AIG-302 Series User Manual

Version 2.0, June 2026

www.moxa.com/products

AIG-302 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-302 Series advanced IIoT gateways are designed for Industrial IoT applications and meticulously tailored to excel in challenging operating environments commonly found in distributed and unmanned sites. This series seamlessly integrates Modbus RTU/TCP Master (Client) and Slave (Server) protocols, streamlining the collection of data from Modbus devices. Additionally, the AIG-302 Series is preloaded with Azure IoT Edge, Azure IoT device, and MQTT, ensuring a seamless integration process and providing a secure sensor-to-cloud connectivity solution for efficient data acquisition.

The AIG operates as a highly efficient data conduit, expertly facilitating telemetry transmission through its dedicated WAN interfaces (Ethernet, Wi-Fi, and cellular). These interfaces are meticulously optimized to deliver secure, reliable, and high-performance data transfer, focusing on robust communication rather than providing general Internet access to connected devices.

CAUTION

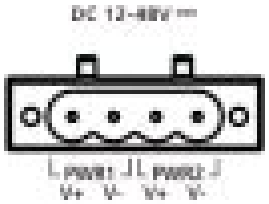
The AIG is not designed to operate in NAT mode. Doing so may compromise its performance and security. Refrain from using NAT mode to ensure optimal functionality. For further guidance on strengthening security, consult the comprehensive Security Hardening Guide for the AIG-302 Series.

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.

2. Getting Started

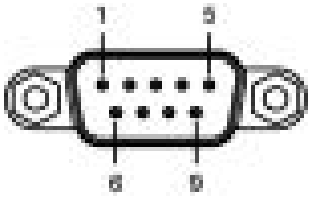
Connecting the Power

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 USR LED will light up. All models support dual power inputs for redundancy.



Connecting Serial Devices

The AIG device supports connecting 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 the AIG's 10/100/1000M Ethernet port and the other end of the cable to the Ethernet network. The AIG will show a valid connection to the Ethernet by LAN1/LAN2 maintaining solid green/yellow color. For details on the behavior of the LEDs, refer to the *AIG-302 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.

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

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

   Default account: **admin**

   Password: **admin@123**

You will see the following homepage after logging in successfully.

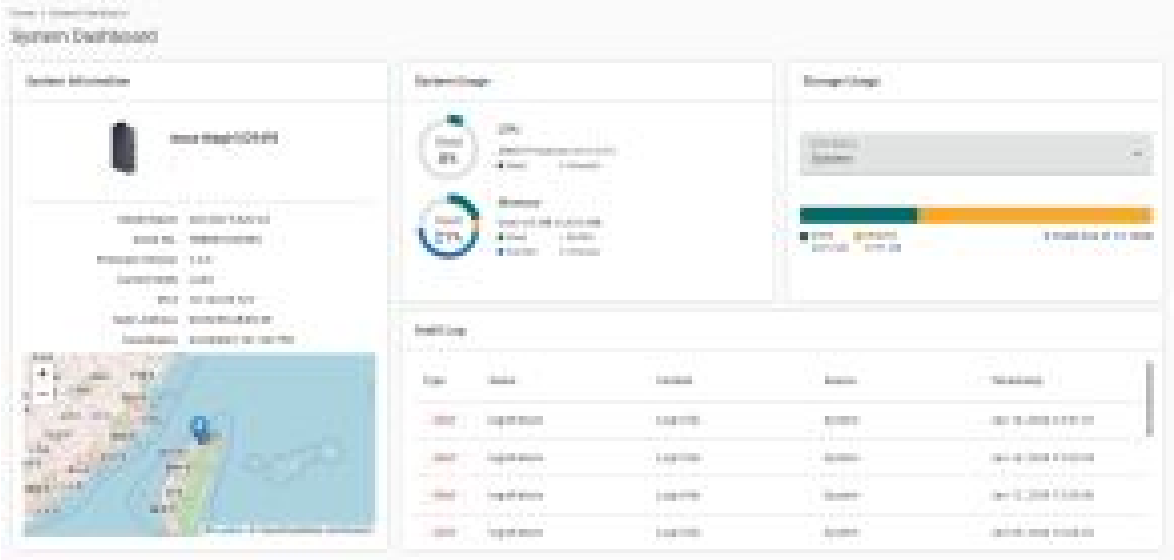
NOTE

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.

Dashboard

System Dashboard

This page gives you an overview of the gateway's system status. Basic system information such as model name, serial No., firmware version, system usage, storage usage, and audit log are displayed.

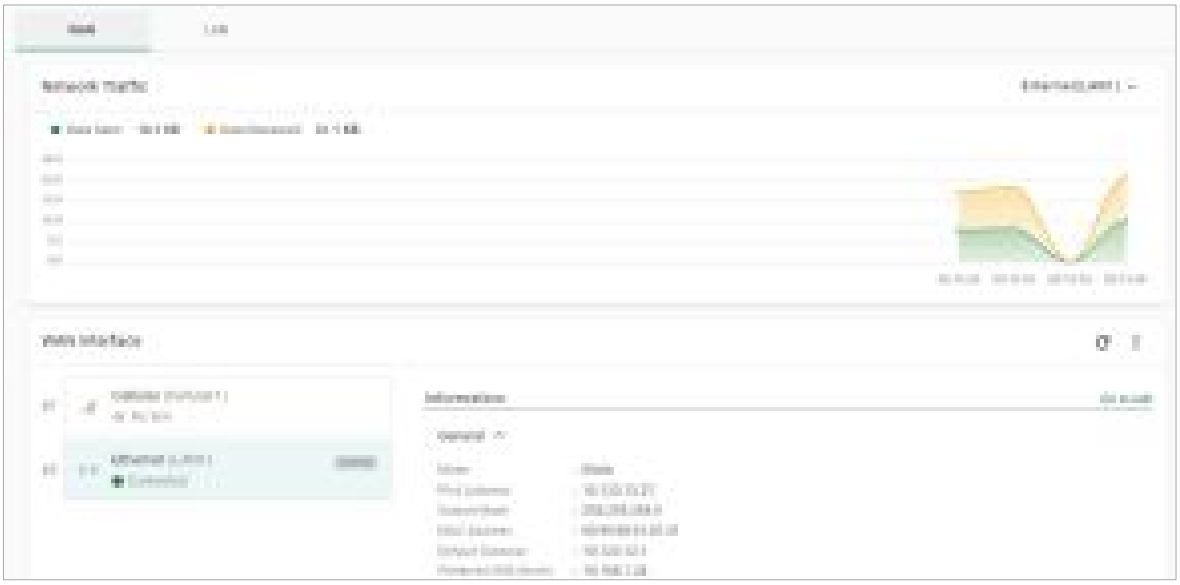


Network Dashboard

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.

Tag Dashboard

In this page, you can create and monitor the real-time tag value for troubleshooting purposes. To see the tag's real-time value, do the following steps:

1. Click + **Edit Tags**.

2. (Optional) use Search to find the tags quickly.

3. Select the tags to monitor in the list.

4. Click **Save**.

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

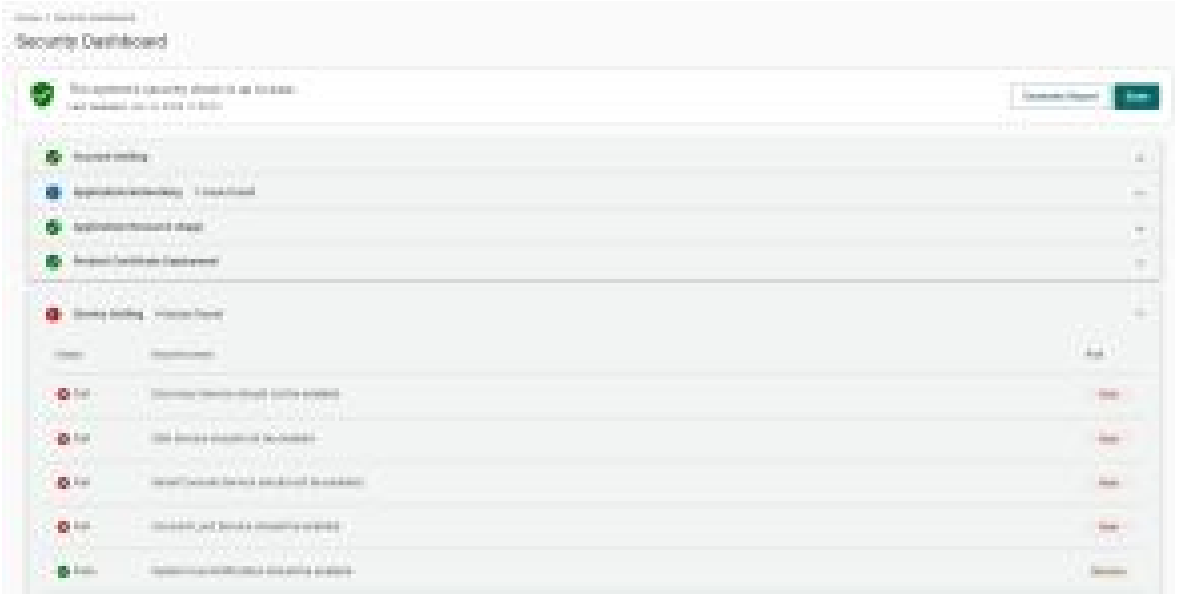
6. (Optional) press the icon to write value for test purposes.

NOTE

Because of the browser precision limitations, you must use RESTful API to write int64/uint64 tags.

Security Dashboard

On this page, you will find a tool that checks the security status of the gateway. Clicking the Scan button initiates the process of identifying potential security risks. Subsequently, you can use the results to configure the gateway and eliminate any identified cyber security threat. Refer to the hardening guide for your product for details.



Parameter	Value	Description
	Pass	No risks.
	Information	There are low-risk failures
	Warning	There are medium-risk failures
	Alert	There are high-risk failures

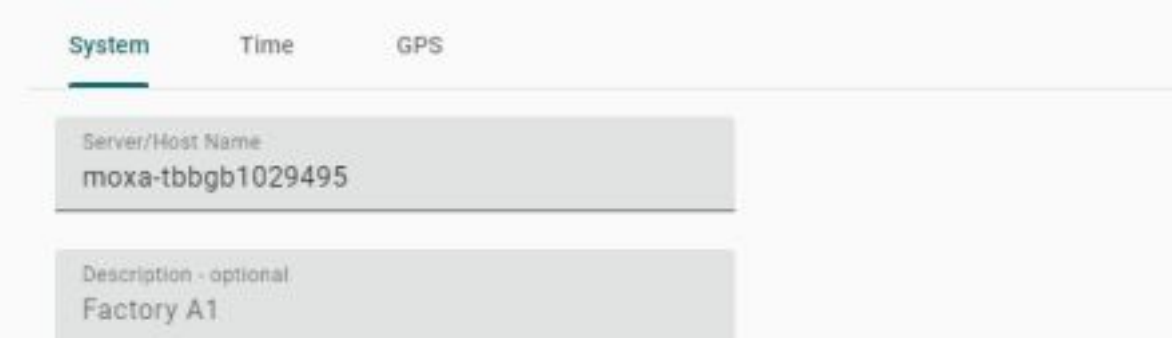
Category	Security Check Criteria	Threat Mitigation/handling
Account Settings	Password should be changed within the set time.	Go to **Account Management > Accounts** to change the password.
	An account should only have one active session at any given time.	Go to **Security > Session Management** to monitor and manage concurrent sessions.
	An account should not have abnormal connections (E.g., more than one session per account from different source IPs).	
Application Networking	System should not have open network ports.	Go to **Security > Firewall** and check the allow list.
Application Resource Usage	IoT Edge modules should not utilize system disk's configurable space.	Ensure that the IoT Edge modules are deployed only in specific directories/paths, such as **/var/run/** and **/tmp/**, in the system storage.
	IoT Edge modules should not utilize system disk's non-configurable space.	
	IoT Edge modules should not be granted direct privileges.	To grant permissions to IoT Edge modules, go to **Cloud Connectivity > Azure IoT Edge > Module Permission**, create a service account, and grant the required permissions to the IoT Edge module.

Category	Security Check Criteria	Threat Mitigation/handling
Product Certificate Deployment	Production certificate should be configured as an Azure IoT Edge downstream certificate.	For enhanced security robustness, we recommend using your own certificate instead of the default one. Go to **Cloud Connectivity > Azure IoT Edge > Downstream Certificate** to upload a certificate.
	Azure IoT Edge should not use a connection string for provisioning.	For enhanced security robustness, we recommend using a TPM or a X.509 certificate.
	All certificates should not expire within the next three months.	Go to **Security > Certificate Center** to check the status of each certificate. If you find that a certificate will expire soon or has already expired, go to **Cloud Connectivity > Azure IoT Edge/Azure IoT Device/MQTT Client or Security > HTTPS** to check and replace the certificates.
	All certificates should not have expired.	
Service Settings	Discovery Service should not be enabled.	Go to **Maintenance > Service** to disable the Discovery Service.
	SSH service should not be enabled.	Go to **Maintenance > Service** to disable the Debug Mode.
	Serial Console Service should not be enabled.	Go to **Security > Service** to disable the local console.
	Account Lock Service should be enabled.	Go to **Security > Login Lockout** to enable the **Login Failure Lockout** option.
	System Use Notification Service should be enabled.	Go to **Security > System Use Notification** to enable the System Use Notification Service.
System Status Check	Product software package should be up to date.	Go to **Maintenance > Software Upgrade** and click **Check for Upgrade** to retrieve the latest upgrade pack information.
	System backup should be performed at least once a year.	Go to **Maintenance > Backup & Restore** and click **Manage** to back up the system.

System Settings

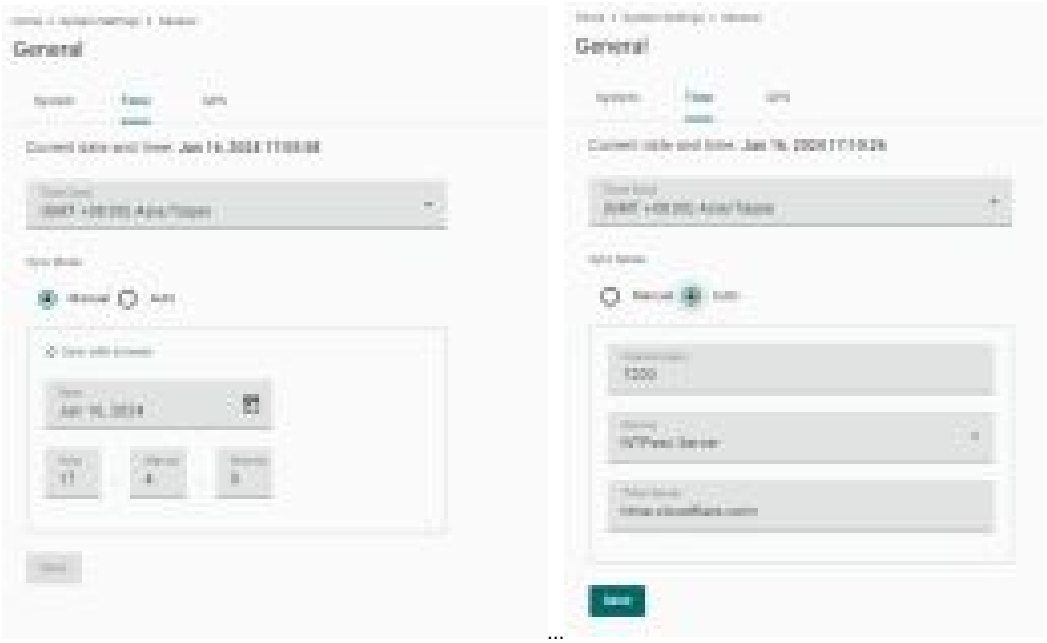
General

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 the function, etc.
Description - optional	Alphanumeric string	You can enter a description to help identify the unit location such as "Cabinet A001."

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



...

Parameter	Value	Description
Time Zone	User's selectable time zone	The field allows you to select a different time zone.
Sync Mode	Manual Auto	Manual: input the time parameters by yourself Auto: it will automatically sync with time source. NTP and GPS can be selected. NOTE: When the Auto mode is selected, in general, it takes 2 to 4 minutes. If the satellite search is slower, it could take up to 12 minutes (worst-case scenario)
Interval (sec)	3600 to 86400	The time interval to sync the time source
Source	NTPsec Server NTP Server GPS	The way to sync the time clock
Time Sever	IP or Domain address (e.g., 192.168.1.1 or time.cloudflare.com)	This field is required to specify your time server's IP or domain name if you choose the NTP server as the source

NOTE

When using GPS as a time-synchronization source, set the GPS mode to **Auto** before entering the configuration page.

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.

Serial

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

To configure serial setting, do the following:

1. Choose the COM port to configure.

2. Set the baudrate, parity, data bits, and stop bits.

NOTE

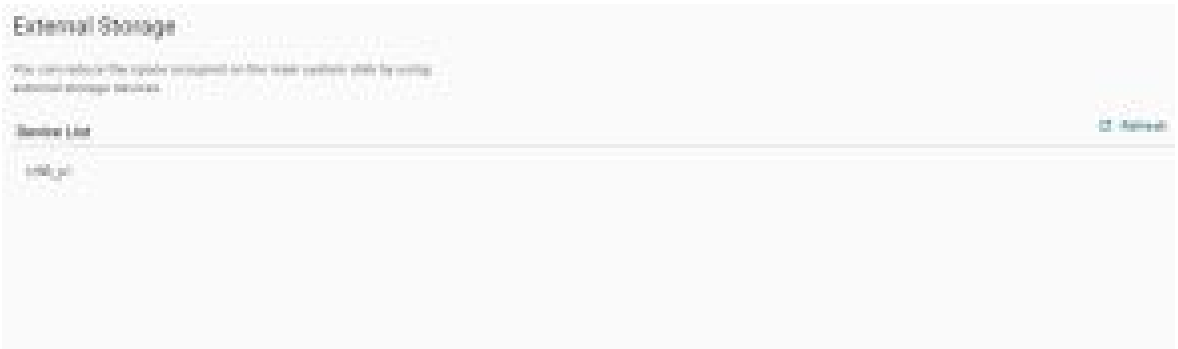
Incorrect settings will cause communication failures.

3. Click **Save** for the settings to take effect.

Parameter	Value	Description
Interface	rs232, rs422, rs485-2w	
Baud Rate	300 to 921600	
Parity	none, odd, even, space, mark	
Data Bits	5, 6, 7, 8	
Stop Bits	1, 2	
Flow Control	None, hardware, software	Hardware: flow control by RTS/CTS signal

External Storage

You can attach external storage to the AIG for saving logs, buffer space for Store and Forward, and creating system backups. Once you attach a storage, you will find it in the **Device List**.



NOTE

LIMITATION:

- AIG does not allow the connection of multiple USB devices through a USB hub.
- The external USB format supported for AIG is FAT.

I/O

The AIG-302 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, click 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 OFF	High voltage Low voltage

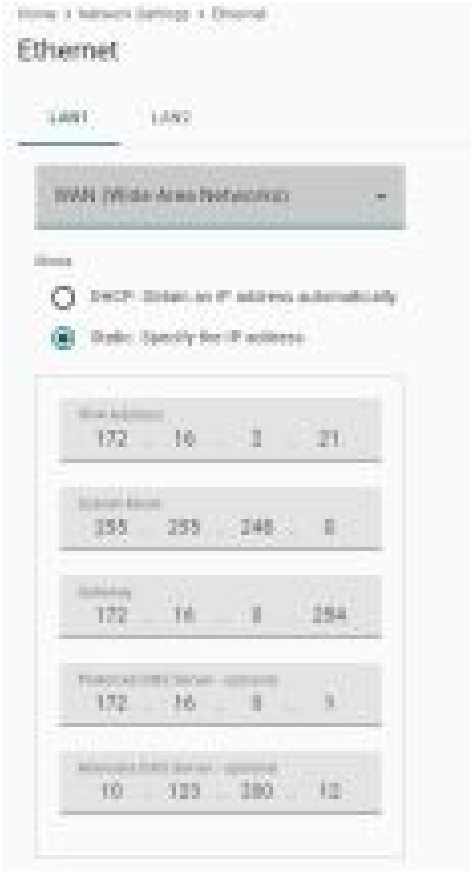
Network Settings

Ethernet

Go to **Network Settings > Ethernet** 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.

Parameter	Value	Description
Alternate DNS Server— optional	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

NOTE

If the LAN interface is assigned DNS and gateway settings via a DHCP server, the settings will be automatically applied to other interfaces, such as cellular and Wi-Fi client.

If the LAN option is selected, the AIG can be configured to operate as a DHCP server, offering the additional benefit of dynamically assigning IP addresses to devices on the network.

To configure DHCP server settings, do the following:

1. Check Enable DHCP Server.
2. Input IP Address Range parameters.
3. Specify Lease Time.
4. Click **Save**.

NOTE

LIMITATION: When AIG acts as the DHCP server, it will not allocate the DNS IP to the DHCP client.

Cellular

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

You can create customized cellular profiles 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.
5. Input **APN**.

NOTE

To prevent the SIM from being locked due to three incorrect attempts, a mechanism in the AIG stops attempting to unlock the SIM when the PIN Retry count reaches 2 (only one attempt is remaining). At this point, insert the SIM into another device (e.g., cellphone) and attempt to unlock it. This way, when you reinsert the SIM card into the AIG and restart, the PIN Retry count is reset to 3.

NOTE

LIMITATION: AIG does not support hot-plugging of the SIM card; device restart is required after inserting or removing the SIM card.

6. Click **Done**.
7. 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.

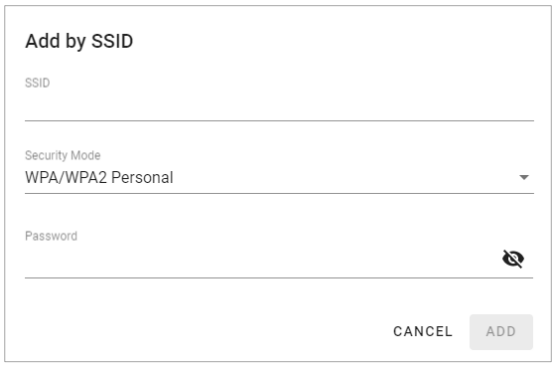
Go to **Network Dashboard > WAN** if you want to check the cellular network's connection status afterwards.

Wi-Fi Client

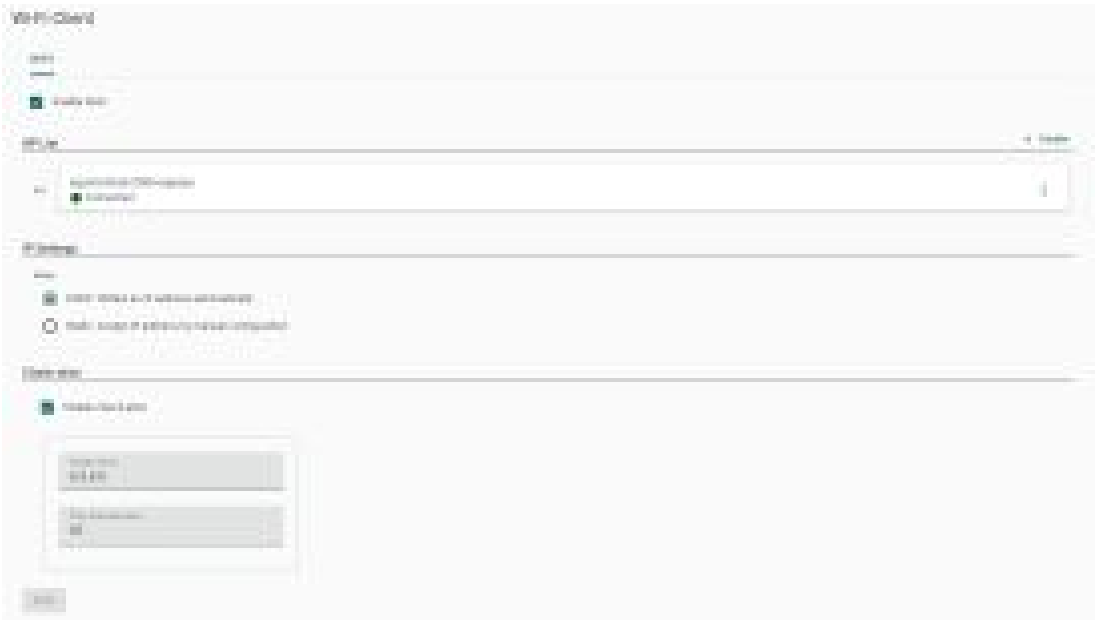
Go to **Network Settings > Wi-Fi** to view the Wi-Fi settings.

To configure Wi-Fi settings, check **Enable Wi-Fi** and do the following:

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



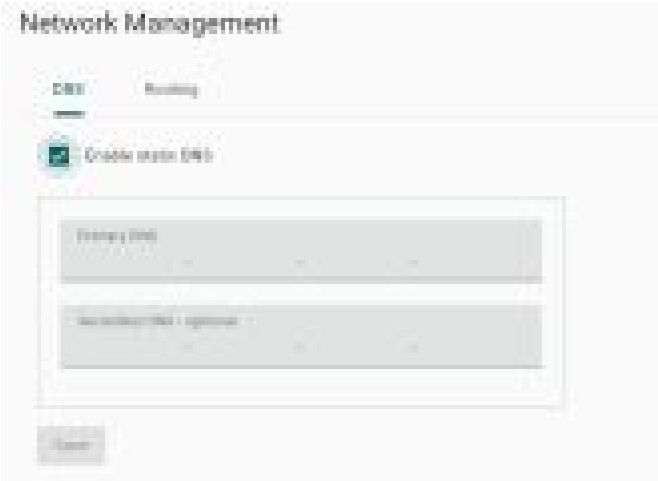
2. Select **DHCP** or **Static mode**.
3. Check **Check-alive** function which can be used to ensure Internet connectivity.
4. Click **Save**.



Network Management

DNS

By manually configuring specific DNS server addresses, users can ensure stable and predictable internet connectivity without relying on potentially fluctuating or unreliable DNS settings provided by dynamic configurations (such as those obtained from a DHCP server). This helps to improve DNS resolution speed, enhance overall network performance, and strengthen control over network traffic and security by specifying trusted DNS servers.



Routing

The Routing priority feature allows the IIoT Gateway to prioritize different network interfaces (such as cellular, LAN, and Wi-Fi) as needed to optimize network performance.

Cloud Connectivity

Azure IoT Edge

Connect to Azure IoT Hub

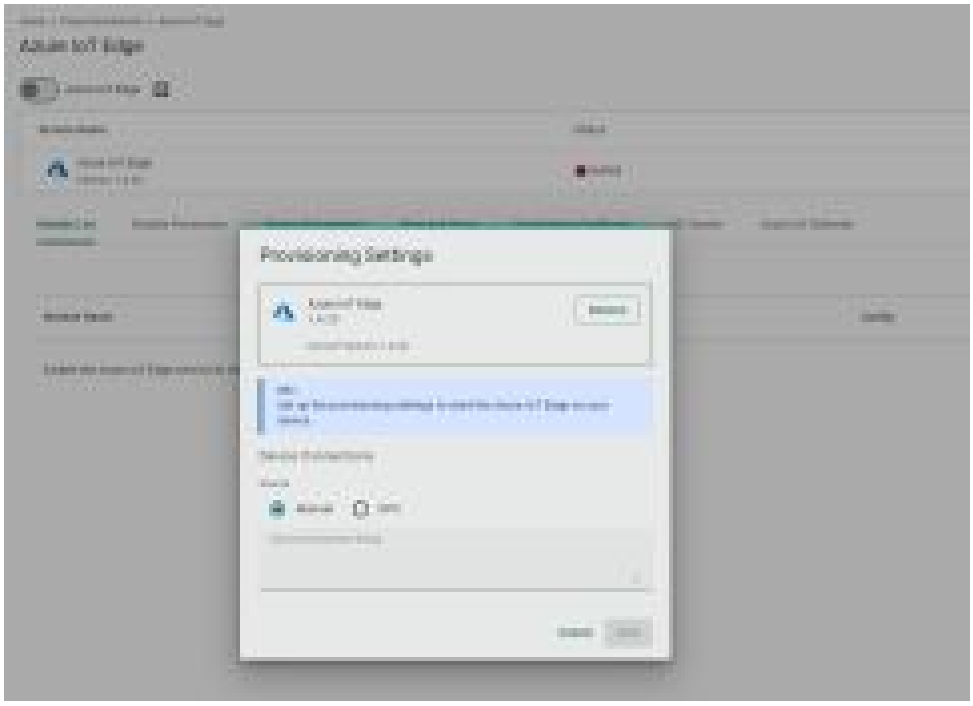
To configure the Azure IoT Edge settings. You can enable/disable the Azure IoT Edge service and enroll the device via manual setting or DPS (Device Provisioning Service) here.

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.



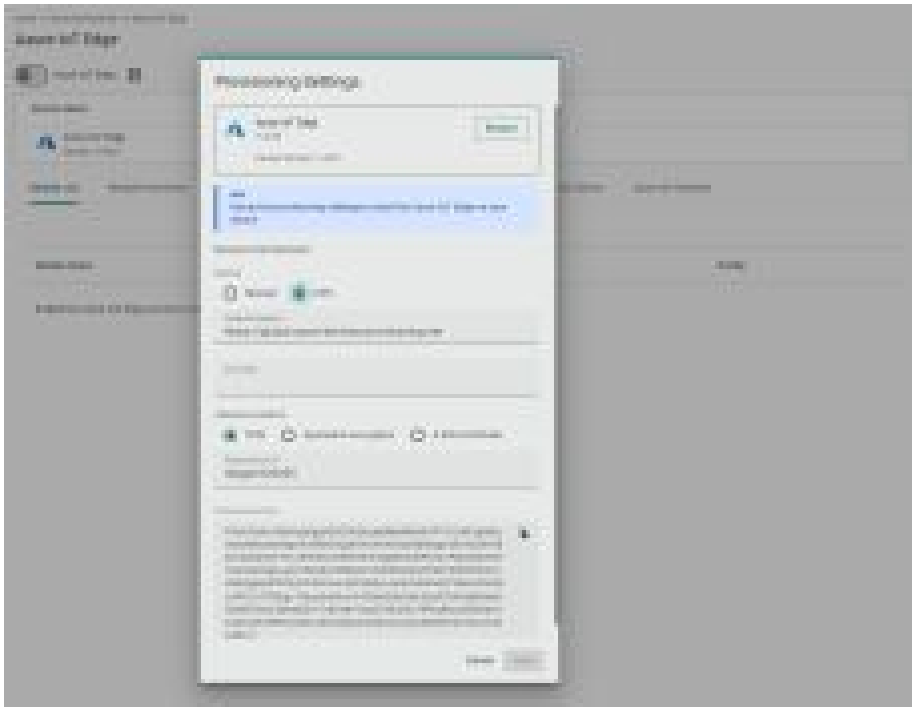
4. Click **Save.**

To create an Azure IoT Edge connection for your gateway 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 based on your gateway 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 Symmetric Key.

For X.509, upload the X.509 Certificate and Private Key.

4. Click **Save**.

Detailed information about the Azure DPS configuration in the Azure IoT Hub is available at Set up a DPS.

Module Permission

When executing an Azure IoT Edge module, for the sake of gateway security, it is necessary to generate the access key first and then import the environment variables for that module from Azure IoT Hub.

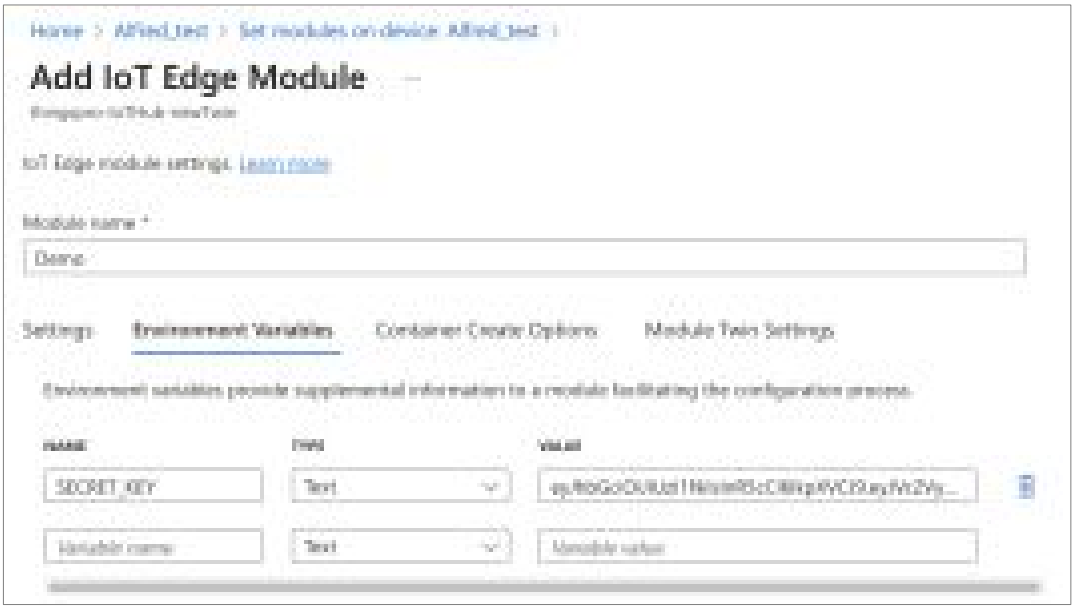
To generate the access key for a module, do the following:

1. Click the Module Permission tab and click **Create**.

2. Specify a module name and grant permissions to the module. (NOTE: the module name must be the same as the one created in Azure IoT Hub).

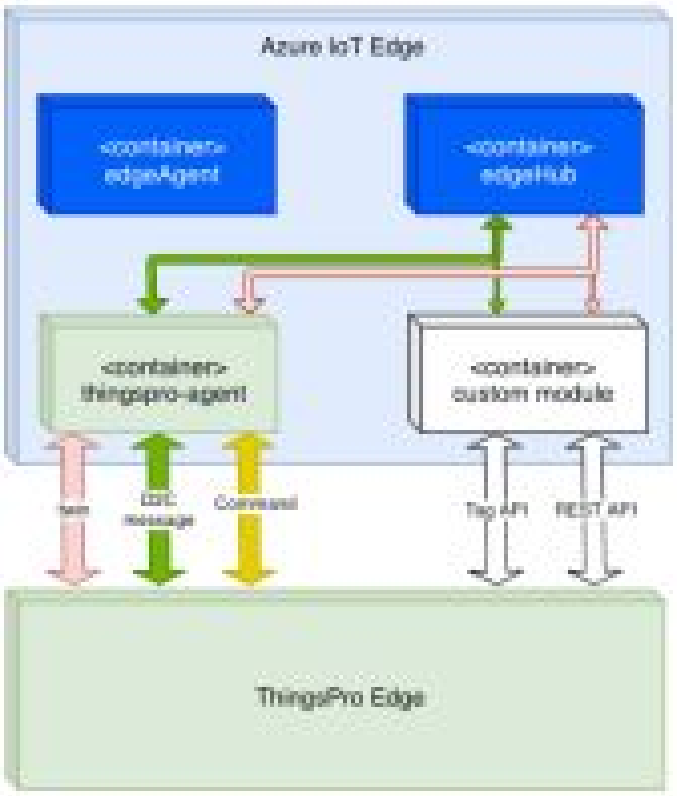
3. Click **Save**.

4. Click Download Key to save the secret access key or click to copy the key and paste it in the Azure IoT Hub.



ThingsPro Agent

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



To install the ThingsPro Agent, do the following:

1. Create an IoT Edge device.
2. Add a module from the Azure IoT Hub based on the following information

Docker Image:

```
moxa2019/thingspro-agent:3.1.0-armhf
```

Container Create Option:

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

Module Twin

ThingsPro Agent exposes up-to-date configuration of connected devices via Reported Properties and allows you to re-configure devices and turn on/off services via Desired Properties. In the current version, ThingsPro Agent allows the following sections to be updated via Desired Properties.

Reported Properties:

Properties	Sample

httpserver	{
	"httpserver": {
	"httpPort": 80,
	"httpsEnable": true,
	"httpsPort": 8443,
	"ipv6Enable": true,
	"keyFileName": "client_nopassphrase.key",
	"certFileName": "client.pem",
	"httpEnable": true
	}
	}

discovery	{
	"discovery": {
	"enable": true,
	"schedule": {
	"enable": true,
	"disableAfterSec": 900
	}
	}
	}

wan	{
	"wan": {
	"displayName": "LAN1",
	"dns": {
	"0": "10.128.8.5",
	"arraySize": 1
	},
	"gateway": "10.144.51.254",
	"ip": "10.144.48.128",
	"name": "eth0",
	"netmask": "255.255.252.0"
	}
	}

route	{
	"route": {
	"defaultRoute": "LAN1",
	"priorityList": {
	"0": "Cellular1",
	"1": "LAN1",
	"arraySize": 2
	}
	}
	}

Properties	Sample

serials	{
	"serials": {
	"0": {
	"baudRate": 9600,
	"dataBits": 8,
	"device": "/dev/ttyM0",
	"displayName": "PORT 1",
	"flowControl": "none",
	"id": 1,
	"mode": "rs232",
	"parity": "none",
	"stopBits": 1
	},
	"arraySize": 1
	}
	}

time	{
	"time": {
	"lastUpdateTime": "2023-05-24T23:22:05+00:00",
	"ntp": {
	"enable": false,
	"interval": 7200,
	"server": "time.cloudflare.com",
	"source": "timeserver"
	},
	"timezone": "Asia/Taipei"
	}
	}

ethernets	{
	"ethernets": {
	"0": {
	"enable": true,
	"enableDhcp": false,
	"id": 1,
	"name": "enp0s31f6",
	"status": "connected",
	"displayName": "LAN1",
	"gateway": "10.123.12.1",
	"ip": "10.123.13.11",
	"linkSpeed": 1000,
	"mac": "00:90:E8:A6:61:88",
	"netmask": "255.255.252.0",
	"wan": true,
	"dns": {
	"0": "10.123.200.11",
	"1": "10.123.200.12",
	"arraySize": 2
	}
	},
	"arraySize": 1
	}
	}

Properties	Sample

general	<pre>{
	  "general": {
	  "biosVersion": "V1.0.0S01",
	  "firmwareVersion": "0.15.0",
	  "serialNumber": "TBBCE1070929",
	  "softwareVersion": "0.15.0+2045",
	  "cpu": "Intel(R) Core(TM) i7-7600U CPU @ 2.80GHz",
	  "description": "",
	  "hostName": "moxa-tbbce1070929",
	  "lastBootTime": "2023-05-24T23:06:57+00:00",
	  "memorySize": 16635346944,
	  "modelName": "AIG-302-T-AP-AZU-LX"
	  }
	}</pre>

gps	<pre>{
	  "gps":{
	  "mode": "manual",
	  "interface": "",
	  "location": {
	  "lat": 24.984129,
	  "lng": 121.551753
	  }
	}</pre>

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

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

Properties	Sample

	"pinCode": "",
	"simSlot": 2
	},
	"arraySize": 1
	},
	"currentProfileName": "Profile-1",
	"imsi": "",
	"keepalive": {
	"enable": true,
	"intervalSec": 60,
	"targetHost": "8.8.8.8"
	},
	"mac": "",
	"gateway": "",
	"id": 1,
	"name": "wwan0",
	"profileTimeout": 120,
	"cellId": "",
	"displayName": "Cellular1",
	"dns": {
	"arraySize": 0
	},
	"enable": false,
	"status": "sim_pin_locked",
	"signalStrength": 0,
	"capabilities": {
	"sim": 2
	},
	"iccId": "89886972203703305466",
	"ip": "",
	"mode": "unknown",
	"imei": "357575100284579",
	"lac": "",
	"netmask": "",
	"tac": ""
	},
	"arraySize": 1
	}
	}

Wi-Fi	{
	"wifi":{
	"0":{
	"client":{
	"checkalive":{
	"enable":false,
	"intervalSec":60,
	"targetHost":"8.8.8.8"
	},
	"connectState":"disabled",
	"currentAp":"",
	"ipSetting":{
	"dns":{
	"arraySize":0
	},
	"enableDhcp":true,
	"gateway":"",
	"mac":""
	},
	"networks":{
	"0":{
	"band":"band24",

Properties	Sample

	"bssid":"18:62:E4:0F:5E:DB",
	"security":{
	"mode":"wpa2-personal",
	"password":"12345678",
	"support":true
	},
	"signal":0,
	"signalStrength":0,
	"ssid":"TESTAP",
	"uuid":"Z3djNkHNR"
	},
	"1":{
	"band":"band24",
	"bssid":"",
	"security":{
	"mode":"wpa2-personal",
	"password":"admin@123",
	"support":true
	},
	"signal":0,
	"signalStrength":0,
	"ssid":"moxa",
	"uuid":"WqOjNzNHRz"
	},
	"arraySize":2
	},
	"priority":{
	"0":"Z3djNkHNR",
	"1":"WqOjNzNHRz",
	"arraySize":2
	}
	},
	"displayName":"WiFi2",
	"enable":false,
	"id":1,
	"mode":"client",
	"name":"wlp2s0"
	},
	"arraySize":1
	}
	}

Desired Properties:

Properties	Sample

httpserver	{
	"desired": {
	"httpserver": {
	"httpEnable": true,
	"httpsEnable": true,
	"httpsPort": 8443
	"ipv6Enable": true
	}
	}
	}

discovery	{
	"desired": {
	"discovery": {
	"enable": true,
	"schedule": {
	"enable": true,
	"disableAfterSec": 900
	}
	}
	}
	}

serials	{
	"desired": {
	"serials": {
	"0": {
	"mode": "rs232",
	"stopBits": 1,
	"baudRate": 9600,
	"dataBits": 8,
	"parity": "none",
	"flowControl": "none",
	"id": 1
	},
	"arraySize": 1
	}
	}
	}

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

Properties	Sample

general	Update gateway host name:
	{
	"desired": {
	"general": {
	"hostName": "MyHost"
	}
	}
	}
	
	Update gateway description:
	{
	"desired": {
	"general": {
	"description": "MyDevice"
	}
	}
	}

gps	Update GPS latitude and longitude by manual mode:
	{
	"desired": {
	"gps":{
	"mode": "manual",
	"location": {
	"lat": 11,
	"lng": 12
	}
	}
	}
	}
	Update GPS by auto mode:
	{
	"desired": {
	"gps":{
	"mode": "auto",
	"interface": "GPS1"
	}
	}
	}

ethernets	{
	"ethernets": {
	"0": {
	"dns": {
	"0": "10.128.8.5",
	"arraySize": 1
	},
	"enable": true,
	"enableDhcp": false,
	"gateway": "10.144.51.254",
	"id": 1,
	"ip": "10.144.48.128",
	"netmask": "255.255.252.0",
	"wan": true
	},
	"arraySize": 1
	}
	}

Properties	Sample

SoftwareUpgrade	{
	"desired": {
	"softwareUpgrade": {
	"allowUpdate": true,
	"allowOverCellular": false,
	"snapshotBeforeUpdate": true,
	"autoScan": false,
	"autoScanExpression": "0 3 * * 1-5"
	}
	}
	}

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

Properties	Sample

Wi-Fi	<pre>{
	  "wifis":{
	  "0":{
	  "id":1,
	  "enable":true,
	  "enableDhcp":false,
	  "mode":"ap",
	  "ap":{
	  "band":"band24",
	  "ssid":"AIG302-WiFi-AP",
	  "password":"!2345678",
	  "security":"wpa2",
	  "network":{
	  "ipAddress":"192.168.5.1",
	  "ipNetmask":"255.255.254.0"
	  },
	  "dhcpserver":{
	  "startip":"192.168.5.101",
	  "stopip":"192.168.5.254",
	  "dns":[
	  "1.1.1.1",
	  "1.1.0.0"
	  ],
	  "leasetime":12
	  }
	  }
	  },
	  "arraySize":1
	  }
	}</pre>

Direct Method:

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

No	Method Name	Description
1	thingspro-api-v1	Universal direct method that invokes all Restful APIs of AIG
2	system-reboot	Restarts the gateway
3	thingspro-software-upgrade-check	Check product package is available to upgrade or up-to-date
4	thingspro-software-upgrade	Performs over-the-air (OTA) software upgrades with product package
5	upload-audit-logs	Upload audit logs to Azure blob storage
6	upload-system-logs	Upload system logs to Azure blob storage

Thingspro-api-v1

Method Name:

```
thingspro-api-v1
```

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

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

Key	Description
path	AIG-302 Restful API endpoint
method	The method associated with the API endpoint
headers	Required by the application/JSON payload
requestBody	Used to post data required by the API endpoint

Response:

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

NOTE

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

system-reboot

Method Name:

```
system--reboot
```

Request Payload:

```
{}
```

Response:

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

thingspro-software-upgrade-check

Method Name:

```
thingspro-software-upgrade-check
```

Request Payload:

```
{}
```

Response (available response):

```
{
   "status": 200,
   "payload": {
      "checktime": "2023-04-27T07:51:36Z",
      "count": 1,
      "data": [
         {
            "name": "moxa-aig-302-tpe",
            "size": 31076,
            "currentVersion": "0.11.1",
            "newVersion": "0.12.0+1533",
            "category": "software"
         }
      ]
   }
}
```

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

```
{
   "status": 200,
   "payload": {
      "checktime": "2023-04-27T08:08:38Z",
      "count": 0,
      "data": []
   }
}
```

NOTE

AIG-302 allows only one active software upgrade job at a time. We recommend changing the response timeout parameters to 1 minute to prevent system exceptions.

Thingspro-software-upgrade

Method Name:

```
thingspro-software-upgrade
```

Request Payload:

```
{}
```

Response:

```
{
   "status": 200,
   "payload": {
      "data": [
         "moxa-aig-302-tpe"
      ],
      "message": "Successfully trigger"
   }
}
```

NOTE

AIG-302 allows only one active software upgrade job at a time. We recommend changing the response timeout parameters to 1 minute to prevent system exceptions.

Upload-audit-logs

Method Name:

```
upload-audit-logs
```

Request Payload (Set HTTP/HTTPS configuration as an example):

```
{
  "connectionString":
"DefaultEndpointsProtocol=https;AccountName=thingsproedge;AccountKey=hgnYe/08sWqlcGK
d7VR8XNRvjydebzzSeVZxFvRCmepUqA69LTtNY13UZ5fejgZgcys+jC5B+qf3+AStsEkNzg==;End
pointSuffix=core.windows.net",
  "containerName": "aig302"
}
```

Variable	Description
connectionString	The connection string is the access key or shared access signature of the Azure blob storage
containerName	Upload to the container which belongs to the Azure blob storage

Response:

```
{
   "status": 200,
   "payload": {
      "data": "upload successfully"
   }
}
```

NOTE

We recommend changing the timeout parameters to 1 minute to prevent system exceptions. In addition, take the upload speed and log size into consideration when adjusting timeouts.

Upload-system-logs

Method Name:

```
upload-system-logs
```

Request Payload (Set HTTP/HTTPS configuration as an example):

```
{
"connectionString":
"DefaultEndpointsProtocol=https;AccountName=thingsproedge;AccountKey=hgnYe/08sWqlcGK
d7VR8XNRvjydebzzSeVZxFvRCmepUqA69LTtNY13UZ5fejgZgcys+jC5B+qf3+AStsEkNzg==;End
pointSuffix=core.windows.net",
 "containerName": "aig302"
}
```

Variable	Description
connectionString	The connection string is the access key or shared access signature of the Azure blob storage.
containerName	Upload to the container which belongs to the Azure blob storage.

Response:

```
{
   "status": 200,
   "payload": {
      "data": "upload successfully"
   }
}
```

NOTE

We recommend changing the timeout parameters to 1 minute to prevent system exceptions. (You may also consider adjusting the corresponding timeout based on the upload speed and log size.)

Device Management

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

Message Group

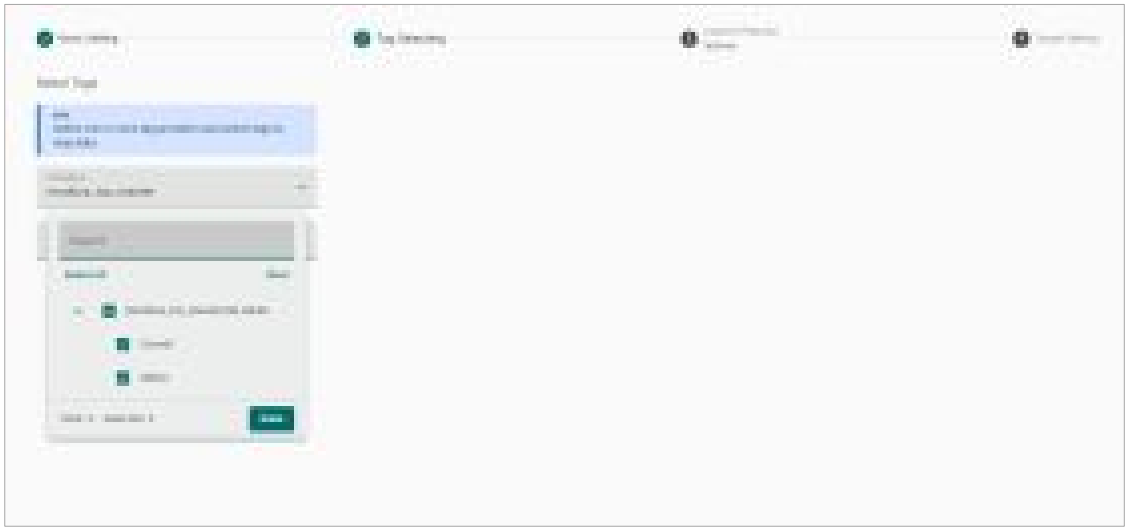
The simplest message type for sending IoT device data to your IIoT applications is a telemetry message. To create a telemetry message, do the following:

1. Click **+ Create** to create a new message group.

2. Specify a name for the **Message Group**.
3. Select a **Publish Mode**.

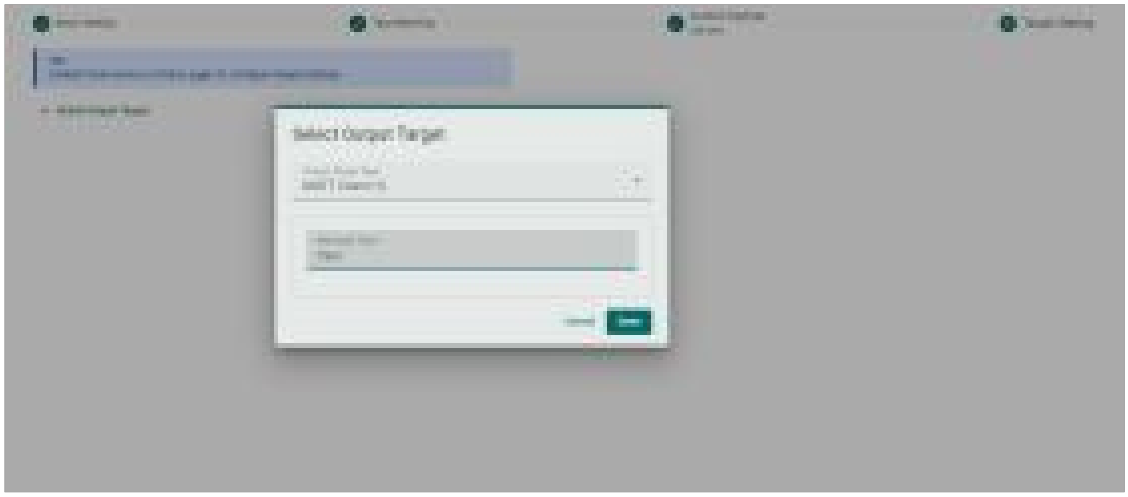
   For details, see Publish Mode.

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



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. Select **Output Target Type**.
10. (Optional) Enter Property Key and Value.

11. Click **Done** and **Save**.

Downstream Certification

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 Edge (AIE) Configuration Checks

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**. ThingsPro Edge provides a result after checking for issues. 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, Device Management, and Downstream/Upstream credentials.

Azure IoT Defender

The web console is currently unavailable for configuring the Azure IoT Defender; configuration is done via a RESTful API.

Enabling the API

```
curl "http://127.0.0.1:59000/api/v1/azure-iotedge" \
    -X PATCH \
    -H "Content-Type:application/json" \
    -H "Authorization:Bearer $(cat ./token)" \
    -d '{"provisioning":{"defenderEnable":true}}'
```

Using the API to Check the Status of the Defender Service

```
curl "http://127.0.0.1:8443/api/v1/azure-iotedge/defender" \
   -X GET \
   -H "Content-Type:application/json" \
   -H "Authorization:Bearer ${token}"
```

Using the API to Restart the Defender Service

```
curl "http://127.0.0.1:59000/api/v1/azure-iotedge/defender/reload" \
    -X PUT \
    -H "Content-Type:application/json" \
    -H "Authorization:Bearer $(cat ./token)"
```

Monitoring the Log of the Defender Service

```
sudo journalctl -u defender-iot-micro-agent -f
```

Testing the Defender Service by Triggering a Baseline Violation

```
touch /tmp/DefenderForIoTOSBaselineTrigger.txt
```

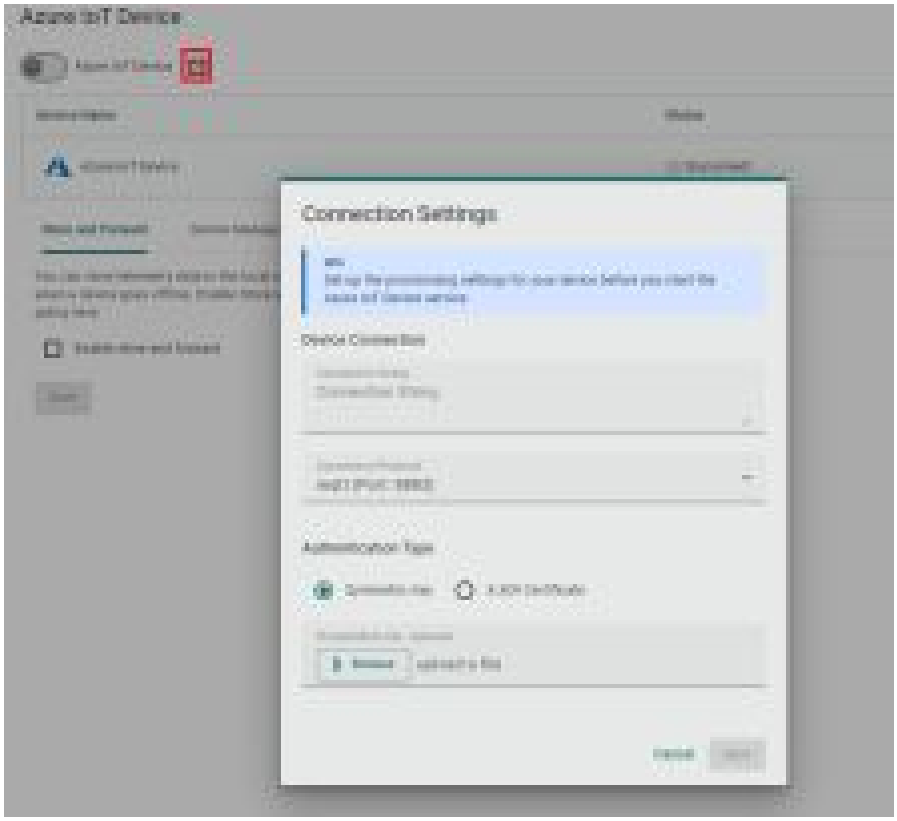
Azure IoT Device

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

> **NOTE**
>
> You will need to register an Azure account to manage the Azure IoT Device service for your IIoT application.

To create the Azure IoT Device connectivity, do the following:

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 **Save**.

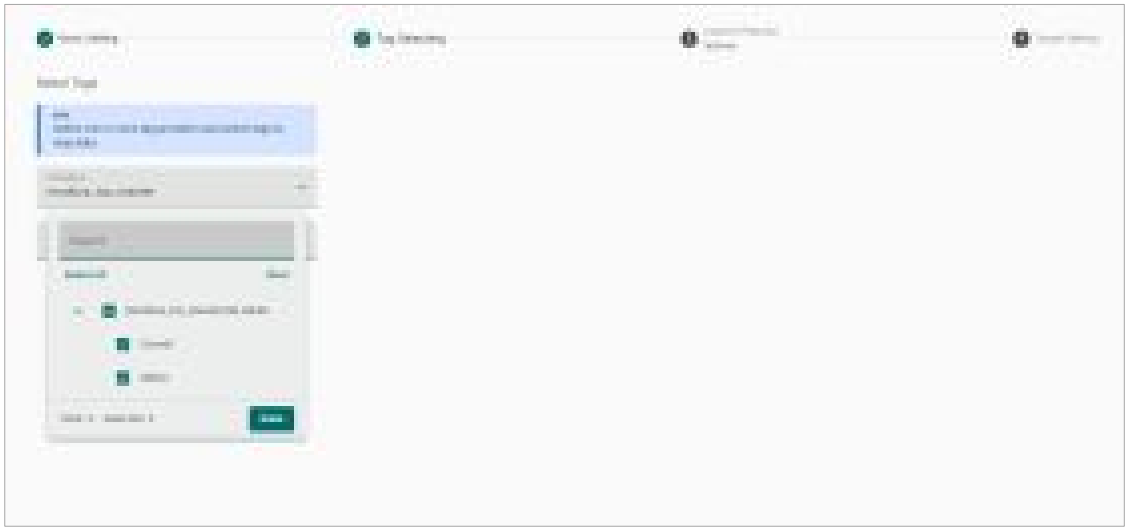
Message Group

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 **+ Create** to create a new message group.

2. Specify a name for the **Message Group**.
3. Select a **Publish Mode**.
   For details, see Publish Mode.

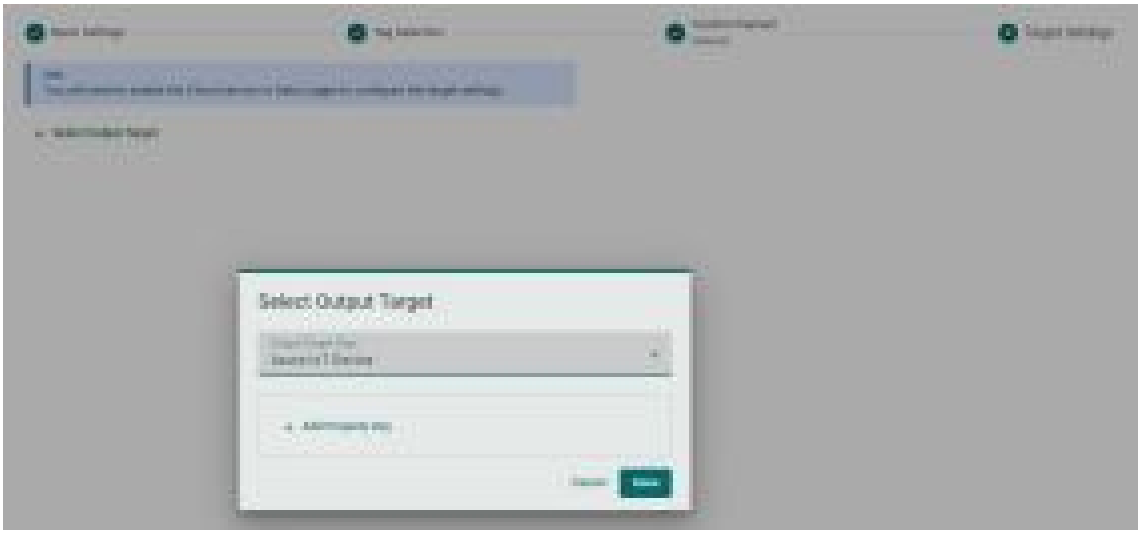
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **Next**.
6. Select tags (e.g., Modbus Master (Client)).



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. Select **Output Target Type**.

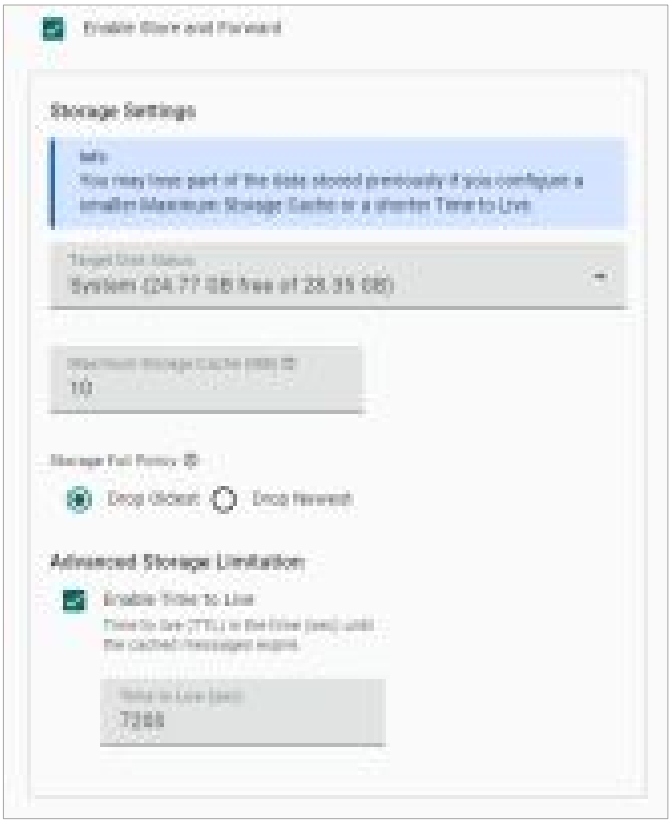


10. (Optional) Enter Property Key and Value.

11. Click **Done** and **Save**.

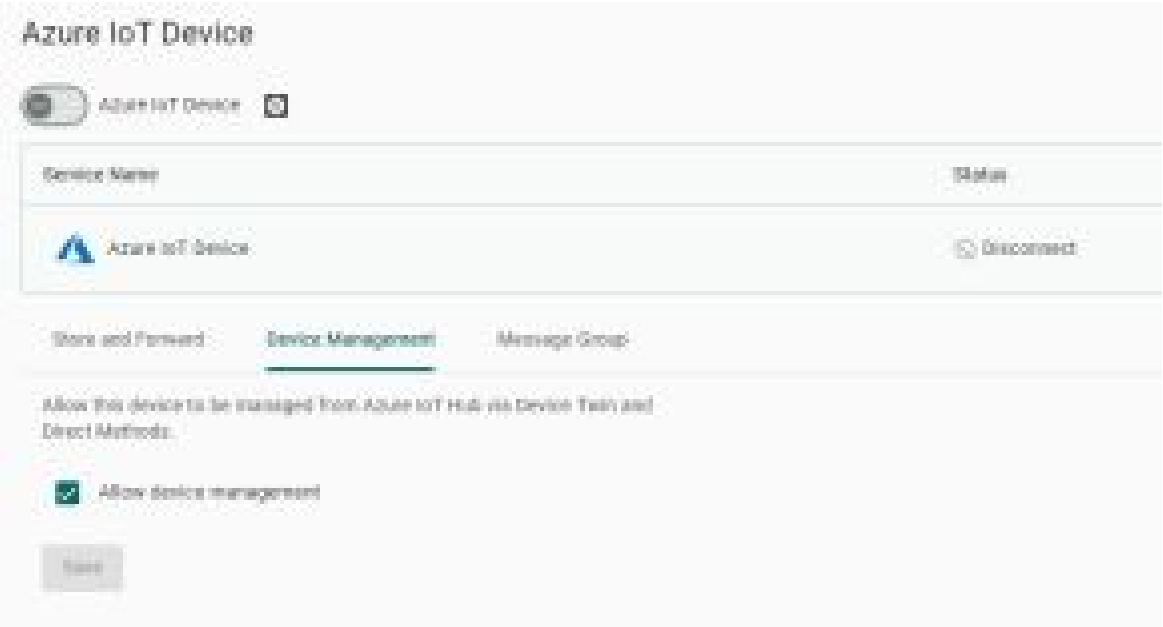
Store and Forward

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

Allows this AIG to be managed from Azure IoT Hub via Device Twin and Direct Methods.



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, do the following:

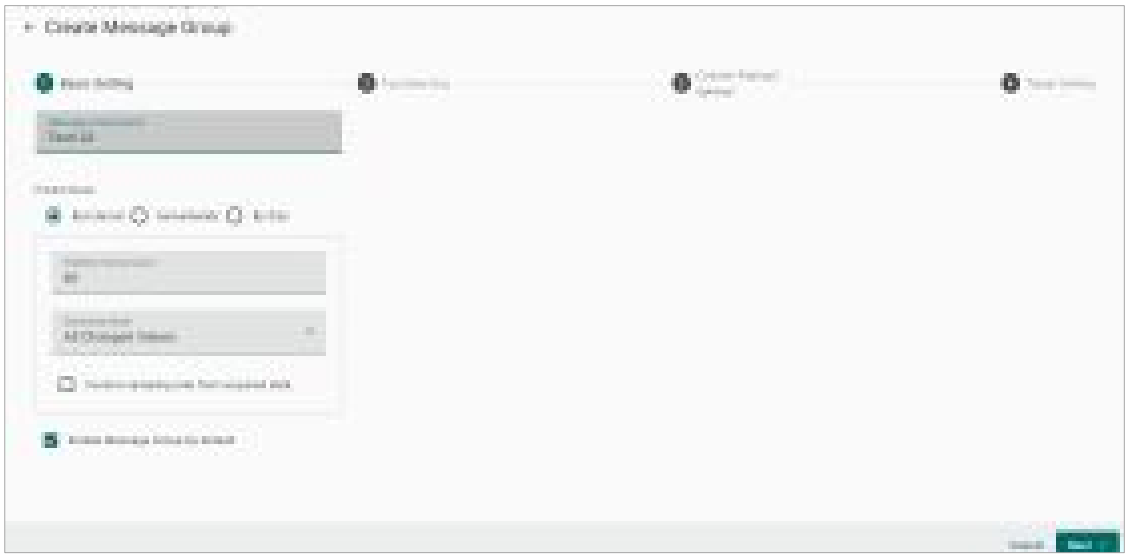
1. Click  to set connection.
2. Enter **Host** (Endpoint). **Port** (default: 8883) .
3. Enter **ThingID**.
4. Input **Keep Alive Time (sec)** .
5. Upload X.509 Certificate, Private key, and (optional) Trusted Root CA.
6. Click **SAVE**.

Message Group

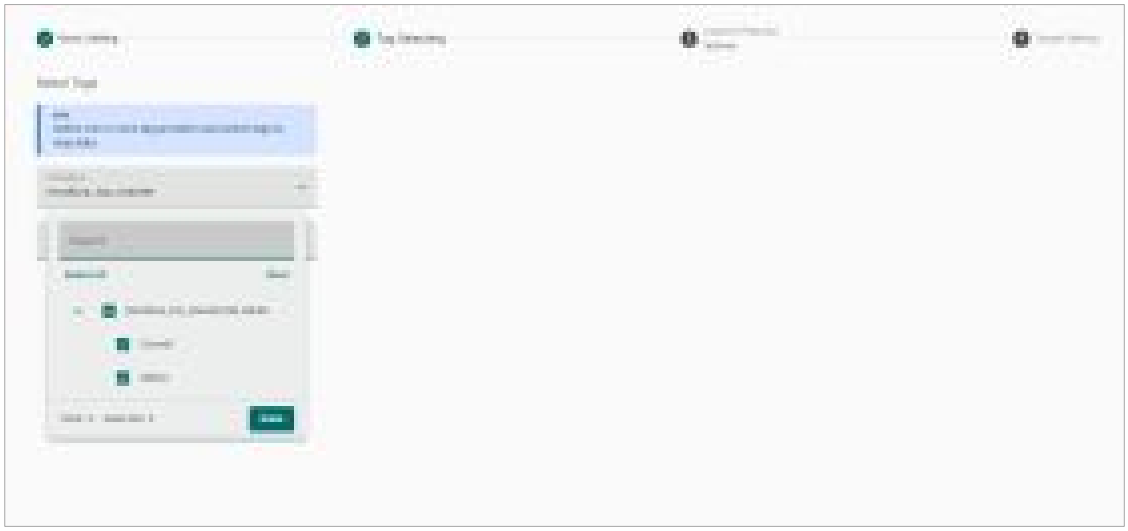
The simplest message type for sending IoT device data to your IIoT applications is a telemetry message. To create a telemetry message, do the following:

1. Click **+ Create** to create a new message group.

2. Specify a name for the **Message Group**.
3. Select a **Publish Mode**.
   For details, see Publish Mode.



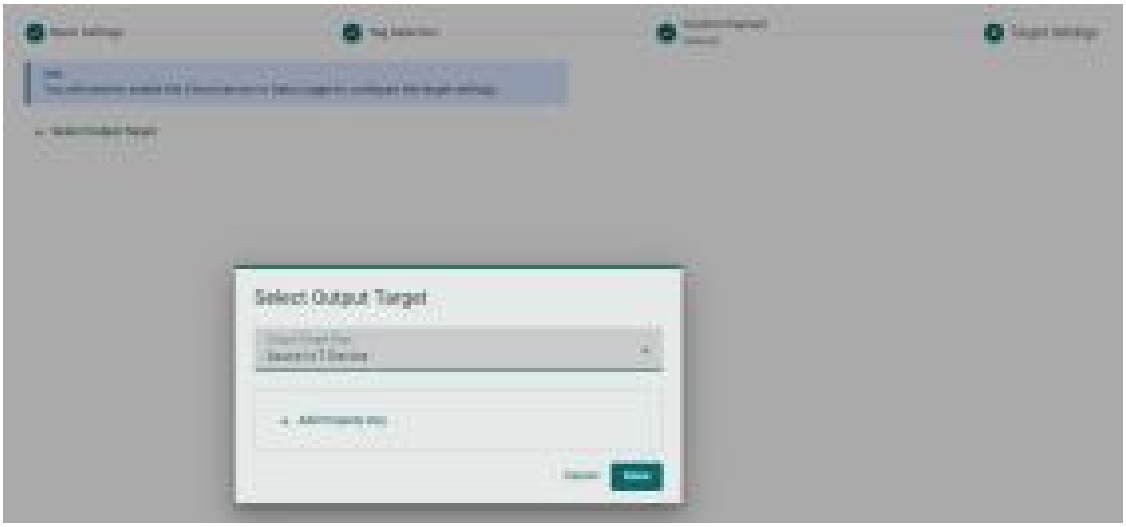
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **Next**.
6. Select tags (e.g., Modbus Master (Client)).



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. Select **Output Target Type**.

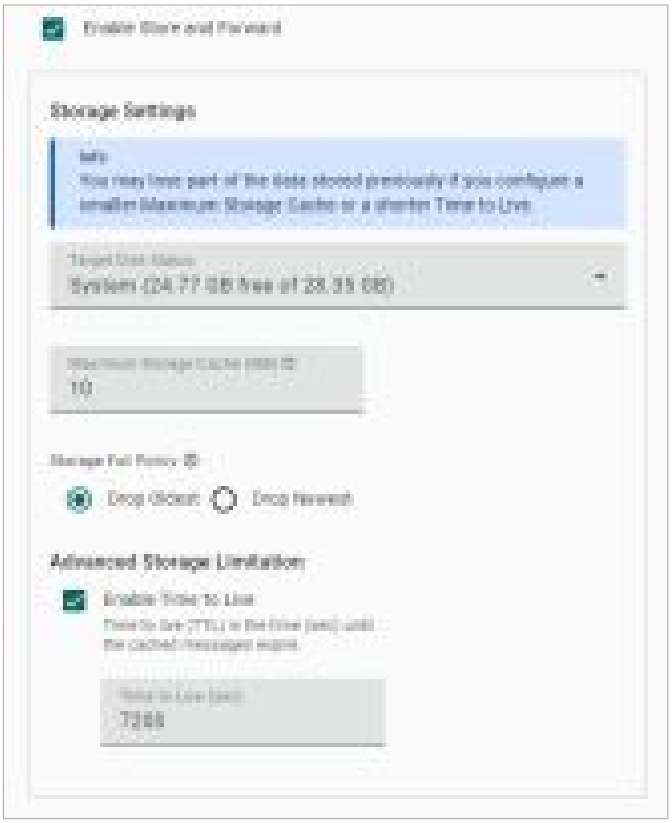


10. (Optional) Enter Property Key and Value.

11. Click **Done** and **Save**.

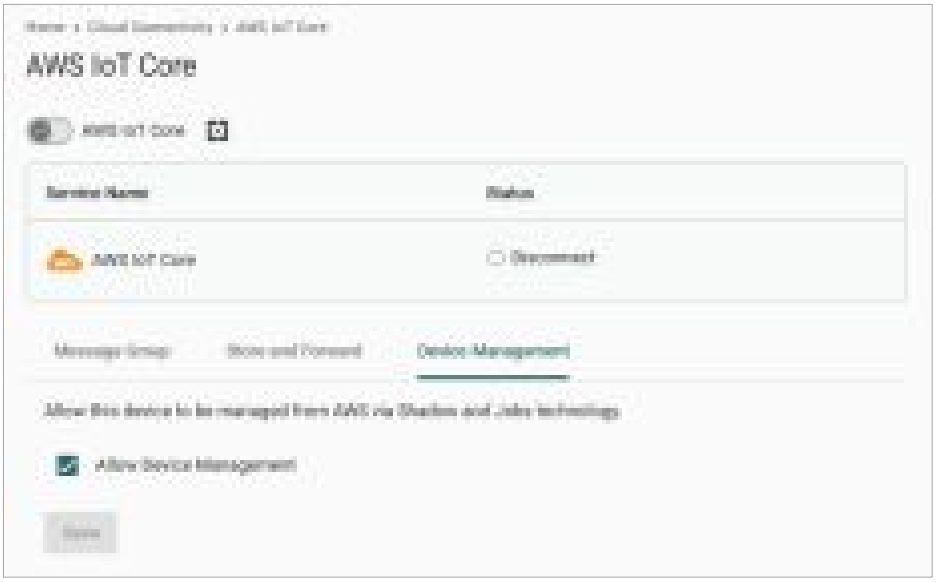
Store and Forward

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

Allows this AIG to be managed from AWS IoT Core via Shadow and Job.



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.

To enable Sparkplug B and communication, go to **Cloud Connectivity > Sparkplug**. The configuration process consists of the following:

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

Enabling Sparkplug

1. Click on the .
2. Specify an **Edge Node ID**, a **Group ID**.
3. (Optional) Specify a **Primary Host ID**.
4. Click **SAVE**.

Configuring a Broker

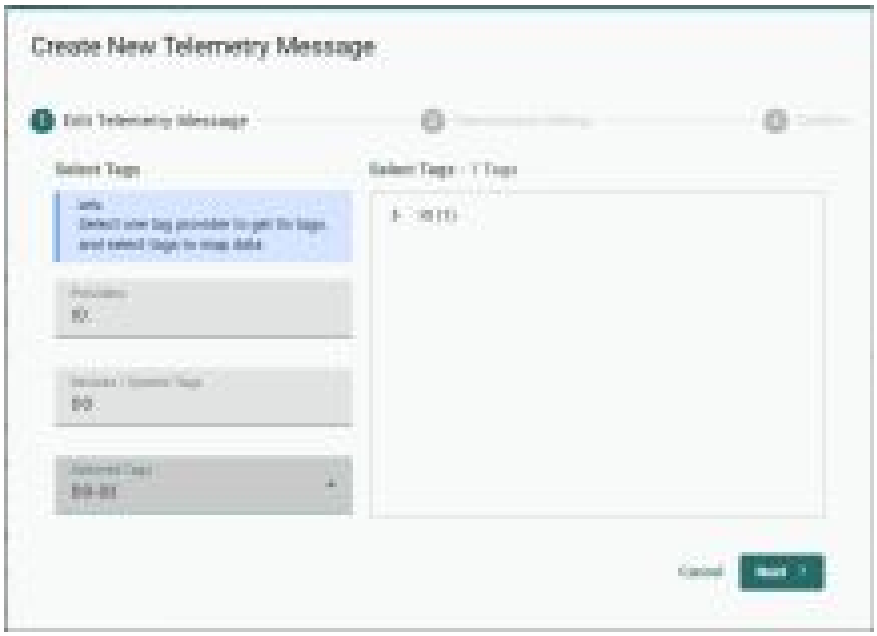
1. Click on the **+ Create**.
2. Specify a **Server** (default port: 8883).
3. (Optional) Enter **Client ID**, **Username**, and **Password**.
4. Specify an interval of **Keep Alive Time** (default 60 seconds).
5. (Optional) Enable **SSL/TLS** and upload **Client Certificate**, **Key**, and **Trusted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

NOTE

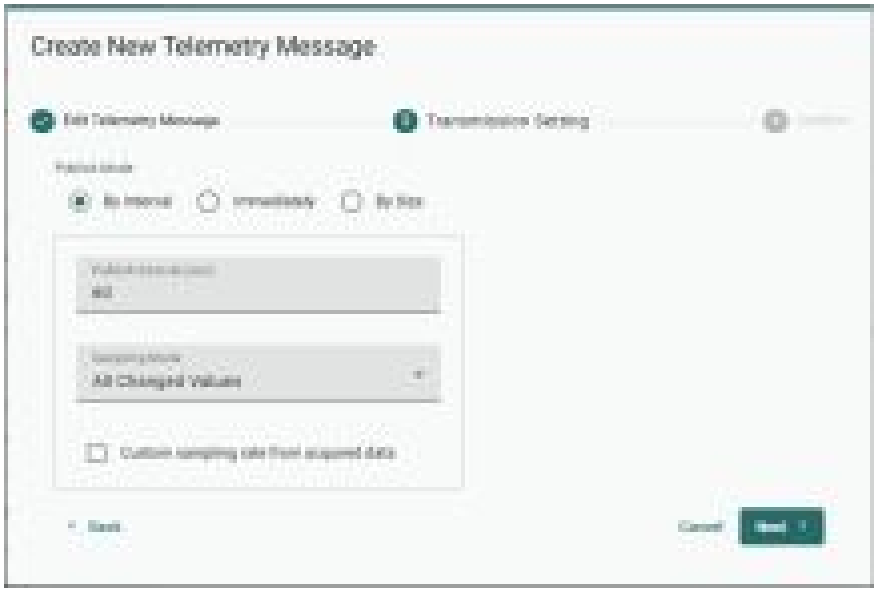
Data loss might occur during the period of connection interval prior to network connection check (Keep Alive Time). We suggest setting a shorter interval of Keep Alive Time (E.g., 10 seconds)

Configuring a Telemetry Message

1. Click on the **+ Message**.
2. Select tags from providers (e.g., IO).
3. Select devices or system tags.
4. Click **Next**.



5. Select a publish mode (For more details, see Appendix A. Publish Mode session.)
6. Select a sampling mode.
7. Click **Next**.

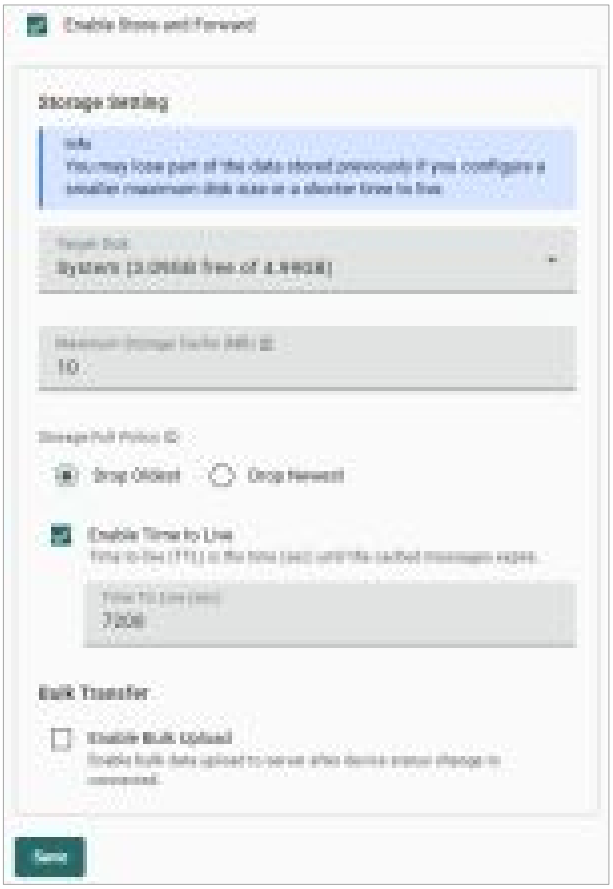


8. (Optional) Specify a description.

9. Click **Save**.

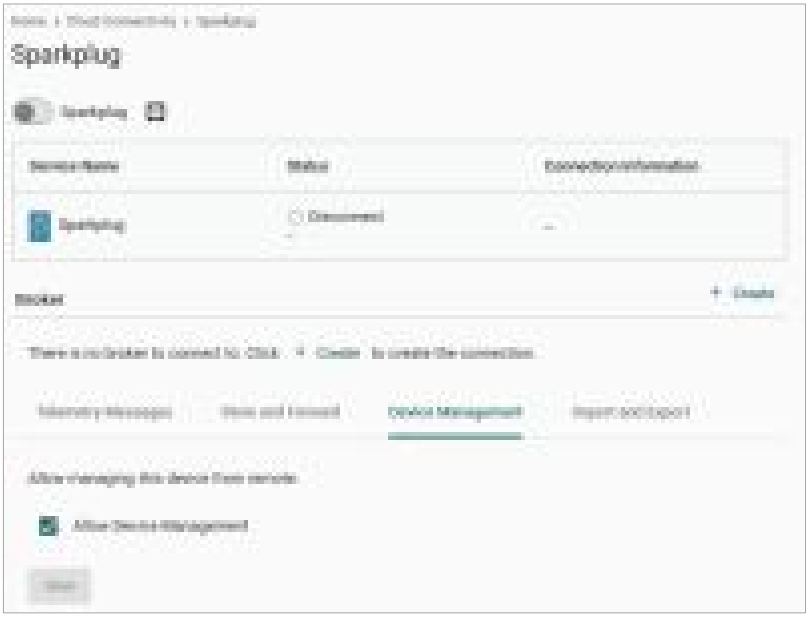
Store and Forward

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.



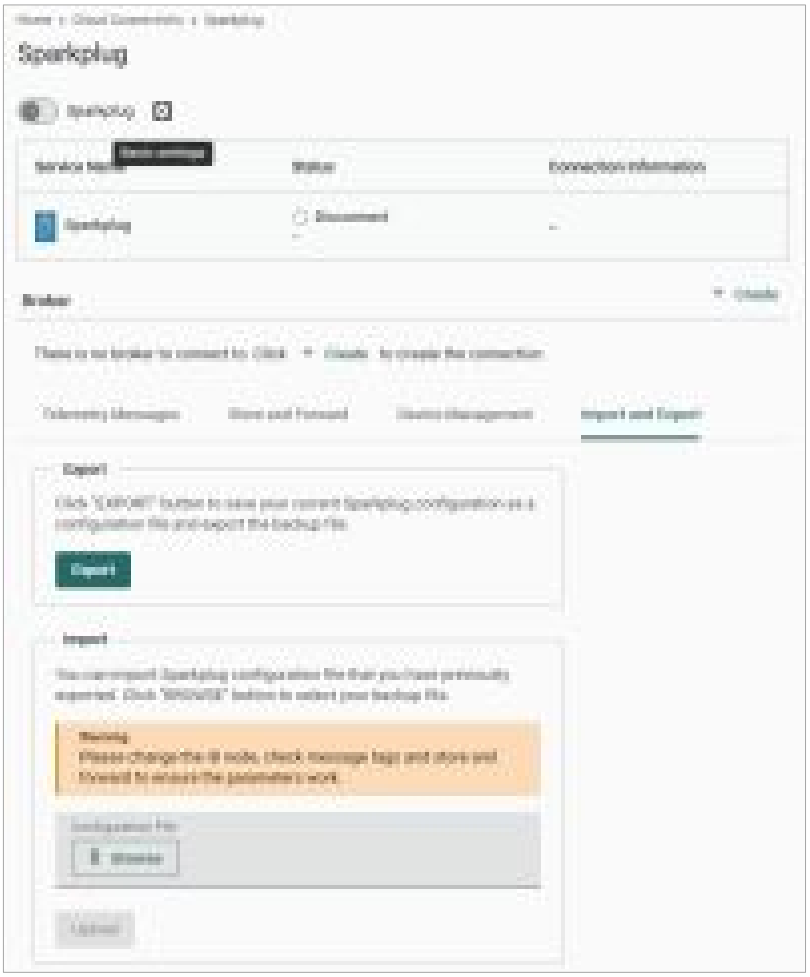
Device Management

Enabling this feature allows cloud service providers to manage IoT devices remotely.



Import and Export

To back up the configuration of Sparkplug, you can export the configuration as an external file.



NOTE

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

NOTE

if you want to use a direct method to write tags from the cloud, refer to https://tpe-tiger.github.io/AIG302/V1.0.0/#tag/taghub/paths/~1tags~1access~1{provider}~1{source}~1{tag}/put

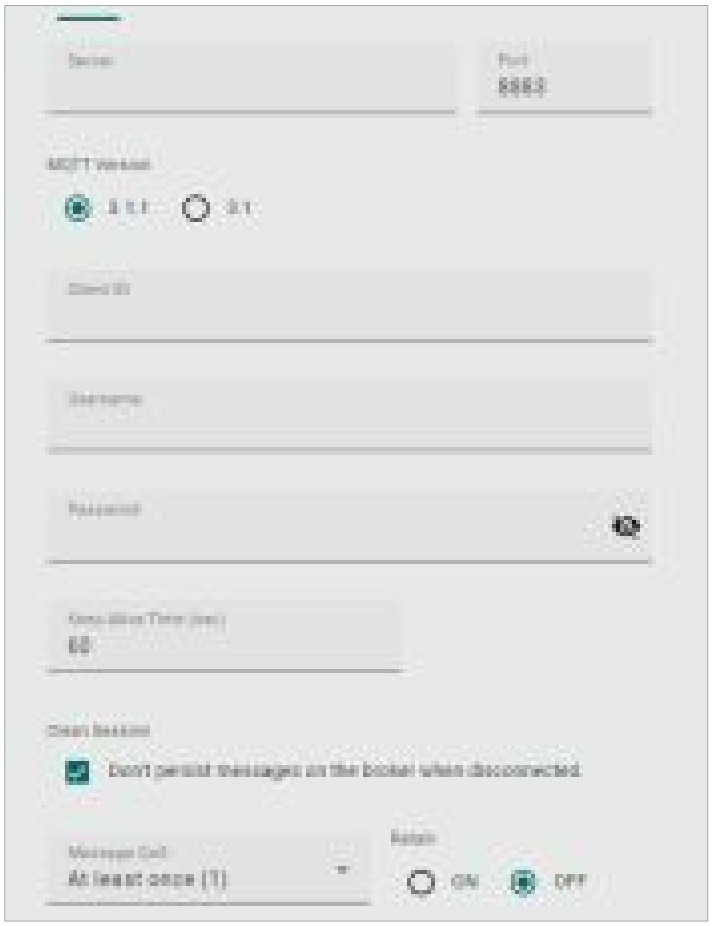
MQTT Client

Go to **Cloud Connectivity > MQTT Client**, and you can add many connections to 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, do the following:

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.
   Select a type of **QoS** and **retain function on/off**.

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

7. (optional) Enable Will flag.
8. (optional) Select type of QoS and retain function for Will flag.
9. Click **Save**.

Message Group

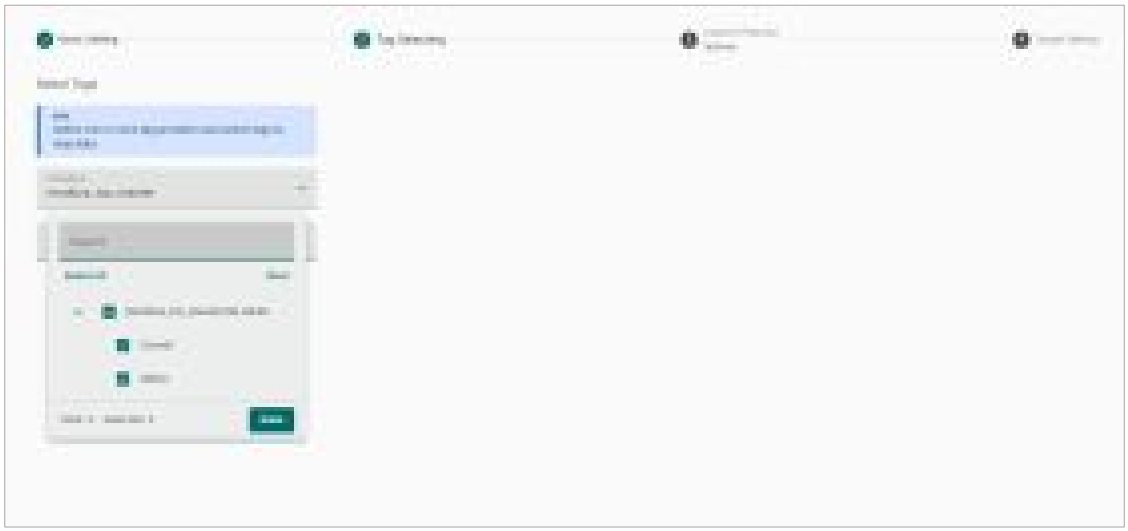
The simplest message type for sending IoT device data to your IIoT applications is a telemetry message. To create a telemetry message, do the following:

1. Click **+ Create** to create a new message group.

2. Specify a name for the **Message Group**.

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

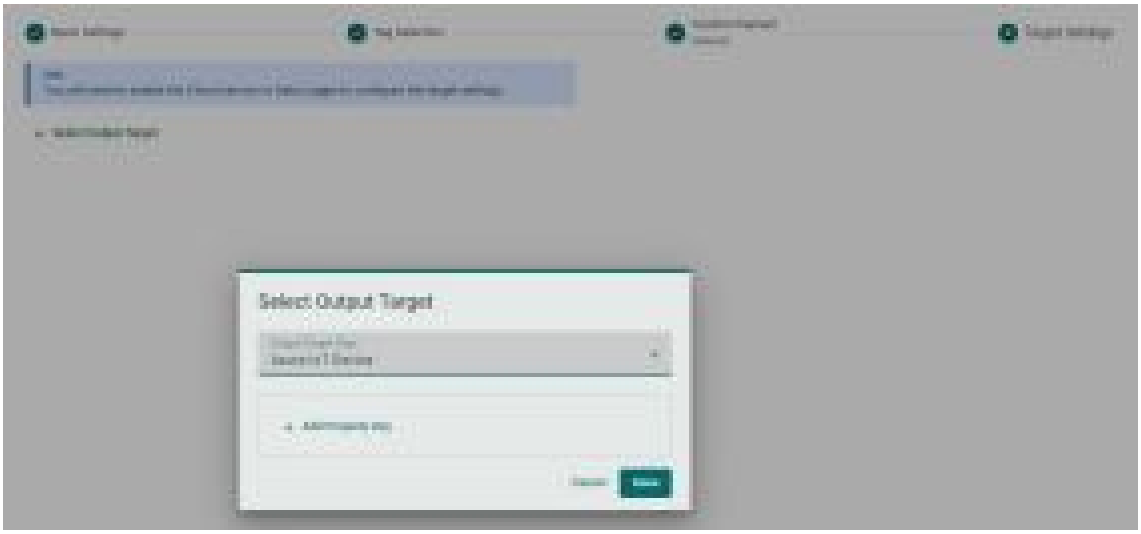
4. Input corresponding parameters such as publish interval, sampling mode, and publish.
5. Click **Next**.
6. Select tags (e.g., Modbus Master (Client)).



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

8. 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/).

9. Click **Next**.
10. Select **Output Target Type**.

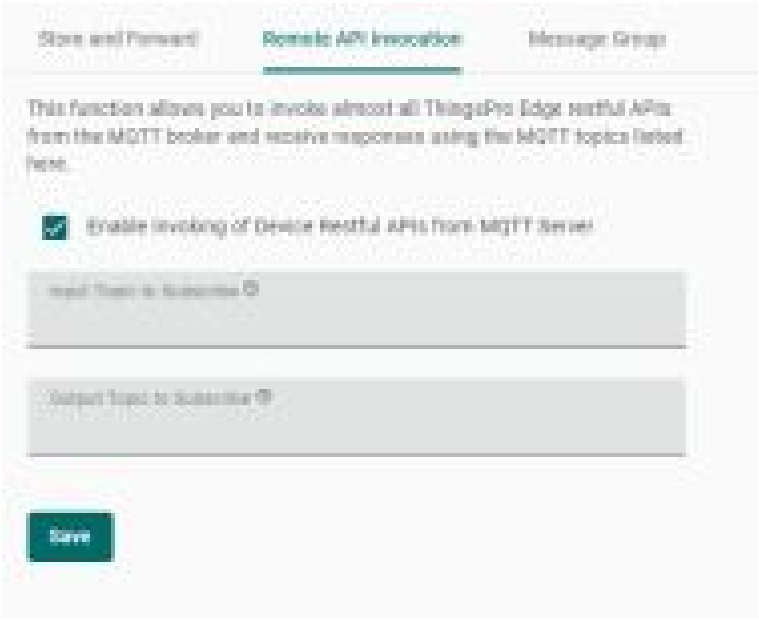


11. (Optional) Enter Property Key and Value.

12. Click **Done** and **Save**.

Remote API Invocation

This function allows you to invoke this device's RESTful APIs from the MQTT broker and receive responses using the MQTT topics listed here.

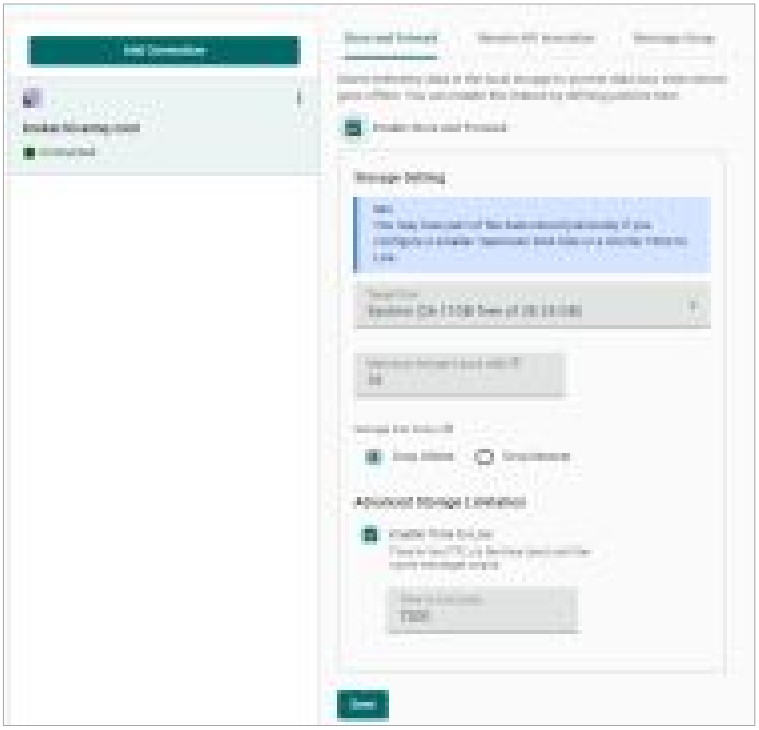


NOTE

if you want to use the direct method to write tags from the cloud, refer to https://tpe-tiger.github.io/AIG302/V1.0.0/#tag/taghub/paths/~1tags~1access~1{provider}~1{source}~1{tag}/put

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.



Data Logger

The data logger function saves data when communication is lost. It stores data on a chosen disk with a set maximum size. Whether data is logged internally or sent to a cloud application depends on the behavior of Message Group.

NOTE

When the logged data reaches the configured **Maximum Storage Cache** size, the oldest data will be deleted, allowing for the storage to have up-to-date data.

NOTE

LIMITATION: Hot swapping of external storage is not supported. When inserting external storage devices, it is advisable to power on/off the AIG to ensure proper functionality. Additionally, we do not endorse the use of USB hubs to simultaneously connect multiple USB devices.

Message Group

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:

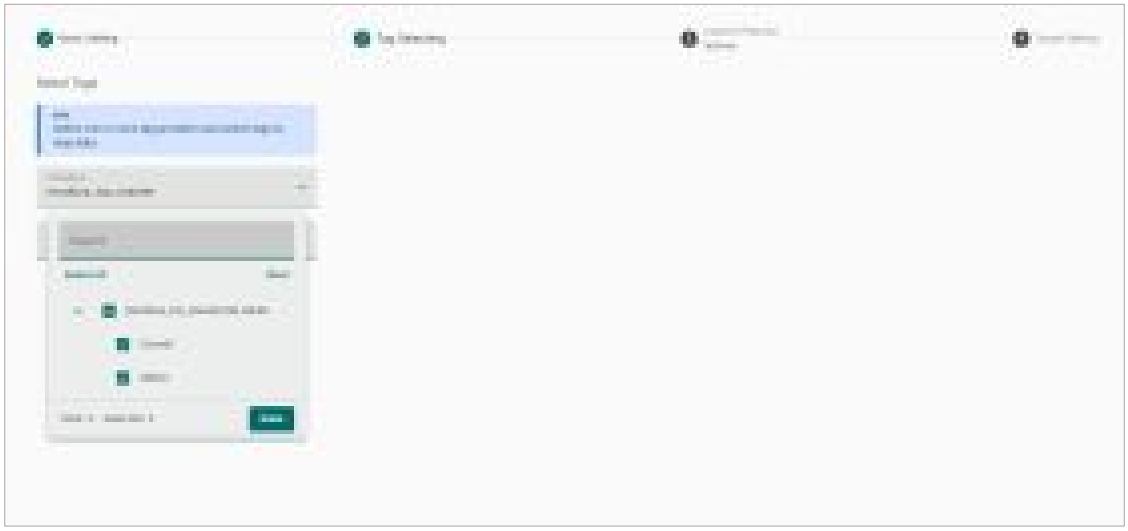
1. Click **+ Create** to create a new message group.

2. Specify a name for the **Message Group**.
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**.

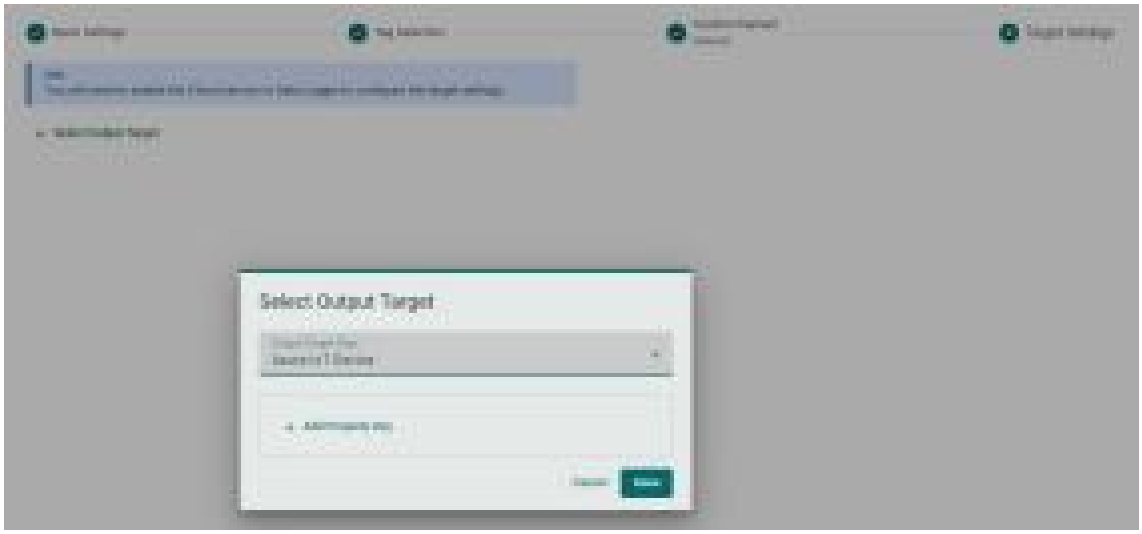
6. Select tags (e.g., Modbus Master (Client)).



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. Select **Output Target Type**.



10. (Optional) Enter Property Key and Value.

11. Click **Done** and **Save**.

Fieldbus Protocol

Modbus Master (Client)

Modbus TCP

Basic Settings

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

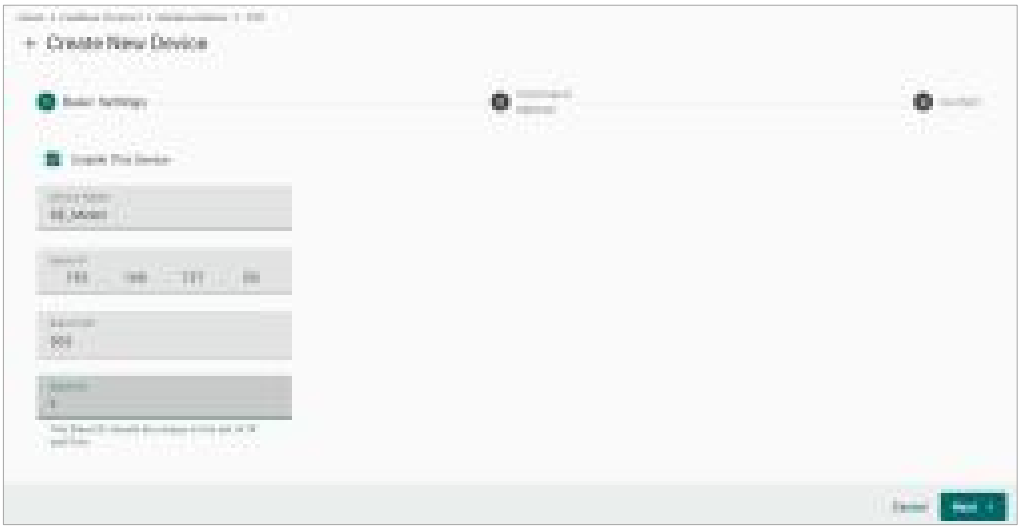
Parameter	Value	Default	Description
Initial Delay (ms)	0 to 30000	0	Some Modbus Slaves (Servers) may take more time to boot up than other devices. In some environments, this may cause the entire system to suffer from repeated exceptions during the initial bootup. After booting up, you can force the AIG to wait some time before sending the first request by setting a value for this parameter.
Maximum Retry	0 to 5	3	This is used to configure how many times AIG will retry to communicate with the Modbus Slaves (Servers) when the Modbus command times out.
Response Timeout (ms)	10 to 120000	1000	You can configure a Modbus Master (Client) to wait a certain amount of time for a Modbus Slave (Server)'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
Slave IP	0.0.0.0 to 255.255.255.255	–	The IP address of a remote Modbus Slave (Server) device.
Slave Port	1 to 65535	502	The TCP port number of a remote Modbus Slave (Server) device.
Slave ID	1 to 255	–	The ID of a remote Modbus Slave (Server) 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.

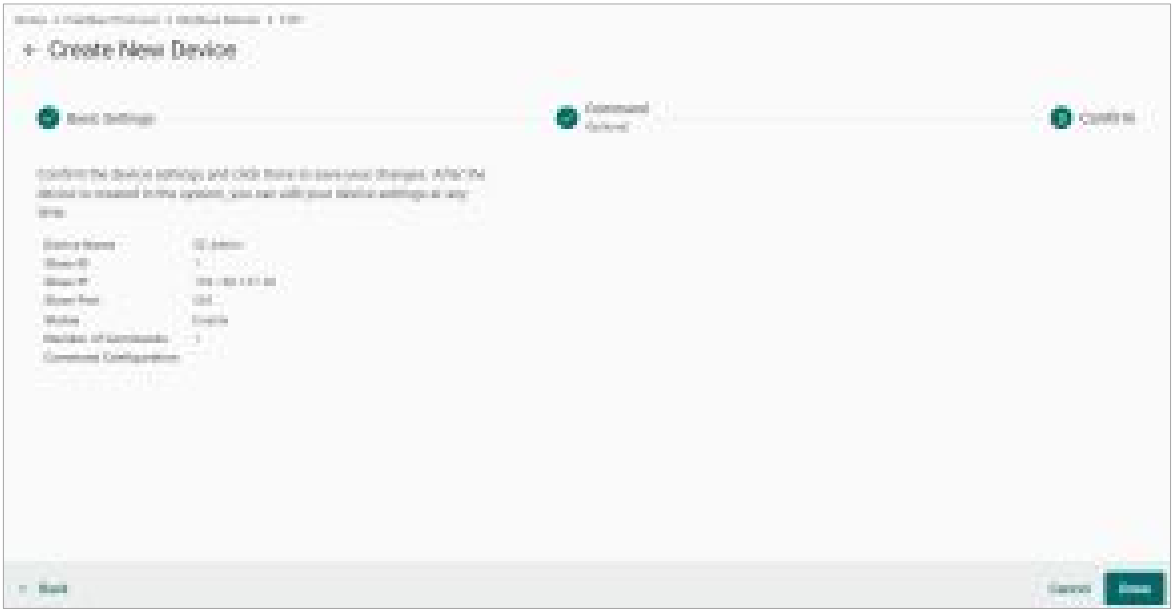
Parameter	Value	Default	Description
Command Name	Alphanumeric string	–	Name the command
Function	01 – Read Coils 02 – Read Discrete Inputs 03 – Read Holding Registers 04 – Read Inputs Registers 05 – Write Single Coil 06 – Write Single Register 15 – Write Multiple Coils 16 – Write Multiple Registers 23 – 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

Parameter	Value	Default	Description
Write quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1to 123	1	Specifying how much data to write.
Trigger	Cyclic Data Change	–	Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Poll interval (ms)	100 to 1200000	1000	Polling intervals are in milliseconds. Since the module sends all requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.
Endian swap	None Byte Word Byte and Word	None	**None:** not to swap **Byte:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C **Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. **Byte and Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Status Term	Pause Proceed - Clear data to zero Proceed - Set to User-defined value	Pause	The defined value of the Status Term will be effective when a read command encounters an error or times out.
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**. Importing a configuration file will help you reduce configuration time.

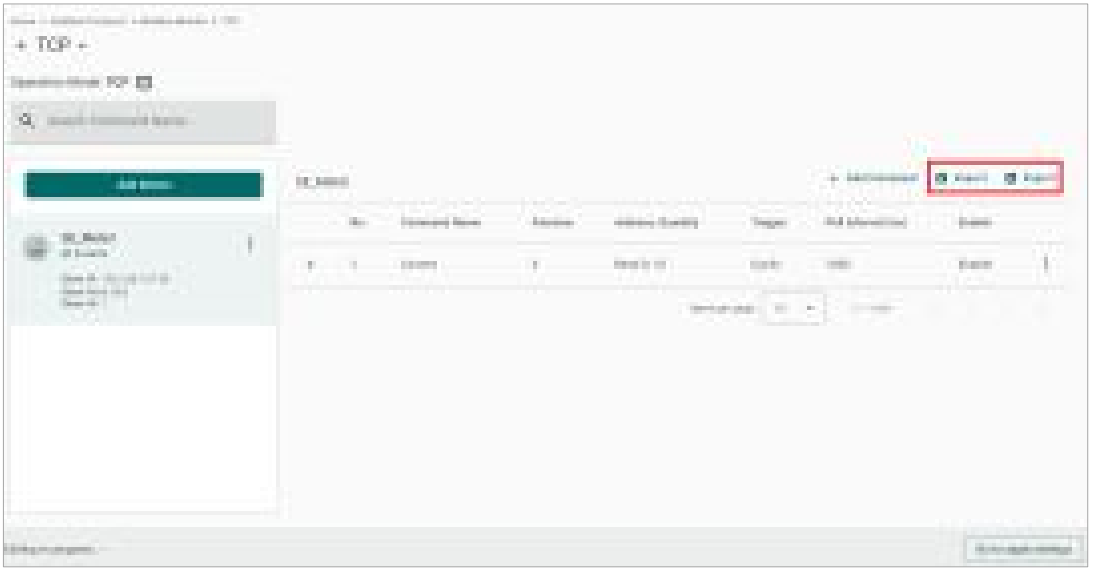
Step 3. Confirm

Review whether the information of the settings is correct.

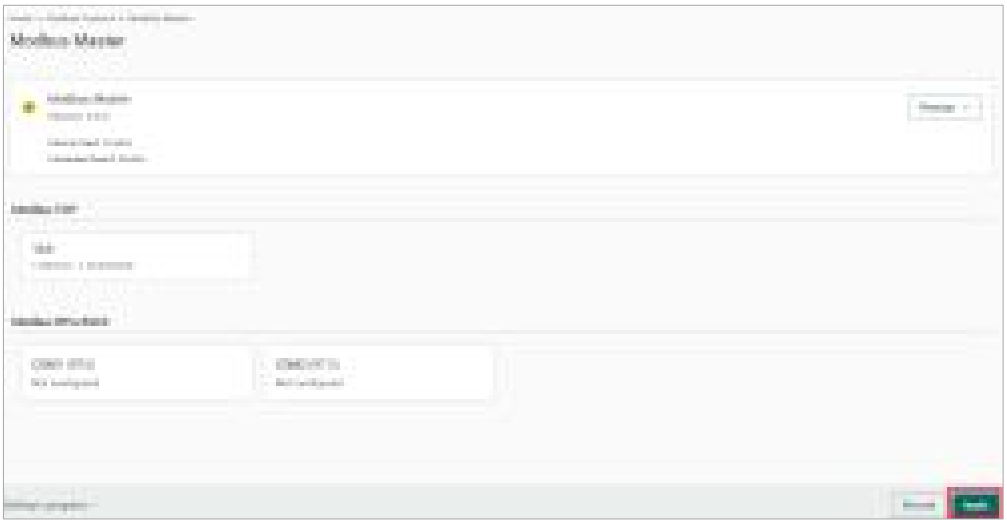


Then, you will see the setting results.

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



After finishing all the settings, press **Go to apply settings** and click **Apply** for the settings take effect.



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

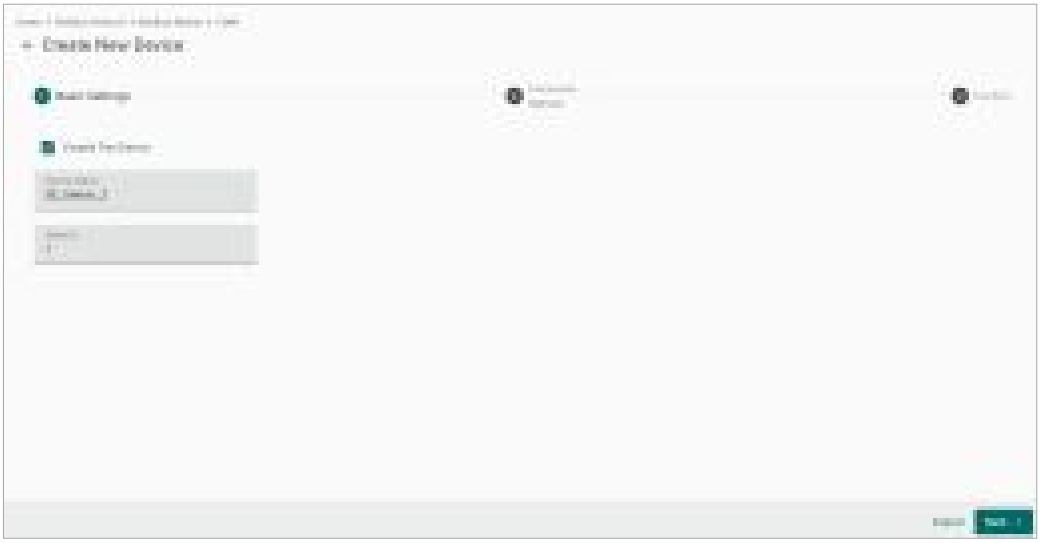
Parameter	Value	Default	Description
Automatically determine the inter-frame delay (ms)	Check uncheck: 10 to 500	check	Inter-frame delay is the time between the response and the next request. This is to ensure a legacy Modbus Slave (Server) device can handle packets in a short time. **Check:** The AIG will automatically determine the time interval. **Uncheck:** You can input a time interval.
Automatically determines the intercharacter timeout (ms)	Check uncheck: 10 to 500	check	Use this function to determine the timeout interval between characters for receiving Modbus responses. If AIG can't receive Rx signals within an expected time interval, all received data will be discarded. **Check:** The AIG will automatically determine the time out. **Uncheck:** You can input a specific timeout value.

Modbus Device Settings

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

Step 1. Basic Settings

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

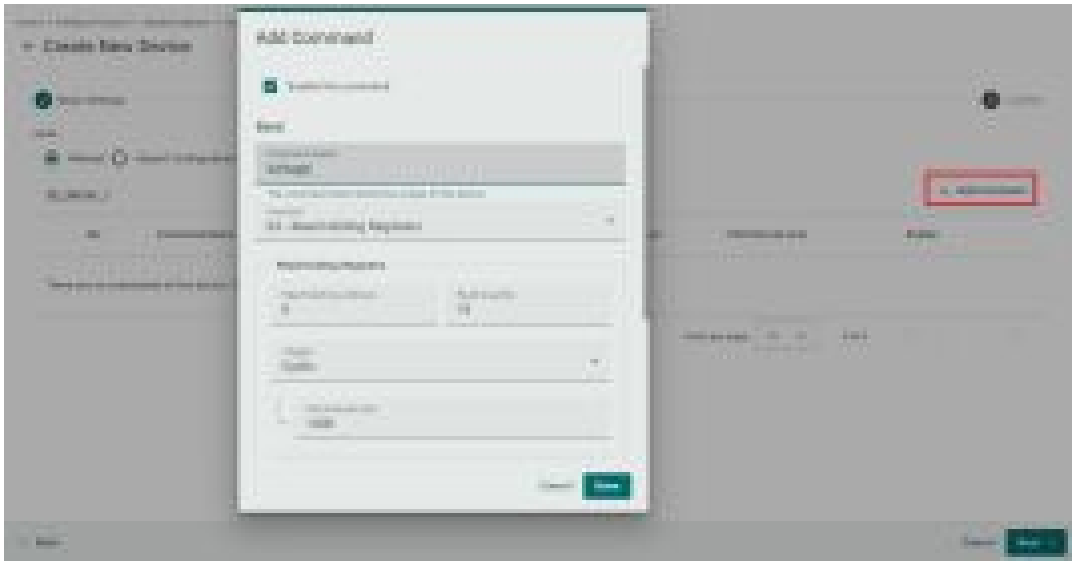


Parameter	Value	Default	Description
Device Name	Alphanumeric string and characters (~ . _ -) are allowed	–	Name your Modbus device
Slave ID	1 to 255	–	The ID of a remote Modbus Slave (Server) device.

Step 2. Command

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

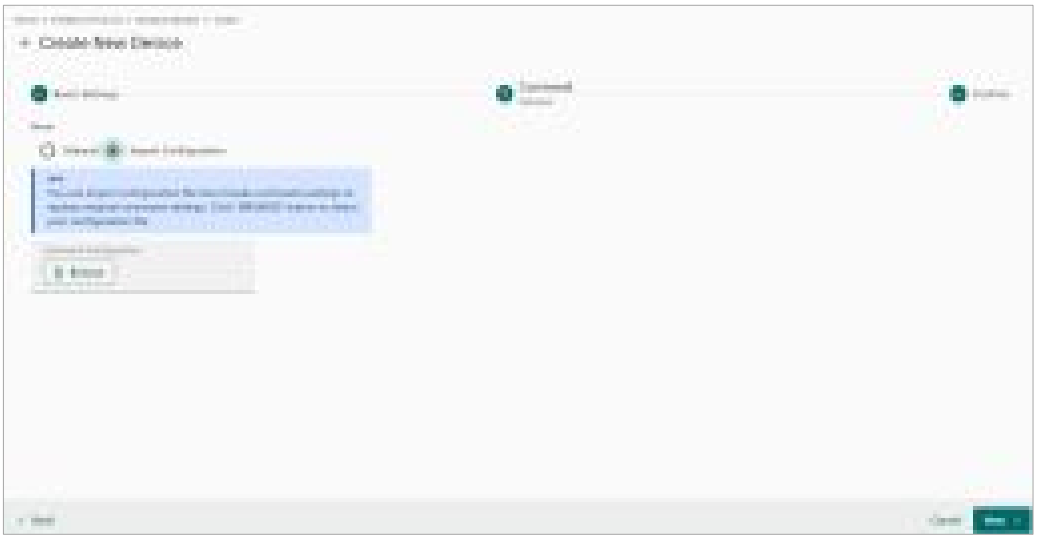
The command settings will pop up.



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

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



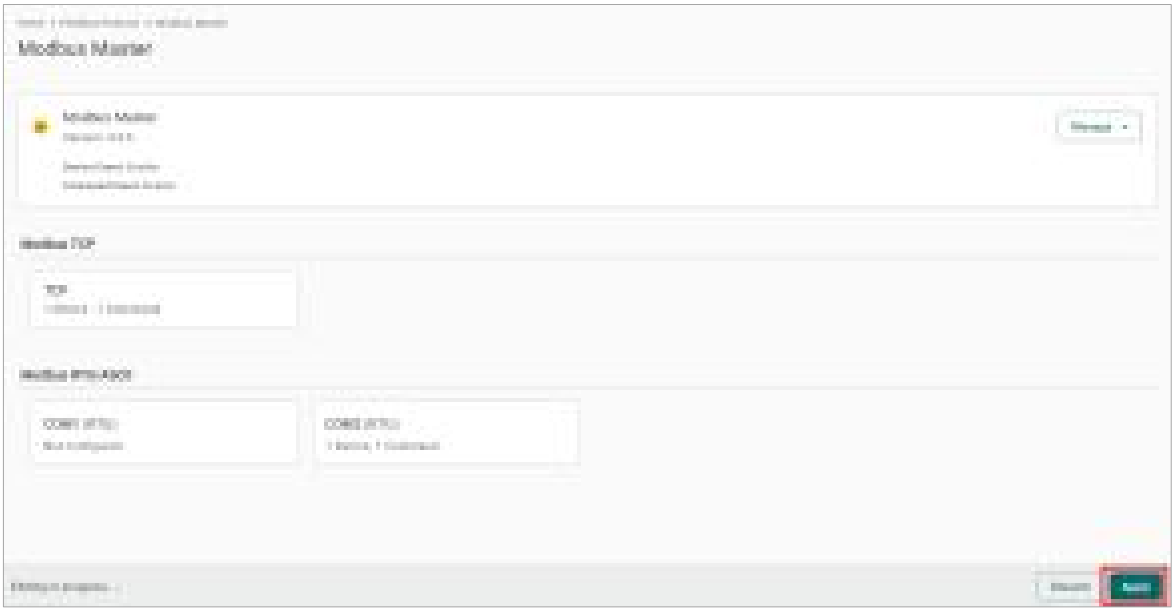
Step 3. Confirm

Review whether the information of the settings is correct.

Then, you will see the setting results.

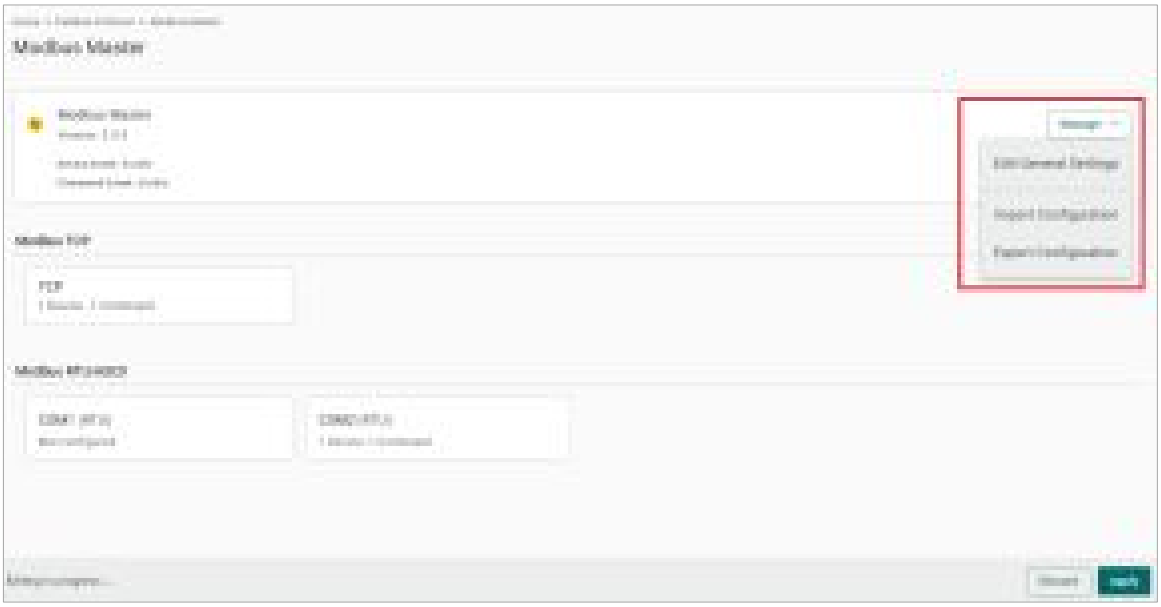
Moreover, the product provides an easier way for installation and maintenance. You can **Export** all the Modbus commands into a file for backup purposes; or you can **Import** a file (golden sample) to reduce configuration time.

After finishing all the settings, press **Go to apply settings** and click **Apply** for the settings to take effect.



Manage

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



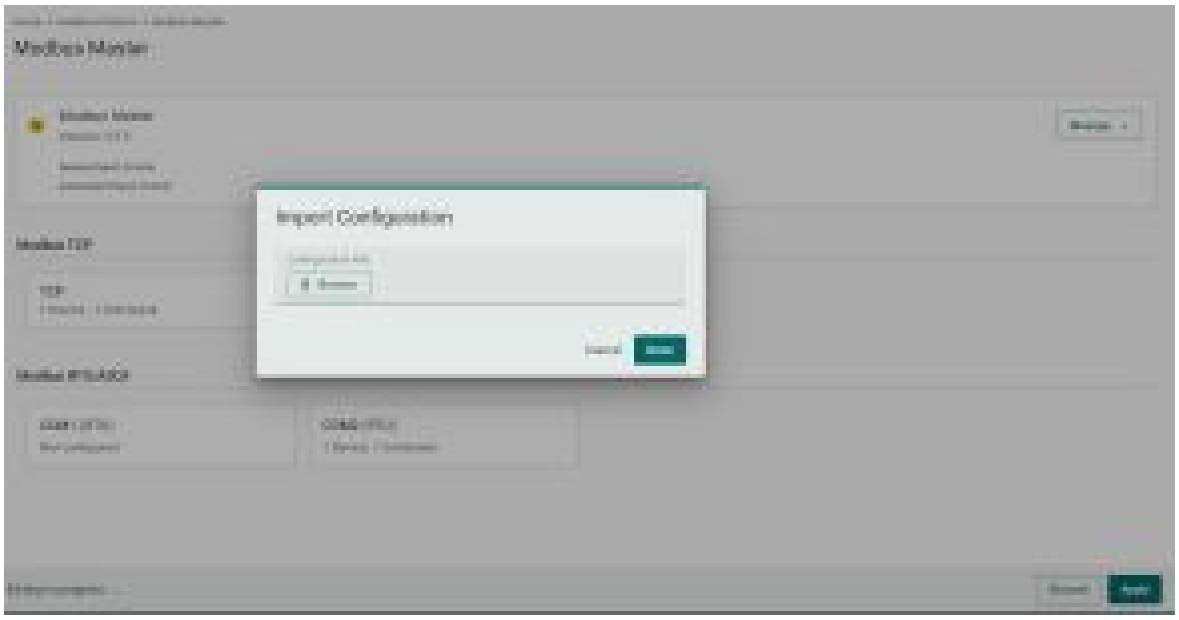
Edit General Settings

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

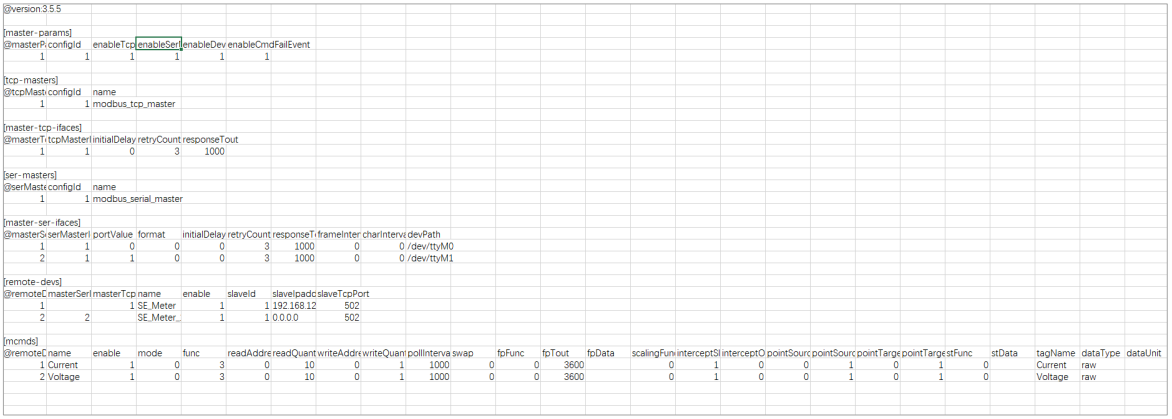
Parameter	Value	Default	Description
Enable device event	Check uncheck	Check	**Check:** If the Modbus communication fails, e.g., Modbus exception code is received The Modbus response timeout and the value of the status tag in the tag hub will change to 1. **Uncheck:** Disable the function
Enable command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



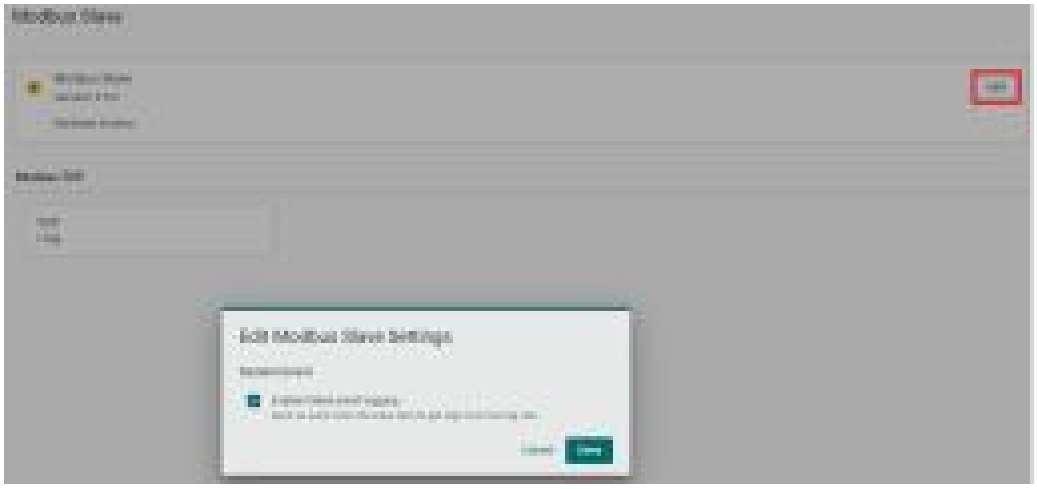
An example of an exported file that can be viewed/edited by EXCEL.



@version:3.5.5																														
[master-params]																														
@masterPa	configId	enableTcp	enableSer	enableDev	enableCmdFailEvent																									
	1	1	1	1	1	1																								
[tcp-masters]																														
@tcpMaste	configId	name																												
	1	1	modbus_tcp_master																											
[master-tcp-ifaces]																														
@masterTc	tcpMasterI	initialDelay	retryCount	responseTout																										
	1	1	0	3	1000																									
[ser-masters]																														
@serMaste	configId	name																												
	1	1	modbus_serial_master																											
[master-ser-ifaces]																														
@masterSe	serMasterI	portValue	format	initialDelay	retryCount	responseTi	frameInter	charInterv	devPath																					
	1	1	0	0	0	3	1000	0	0	/dev/ttyM0																				
	2	1	1	0	0	3	1000	0	0	/dev/ttyM1																				
[remote-devs]																														
@remoteD	masterSerI	masterTcp	name	enable	slaveId	slaveIpadd	slaveTcpPort																							
	1		1 SE_Meter	1	1	192.168.12	502																							
	2	2	SE_Meter_	1	1	0.0.0.0	502																							
[mcmds]																														
@remoteD	name	enable	mode	func	readAddre	readQuant	writeAddre	writeQuan	pollInterva	swap	fpFunc	fpTout	fpData	scalingFun	interceptSl	interceptO	pointSourc	pointSourc	pointTarge	pointTarge	stFunc	stData	tagName	dataType	dataUnit					
	1 Current	1	0	3	0	10	0	1	1000	0	0	3600		0	1	0	0	1	0	1	0		Current	raw						
	2 Voltage	1	0	3	0	10	0	1	1000	0	0	3600		0	1	0	0	1	0	1	0		Voltage	raw						

Modbus Slave (Server)

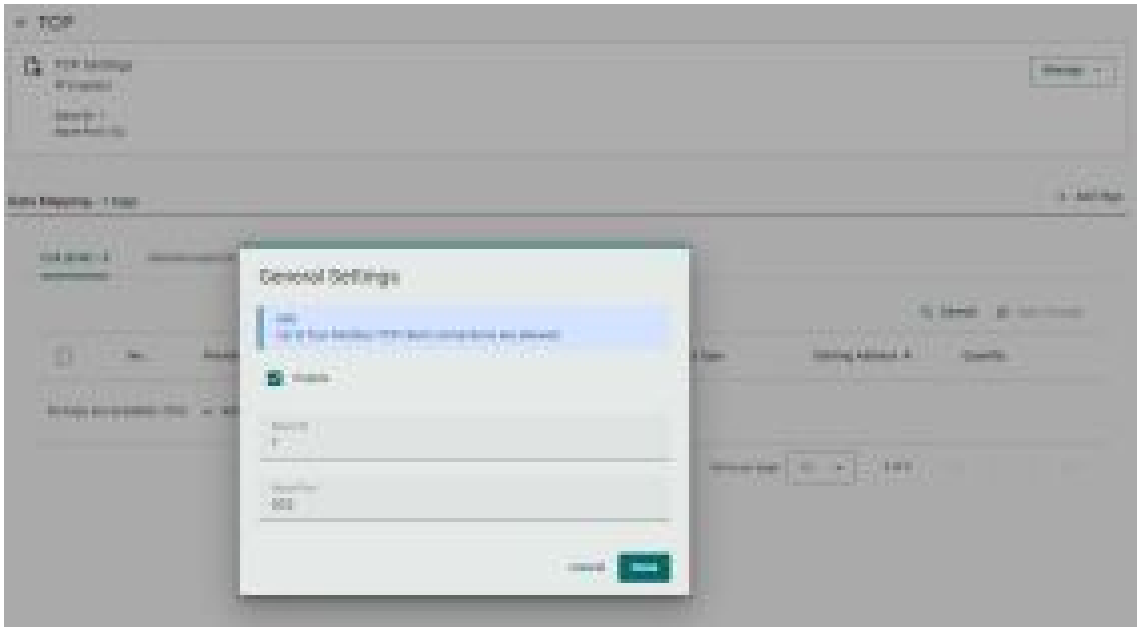
Click **Edit** for Modbus Slave (Server) advanced settings. If you want to create an event under the event log for when the Modbus TCP connection might get disconnected, you can enable the fail event function.



To create a Modbus TCP Slave (Server), do the following:

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

2. Click **Manage > General Settings.**



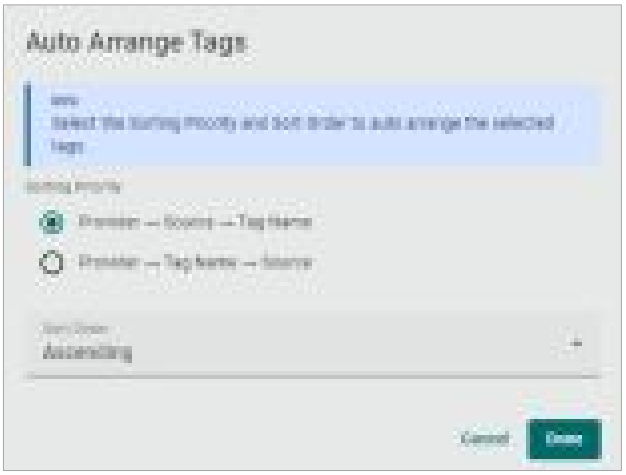
3. Check **Enable this slave**, input **Slave ID** and **Slave Port**, then click **Done.**
4. Click **+Add Tags** to select tags (e.g., Modbus Master (Client)).

5. Click **Done** to finish settings.

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

	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.



Edge Computing

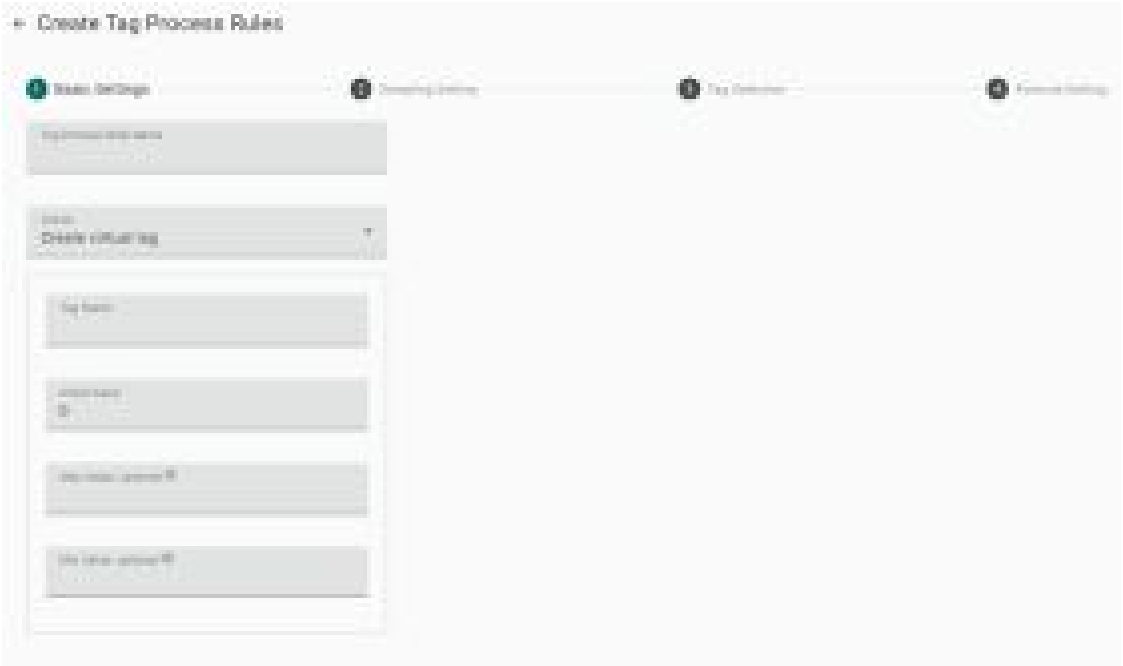
Logic Engine

The device has a built-in intuitive no-code solution that can help write rules for processing data and calculate values or create simple logic control to fulfill specific scenarios, which can then be used to trigger some actions. This feature helps eliminate the programming effort in data processing.

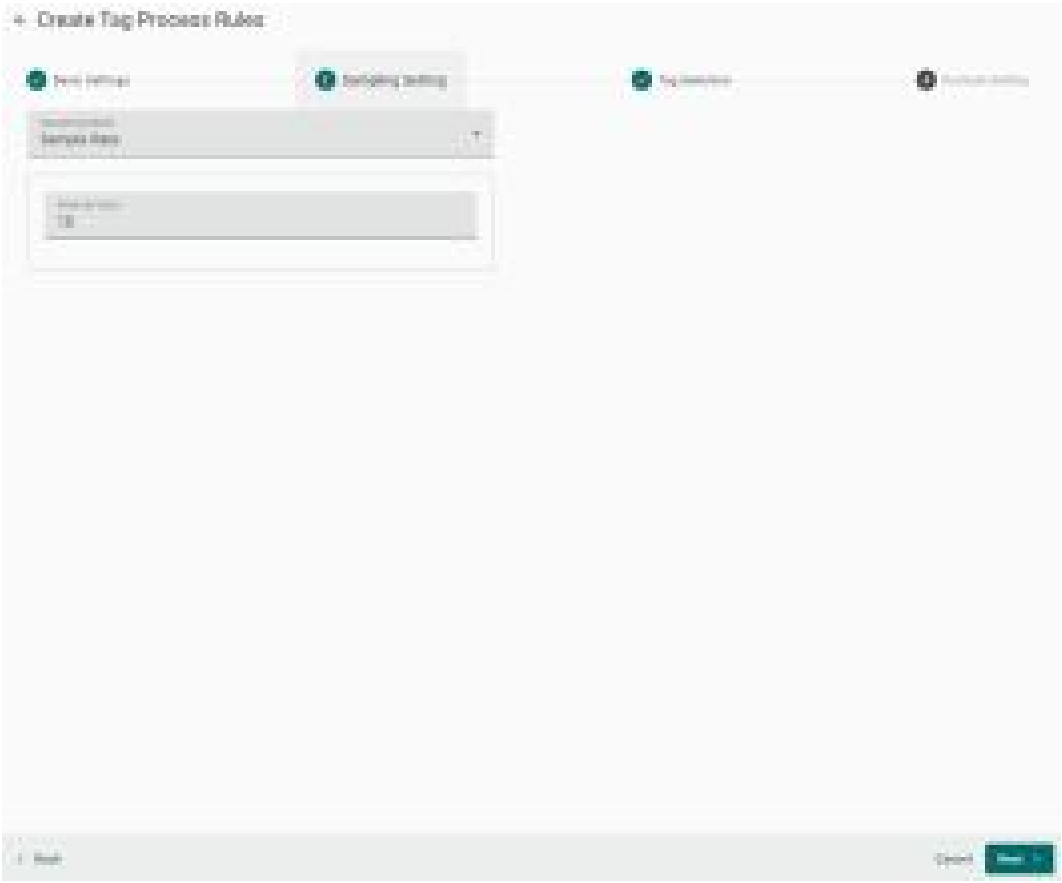
To process data and calculate data values, do the following:

1. Click **+ Create**.

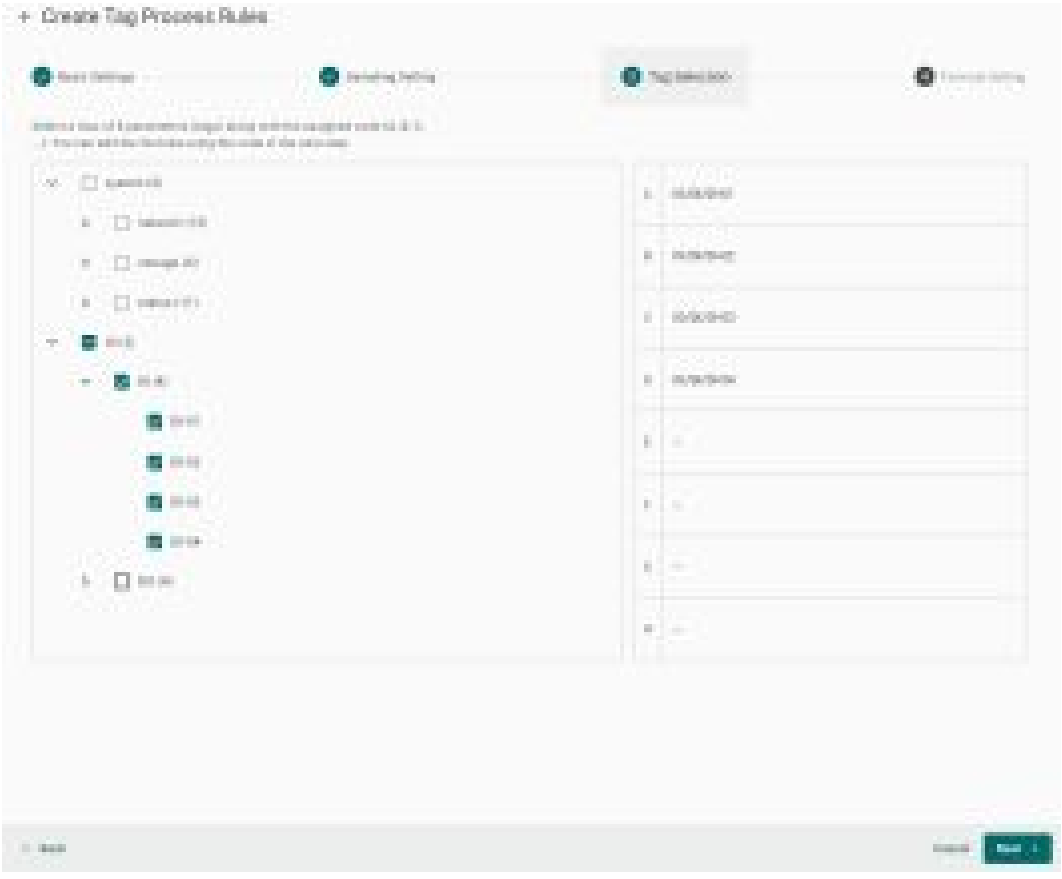
2. Specify **Rule Name**, select **Create virtual tag** under **Action** and configure **Tag Name** and following parameters, then click **Next**.



3. Select a sampling setting and click **Next**.



4. Select the tags from system or Modbus that you want to process and click **Next**.



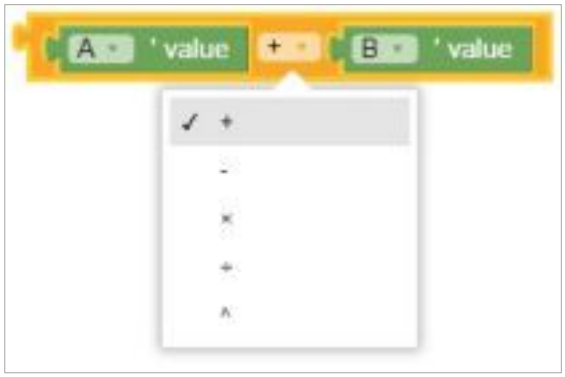
5. Drag and drop the formula and tags from **Math** and **Tag** and click **Save**.

6. After the rule is created successfully, you can find the virtual tag on the **Tag Dashboard**.

> **NOTE**
>
> The **Status** column indicates if the rule contains any errors or not.

The following Math formulas are supported:

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



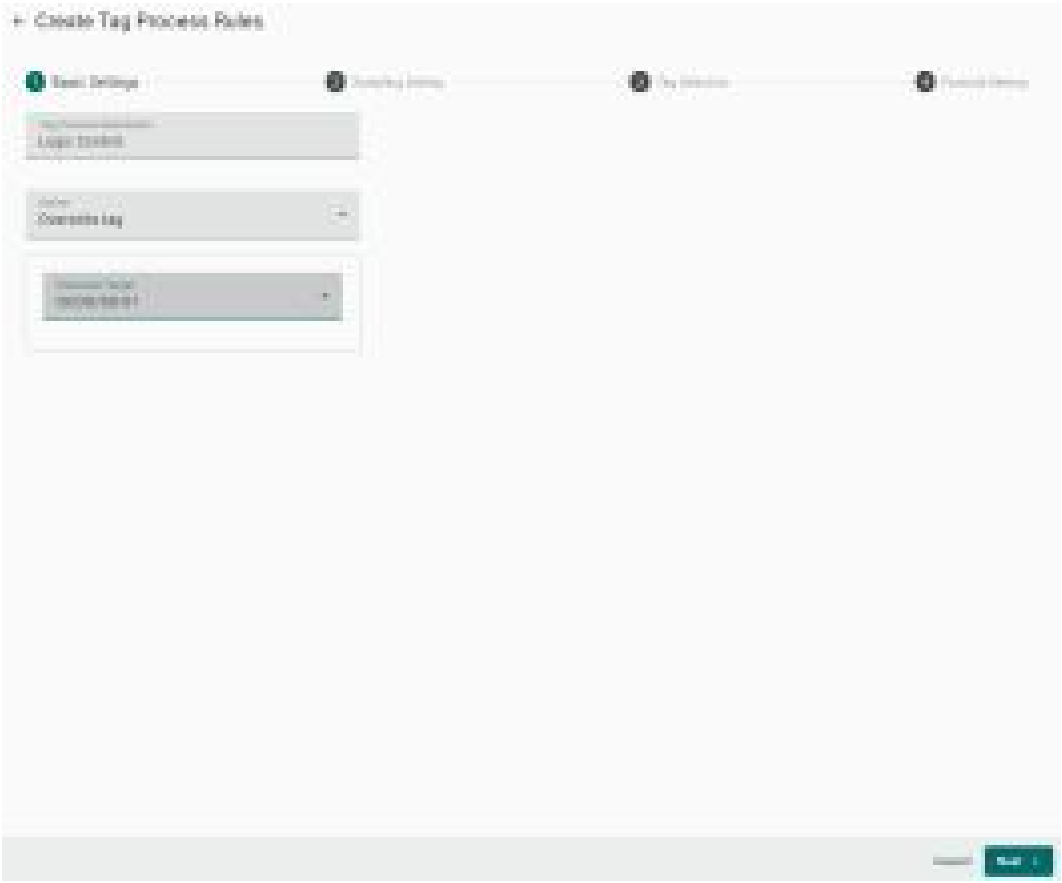
- **round, round up, round down**

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

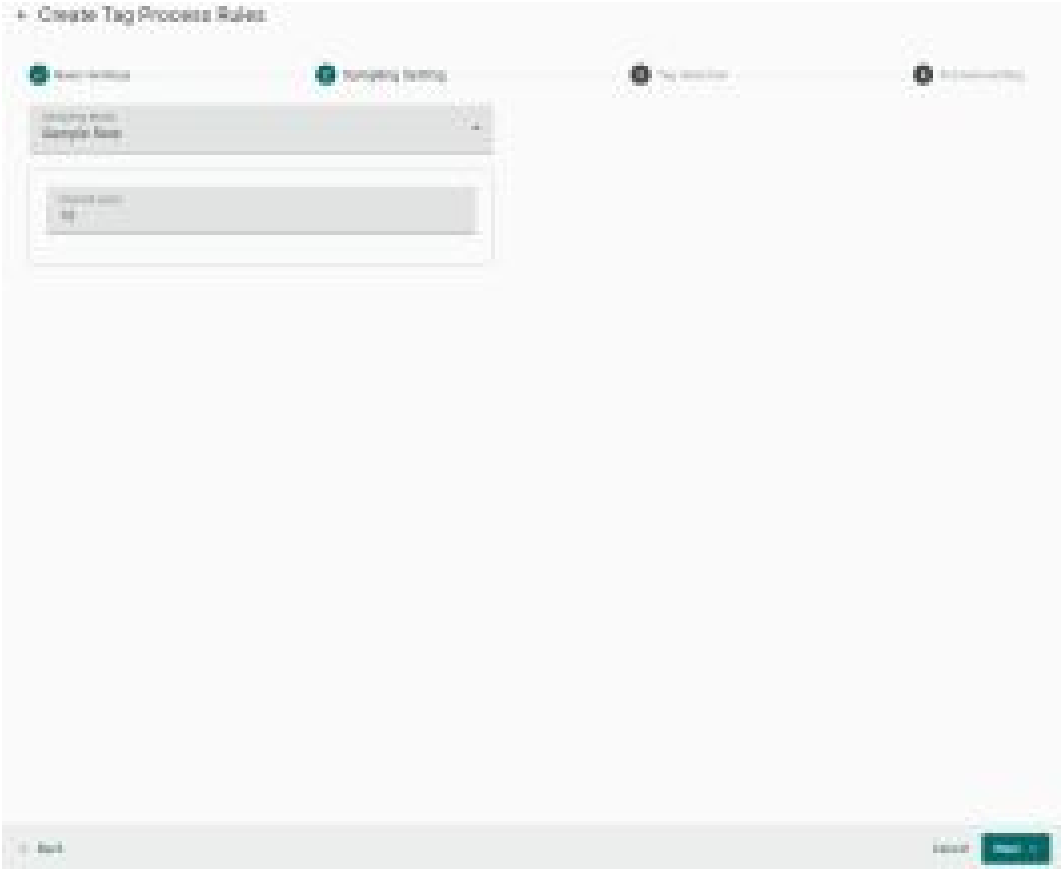
To create a logic control rule, do the following:

1. Click **+ Create**.

2. Input the **Rule Name**, configure **Overwrite Tag** under **Action,** and select the **Overwrite Target**, then click **Next**.

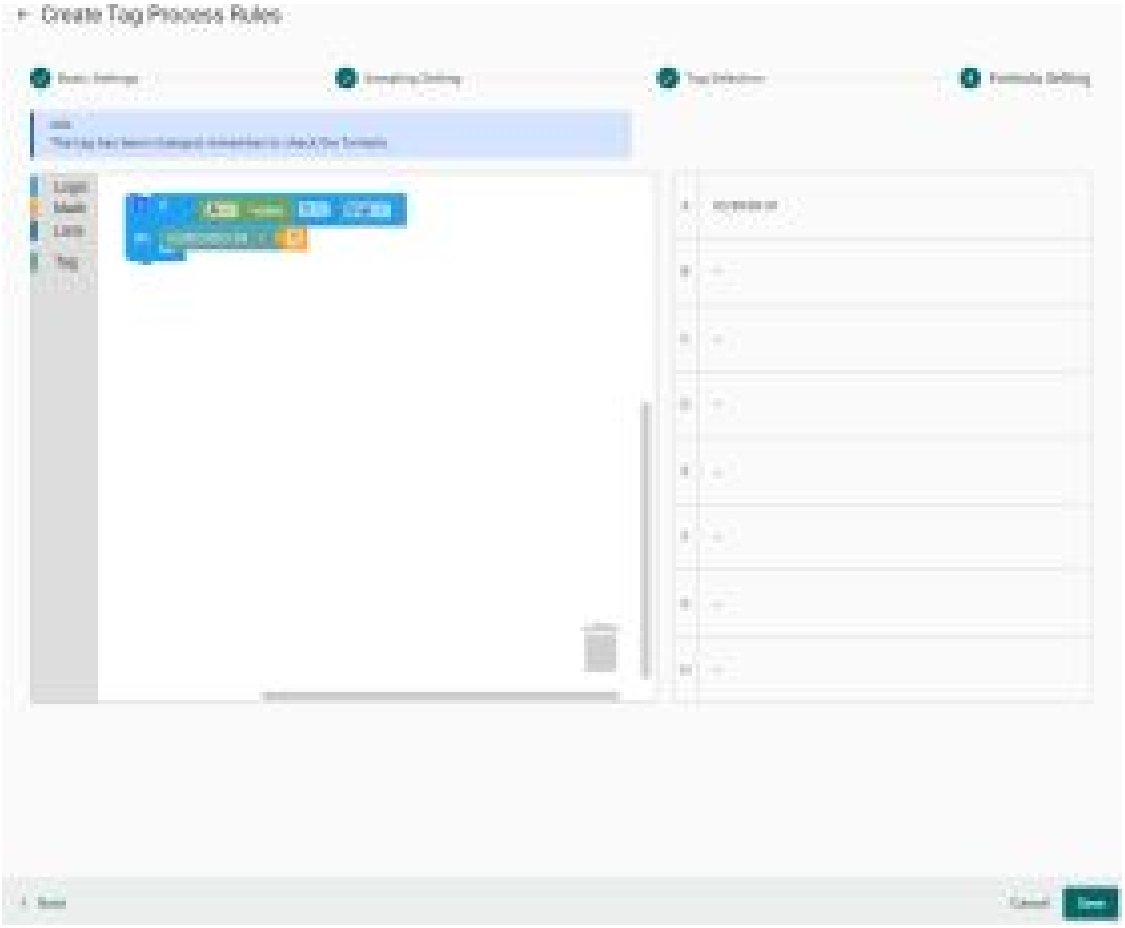


3. Configure the **Sampling Mode** and click **Next**.



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

5. Drag and drop the formula and tags from **Logic, Math,** and **Tag**, then click **Save**.



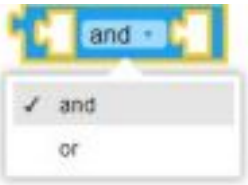
6. You will see the rule has been created successfully.

The following logic sets are supported:

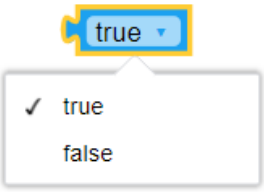
- **If, else if, else**

- **Equal (=), not equal to (≠), greater than (>), greater than or equal to (≥), less than (<), less than or equal to (≤)**

- **And, Or**



- **True, False**

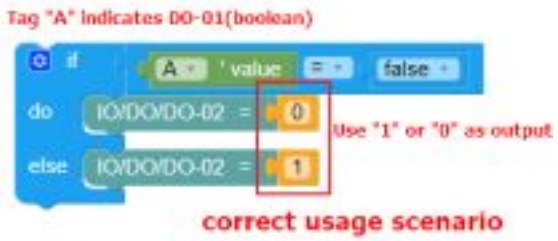


LIMITATIONS:

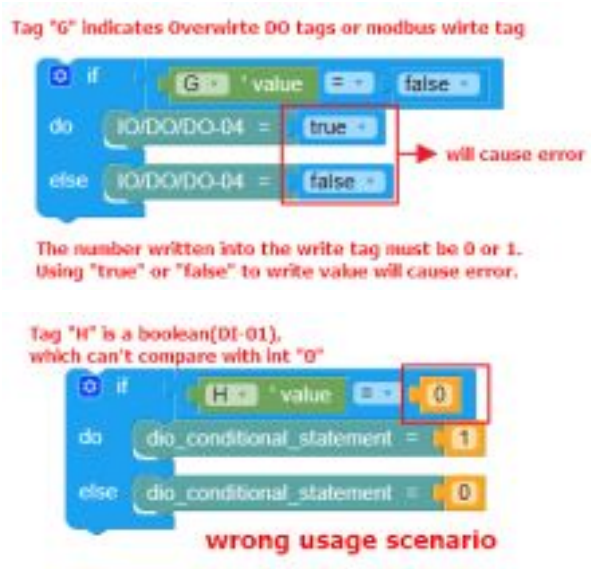
When a Tag Type is boolean, the following restrictions apply:

1. When used as a condition, it needs to be evaluated using True (1) or False (0).
2. When used in execution, it needs to be operated with numerical values 1 or 0.

Correct Usage Example:



Incorrect Usage Example:



Function Management

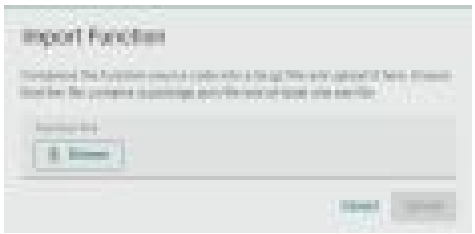
AIG-302 Series provides a functionality to trigger actions based on specific data or time frame. For example, you can create a function that implements a defined action such as a device reboot or a **cron** job triggered by a specified change in a tag value or newly generated tags/events.

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

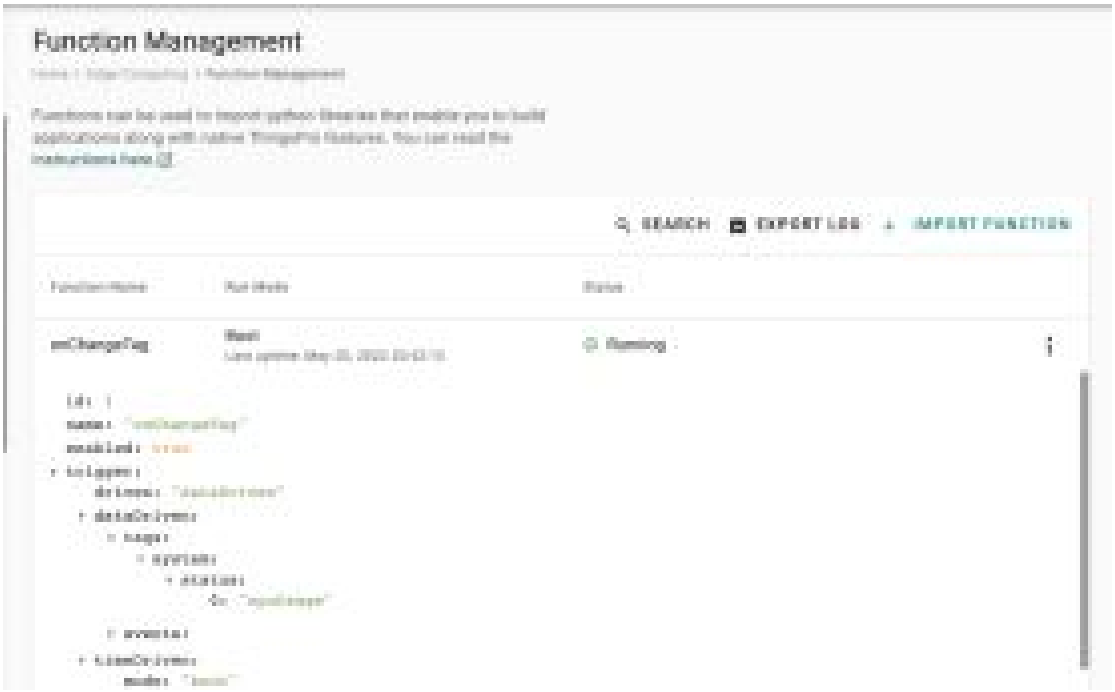
To import functions, do the following:

1. Click **Import Function**.

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



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



	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.

Security

Certificate Center

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

The **ThingsPro Edge Root CA for HTTPS** 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 certain services and purposes as indicated in the table below.

No.	Service/purpose	Port
1	HTTP service	80
2	HTTPS service	8443
3	SSH server	22
4	Discovery service	5353
5	Modbus TCP Slave (Server) port	502

NOTE

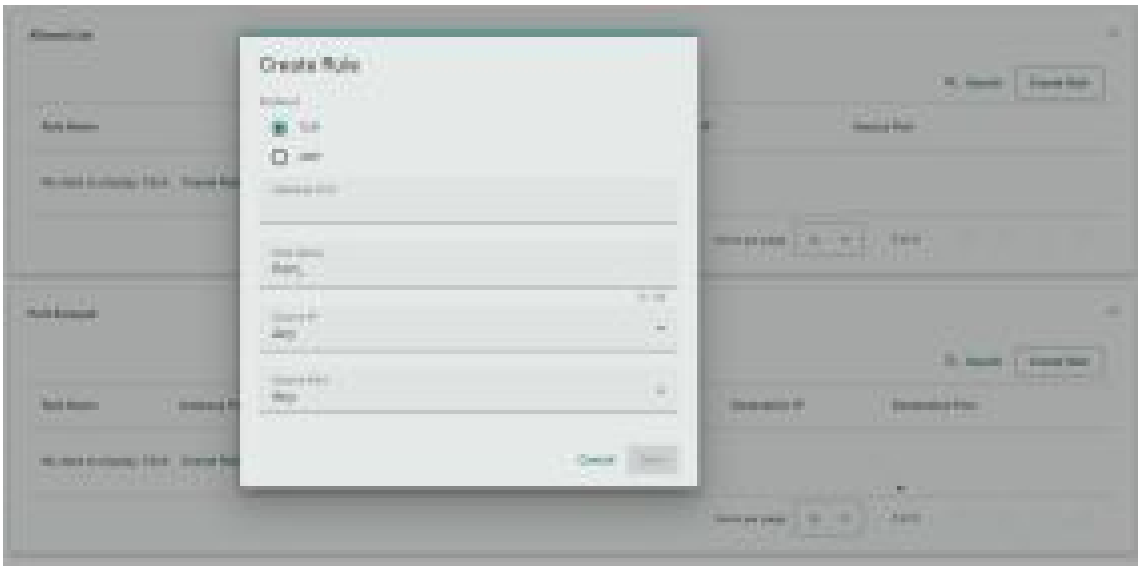
The AIG disables all ports by default excluding the reserved ports mentioned above. To enhance the security of your device, we recommend configuring a rule that includes the source IP and source port, thereby granting access only to specific individuals.

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:

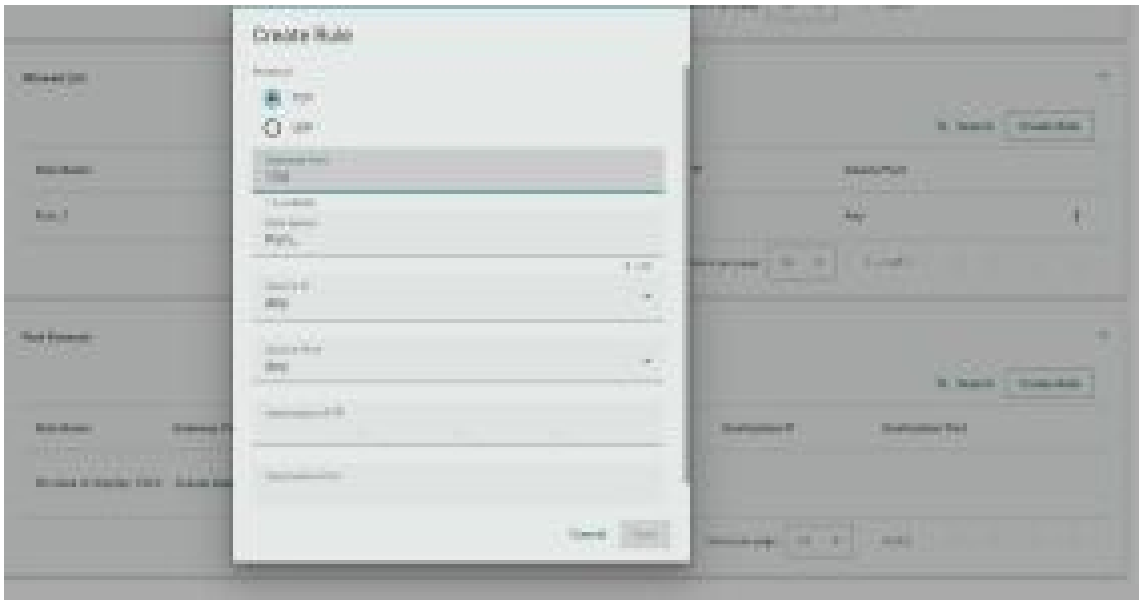
1. Click **+ Create Rule.**
2. Specify the protocol, gateway port, and rule name.
3. Specify a source IP or a subnet.
4. Specify a source port or a range of ports.
5. Click **Save**.



Port Forward

AIG provides port forwarding function. You can create, edit, and delete firewall rules here. To create firewall rules, do the following:

1. Click **+ Create Rule.**
2. Specify the protocol, gateway port, and rule name.
3. Specify a source IP.
4. Specify a destination IP and port.



5. Click **Save.**

NAT Service

Enable the NAT service to allow child devices to connect to external networks.

HTTPS

To ensure the securely access web console of the device, HTTPS has been enabled by default.

To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority. If there are no imported certificates, the AIG Series can generate the "ThingsPro Edge Root CA for HTTPS" certificate instead.

Login Lockout

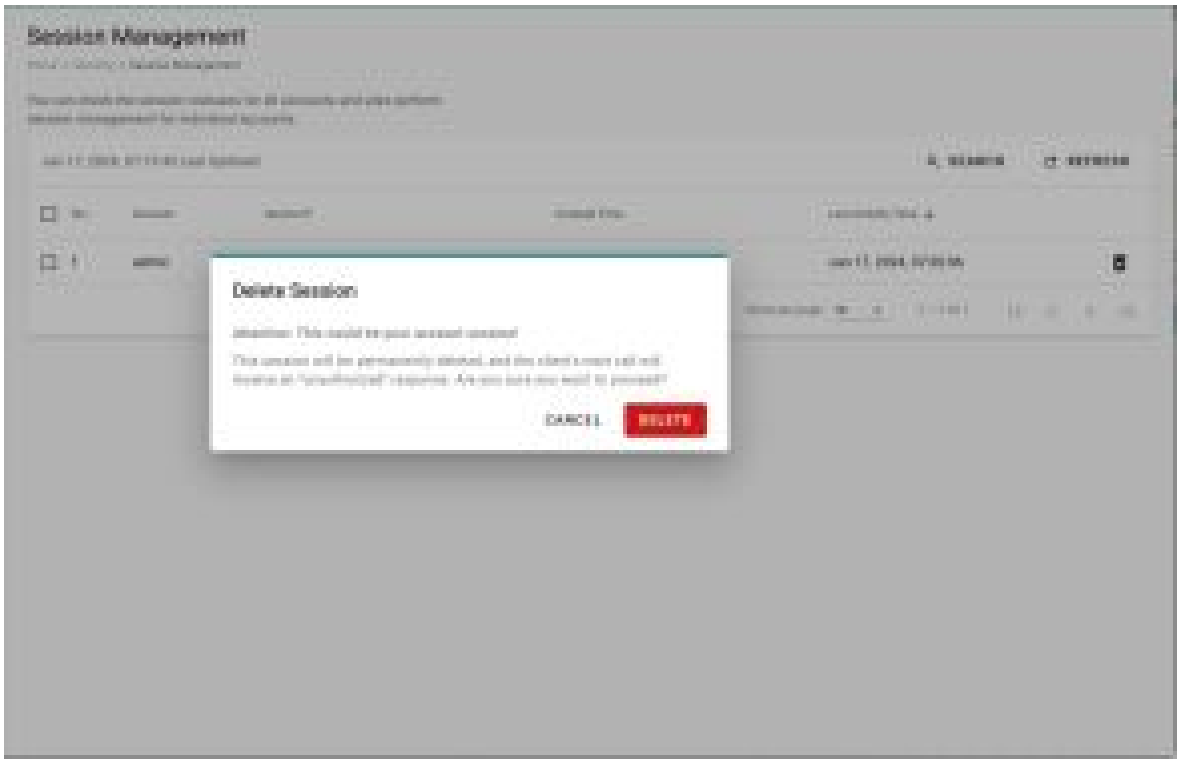
To avoid hackers repeatedly logging into the account to crack the passwords, you may choose to enable the login failure lockout and configure related settings.

Parameter	Value	Description
Max Failure Retry (times)	3 to 32	You can specify the maximum number of failures reties, if exceed the retry times, AIG will lock out for that account login
Failure Counter Reset Period (min)	1 to 60	The login failure counter will be recalculated after the reset period that you have set.
Lockout Time (min)	5 to 1440	When the number of login failures exceeds the Max Failure Retry, the AIG will lock out for a period.

Session Management

You can review session statuses for all accounts and manage sessions for individual accounts.

In the event of detecting unusual connections, you can enhance the security of your device by deleting the respective session.



NOTE

The user sessions used by the AIG QuickON tool to provision the AIG were not released within 15 minutes until session timeout, resulting in session accumulation and the maximum number of sessions per user threshold reached.

OpenVPN Client

OpenVPN allows you to create secure connections over the internet. It provides encryption and authentication to ensure confidentiality and integrity of your data. OpenVPN uses a client-server architecture where the server acts as the VPN endpoint and the client connects to the server to establish a secure connection.

To enable the function, go to **Security > OpenVPN Client** and do the following:

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

   This information includes:

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

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

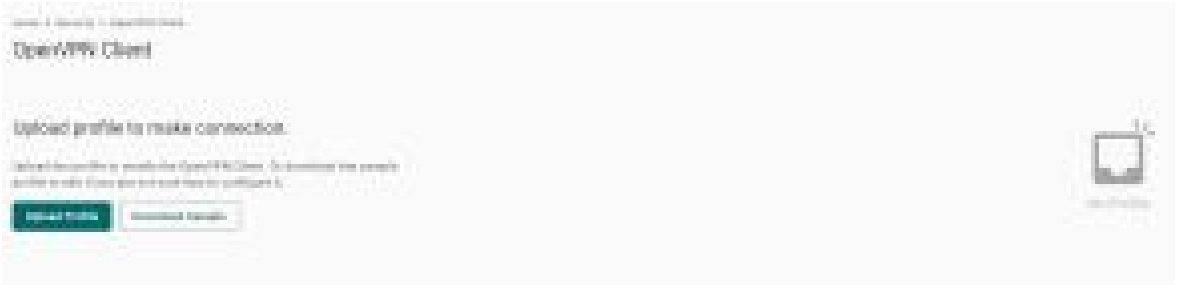
   c. Protocol: The protocol to be used for the VPN connection, such as UDP or TCP.

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

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

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

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



NOTE

OpenVPN cannot be used when the Moxa DLM Service is running.

System Use Notification

The System Use Notification feature is designed to provide users with essential information prior to accessing the main functionalities of the system. These notifications are displayed on the login screen to ensure users are aware of important details before logging in.

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 **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**
>
> To comply with security policy and best practices, 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.)

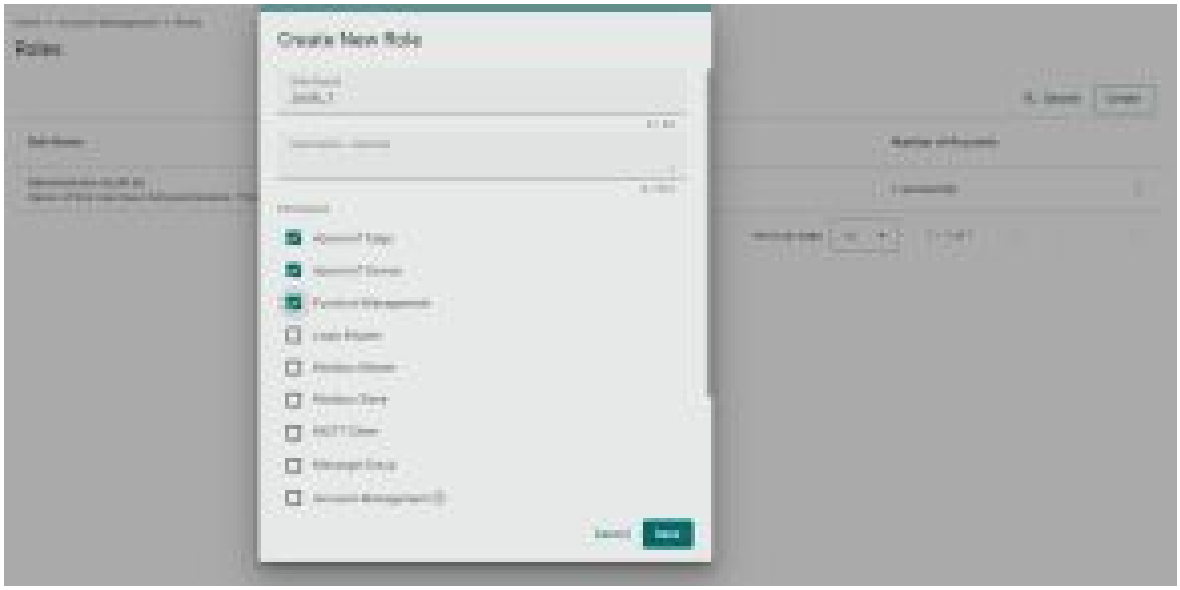
NOTE

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 on your AIG device.

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.

When the Role has been setup, it is available for selection under the Account.

Password Policy

Parameter	Value	Description
Min. Password Length	8 to 256	The minimum password length.
Password Strength Policy		To define how the AIG checks the password’s strength.
Password Change Reminders	10 to 360 days	Notify user to change the password.

Maintenance

Moxa DLM Service

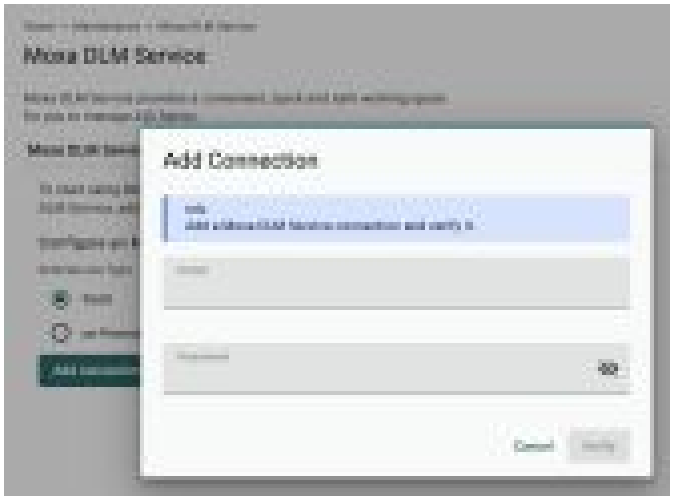
Moxa DLM (device life cycle management) service is used for managing the AIG devices. Imagine sitting in your office and using this service to remotely manage numerous devices distributed around the world. You can monitor the device's health status, upgrade firmware, import/export configuration, and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

You must first enroll your product online with the **Moxa DLM Service** with one of the following connection type:

- SaaS: Moxa DLM SaaS is a centralized platform designed by Moxa to efficiently manage and monitor distributed Moxa devices across various sites.
- On-premises: Moxa DLM on-premises is a self-hosted device life cycle management platform designed for managing large fleets of Moxa cellular devices deployed across remote and distributed sites.

To enroll your device with the **Moxa DLM SaaS**, do the following:

1. Enter the **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 click **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.

To enroll your device with the **Moxa DLM On-premises** , do the following:

1. Enter the DLM Server **email** and **password**, and press **Verify**.

2. Upload the DLM Server certificate when prompted.
3. After the connection is verified, enable the Moxa DLM Service on the top-left corner.

4. Log in to the DLM Server and go to SYSTEM MANAGEMENT > Device Approval to confirm the AIG device is listed and get approval.

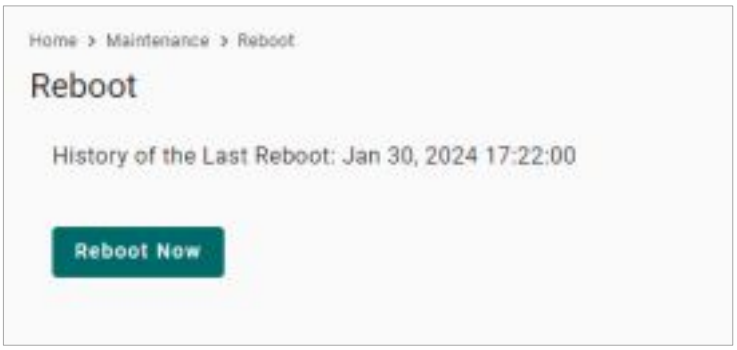
5. Select or create a project to assign your device, and click SAVE.

Service

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

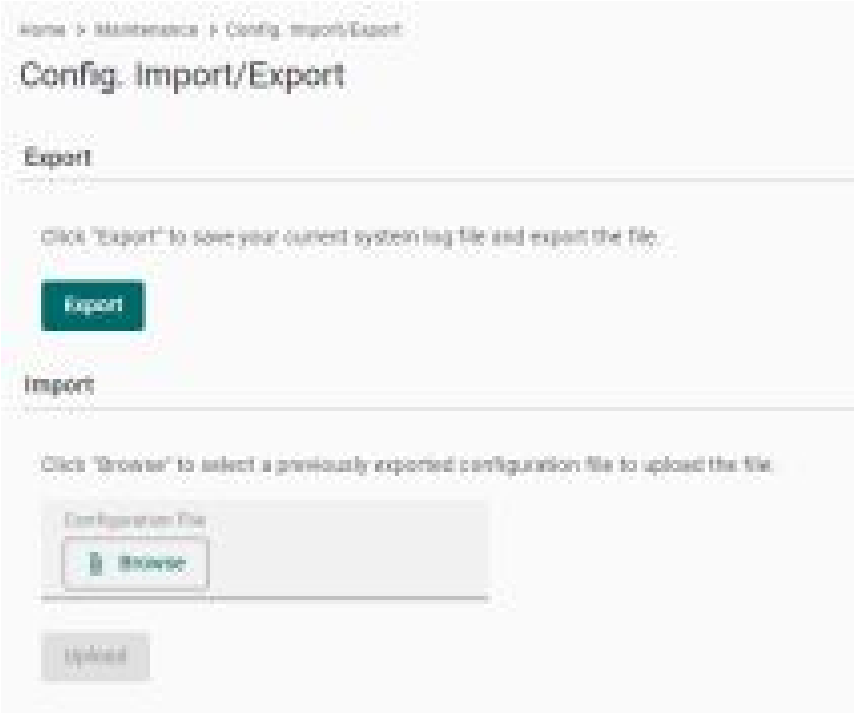
Reboot

If you want to reboot the device, go to **Maintenance > Reboot** and click **Reboot Now**.



Config. Import/Export

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



Backup & Restore

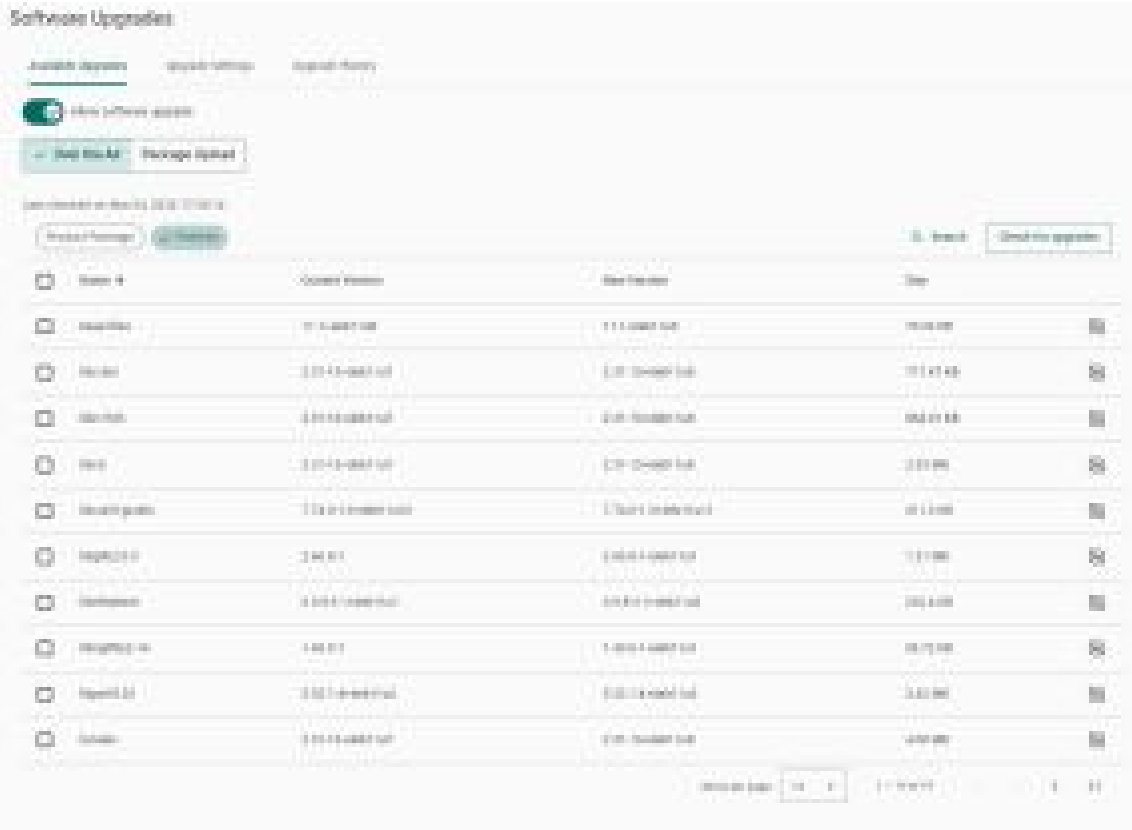
The backup function backs up the data on AIG device to a file (only one back up file can be created at a time). Backup files are encrypted and stored in a designated location on the device. You can restore the data from the backups when needed.

Software Upgrade

There are two approaches to upgrading an AIG: Over the-air and Upload package.

1. Over-the-air

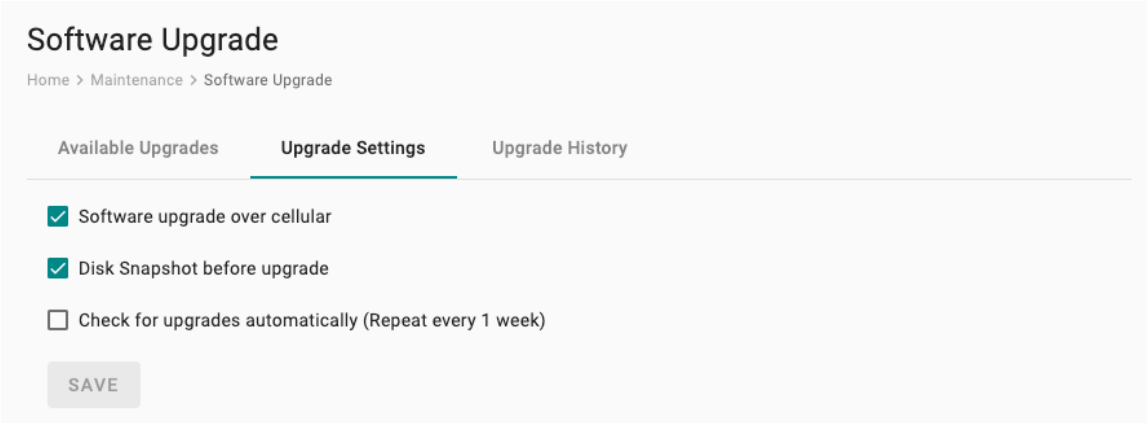
You can press Check for Upgrade to get the latest upgrade information, then select the patches to install. (Patches leverage the Debian APT mechanism, ensuring compatibility and identity. Additionally, all available patches are signed by Moxa, and the communication between AIG-302 and the repository is encrypted for system security.)

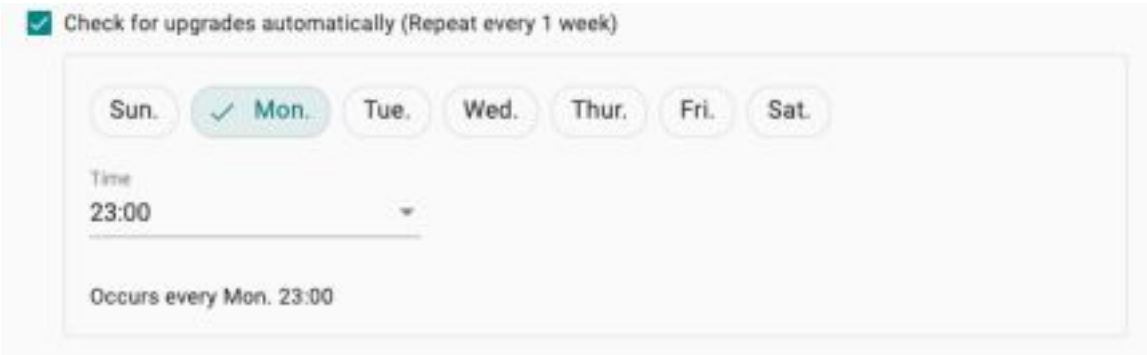


2. Upload Package

A pack that integrates all patches between two versions (e.g., from version 1.0 to version 1.1.) This scenario is applicable when the AIG cannot access the Internet. The upgrade pack can also be downloaded from the Moxa SRS: https://moxa-srs.thingsprocloud.com/home

Upgrade Settings





Parameter	Default	Description
Software upgrade over cellular	Checked	Allows upgrading the system via cellular. If you have a budget data plan for the cellular network, you may uncheck this option to save on data costs.
Disk Snapshot before upgrade	Checked	Takes a snapshot to record the system status before upgrading. We strongly recommend checking this option in case of unexpected situations.
Check for upgrades automatically (repeat every 1 week)	Unchecked	Specify a regular time to check for upgrades every week.

Upgrade History

The installed patches are listed here.

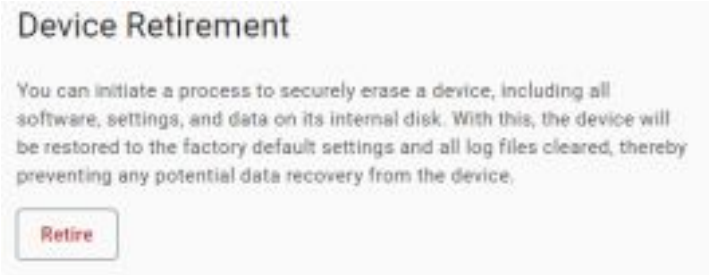
Reset to Default

There are two methods for resetting to default settings:

1. If you only wish to reset the configuration settings, use the **Reset** under **Configuration Reset**.
2. If you want to reset both the configuration settings and revert to the factory default firmware simultaneously, use the **Reset** under **Factory Reset**.

Device Retirement

Utilize this function when the device is being retired and you wish to securely delete all files and logs for security purposes to ensure the data cannot be recovered. Due to the low-level formatting of the memory that is required to erase data, it may take approximately 1.5 hours.



Diagnostics

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.

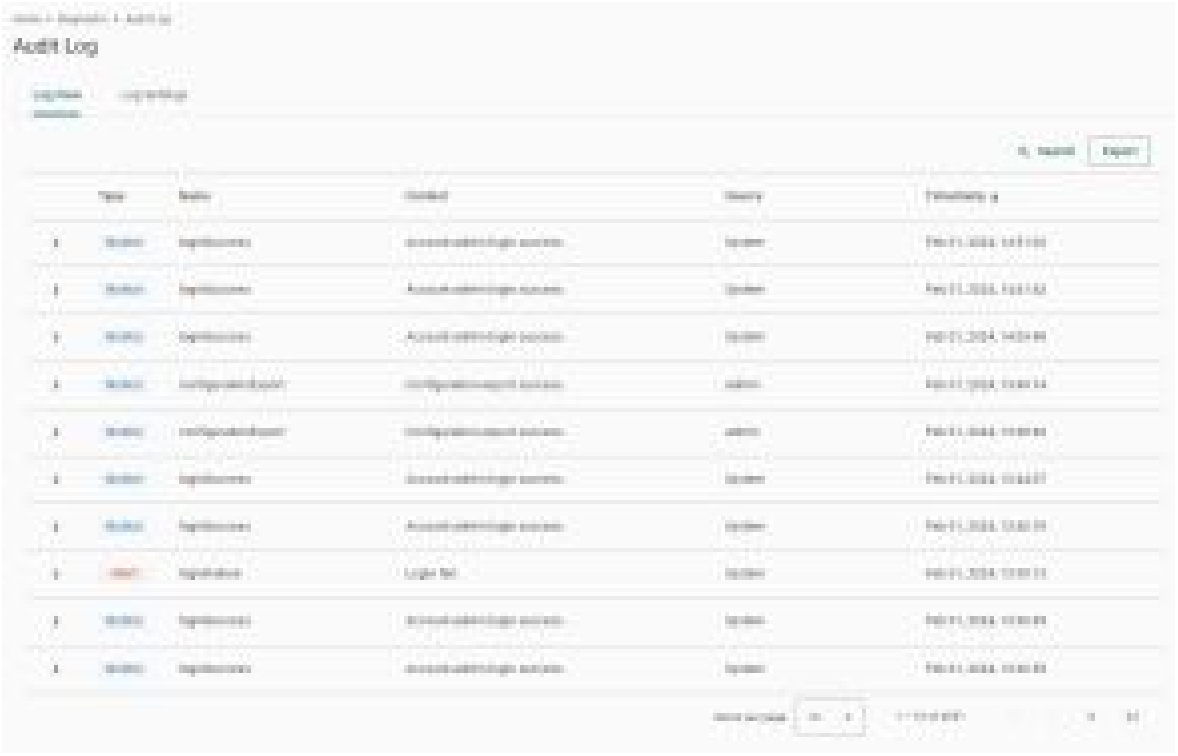
Go to **Diagnostic** > **System Log** to export the system log file and specify the location to save the system logs.

Click **Storage Settings** 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.

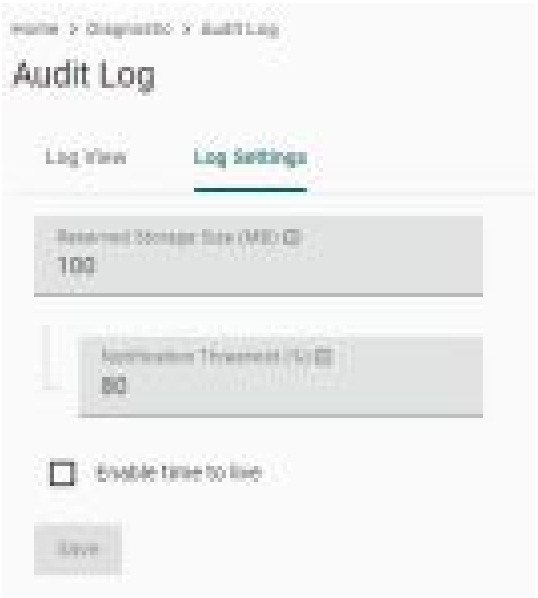
Audit Log

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

The audit logs can be exported and downloaded onto your computer.



In the **Log Settings**, you can specify the storage size to store the logs and notification threshold. Also, you also can enable time to live for maximum stored days.



Security Hardening Guide

Introduction

This section provides guidelines on how to configure and secure the AIG-302 Series. You should consider the recommendations in this document as best practices for securing the AIG-302 in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system to ensure that your applications are not negatively impacted.

General System Information

Basic Information About the Device

Model	Operating System	Firmware
AIG-302	Linux Debian 11	v1.0

Communication Integrity and Authentication

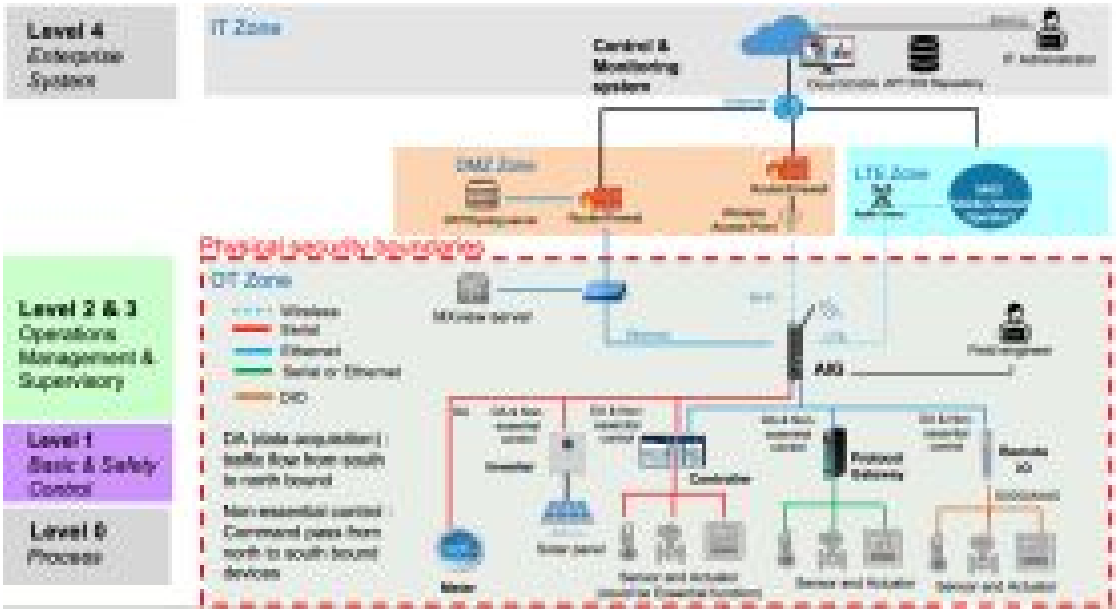
Below is a list of network communication services and protocols available in the AIG-302.

Process Name	Protocol	Type	Port Number	Description	Authenticator	Default Configuration
SSH Server (Debug mode used)	SSH	TCP	22	SSH console	Password	Disabled
Web Service	HTTP	TCP	80	Web console	Password	Enabled
HTTPS Service	HTTP	TCP	8443	Secured web console	Password	Enabled
Discovery Service	mDNS	UDP	5353	Communicate with Moxa utilities	N/A	Enabled
Modbus TCP Server	Modbus	TCP	502	Modbus communication implemented on the server side.	N/A	Disabled
Modbus Master (Client)	Modbus	RS232	N/A	Modbus communication implemented on the client side.	N/A	Disabled
DHCP Server	DHCP	UDP	67, 68	Assign IP addresses to connected DHCP clients	N/A	Disabled
DHCP Client	DHCP	UDP	67, 68	Retrieve a system IP information from a DNS server	N/A	Enabled (LAN1)
Azure IoT Edge/Device	MQTT	TCP	8883	Transfer telemetry data and interoperate with the Azure cloud.	Symmetric Key, X.509 certificate	Enabled
	MQTT over WebSockets	TCP	443		Symmetric Key, X.509 certificate	Disabled
	AMQP	TCP	5671		Symmetric Key, X.509 certificate	Disabled
	AMQP over WebSockets	TCP	443		Symmetric Key, X.509 certificate	Disabled
AWS IoT Core	MQTT	TCP	8883	Transfer telemetry data and interoperate with the AWS cloud.	X.509 certificate	Disabled
MQTT Client	MQTT	TCP	8883	Transfer telemetry data and interoperate with a MQTT Broker.	Password, X.509 certificate	Disabled
OPC UA Server	TCP	TCP	4840	OPC UA communication implemented on the server side.	Password, X.509 certificate	Disabled

Process Name	Protocol	Type	Port Number	Description	Authenticator	Default Configuration
Sparkplug	MQTT	TCP	8883	Sparkplug B communication implemented on the client side	X.509 certificate	Disabled

Potential Threats and Corresponding Security Measures

The below diagram depicts the location/position of AIG-302 in systems. A list of potential security threats to the AIG-302, and the corresponding security measures that need to be taken by the asset owner if the threats apply are 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	Enabling HTTP to HTTPS redirection make sure secure protocol with encryption and authentication are used for data transmission.
2	An attacker via WAN spoofs a browser, 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	

Threat ID	Threat mitigated/ handled	Security measures
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. • Secure crucial data, like telemetry messages, on encrypted external storage (e.g., USB). • 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 audit or system logs might dominate storage space, reducing room for critical information or telemetry message buffers when the network is down.	• Back up the logs to Azure Blob storage for safekeeping. • Store system logs on external storage, freeing the log partition for audit logs exclusively. AIG-302 originally supports: • A reserved partition in the primary system for audit/system logs is provided. • Logs don't override each other. • A log generation mechanism to reduce redundancy, capturing crucial logs.
8	Network data flow could be potentially interrupted, crashed or stopped by DOS attack.	• Configure an alternative WAN interface for connection failover, like Ethernet or Wi-Fi • 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 10 requests per second maximum. Find the corresponding API "limit_req", please refer to https://github.com/TPE-TIGER/TPE-TIGER.github.io Note that there's no public access to the shared memory used by tagHub. 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

- AIG-302 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.
- AIG-302 has anti-tamper labels on the enclosures. This allows the administrator to tell whether the device has been tampered with.
- AIG-302 uses security screw on the enclosures as physical tamper resistance measure to increase the difficulty of probing the product internals in case of physical security breach.
- AIG-302 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

- If AIG-302 must connect to an untrusted network (e.g., Internet) via Ethernet or Wi-Fi, it MUST NOT directly be connected to the untrusted network, which means a firewall must be setup between Ethernet and Wi-Fi connection from AIG-302 and the untrusted network.
- For security-critical applications, we strongly recommend using a private APN for cellular networks.

Access Control

- The default password policy requires the password to be at least 8 characters in length.
- Update user passwords on a timely manner. For administrator, we recommend refreshing password at least every 3 months.
- Bootloader configuration menu comes with a single administrator account shared by all users. Asset owner MUST have access and identity records of the personnel who accessed the Bootloader to ensure non-repudiation in case of security breach incidents.
- Enabling Debug Mode activates the SSH server service for remote terminal access. Asset owners MUST disable Debug Mode in the production stage.

Operation

- Disabled communication interfaces that are not in use.
- Make sure only trusted and reliable persons are registered in AIG-302.
- Frequently run the scan from the Security Dashboard, and execute the corresponding configuration or actions.
- We recommend you reset AIG-302 to factory default upon receiving it to avoid the risk of potential software tampering before the AIG-302 reaches your hand.

Maintenance

- Perform software upgrade frequently to enhance feature, security patches or fix bugs.
- Perform backup of system on timely manner.
- Examine audit logs frequently to detect any anomalies.
- To report vulnerabilities of Moxa products, please submit your finding on the following webpage: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

Retirement

To avoid any sensitive information such as your account password or certificate from being disclosed, always use Device Retirement to reset the AIG-302 to factory default and further wipe out all user data, including logs, in an unrecoverable manner before removing the AIG-302 from.

Configuration and Hardening Information

Forcing a Password Change After First Login

For security reasons, account and password protection is enabled by default. Users must provide the correct user account and password to unlock the device to gain access to the web console of the gateway.

The default account and password are **admin** and **admin@123** (both in lowercase letters), respectively.

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

Security Dashboard

Once device provisioning is completed, you can log in into the AIG web console, go to **Security Dashboard**, and press **Scan** to check the security status of the device.

You can utilize the **Security Dashboard** results to fix security issues to enhance the security of your AIG gateway as per the following guidelines:

Category	Security Check Criteria	Threat Mitigation/handling
Account Settings	Password should be changed within the preset interval.	Go to **Account Management > Accounts** to change the password.
	An account should only have one active session at any given time.	Go to **Security > Session Management** monitor and manage concurrent sessions.
	An account should not have abnormal connections (E.g., more than one session per account from different source IPs).	
Application Networking	System should not have open network ports.	Go to **Security > Firewall** and check the allow list.
Application Resource Usage	IoT Edge modules should not utilize system disk's configurable space.	Ensure the IoT Edge modules are deployed in the system storage paths **/var/run/** and **/tmp/**.
	IoT Edge modules should not utilize system disk's non-configurable space.	
	IoT Edge modules should not be granted direct privileges.	To grant permissions to the IoT Edge modules, go to **Cloud Connectivity > Azure IoT Edge > Module Permission**, create a service account, and grant the required permissions to the IoT Edge module.
Product Certificate Deployment	Production certificate should be configured as an Azure IoT Edge downstream certificate.	For enhanced security robustness, we recommend using your own certificate instead of the default one. Go to **Cloud Connectivity > Azure IoT Edge > Downstream Certificate** to upload a certificate.
	Azure IoT Edge should not use a connection string for provisioning.	For enhanced security robustness, we recommend using a TPM or a X.509 certificate.
	All certificates should not expire within the next three months.	Go to **Security > Certificate Center** to check the status of each certificate.
	All certificates should have expired.	If you find that a certificate will expire soon or has already expired, go to **Cloud Connectivity > Azure IoT Edge/Azure IoT Device/MQTT Client or Security > HTTPS** to check and replace the certificates.
Service Settings	Discovery Service should not be enabled.	Go to **Maintenance > Service** to disable Discovery Service.
	SSH Service should not be enabled.	Go to **Maintenance > Service** to disable the Debug Mode.
	Serial Console Service should not be enabled.	Go to **Security > Service** to disable local console.

Category	Security Check Criteria	Threat Mitigation/handling
	Account Lock Service should be enabled.	Go to **Security > Login Lockout** to enable the **Login Failure Lockout** option.
	System Use Notification Service should be enabled.	Go to **Security > System Use Notification** to enable System Use Notification Service.
System Status Check	Product software package should be up to date.	Go to **Maintenance > Software Upgrade** and click **Check for Upgrade** to retrieve the latest upgrade pack information.
	System backup should be performed at least once a year.	Go to **Maintenance > Backup & Restore** and click **Manage** to back up the system.

Account Settings

- Security Check Criteria: Password should be changed within the preset interval.

  Go to **Account Management** > **Accounts** to change the password. We recommend changing the password within the preset interval.

  To configure a preset interval for changing the password, go to **Account Managements** > **Password Policy** > **Reminder Threshold**.

- Security Check Criteria: An account should have only one active session at any given time.

  Go to **Security** > **Session Management** to identify and manage accounts with more than one session. We recommend deleting connections that you are unaware of, especially in cases where an account has more than one active session.

- An account should not have abnormal connections.

  Go to **Security** > **Session Management** to identify and manage abnormal sessions, such as more than one session per account from different source IPs. We recommend deleting the connections of which you are not aware.

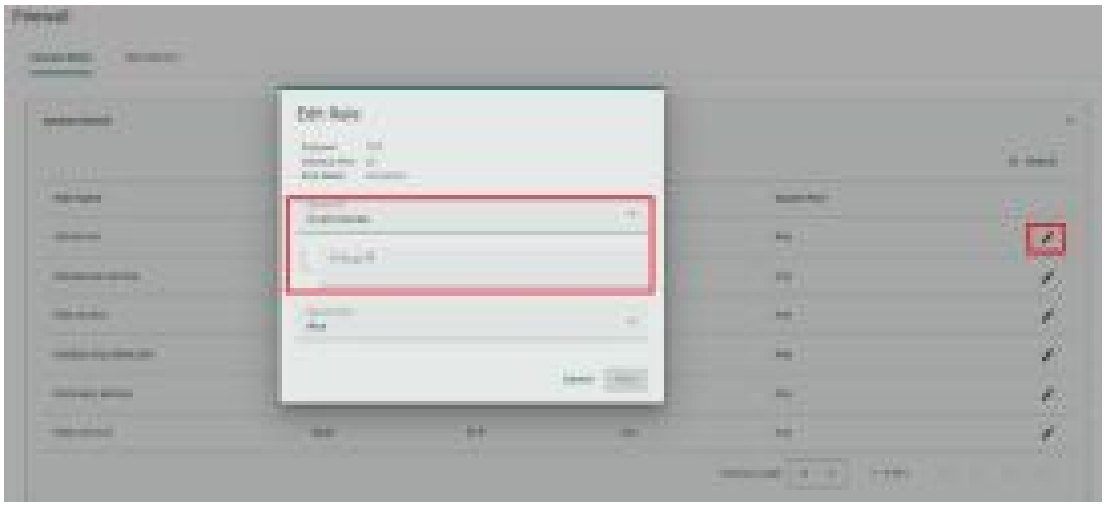
  To ensure enhanced security for your AIG-302, create user roles with specific permissions for user accounts. In consideration of the security requirements of the AIG-302, we recommend creating the following roles with the specified permissions.

Role	Permissions
Administrator	All
Monitoring personnel	(Default) Monitoring Data Management
OT – Field site operator	(Default) Monitoring Security Management System Settings & Network Settings Maintenance Data Management (Optional) Add-on Applications such as Modbus
IT – maintenance personnel	(Default) Monitoring System Settings & Network Settings Maintenance Data Management (Optional) Add-on Applications such as Azure

Application Networking

Security Check Criteria: System should not have open network ports.

Understanding which network ports are open is crucial for improving security, preventing vulnerabilities, safeguarding data, staying compliant, and optimizing system resources. We advise minimizing open network ports to reduce cybersecurity risks. To check for open ports in the system, navigate to **Security** > **Firewall**. If there are open ports that are not in use, we strongly recommend disabling them. For the essential open ports, we recommend adding rules to limit access.



Application Resource Usage

- Security Check Criteria: IoT Edge modules should not utilize system disk's configurable space.

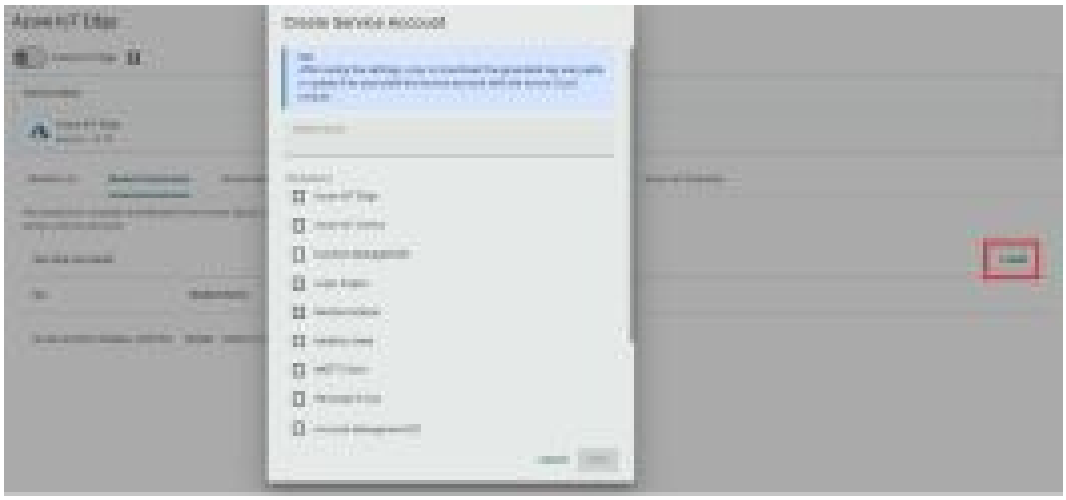
  Our recommendation is for the IoT Edge modules to be deployed only in specific system storage directories/paths such as **/var/run/** and **/tmp/.**

- Security Check Criteria: IoT Edge modules should not utilize system disk's non-configurable space.

  Our recommendation is for the IoT Edge modules to be deployed only in specific system storage directories/paths such as **/var/run/** and **/tmp/.**

- Security Check Criteria: IoT Edge modules should not granted direct privileges.

  Granting permissions to IoT Edge modules in a controlled manner is important for cybersecurity because it reduces the risk of unauthorized access, protects sensitive data, and ensures that each module has access only to what it needs to function properly. To grant permissions to IoT Edges, go to **Cloud Connectivity > Azure IoT Edge > Module Permission**, create a service account, and grant permission to the IoT Edge module.



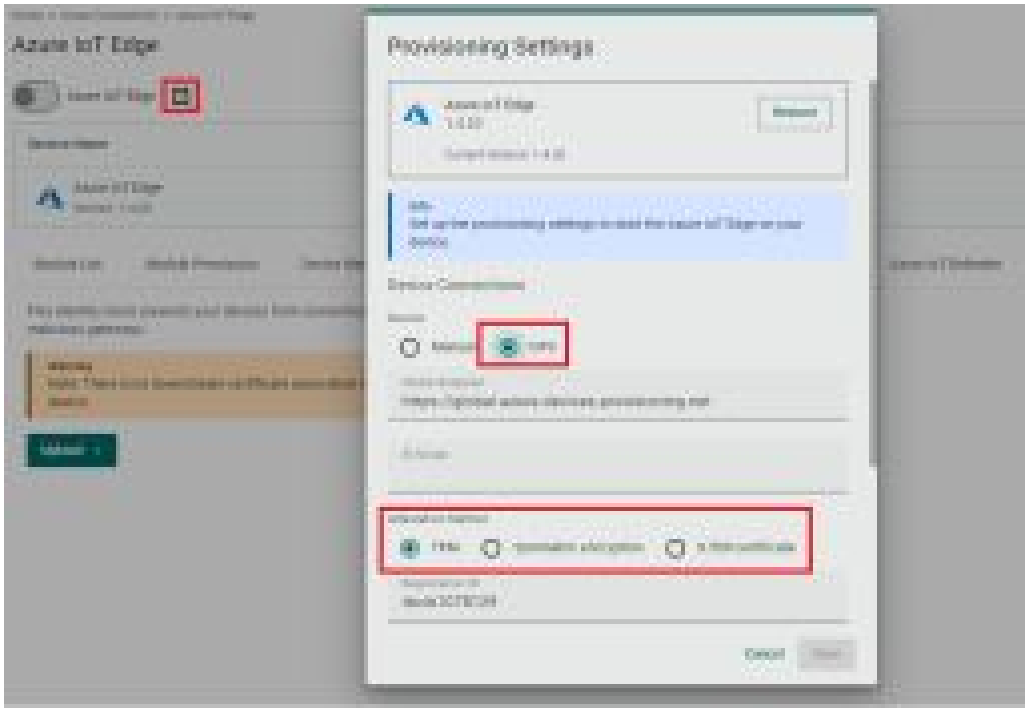
Product Certificate Deployment

- Security Check Criteria: Production Certificate should be configured as an Azure IoT Edge downstream certificate.

  For enhanced security robustness, we recommend using your own certificate instead of the default one. Go to **Cloud Connectivity** > **Azure IoT Edge** > **Downstream Certificate** to upload a certificate.

- Security Check Criteria: Azure IoT Edge should not use connection string for provisioning.

  We recommend an attestation method, which uses a TPM or a X.509 certificate, instead of a manual confirmation using a connection string. You can configure this at **Cloud Connectivity** > **Provisioning Settings** > **DPS**.



- Security Check Criteria: All certificates should not expire within the next three months.

  You can check the status of all the certificates being used by the AIG at **Security** > **Certificate Center**. We recommend regular inspection of the status of the certificates and importing new certificates to replace the ones that are about to expire.

- Security Check Criteria: All certificates should not have expired.

  You can check the status of all the certificates being used by the AIG at **Security** > **Certificate Center**. We recommend regular inspection of the status of the certificates and importing new certificates to replace the ones that are about to expire.

Service Setting

- Security Check Criteria: Discovery Service should not be enabled.

  We recommend disabling the **Discovery Service** in the commissioning stage. Go to **Maintenance** > **Service** to disable the service.

- Security Check Criteria: SSH Service should not be enabled.

  We recommend disabling the SSH Service in the commissioning stage. Go to **Maintenance** > **Service** to disable Debug Mode.

- Security Check Criteria: Serial Console Service should not be enabled.

  We recommend disabling Serial Console Service in commissioning stage. Go to **Maintenance** > **Service** to disable the Local Console.

- Security Check Criteria: Account Lock Service should be enabled.

  To thwart brute-force attacks, we recommend activating the Account Lock Service. When AIG detects multiple failed login attempts surpassing the set threshold, it will automatically lock the account for the specified duration. Go to **Security** > **Login Lockout** to enable and configure parameters for this service.

- Security Check Criteria: System Use Notification Service should be enabled.

  It is important to display system usage notifications prior to the login page so users know the rules and risks involved in using the system. This helps meet legal requirements, reduces risks, and holds users accountable for their actions.

  Go to **Security** > **System Usage Notification** to enable this function.

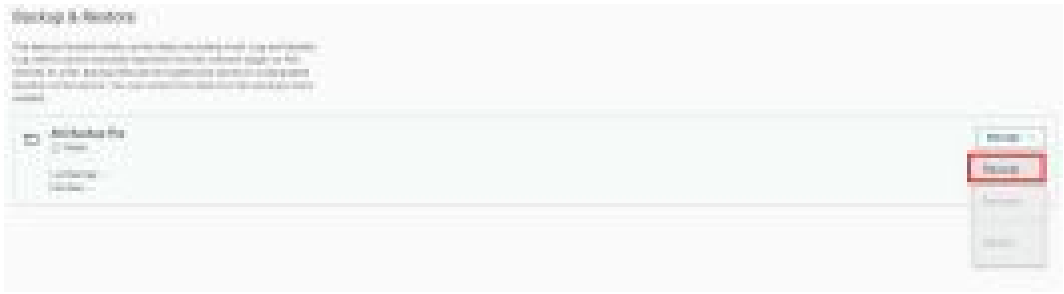
System Status Check

- Security Check Criteria: Product software package should be up to date.

  The importance of security cannot be overstated when it comes to keeping your product software up to date. Regular updates help patch vulnerabilities, reduce the risk of cyberattacks, and protect sensitive data, safeguarding your system and users from potential security threats. Go to **Maintenance** > **Software Upgrades** to retrieve up-to-date software for your AIG.

- Security Check Criteria: System backup should be performed at least once a year.

  Performing a system backup annually is important to protect your data in case of system failures, cyberattacks, or disasters. It ensures you can quickly recover your information, stay compliant with regulations, and maintain business continuity. Go to **Maintenance** > **Backup & Restore** to back up your system.



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 the access to the device.

Accounts

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

Creating a New User Account

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

NOTE

To comply with security policy and best practices, 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 the device
Delete	Delete the user account (**NOTE:** This operation is irreversible.)

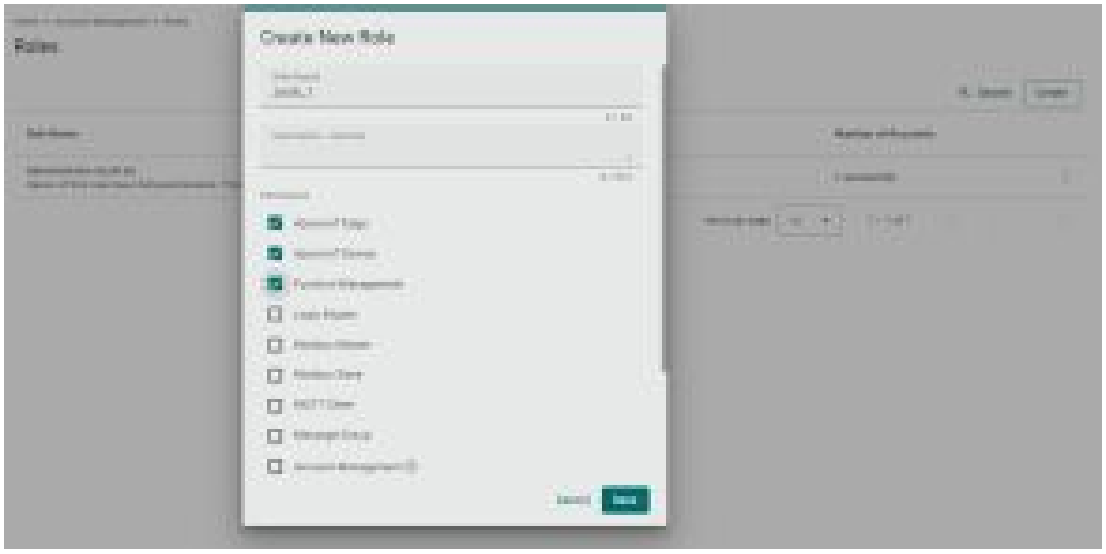
NOTE

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

Roles

You can **View**, **Create**, **Edit**, and **Delete** user roles for your AIG device here.

Click **+ Create** to set up a new user role. Specify a unique name for the role and assign the appropriate permissions and 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.

When the role has been set up, it is available for selection by accounts.

Password Policy

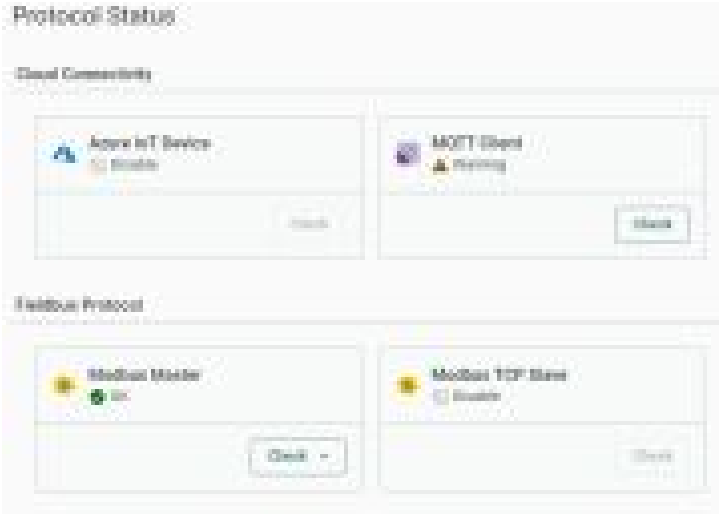
Parameter	Value	Description
Min. Password Length	8 to 256	The minimum password length
Password Strength Policy		To define how the AIG checks the password strength
Password Change Reminders	10 to 360 days	Notify user to change the password

Protocol Status

In case of A communication issue, go to **Diagnostic > Protocol Status**. The device provides comprehensive troubleshooting tools to help you identify the issue easily. When you access the page, you can see an overview of the status for Cloud Connectivity and Fieldbus Protocol.

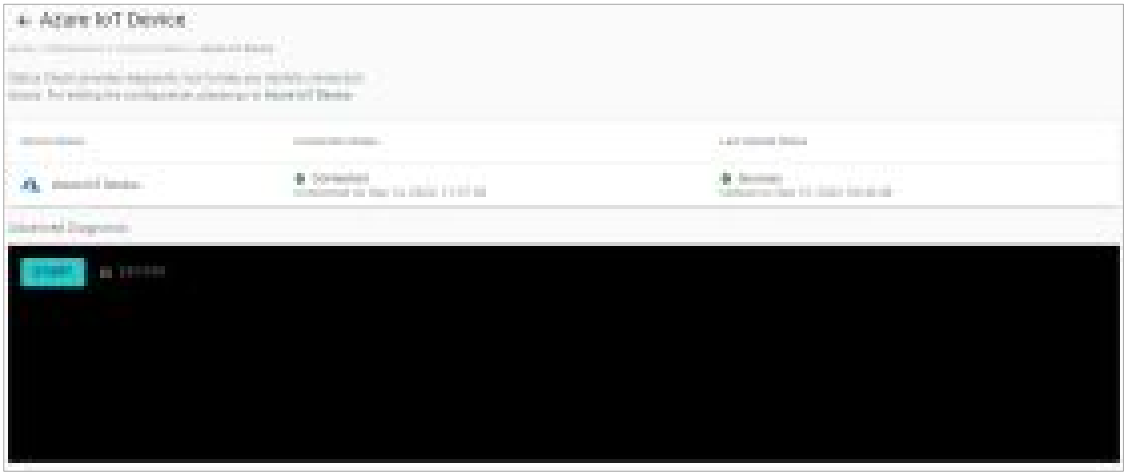
For troubleshooting issues related to Azure and MQTT Client, do the following:

1. Click **Check**.

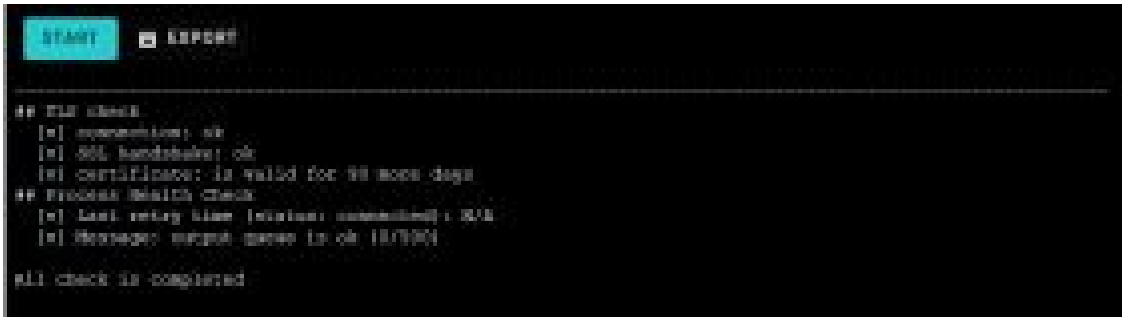


2. Click **Start.**

   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.

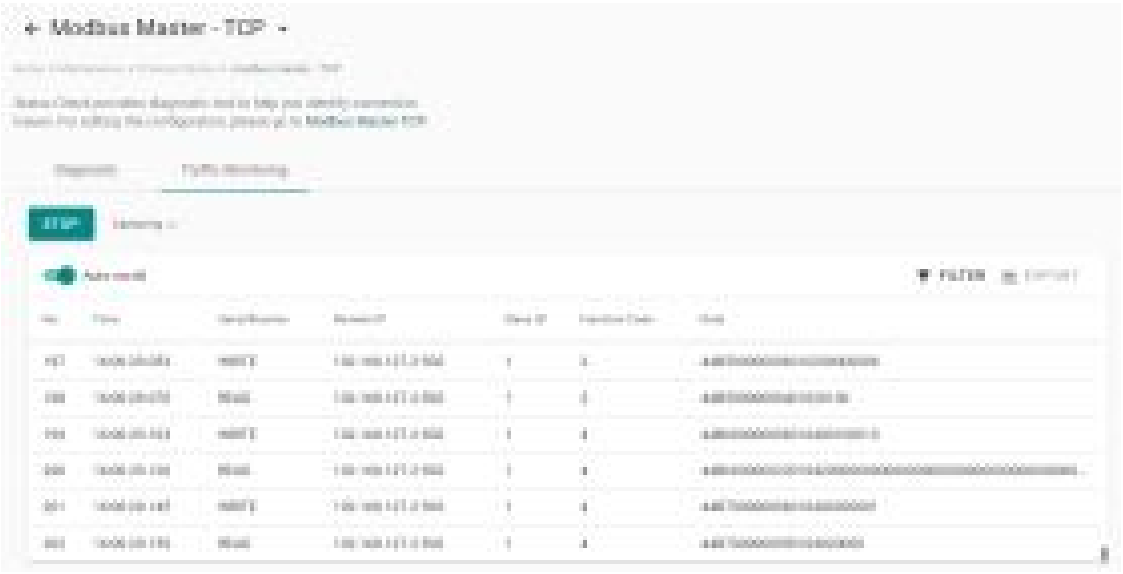


4. (Optional) **Export** the logs.

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 engineer for further analysis.

A. Appendix A

Publish Mode

Publish Mode	Parameters	Value	Description
By Interval	Publish Intervals (sec)	1 to 86400	The frequency of data uploads 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)	1 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)	1 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. Audit Log Index

Categories

Category Name	Description
Account & Access	Account management operations, login/logout, account lock/unlock, session termination.
Configuration Update	Configuration updates, service enable/disable.
Connection & Interface	Incoming connections, outgoing connections, physical interface connections.
Command & Message	Received commands, sent messages.
Maintenance	Backup, restore, software updates, reboot, export operations.
Performance & Health	Performance, security, resource availability.
Application Management	Application management operations.

Account & Access

ID	Name	Content	Type	Conditions
AA01	roleCreate	Role: `$roleName` be created	NOTICE	
AA02	roleDelete	Role: `$roleName` be deleted	NOTICE	
AA03	roleUpdate	Role: `$roleName` be updated	NOTICE	
AA04	accountCreate	Account: `$accountName` be created	NOTICE	
AA05	accountDelete	Account: `$accountName` be deleted	NOTICE	
AA06	accountUpdate	Account: `$accountName` be updated	NOTICE	
AA07	passwordChange	Account: `$accountName` password changed	NOTICE	
AA08	loginSuccess	Account: `$accountName` login success	NOTICE	
AA09	loginFailure	Login Fail	ALERT	reasons • invalid account/password • account `$accountName` inactive
AA10	accountLock	Account: `$accountName` be locked	ALERT	
AA11	accountUnlock	Account: `$accountName` unlocked	NOTICE	

Configuration Update

ID	Name	Content	Type	Conditions
CU01	configurationChange	`$serviceName` configuration changed	NOTICE	When user modified system settings

Connection & Interface

ID	Name	Content	Type	Conditions
CI01	ipRenew	IP renew on interface: `$interfaceName`	NOTICE	every ip renew && different wtih last time
CI02	connectionStatusConnect	Interface: `$interfaceName` connected	NOTICE	interface connection status change to connected
CI03	connectionStatusDisconnect	Interface: `$interfaceName` disconnected	NOTICE	interface connection status change to disconnected
CI04	appServerConnectionEstablish	Service: `$serviceName` accepted connection request from client	NOTICE	
CI05	appServerConnectionDrop	Service: `$serviceName` drop connection from client	NOTICE	
CI06	appClientConnectionConnect	Service: `$serviceName` connected	NOTICE	service connection status change to connected
CI07	appClientConnectionDisconnect	Service: `$serviceName` disconnected	NOTICE	service connection status change to disconnected
CI08	appClientConnectFailure	Service: `$serviceName` connect fail	NOTICE	service connection fail
CI11	ethernetPortPlugIn	Ethernet port: `$interfaceName` plugged-in	NOTICE	
CI12	ethernetPortPlugOut	Ethernet port: `$interfaceName` plugged-out	NOTICE	
CI13	externalStoragePlugIn	External storage: `$interfaceName` plugged-in	NOTICE	
CI14	externalStoragePlugOut	External storage: `$interfaceName` plugged-out	NOTICE	
CI15	internetConnectionStatusChange	Internet Connection changed to `$status`	NOTICE	status changed, status: • NotConnected • NoInternetAccess • ConnectedToInternet
CI16	externalStorageEncrypted	New External storage `$status`	NOTICE	status • encrypted • decrypted
CI17	appOpenPortSuccess	Service: `$serviceName` port opened	NOTICE	every time service open
CI18	appOpenPortFailure	Service: `$serviceName` failed to open port	ALERT	every time service open failure

Command & Message

ID	Name	Content	Type	Conditions
CM01	commandReceive	Service received command: `$commandName`	NOTICE	commandResponse • Success • Fail
CM02	commandRequestError	Service request failed	ALERT	when request result from success to fail
CM03	commandRequestRecover	Service request recover	NOTICE	when request result from fail to success

Maintenance

ID	Name	Content	Type	Conditions
MA01	systemBackup	System backup success	NOTICE	
MA02	systemRestore	System restore success	NOTICE	
MA03	configurationExport	Configuration export success	NOTICE	
MA04	configuraitonImport	Configuration import success	NOTICE	
MA05	deviceReboot	Device reboot	NOTICE	
MA06	softwarePackageUpdate	Software package update `$status`	NOTICE	status: • success • fail packages: • packages update success
MA07	newSoftwareAvailable	New software package available	NOTICE	new packages discovered when software auto scan
MA08	auditLogExport	Audit log export success	NOTICE	
MA09	systemLogExport	System log export success	NOTICE	
MA10	resetToFactoryDefault	Reset to Factory Default	NOTICE	status: • success • fail
MA11	resetToConfigurationDefault	Reset to configuration Default	NOTICE	
MA12	timeUpdate	System Time update success.	NOTICE	source: • NTP • Manual when • success
MA13	timeUpdateFailure	System Time update failure.	ALERT	source: • NTP • Manual when • fail

Performance & Health

ID	Name	Content	Type	Conditions
PH01	untrustExecutionEnvironment	ThingsPro Edge is running on an untrust execution environment.	ALERT	bootup
PH02	storageUsageAlarm	System detects `$diskName` storage usage reach 95%. You shall take necessarry action immediately, before lose control from the device.	ALERT	every hour
PH03	storageUsageNotice	System detects `$diskName` storage usage reach 80%. You shall take necessarry action, before lose control from the device.	NOTICE	• every hour • skip if reach PH02
PH04	systemLoadingAlarm	System detects unexpect system loading. You may upgrade device hardware spec or reduce unnecessarry processes, to avoid system outage risk.	NOTICE	• load average 15min > 2 • every hour
PH05	auditLogReachThreshold	Audit log run out of space, log rotate triggered.	ALERT	• When the system runs out of log storage space (entering rotate mode) • And this log has not been generated after the TPE is started/restarted or the log configuration is updated.

ID	Name	Content	Type	Conditions
PH06	httpMaxSessionExceeded	Reach max HTTP/HTTPS session limit	ALERT	every connection create && reach max limitation
PH07	certificateExpired	Certificate: `$certDisplayName` is going to expired	NOTICE	• every day • when a certificate is going to be expired within 90 days.
PH08	certificateAdd	Certificate (`$certDisplayName`) be added	NOTICE	
PH09	certificateRemove	Certificate (`$certDisplayName`) be removed	NOTICE	
PH11	auditLogReachAlertThreshold	System detects audit log storage usage reach `$configurePercentage%`	ALERT	When • first boot check usage exceeds `$configurePercentage` • the usage check usage exceeds `$configurePercentage` did not exceed previous time
PH12	systemInitialize	System initialized	NOTICE	When system initialization is completed.
PH13	unlockPinFailure	Failed to unlock SIM card's PIN code on interface: `$interfaceName`	ALERT	unlock pin code fail
PH14	certificateUpdate	Certificate (`$certDisplayName`) be added	NOTICE	
PH15	secretsAdd	Secrets (`$secretsDisplayName`) be added	NOTICE	private key be added
PH16	secretsUpdate	Secrets (`$secretsDisplayName`) be updated	NOTICE	private key be updated
PH17	secretsRemove	Secrets (`$secretsDisplayName`) be removed	NOTICE	private key be removed
PH18	auditLogReachTTL	Audit log have exceeded the configured live time, log rotate triggered.	ALERT	• When the system check the logs exceeds live time (entering rotate mode) • And this log has not been generated after the TPE is started/restarted or the log configuration is updated.

C. System Tag List

Provider Name	Source Name	Tag Name	Data Type	Remark
system	status	cpuUsage	uint64	
system	status	cpuTemperature	uint64	
system	status	memoryBuffers	uint64	
system	status	memoryUsed	uint64	
system	status	memoryUnused	uint64	
system	status	memoryCached	uint64	
system	status	memoryUsage	uint64	
system	status	memoryTotal	uint64	
system	status	gpsLat	double	
system	status	gpsLong	double	
system	network	networkStatus	string	
system	network	networkTx	uint64	
system	network	networkRx	uint64	
system	network	networkUsage	uint64	
system	network	$(name)NetworkUsage	uint64	$name = network interface's display name(low case)
system	network	$(name)NetworkRx	uint64	$name = network interface's display name(low case)
system	network	$(name)NetworkTx	uint64	$name = network interface's display name(low case)
system	network	$(name)Signal	double	unit: dBm $name = cellular interface's display name(low case)
system	network	$(name)SignalLevel	int32	$name = cellular interface's display name(low case)
system	storage	systemDiskUsed	uint64	
system	storage	systemDiskFree	uint64	
system	storage	systemDiskPercent	double	
system	storage	$(storage)Used	uint64	$(storage)=disk's display name(lowcase)
system	storage	$(storage)Free	uint64	$(storage)=disk's display name(lowcase)
system	storage	$(storage)Percent	double	$(storage)=disk's display name(lowcase)

D. Appendix D

Useful Links and Upgrade Information

You can access all the reference information at: https://github.com/TPE-TIGER

Information on all device APIs is available at: https://tpe-tiger.github.io/

There are a couple of methods to upgrade the software on your AIG device. Some of the most common methods are listed below:

Method 1. Upgrade from downloaded packages (web console)

Download all the upgrade packs from https://moxa-srs.thingsprocloud.com/home to your local drive and upgrade your device from the local drive.

Method 2. Upgrade over the air (web console)

The device can receive the most recent upgrade information and then choose which patches to install. For further details, see **Software Upgrade**.

Method 3. Upgrade from the Moxa DLM tool

If you are interested in using the Moxa DLM tool on a trial basis, get in touch with a Moxa sales representative to set up a trial account.

E. Appendix E

NOTE

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance 20 cm between the radiator & your body.

This device and its antenna must not be co located or operating in conjunction with any other antenna or transmitter.

The radiated output power of the Wireless Device is below the Innovation, Science and Economic Development Canada (ISED) radio frequency exposure limits. This wireless device should be used in a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown to be compliant with the ISED RF Exposure limits under mobile exposure conditions (antennas must be at > 20 cm distance from a person's body.

La puissance de sortie rayonnée du dispositif sans fil est inférieure aux limites d'exposition aux radiofréquences d'Innovation, Sciences et Développement économique Canada (ISED). Le dispositif sans fil doit être utilisé de manière à minimiser le potentiel de contact humain pendant le fonctionnement normal.

Cet appareil a également été évalué et montré conforme aux limites d'exposition RF ISED dans des conditions d'exposition mobiles. (Les antennes sont à plus de 20 cm du corps d'une personne).