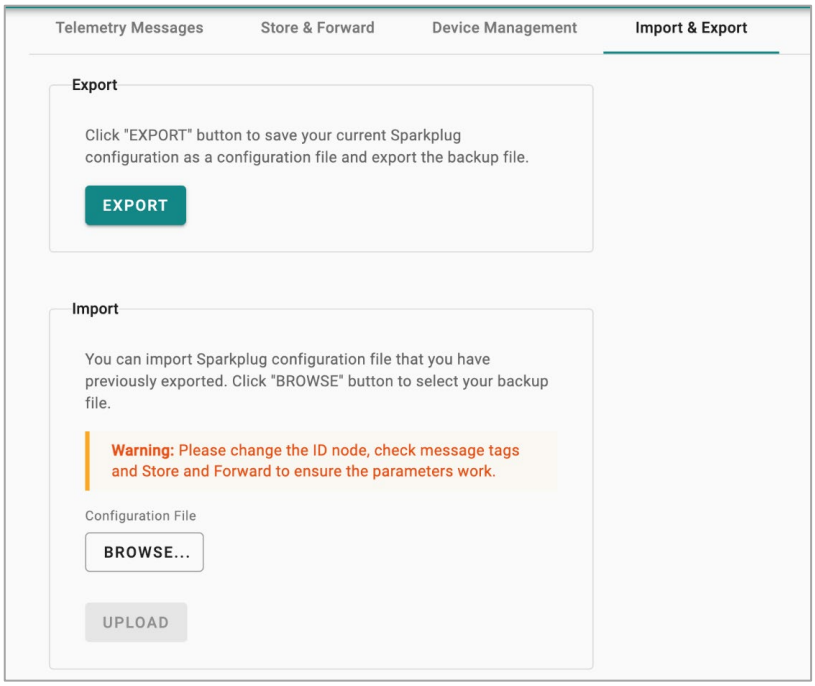
For information on managing the device using API, see https://github.com/TPE-TIGER/TPE-TIGER.github.io.

Import & Export

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

NOTE

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



NOTE

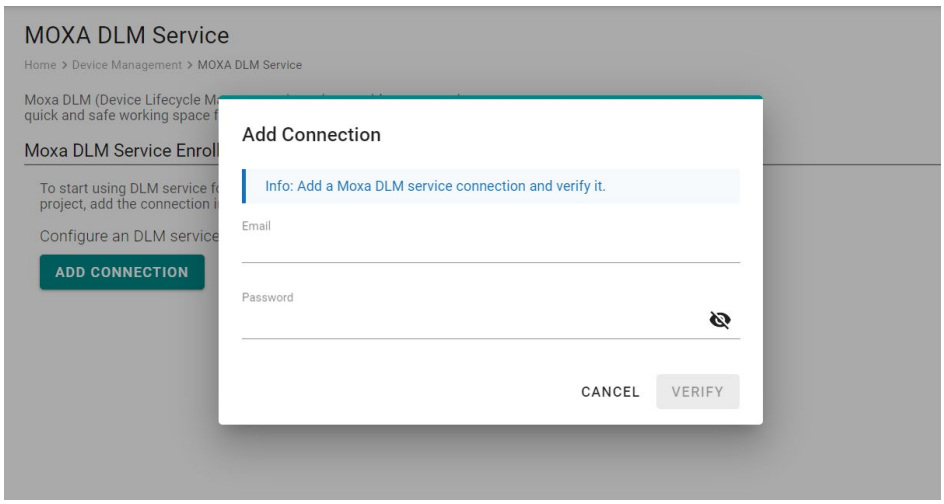
The exported configuration includes credentials, client ID, and policies of D2C messages. You can modify these parameters after the configuration file is imported to other gateways.

Moxa DLM Service

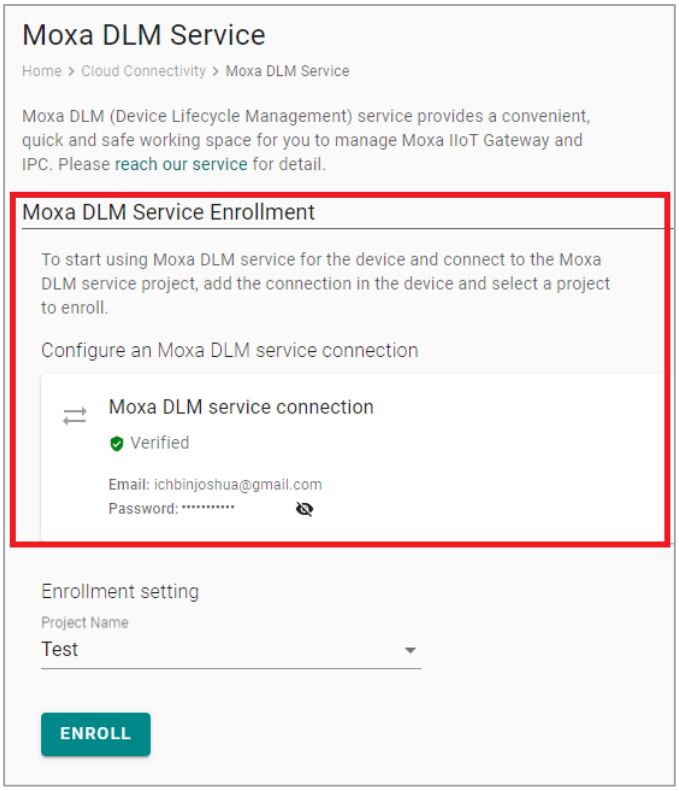
Moxa DLM (device lifecycle management) service is used for managing AIG devices. Imagine sitting in your office and using this service to remotely manage numerous devices distributed around the world. You can monitor the device's health status, upgrade firmware, import/export configuration, and remotely log into the device's web console. If you are interested in applying for this service, please use the following link to register an account: https://dlm.thingsprocloud.com to experience our beta DLM solution.

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

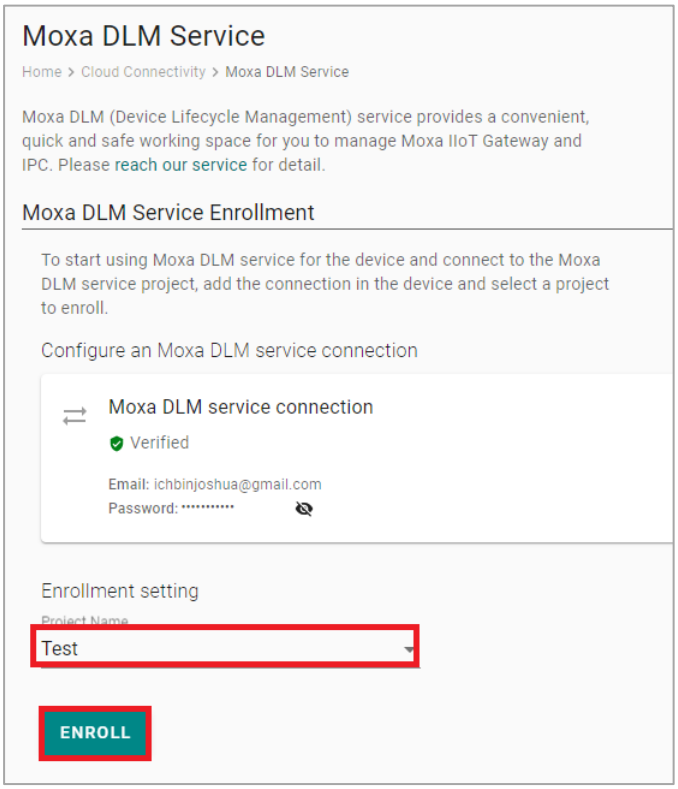
1. Input DLM **email** and **password**, and press **VERIFY**.



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



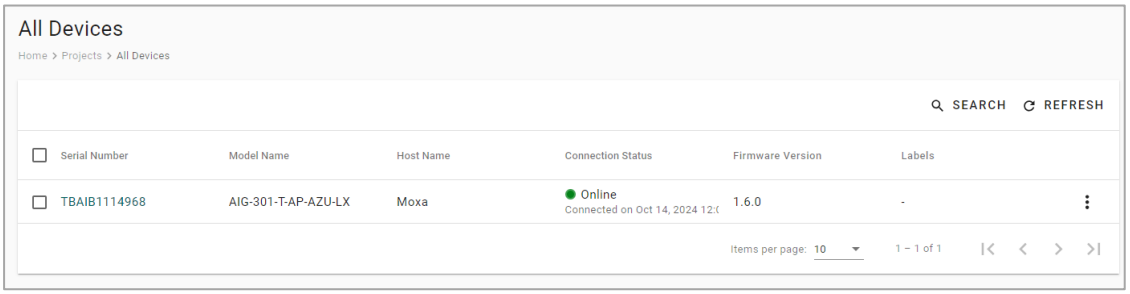
3. Choose the **Project** and Press **ENROLL** to enroll.



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

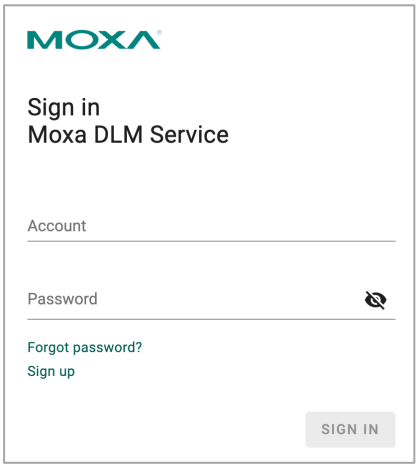
> **NOTE**
>
> Ensure the Moxa DLM service is enabled at the top left corner.

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

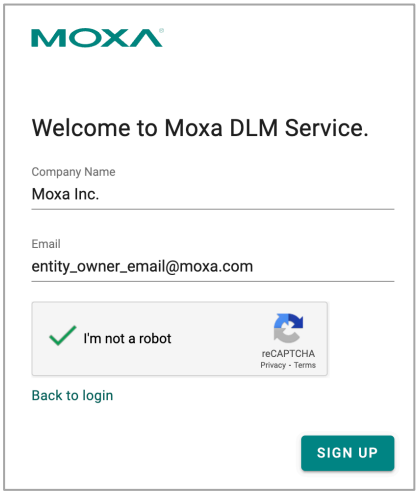


Sign Up DLM Account

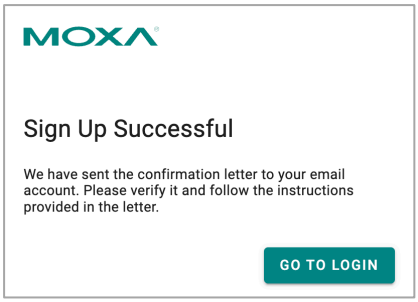
1. Go to the website: https://dlm.thingsprocloud.com/



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.



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



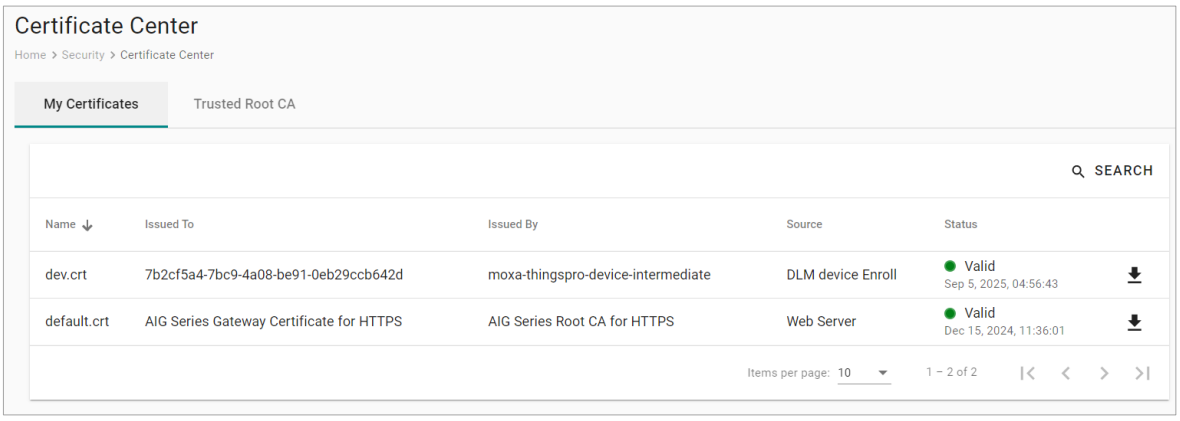
Security

Certificate Center

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

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

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



Firewall

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

Inbound

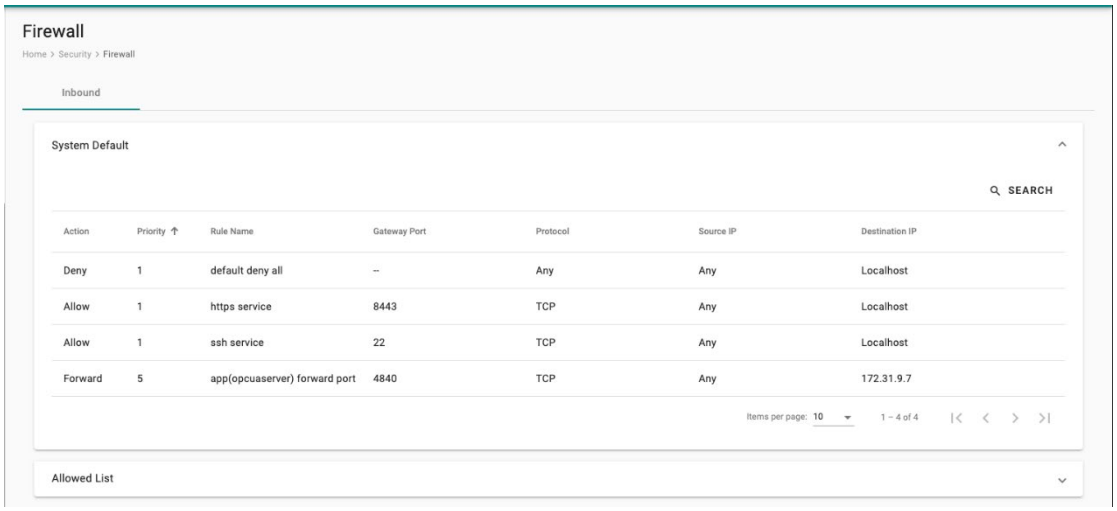
System Default

AIG reserves ports for the services below.

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

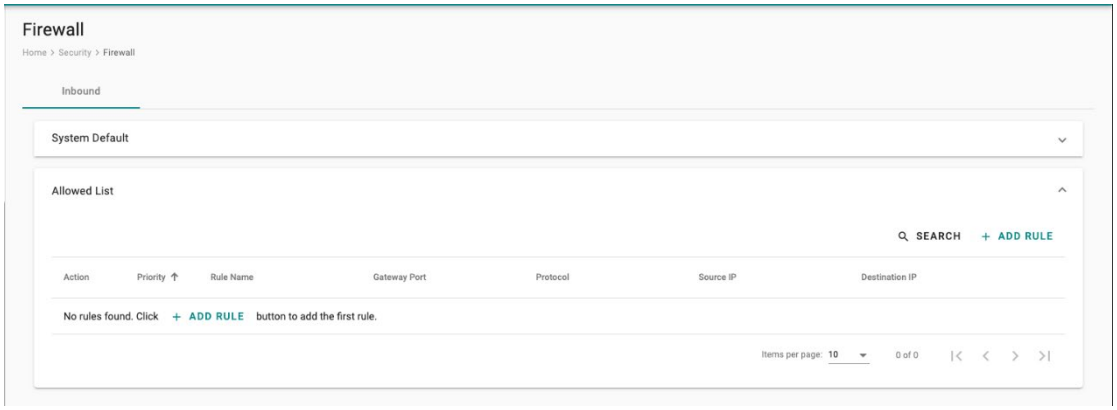
NOTE

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



Allowed List

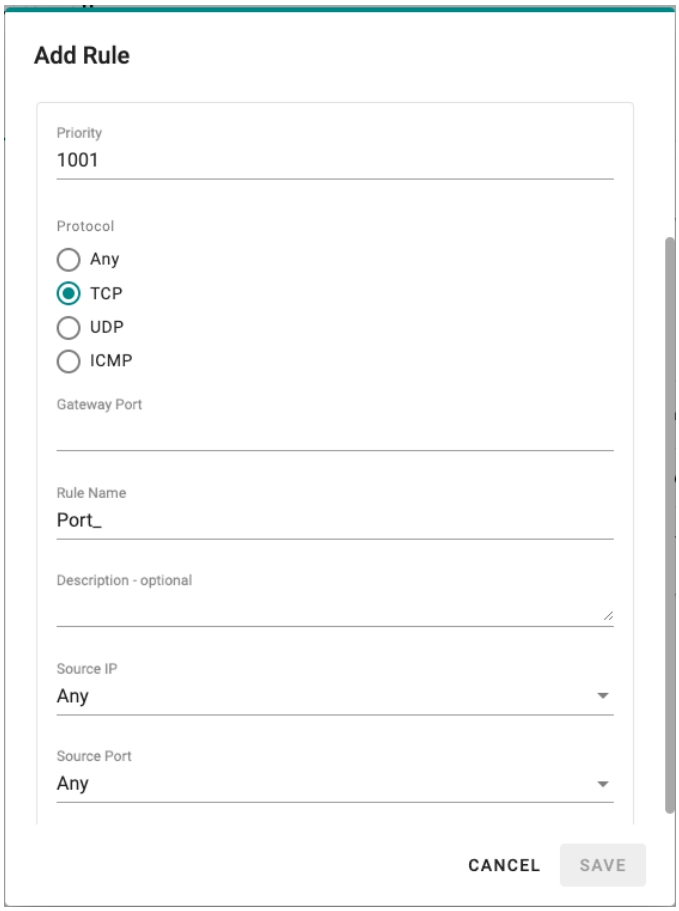
AIG provides an allowed list for creating firewall rules. You can create, edit, and delete firewall rules here.



To create firewall rules, do the following:

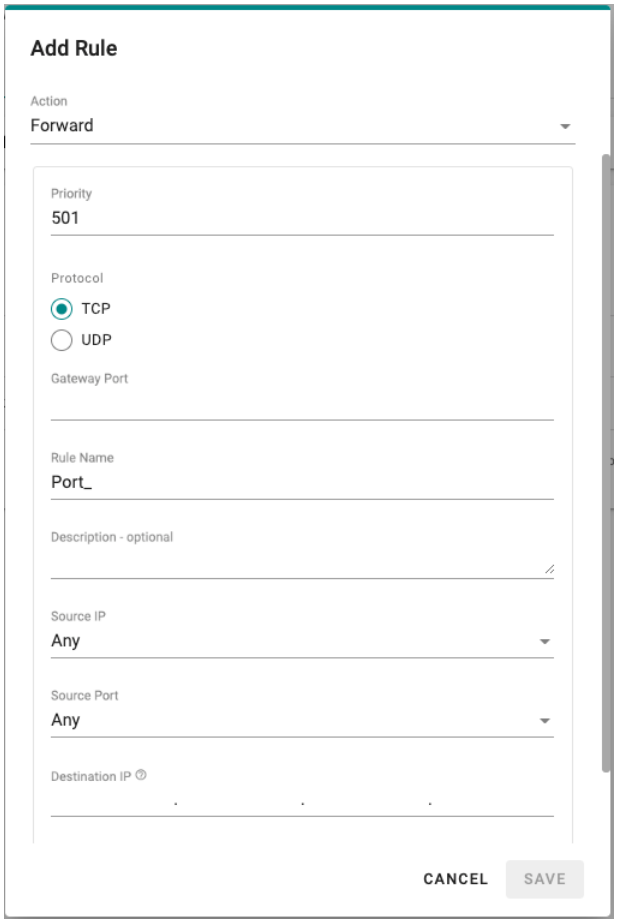
Create Allow Rule:

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



Create Forward Rule:

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



6. Click **SAVE.**

NOTE

AIG Edge reserves priority 1 to 500 for system default rules. The priority range 501 to1000 is for **Forward** action rules; while the range 1001 to 1500 is for **Allow** action rules.

OpenVPN Client

OpenVPN allows you to create secure connections over the internet. It provides encryption and authentication to ensure confidentiality and integrity of your data. OpenVPN uses a client-server architecture where the server acts as the VPN endpoint and the client connects to the server to establish a secure connection. To enable the function, go to **Security > OpenVPN Client** and do the following:

1. Download the OpenVPN profile template.
2. Revise the profile by inputting the necessary information provided by your VPN service provider.

   This information includes:

   a. Remote server IP: This is the address of the VPN server you want to connect to.

   b. Port number: The port through which the VPN connection will be established. The default is usually 1194.

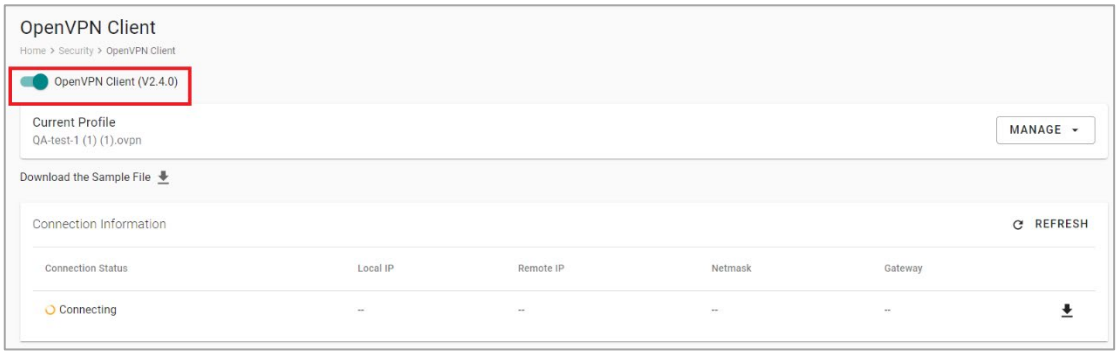
   c. Protocol: The protocol to be used for the VPN connection, such as UDP or TCP.

   d. Authentication method: The method used to authenticate your connection.

   e. Encryption settings: The encryption algorithm to be used for securing the VPN connection.
3. Import the OpenVPN profile.

   You should see it listed in the OpenVPN client.
4. Click the button to enable OpenVPN client to connect.

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

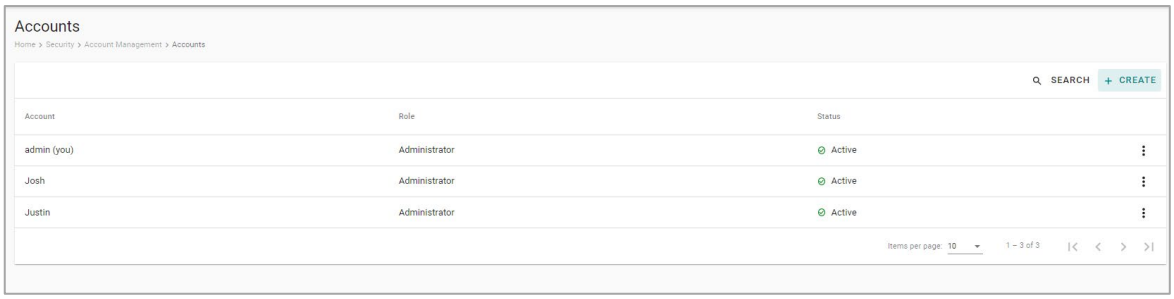


Account Management

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

Accounts

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

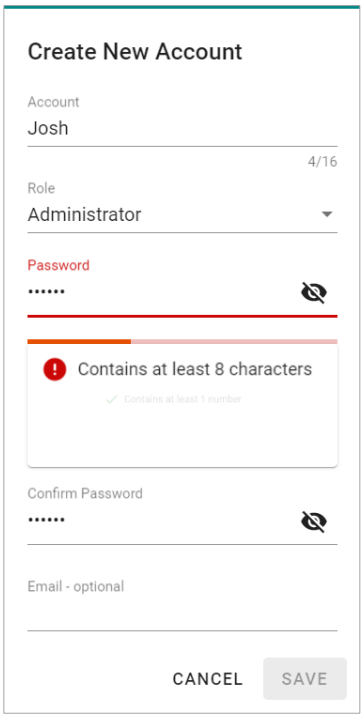
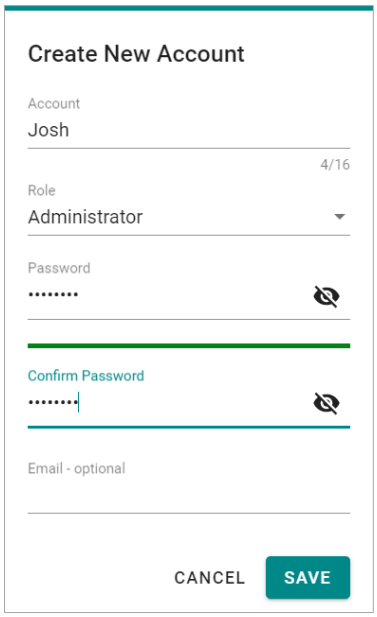


Creating a New User Account

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

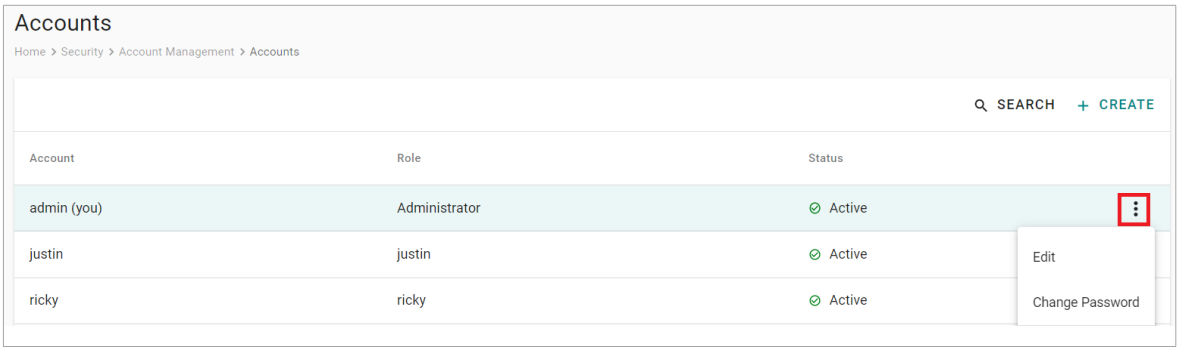
NOTE

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
	

Managing Existing User Accounts

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



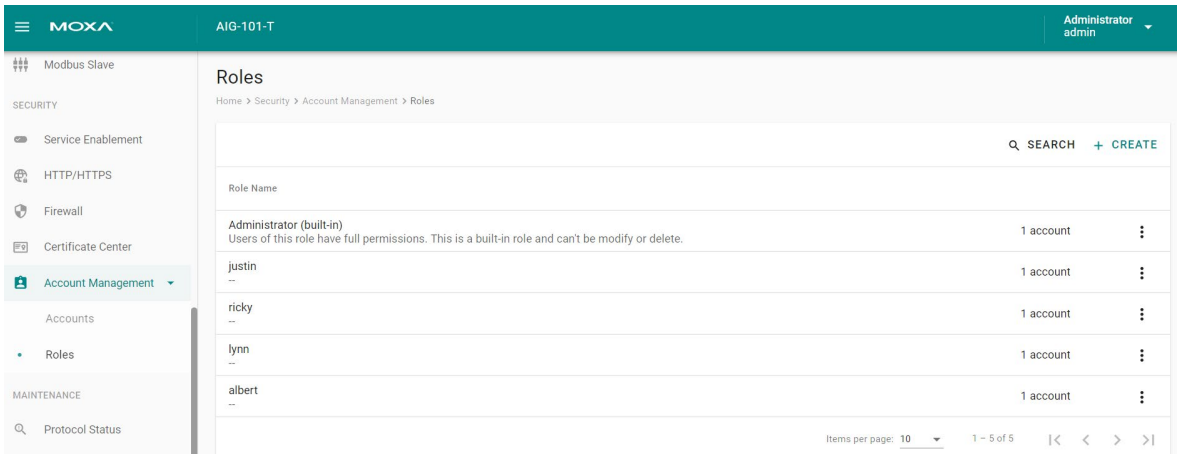
Function	Description
Edit	Change the role, email, or password of an existing account.
Deactivate	Does not allow the user to log in to this device.
Delete	Delete the user account. **NOTE:** This operation is irreversible.

NOTE

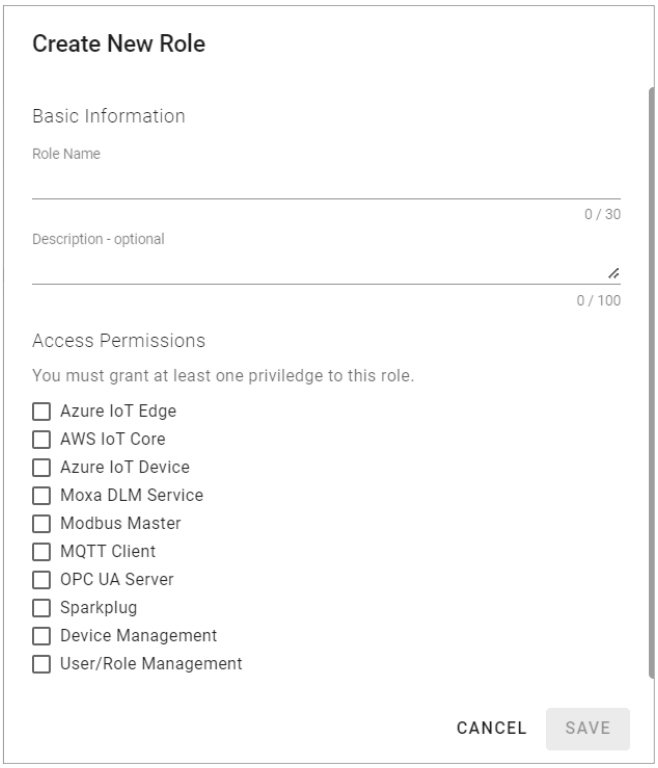
You cannot **Deactivate** or **Delete** the last remaining account with an Administrator role. This is to prevent an unauthorized account from fully managing this system. When the system detects only one active account when the Administrator role is selected, all items in the pop-up menu will be grayed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

Roles

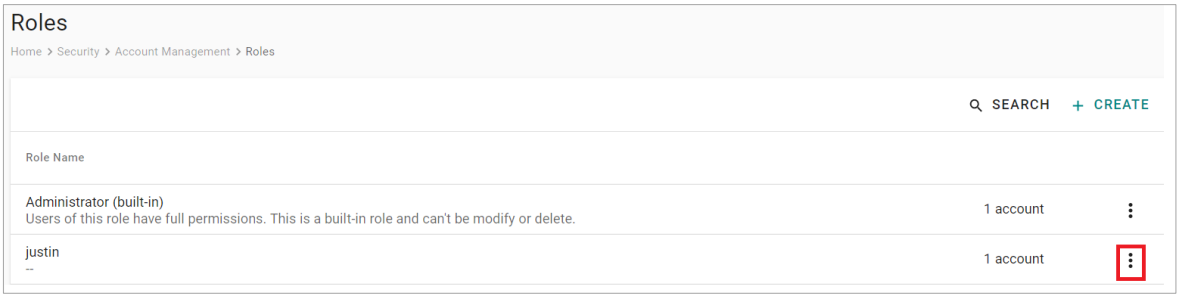
You can **View**, **Create**, **Edit**, and **Delete** user roles in ThingsPro Edge. In the main menu, go to **Security > Account Management > Roles** to manage the user roles.



Click **+ CREATE** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions. When you are done, click **SAVE** to create the role in the system.



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



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

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

Maintenance

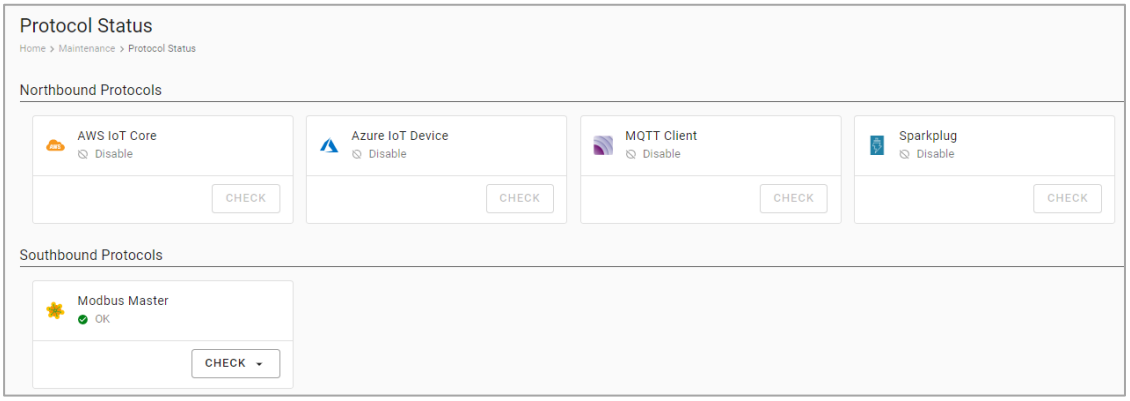
Protocol Status

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

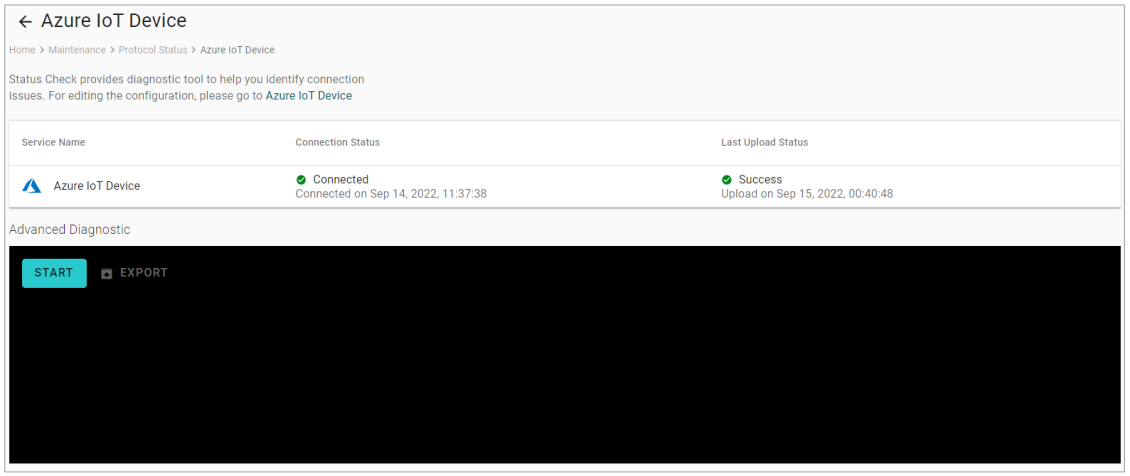
When you access the page, you can see an overview of the status for Northbound Protocols and Southbound Protocols.

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

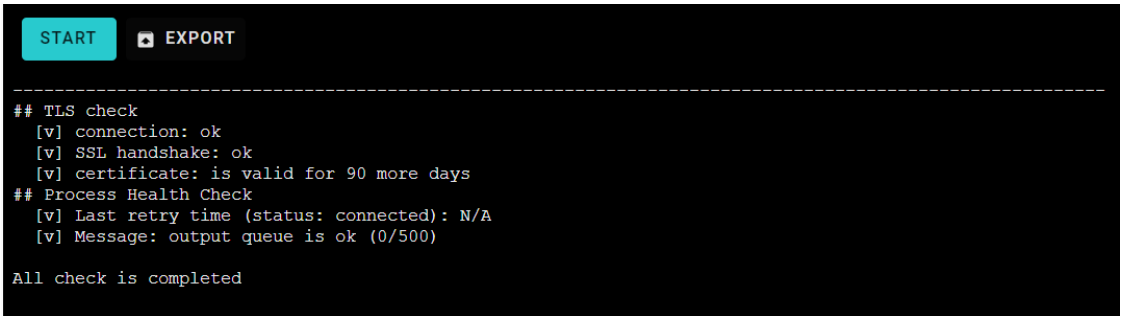
1. Click **CHECK**.



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



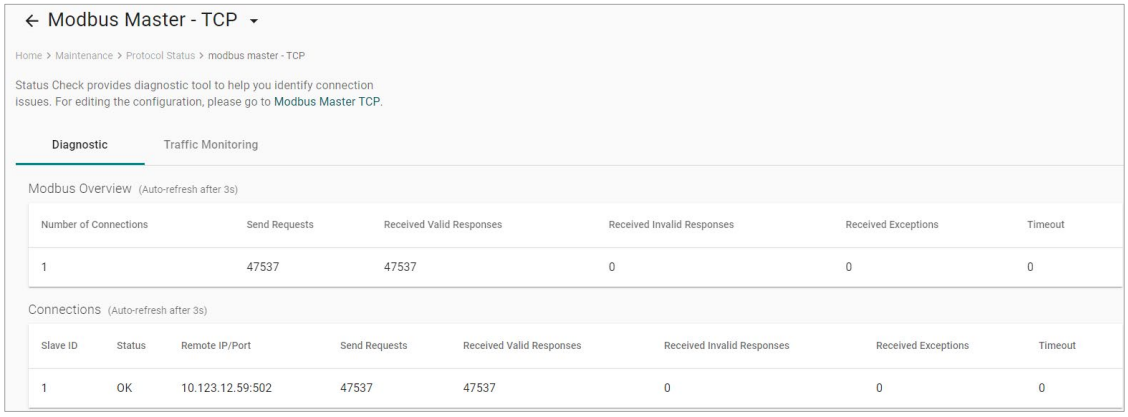
3. View the logs to identify the issue.



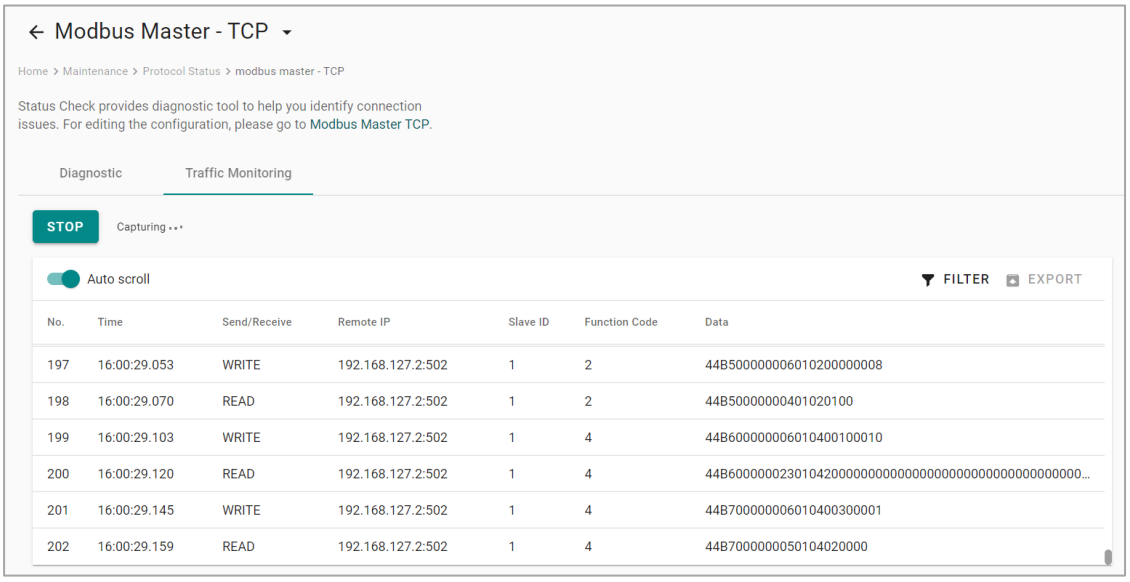
4. (Optional) **Export** the logs.

For Modbus troubleshooting, do the following:

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



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

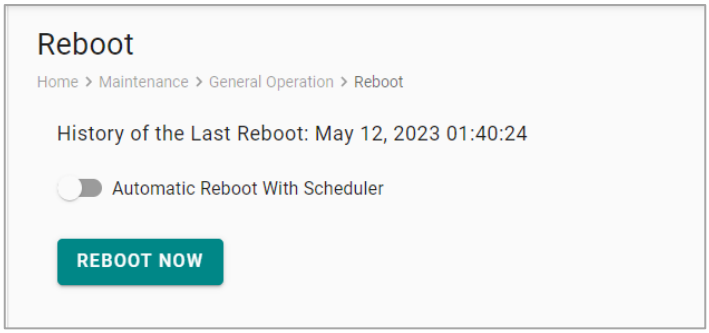


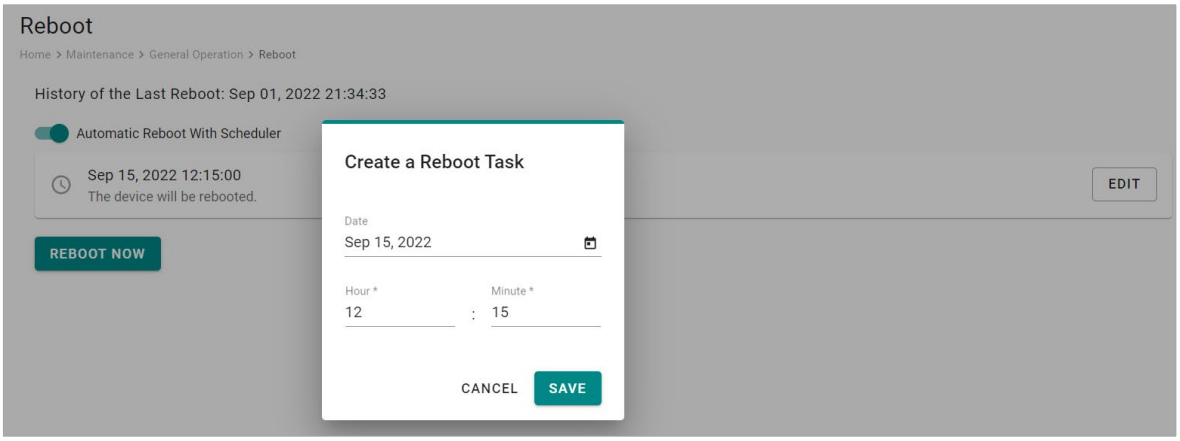
5. (Optional) **Export** the traffic logs to send to experienced engineers for further analysis.

General Operation

Reboot

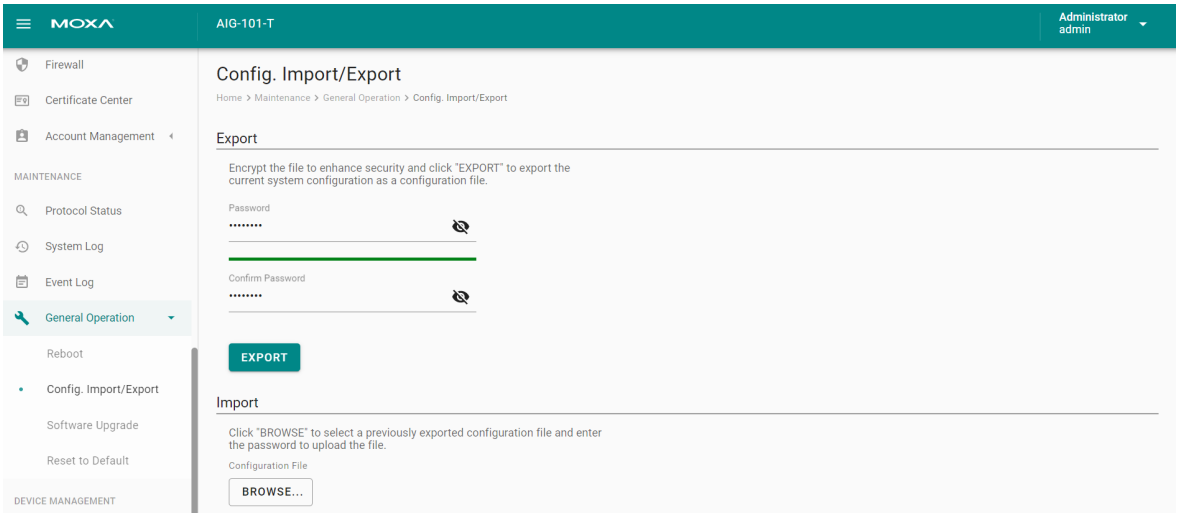
If you want to reboot the device, go to **General Operation > Reboot** and click **REBOOT NOW**. If you want to arrange a specific time to reboot, you can enable **Automatic Reboot With Scheduler** and enter the date, hour, and minutes.





Config. Import/Export

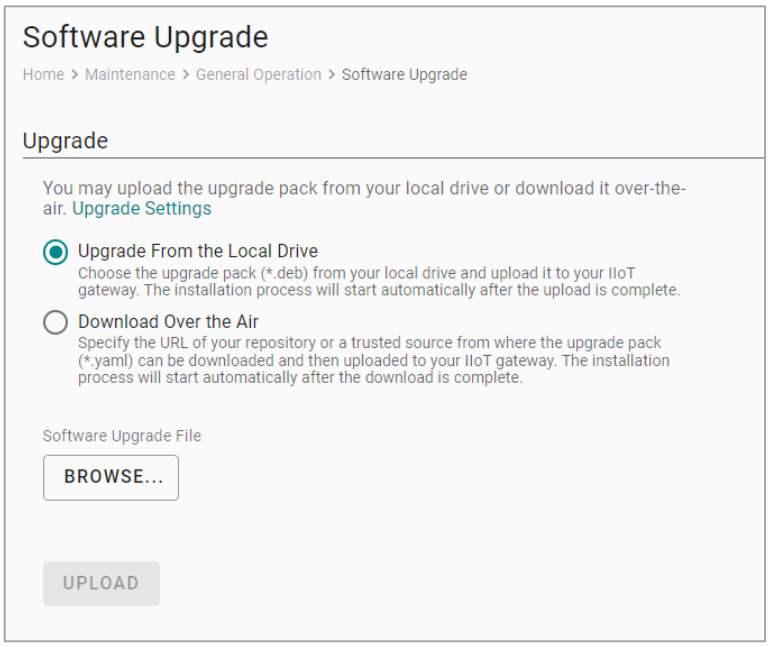
Go to **General Operation > Config. Import/Export,** where you can import or export the gateway configuration file with a given password. The exported configuration file will be compressed to the **tar.gz** format and downloaded on your computer.



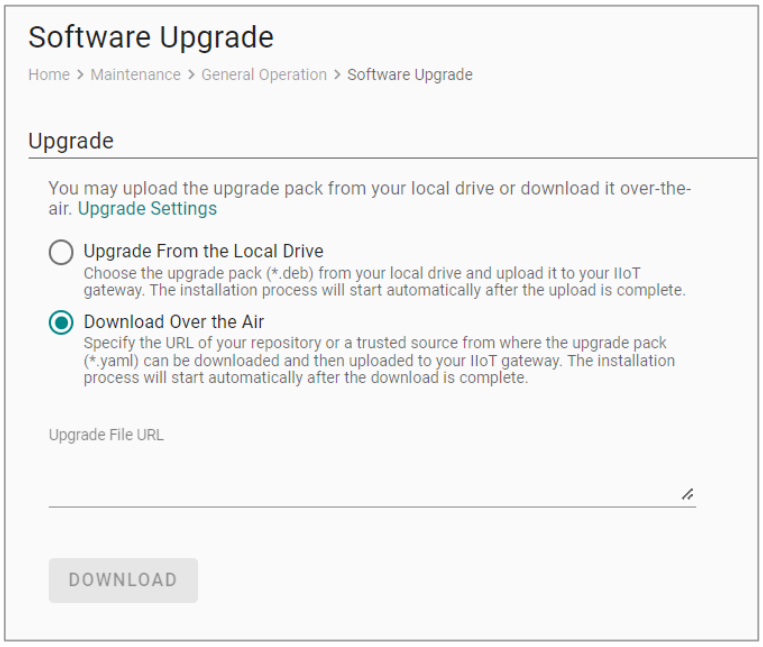
Firmware Upgrade

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

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



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



Reset to Default

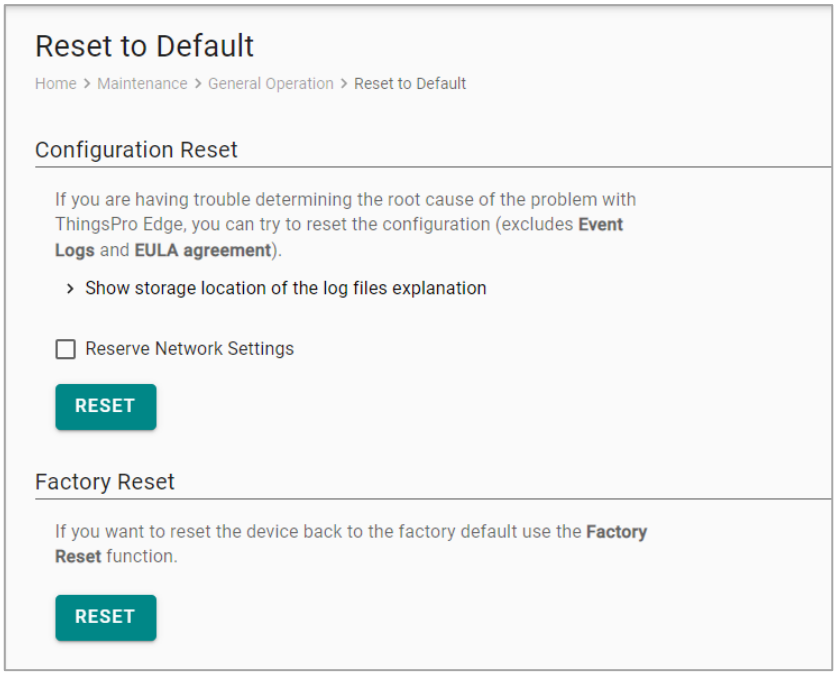
To clear all the settings to configuration default:

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

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

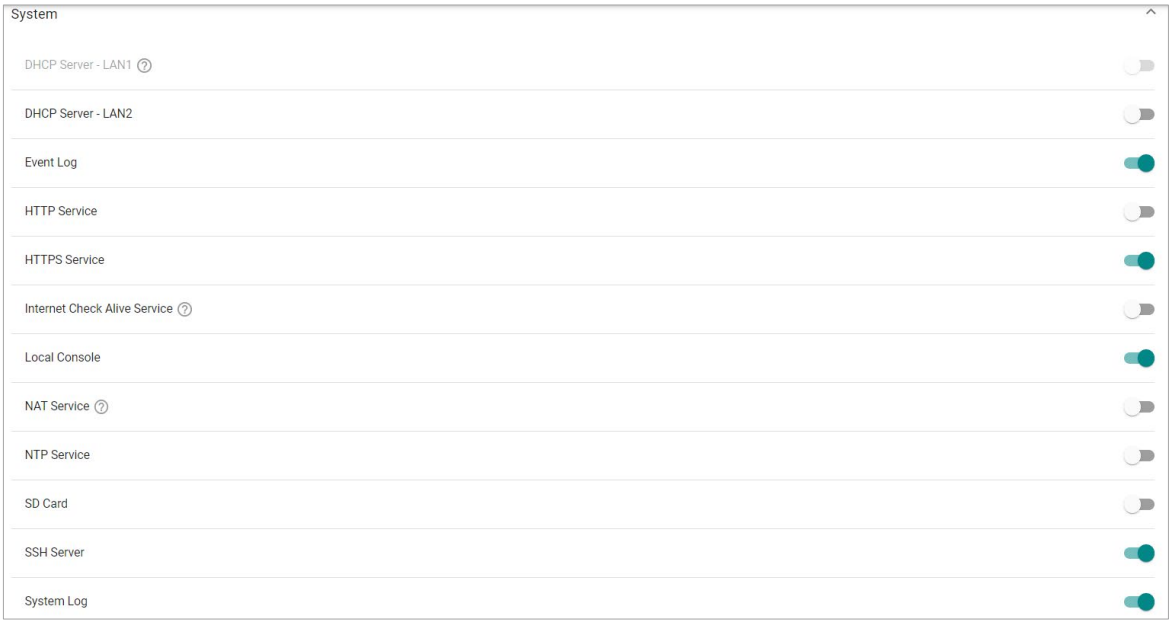
NOTE

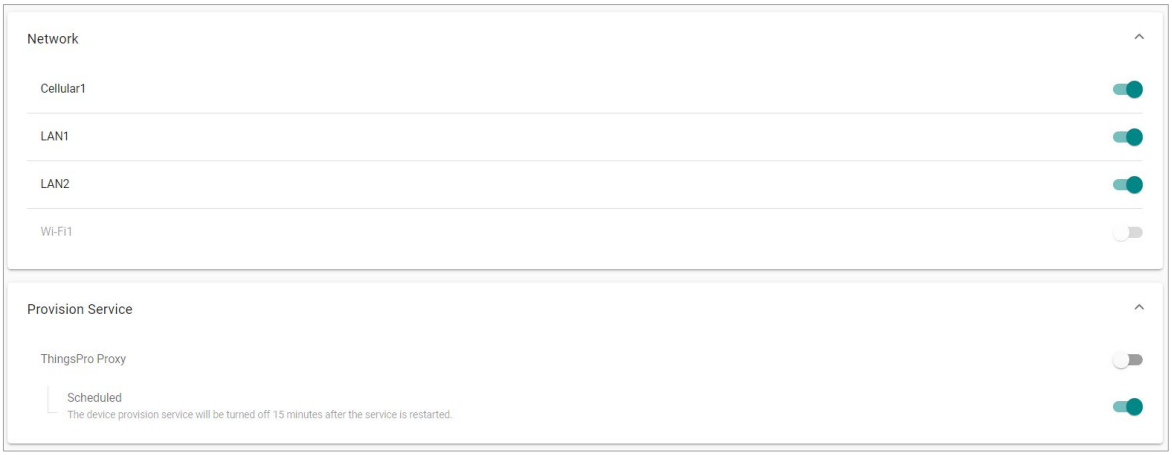
The configurations and firmware will be reset back to the factory default.



Enablement

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





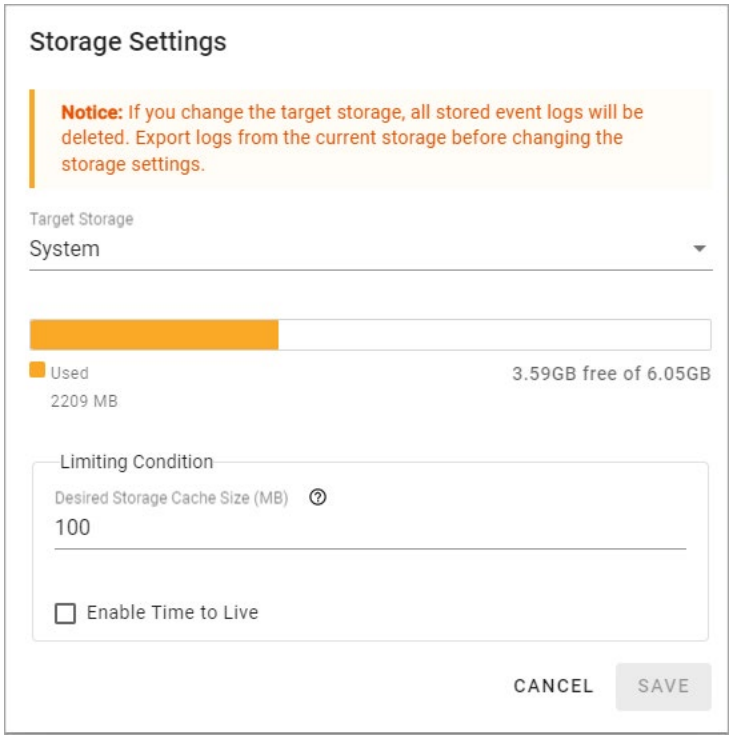
Diagnostic

System Log

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

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

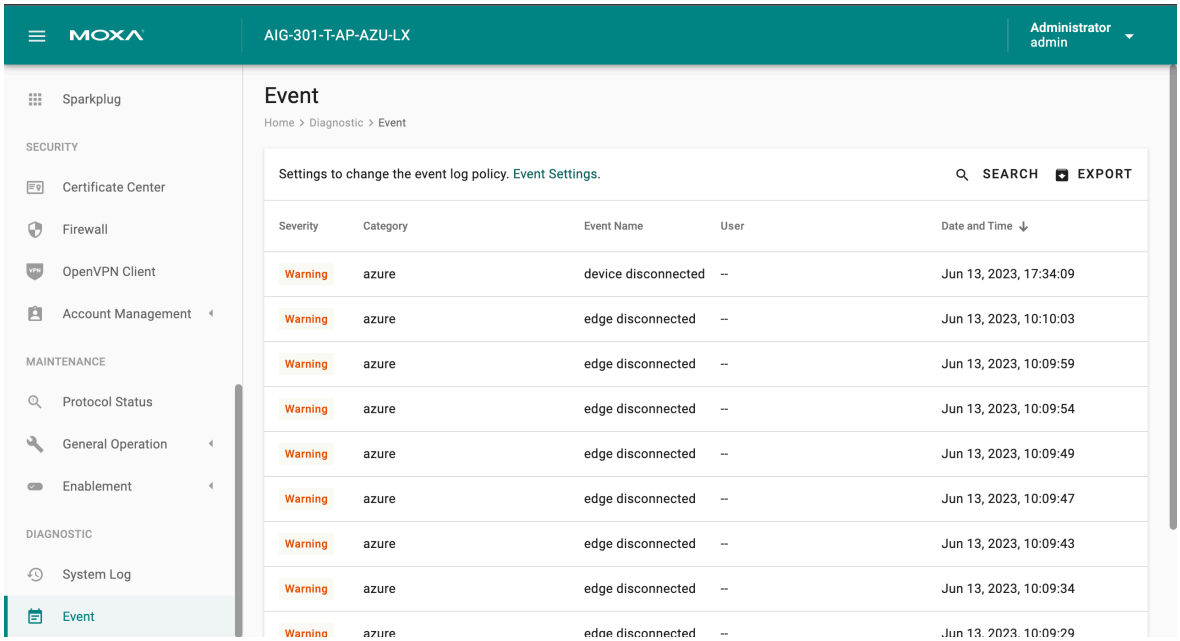
Click  to specify the location to store the event logs. To optimize the use of storage space on your AIG, you can check the Enable **Time to Live** option and specify the maximum storage space for the system logs. Click **SAVE** to confirm your settings.



Events

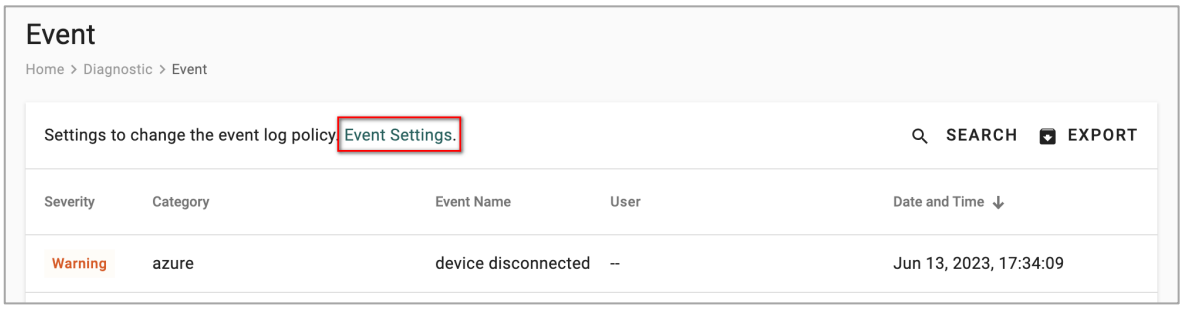
When you face issues, you can go to **Diagnostic** > **Event** check the event logs which record historical events that help you to narrow down the problems. The event logs can also be exported for convenient offline analysis.

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

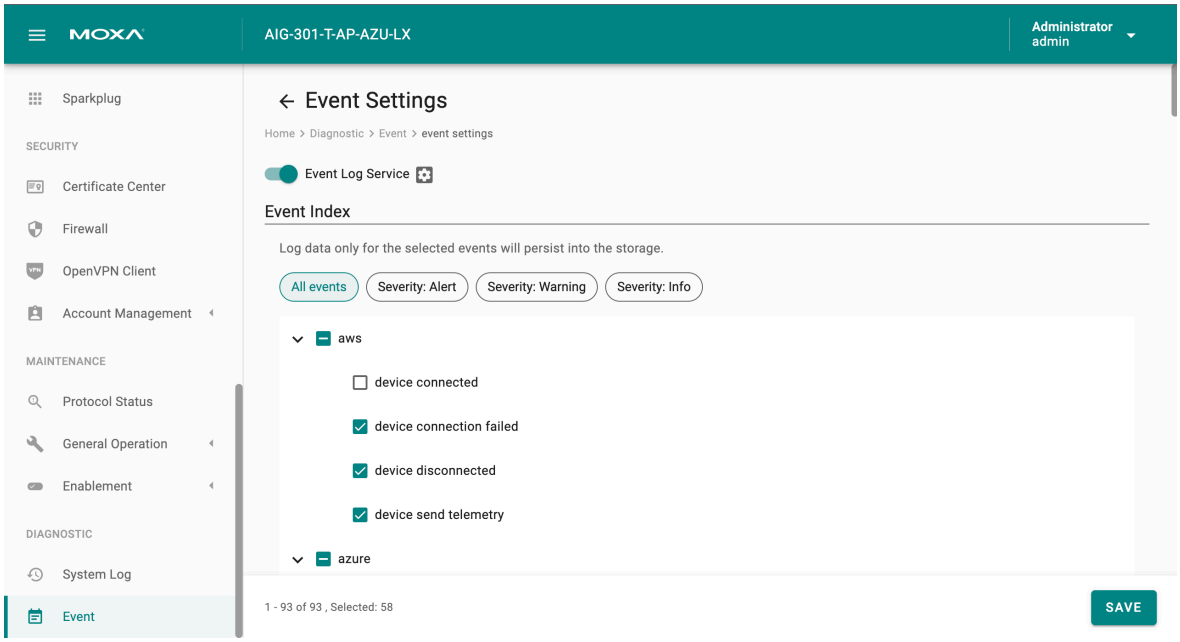


Configuring Event Log Settings

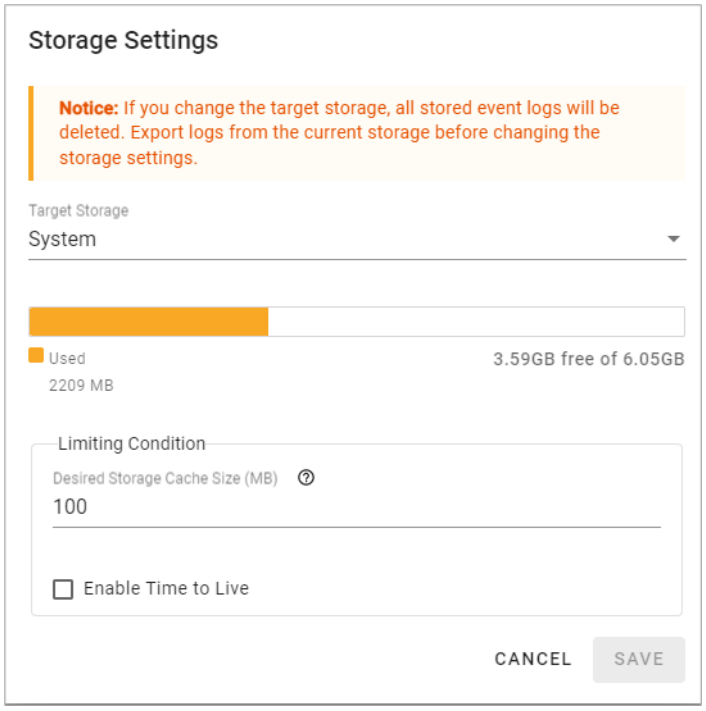
Choose the type of events to store, specify where to keep the logs, and the maximum storage size to use. Click the **Event Settings** to access these settings.



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



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



4. Security Hardening Guide

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

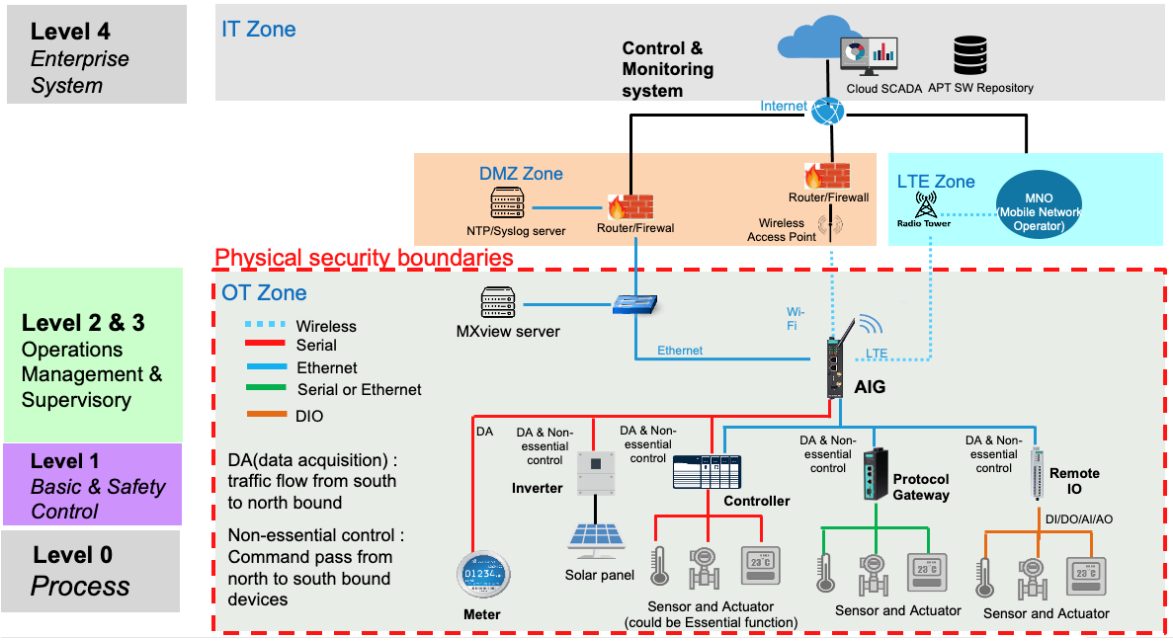
Communication Integrity and Authentication

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

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

Potential Threats and Corresponding Security Measures

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



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

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

Installation

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

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

Publish Mode

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

B. Additional Documentation

Software Downloads

Upgrade Packs:

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

Utility (QuickON):

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

Technical Documentation

https://github.com/TPE-TIGER

OpenAPI Documentation

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