

# **AIG-502 Series User Manual**

---

**Version 1.0, April 2025**

**[www.moxa.com/products](http://www.moxa.com/products)**



© 2025 Moxa Inc. All rights reserved.

# **AIG-502 Series User Manual**

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

## **Copyright Notice**

© 2025 Moxa Inc. All rights reserved.

## **Trademarks**

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

## **Disclaimer**

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

## **Technical Support Contact Information**

[www.moxa.com/support](http://www.moxa.com/support)

# Table of Contents

|                                                |           |
|------------------------------------------------|-----------|
| <b>1. Introduction .....</b>                   | <b>5</b>  |
| Overview .....                                 | 5         |
| Package Checklist .....                        | 5         |
| Product Features .....                         | 5         |
| Hardware Specifications .....                  | 5         |
| Hardware Block Diagram .....                   | 6         |
| <b>2. Hardware Introduction .....</b>          | <b>7</b>  |
| Appearance.....                                | 7         |
| Dimensions .....                               | 8         |
| LED Indicators.....                            | 8         |
| <b>3. Hardware Connection Description.....</b> | <b>9</b>  |
| Installing the AIG-502.....                    | 9         |
| DIN-rail Mounting .....                        | 9         |
| Wall or Cabinet Mounting (DNV).....            | 10        |
| Wiring Requirements.....                       | 11        |
| Connecting the Power .....                     | 12        |
| Grounding the Unit .....                       | 12        |
| Connecting to a Network .....                  | 12        |
| Connecting to a Serial Device.....             | 13        |
| Connecting to a USB Device.....                | 14        |
| Connecting to an HDMI Device .....             | 14        |
| Installing Communications Modules.....         | 15        |
| Installing the Wi-Fi Module .....              | 16        |
| RTC Battery Replacement .....                  | 21        |
| <b>4. BIOS Setup .....</b>                     | <b>22</b> |
| Entering the BIOS Setup.....                   | 22        |
| Main Page.....                                 | 23        |
| Security Settings .....                        | 24        |
| Current TPM Device .....                       | 24        |
| TPM State.....                                 | 24        |
| Clear TPM.....                                 | 24        |
| Set Supervisor Password .....                  | 24        |
| Boot Settings .....                            | 25        |
| USB Boot .....                                 | 25        |
| EFI .....                                      | 25        |
| Exit Settings .....                            | 26        |
| Exit Saving Changes .....                      | 26        |
| Save Change Without Exit .....                 | 26        |
| Exit Discarding Changes.....                   | 26        |
| Load Optimal Defaults.....                     | 26        |
| Discard Changes .....                          | 27        |
| <b>5. Getting Started .....</b>                | <b>28</b> |
| Connecting the Power .....                     | 28        |
| Connecting Serial Devices.....                 | 28        |
| Connecting to a Network .....                  | 28        |
| Access to the Web Console .....                | 29        |
| <b>6. Web Console.....</b>                     | <b>30</b> |
| Dashboard .....                                | 30        |
| System Dashboard .....                         | 30        |
| Network Dashboard .....                        | 30        |
| Tag Dashboard.....                             | 32        |
| Security Dashboard .....                       | 34        |
| System Settings .....                          | 35        |
| General.....                                   | 35        |
| Serial.....                                    | 37        |
| External Storage .....                         | 38        |
| Network Settings .....                         | 39        |
| Ethernet.....                                  | 39        |

|                                                             |            |
|-------------------------------------------------------------|------------|
| Cellular .....                                              | 41         |
| Wi-Fi Client.....                                           | 43         |
| Cloud Connectivity .....                                    | 44         |
| Azure IoT Edge .....                                        | 44         |
| Fieldbus Protocol .....                                     | 71         |
| Modbus Master.....                                          | 71         |
| Security.....                                               | 84         |
| Certificate Center .....                                    | 84         |
| Firewall .....                                              | 84         |
| HTTPS.....                                                  | 87         |
| Login Lockout .....                                         | 87         |
| Session Management .....                                    | 88         |
| System Use Notification .....                               | 89         |
| Account Management.....                                     | 89         |
| Accounts .....                                              | 89         |
| Roles .....                                                 | 91         |
| Password Policy.....                                        | 92         |
| Service .....                                               | 93         |
| Reboot.....                                                 | 93         |
| Config. Import/Export.....                                  | 94         |
| Backup & Restore.....                                       | 94         |
| Software Upgrade .....                                      | 95         |
| Reset to Default .....                                      | 97         |
| Device Retirement.....                                      | 97         |
| Diagnostics .....                                           | 98         |
| System Log .....                                            | 98         |
| Audit Log .....                                             | 98         |
| Protocol Status .....                                       | 99         |
| <b>7. Security Capability.....</b>                          | <b>101</b> |
| Communication Integrity and Authentication .....            | 101        |
| Account Management.....                                     | 101        |
| Login Policy.....                                           | 102        |
| Secure Boot and Disk Encryption .....                       | 102        |
| Managing Resources .....                                    | 104        |
| Audit Logs .....                                            | 104        |
| Security Advisories .....                                   | 105        |
| <b>8. Security Hardening Guide .....</b>                    | <b>106</b> |
| Communication Integrity and Authentication .....            | 106        |
| Potential Threats and Corresponding Security Measures ..... | 107        |
| Installation .....                                          | 108        |
| <b>A. Appendix A .....</b>                                  | <b>110</b> |
| Publish Modes .....                                         | 110        |
| <b>B. Appendix B .....</b>                                  | <b>111</b> |
| Useful Links and Upgrade Information .....                  | 111        |
| <b>C. Audit Log Index .....</b>                             | <b>112</b> |
| Account & Access.....                                       | 112        |
| Configuration Update .....                                  | 112        |
| Connection & Interface.....                                 | 113        |
| Command & Message.....                                      | 113        |
| Maintenance .....                                           | 114        |
| Performance & Health .....                                  | 115        |
| <b>D. System Tag List .....</b>                             | <b>116</b> |
| <b>E. Regulatory Approval Statement.....</b>                | <b>117</b> |

# 1. Introduction

---

## Overview

The AIG-502 Series advanced IIoT gateways are built around a powerful 7th Gen Intel® Core™ i7 processor, featuring versatile connectivity options with 1 HDMI display port, 3 USB 3.0 ports, 2 gigabit LAN ports, and 2 3-in-1 RS-232/422/485 serial ports. Equipped with a 2.5" HDD/SSD slot and a built-in TPM 2.0 module, the AIG-502 is designed to deliver reliable performance in harsh environments, including extreme temperatures, humidity, vibration, and power surges. Tailored for Industrial IoT applications, it seamlessly integrates Modbus RTU/TCP protocols for easy data collection from Modbus devices and comes preloaded with Azure IoT Edge, enabling secure sensor-to-cloud connectivity. Ideal for heavy industry, solar grids, water/wastewater, oil and gas, and transportation applications, the AIG-502 Series ensures robust and efficient data acquisition even in distributed and unmanned sites.

## Package Checklist

- AIG-502 embedded computer
- Terminal block to power jack converter
- DIN-rail mounting kit
- Quick installation guide (printed)
- Warranty card
- Tamper-resistant label



### NOTE

Please notify your sales representative if any of the above items are missing or damaged.

## Product Features

AIG-502 embedded computers come with the following:

- Mini-PCIe sockets for Wi-Fi expansion modules
- 7th Gen Intel® Core™ processor (Kaby Lake U)
- Built-in 32GB DDR4 memory
- ATEX and IECEx Zone 2 compliance
- Built-in TPM 2.0 module
- Variety of interfaces: 2 serial ports, 2 Giga LANs, 3 USB 3.0 (type A) ports

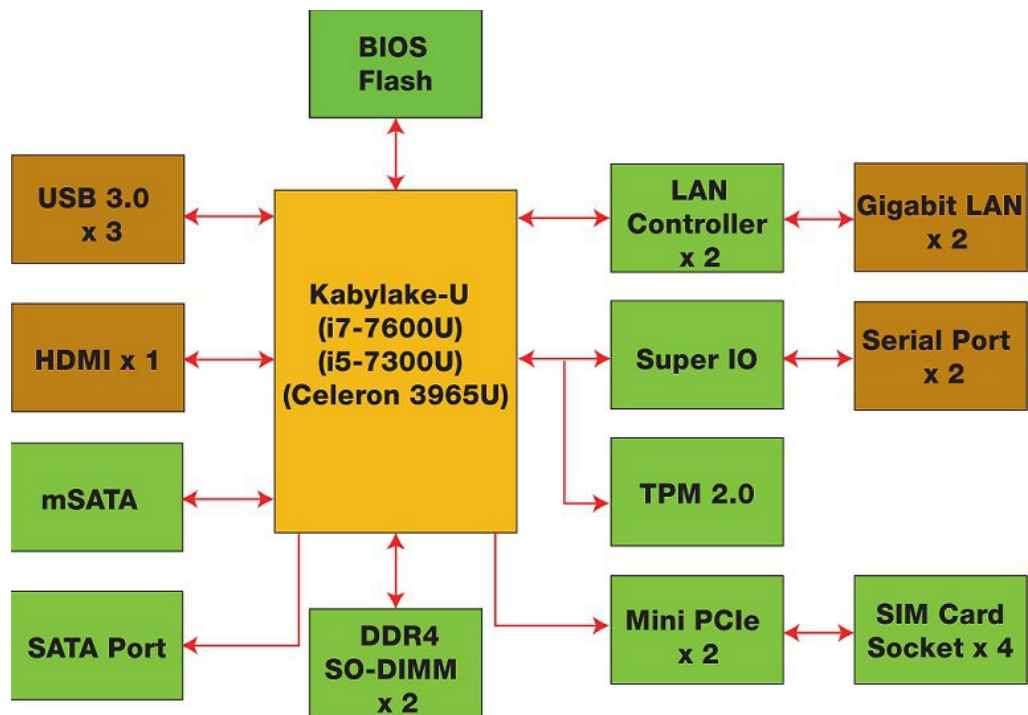
## Hardware Specifications



### NOTE

The latest specifications for Moxa's products can be found at <https://moxa.com>.

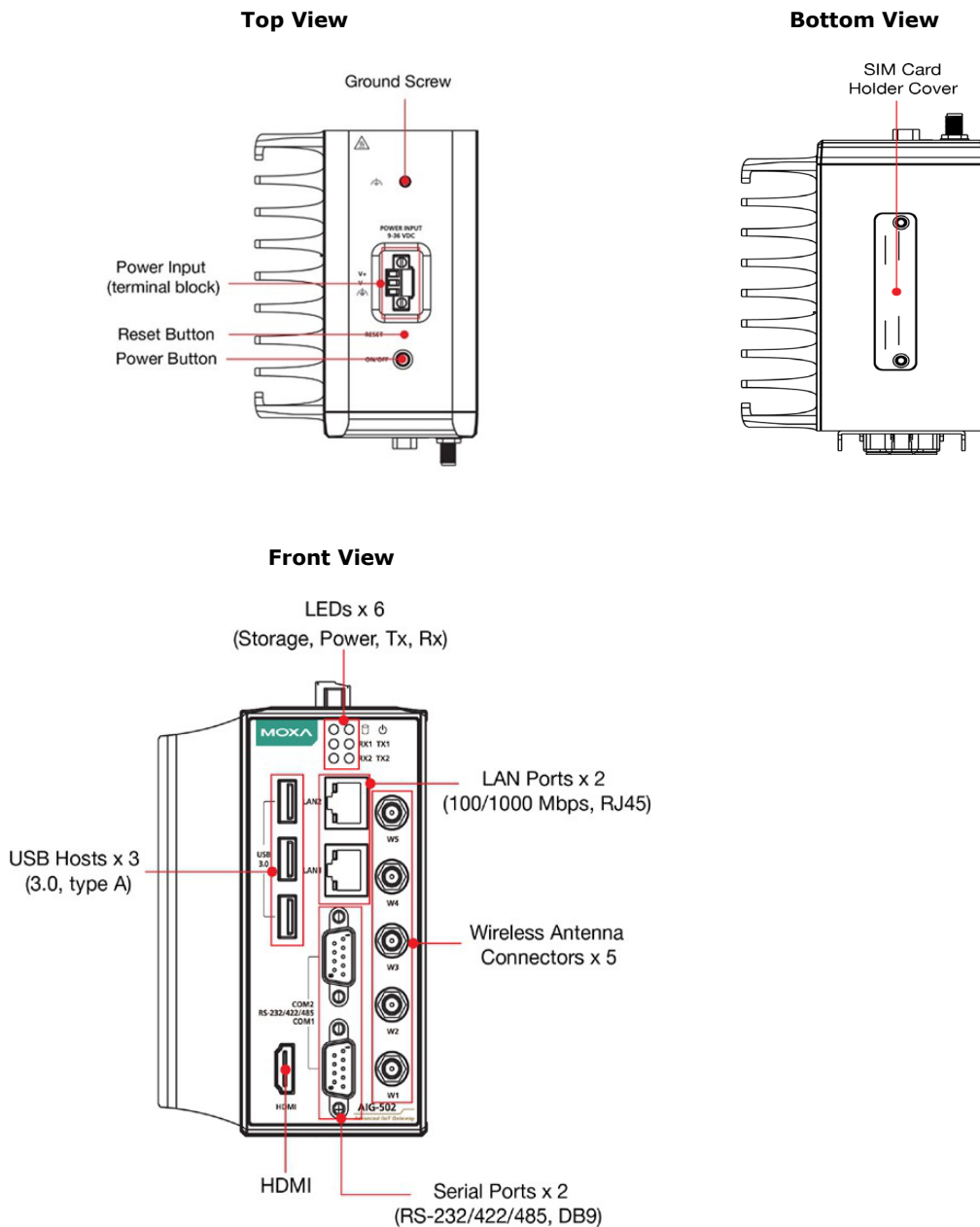
# Hardware Block Diagram



## 2. Hardware Introduction

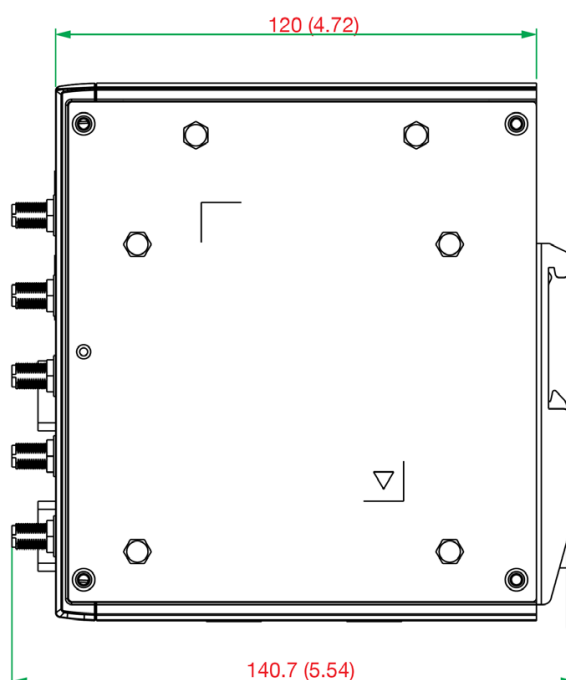
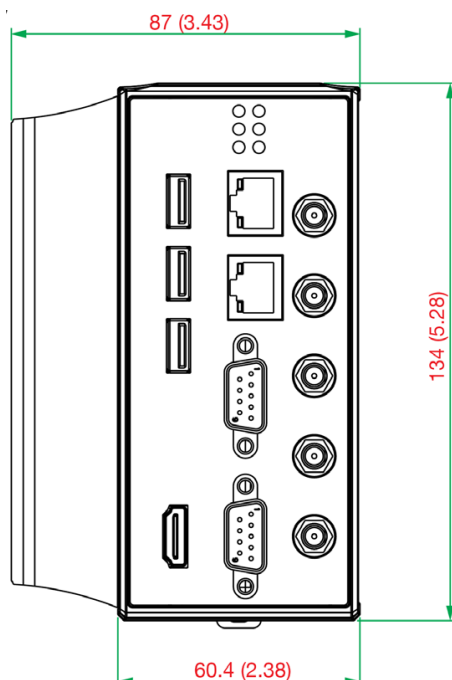
The AIG-502 Series embedded computers are compact, well designed, and rugged enough for industrial applications. LED indicators help you monitor the performance and identify trouble spots. Multiple serial ports allow you to connect different devices for wireless operation and the reliable and stable hardware platform lets you devote your attention to developing your applications.

### Appearance



# Dimensions

Unit: mm (inch)



## LED Indicators

| LED Name                                                                                                 | Status | Function                                                                  |
|----------------------------------------------------------------------------------------------------------|--------|---------------------------------------------------------------------------|
| Power<br>             | Green  | Power is on and computer is functioning normally                          |
|                                                                                                          | Off    | Power is off                                                              |
| Storage 1 (mSATA)<br> | Yellow | Blinking: Data transmission                                               |
|                                                                                                          | Off    | No data transmission.                                                     |
| LAN 1/2<br>(Located on connectors)                                                                       | Green  | Steady On: 100 Mbps Ethernet link<br>Blinking: Data is being transmitted  |
|                                                                                                          | Yellow | Steady On: 1000 Mbps Ethernet link<br>Blinking: Data is being transmitted |
|                                                                                                          | Off    | 10 Mbps Ethernet link or LAN is not connected                             |
| Tx 1/2                                                                                                   | Green  | Blinking: Data is being transmitted                                       |
|                                                                                                          | Off    | No connection                                                             |
| Rx 1/2                                                                                                   | Yellow | Blinking: Data is being transmitted                                       |
|                                                                                                          | Off    | No connection                                                             |

## 3. Hardware Connection Description

---

In this chapter, we describe how to connect the embedded computer to the network and to various devices.

### Installing the AIG-502

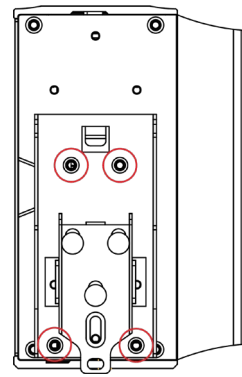
#### DIN-rail Mounting

The AIG-502 comes with a DIN-rail mounting kit for installing the computer on a DIN rail.

##### Installation

**STEP 1:**

Use the 4 screws included with the kit to attach the DIN-rail mounting bracket to the AIG-502's rear panel and tighten the screws to secure the bracket to the AIG-502.

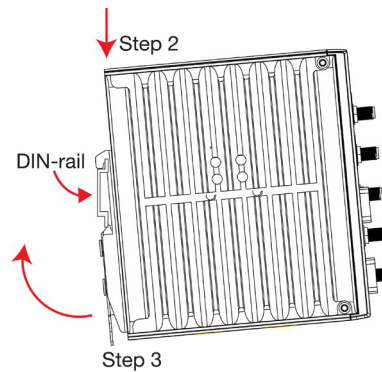


**STEP 2:**

Insert the top of the DIN rail into the slot just below the upper hook of the DIN-rail mounting kit.

**STEP 3:**

Press the AIG-502 towards the DIN rail until it snaps into place.



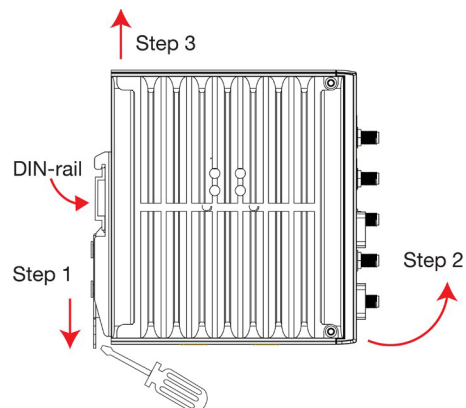
## Removal

### STEP 1:

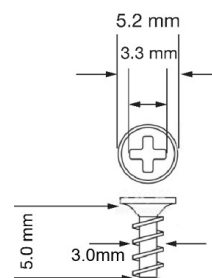
Pull down the latch on the mounting kit with a screwdriver.

### STEP 2 & 3:

Slightly pull the AIG-502 forward and lift it up to remove it from the DIN rail.



For the specifications of the DIN-rail mounting screws, refer to the illustrations on the right and adhere to these values to tighten the DIN-rail bracket on to the rear of the computer.



## Wall or Cabinet Mounting (DNV)

Use the optional wall-mounting kit to install the AIG-502 on to a wall.

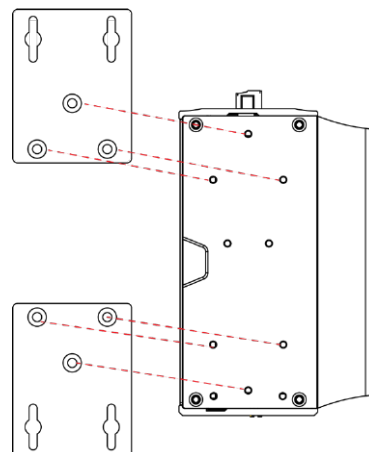


### NOTE

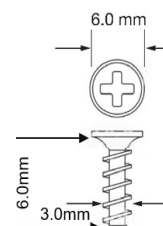
The wall-mounting kit can be purchased separately.

### STEP 1:

Use three screws for each bracket and attach the brackets to the rear of the AIG-502.



Refer to the figure on the right for the specifications of the screws used to attach the brackets.



**STEP 2:**

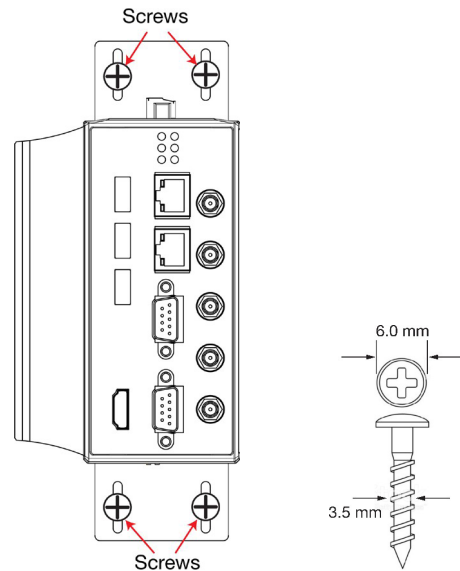
Use two screws per bracket to attach the AIG-502 to a wall or cabinet.

**NOTE:**

Mounting the AIG-502 to a wall requires four screws. Use the AIG-502 computer, with the optional wall-mounting brackets attached, as a guide to mark the correct locations of the screws on the wall.

The heads of the screws should be less than 6.0 mm in diameter, the shafts should be less than 3.5 mm as shown in the figure on the right. The recommended length of the screw is more than 10 mm.

Do not drive the screws in all the way; leave a space of about 2 mm to allow room for sliding the wall-mounting bracket between the wall and the screws.



## Wiring Requirements

In this section, we describe how to connect serial devices to the AIG-502 embedded computer.

Be sure to read and follow these common safety precautions before proceeding with the installation of any electronic device:

- Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the crossing point.

**NOTE**

Do not run signal or communication wiring together with power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.

- Use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separated.
- For future reference, you should label the wiring used for all of your devices.

**ATTENTION****Safety First!**

Be sure to disconnect the power cord before installing and/or wiring your AIG-502.

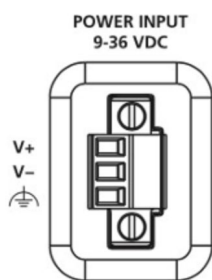
**Wiring Caution!**

Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size. If the current value goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.

**Temperature Caution!**

Be careful when handling the unit. When the unit is plugged in, the internal components generate heat, and consequently the outer casing may feel hot to the touch.

## Connecting the Power



Use an LPS (9-36 VDC) or Class 2 power cord to connect to the AIG-502's terminal block to power jack converter and then turn on the power. If the power is supplied properly, the Power LED will light up. The OS is ready when the Power LED is solid green.

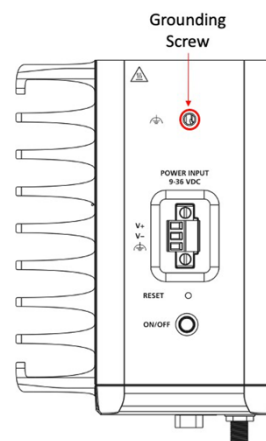


### ATTENTION

This product is intended to be supplied by a Listed Power Supply with output marked LPS and rated to deliver 9 to 36 VDC at a minimum of 8 A. Ensure that the power cord is connected to a socket-outlet with earthing connection, or an equivalent.

## Grounding the Unit

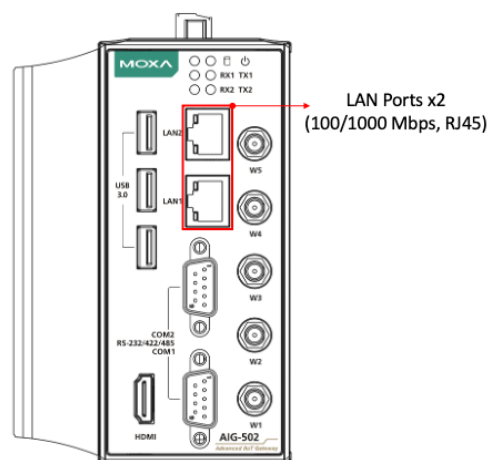
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the grounding screw (M4) to the grounding surface prior to connecting the power.



## Connecting to a Network

To connect the AIG-502 computer to a network, connect a network cable to the embedded computer's Ethernet port and connect the other end of the cable to your Ethernet network. When the cable is properly connected, the LEDs on the embedded computer's Ethernet port turn on to indicate a valid connection.

Two 10/100/1000 Mbps Ethernet ports with RJ45 connectors are located on the front panel of the embedded computer. Refer to the illustration in the right for the location of the Ethernet ports.





## NOTE

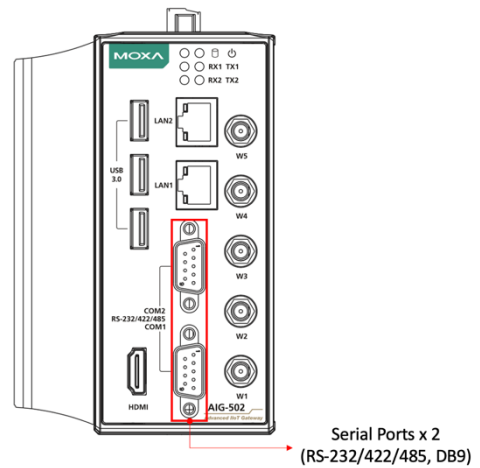
The pin assignments for the AIG-502 computer's Ethernet port are shown in the following figure. If you want to use your own Ethernet cable, ensure that you match the pin assignments of the connector on the Ethernet cable.

|                                                                                           |   |  |  |
|-------------------------------------------------------------------------------------------|---|--|--|
| <br>LAN2 | 1 |  |  |
|                                                                                           | 8 |  |  |
|                                                                                           | 1 |  |  |
|                                                                                           | 8 |  |  |
| <br>LAN1 | 1 |  |  |
|                                                                                           | 8 |  |  |
|                                                                                           | 1 |  |  |
|                                                                                           | 8 |  |  |

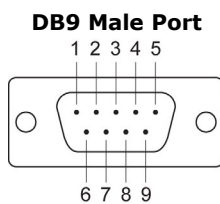
| Pin | 10/100 Mbps | 1000 Mbps |
|-----|-------------|-----------|
| 1   | ETx+        | TRD(0)+   |
| 2   | ETx-        | TRD(0)-   |
| 3   | ERx+        | TRD(1)+   |
| 4   | -           | TRD(2)+   |
| 5   | -           | TRD(2)-   |
| 6   | ERx-        | TRD(1)-   |
| 7   | -           | TRD(3)+   |
| 8   | -           | TRD(3)-   |

## Connecting to a Serial Device

Use a serial cable to connect your serial device to the embedded computer's serial port. The serial ports P1 to P2 have male DB9 connectors and can be configured for RS-232, RS-422, or RS-485 communication. For information on serial port configuration, refer to the *AIG-502 software manual*.



The pin assignments of the serial ports are shown in the following table:

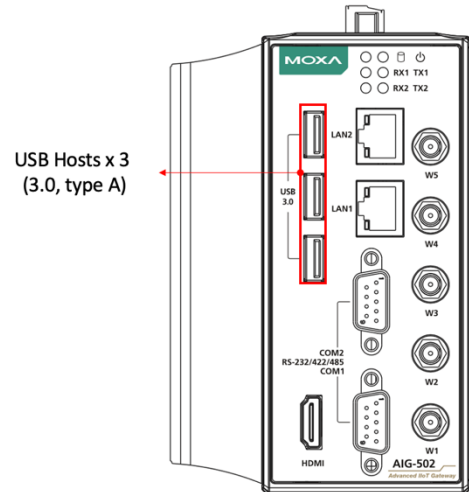


### RS-232/422/485 Pinouts

| Pin | RS-232 | RS-422  | RS-485 (4-wire) | RS-485 (2-wire) |
|-----|--------|---------|-----------------|-----------------|
| 1   | DCD    | TxDA(-) | TxDA(-)         | -               |
| 2   | RxD    | TxDB(+) | TxDB(+)         | -               |
| 3   | TxD    | RxDB(+) | RxDB(+)         | DataB(+)        |
| 4   | DTR    | RxDA(-) | RxDA(-)         | DataA(-)        |
| 5   | GND    | GND     | GND             | GND             |
| 6   | DSR    | -       | -               | -               |
| 7   | RTS    | -       | -               | -               |
| 8   | CTS    | -       | -               | -               |

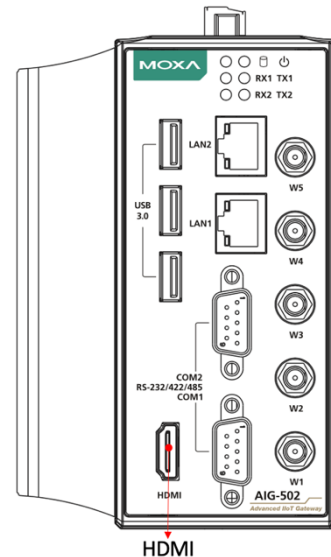
## Connecting to a USB Device

The AIG-502 is provided with three USB 3.0 ports with type-A connectors on the front panel. These ports can be used to connect to an external flash disk or hard drive. You can also use these USB ports to connect to a keyboard or a mouse.



## Connecting to an HDMI Device

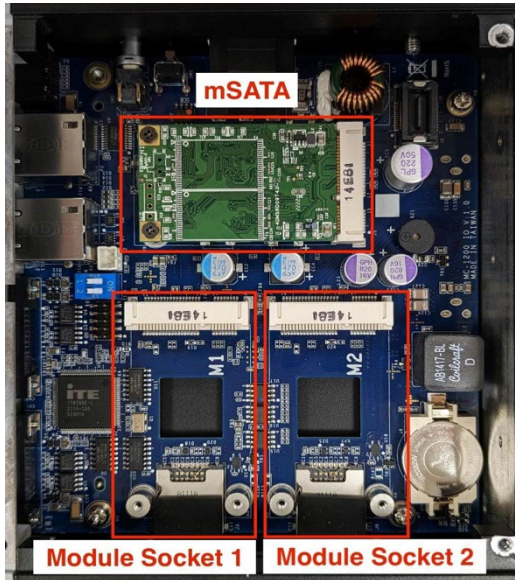
The AIG-502 Series offers an HDMI connector located on the front panel, allowing users to connect to an audio or video device. Make sure you use an HDMI-certified cable for a reliable audio or video connection.



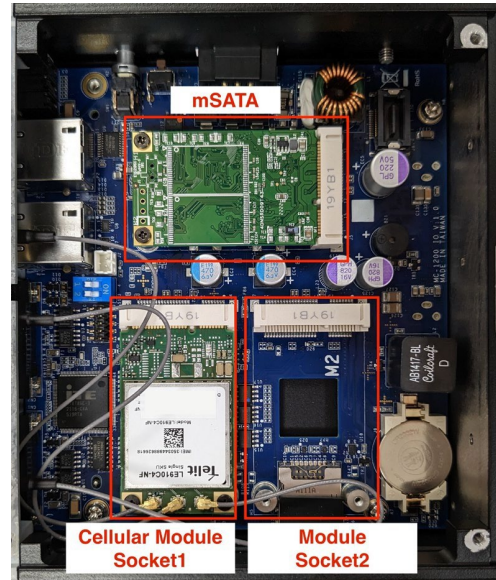
# Installing Communications Modules

The AIG-502 Series comes with three sockets for installing various communications modules. Unfasten the screws on the right side of the computer and remove the cover to find the locations of the sockets as indicated in the following images:

**AIG-502-T-AZU-LX**



**AIG-502-T-US/EU/AP-AZU-LX**

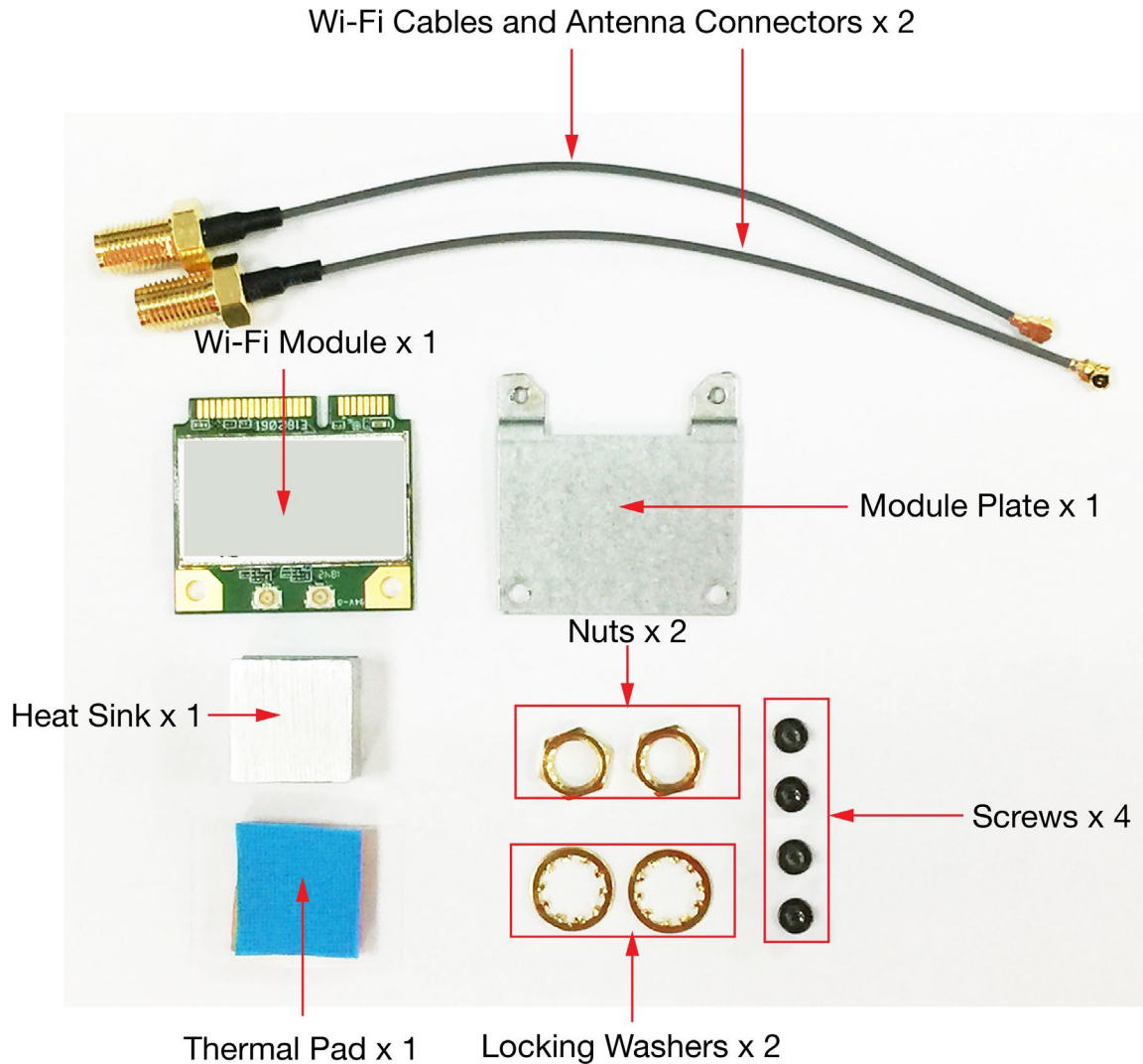


## Installing the Wi-Fi Module

The AIG-502 comes with two sockets for users to install a Wi-Fi module for wireless communication.

### Wi-Fi Module Package

The contents of the Wi-Fi module package are shown in the following image:

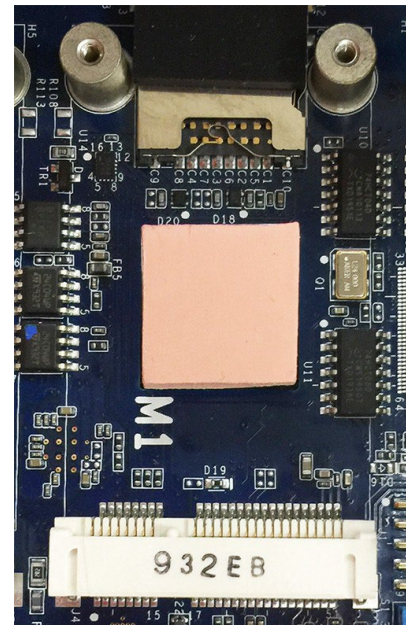


Follow these steps to install the Wi-Fi module in the AIG-502.

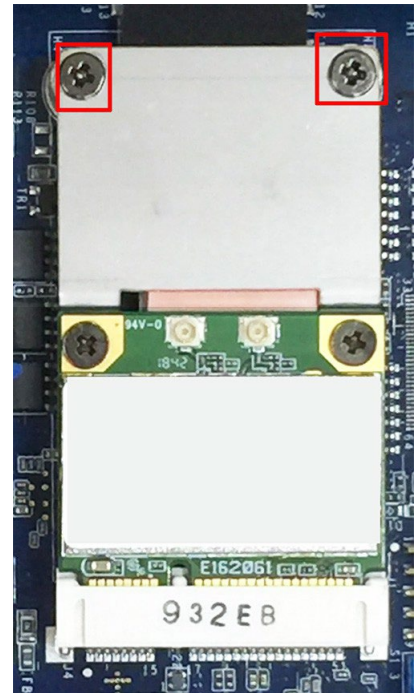
1. Attach the Wi-Fi module to the mounting plate with two screws.



2. Remove the transparent plastic and the blue cover on both sides of the thermal pad and then place it on the top heat sink. Also, remove the blue cover on the heat sink.
3. Place the heat sink with the thermal pad at the center of the wireless module socket.

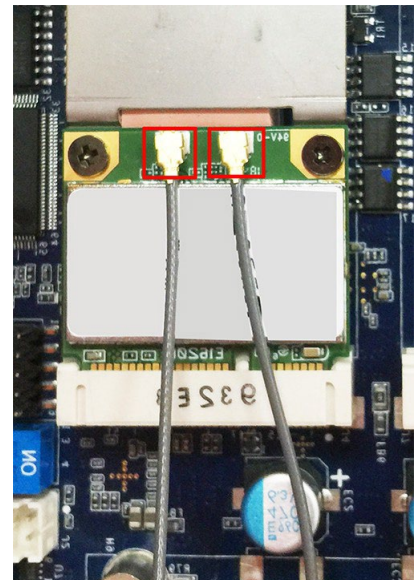


4. Insert the Wi-Fi module (with the mounting plate) into the socket and fasten the two black screws on the mounting plate to secure it.

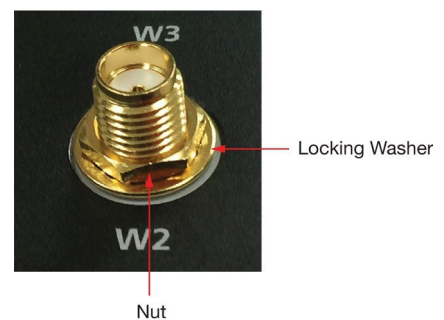


5. Attach one end of the Wi-Fi antenna cable to the connector on the Wi-Fi module and the insert the other end (with the threaded connection ring) through the antenna mounting hole on the front panel of the computer.

Remove the protection cover on the mounting hole before you do so.



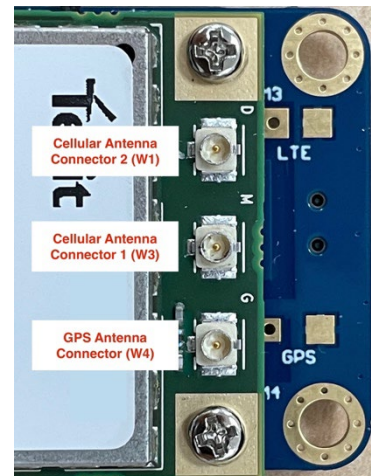
6. Insert the locking washer through the threaded connection ring and hold it against the front panel. Secure the antenna connector in place by tightening a nut onto the threaded protection ring.



7. Connect the Wi-Fi antenna to the connector on the front panel.
8. Use this method to connect another Wi-Fi antenna, if necessary.
9. Reattach the right side cover on to the computer and fasten the screws to secure it.



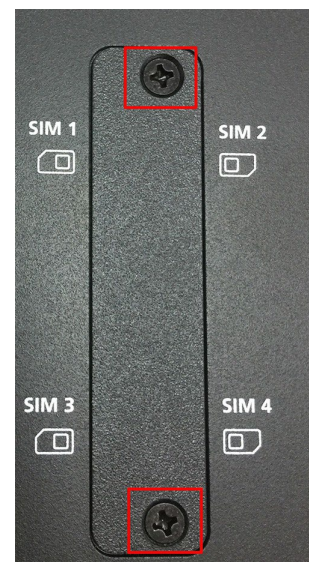
The pre-built cellular module comes with three connectors for a GPS antenna (W4), a primary cellular antenna (W3), and a secondary cellular antenna (W1).



## Installing SIM Cards

Follow these steps to install SIM cards for a cellular module.

1. Remove the screws on the bottom panel of the computer and remove the cover. You will see four SIM card slots.

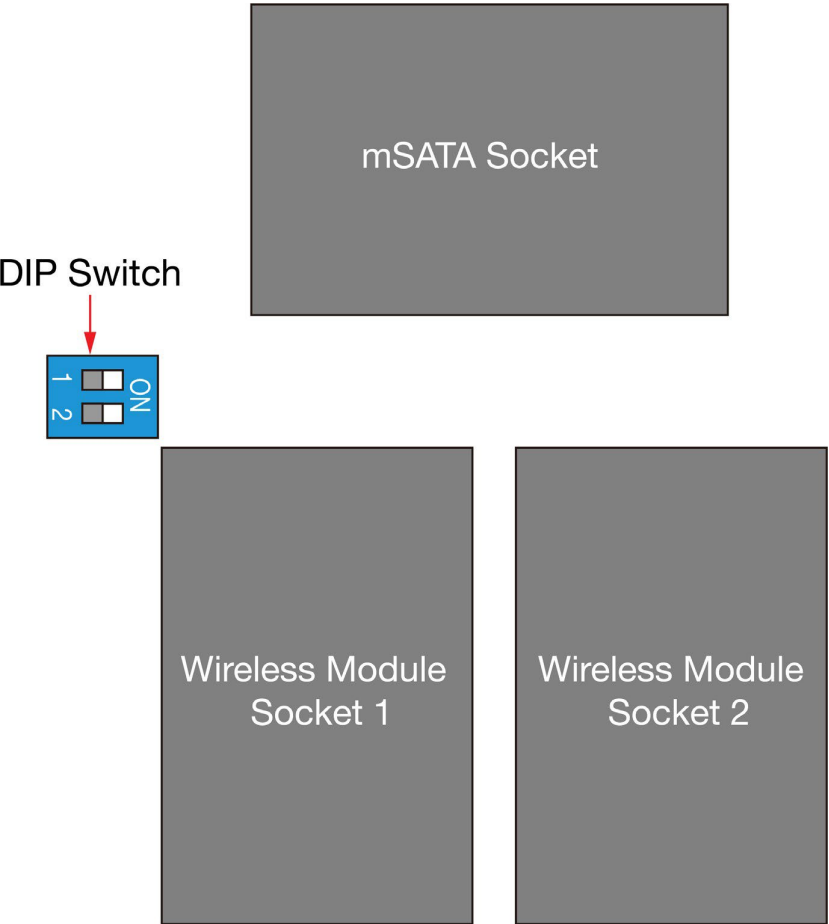


- 2. Insert a card into the SIM 1 slot. Make sure you insert the card in the right direction as indicated in the image beside the slot.
- 3. Insert the other card into the SIM 2 slot, if necessary.
- 4. Replace the computer cover and secure it by fastening the screws.

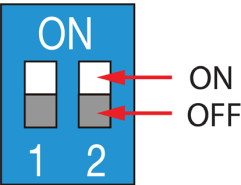


Switching Between the Wireless Module Sockets

As there are two wireless module sockets and you can install a Wi-Fi in both these sockets, a DIP switch is provided to enable selection of the Wi-Fi or cellular module installed. The DIP switch is located below the mSATA socket as shown in the following illustration.



The operation of the DIP switch is as follows:



| Status        | Switch 1 | Switch 2 |
|---------------|----------|----------|
| ON            | Wi-Fi    | Wi-Fi    |
| OFF (default) | Cellular | Cellular |

For example, if you have installed a Wi-Fi module in the first socket, you need to turn the DIP switch 1 to the ON status.



## NOTE

- For AIG-502-T-AZU-LX, you can install the Wi-Fi module in either of the sockets, and turn the corresponding socket ON after installation.
- For AIG-502-T-US/EU/AP-AZU-LX, turn the socket 2 ON after the Wi-Fi module is installed.

# RTC Battery Replacement

The AIG-502's real-time clock is powered by a lithium battery. We strongly recommend that you do not replace the lithium battery without help from a qualified Moxa support engineer. If you need to change the battery, contact the Moxa RMA service team.



## ATTENTION

There is a risk of explosion if the battery is replaced by an incorrect type of battery.



## NOTE

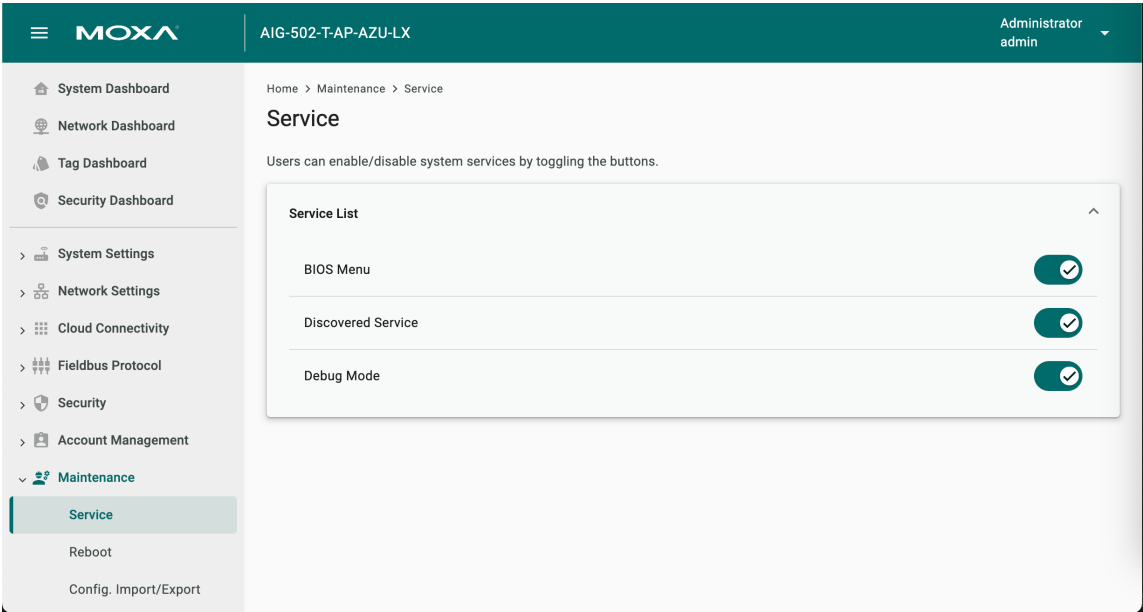
The AIG-502 embedded computer can be customized to support an easy RTC battery replacement function. Please contact your Moxa sales representative for details.

# 4. BIOS Setup

In this chapter, we describe the BIOS settings for the AIG-502 embedded computer. The BIOS firmware helps boot up the system before the operating system is loaded. All the configurations are stored in the flash ROM.

## Entering the BIOS Setup

First, you need to enable BIOS option through the AIG-502 Web Console. You may refer the user manual to configure it by following this path: **Maintenance > Service > BIOS Menu**.

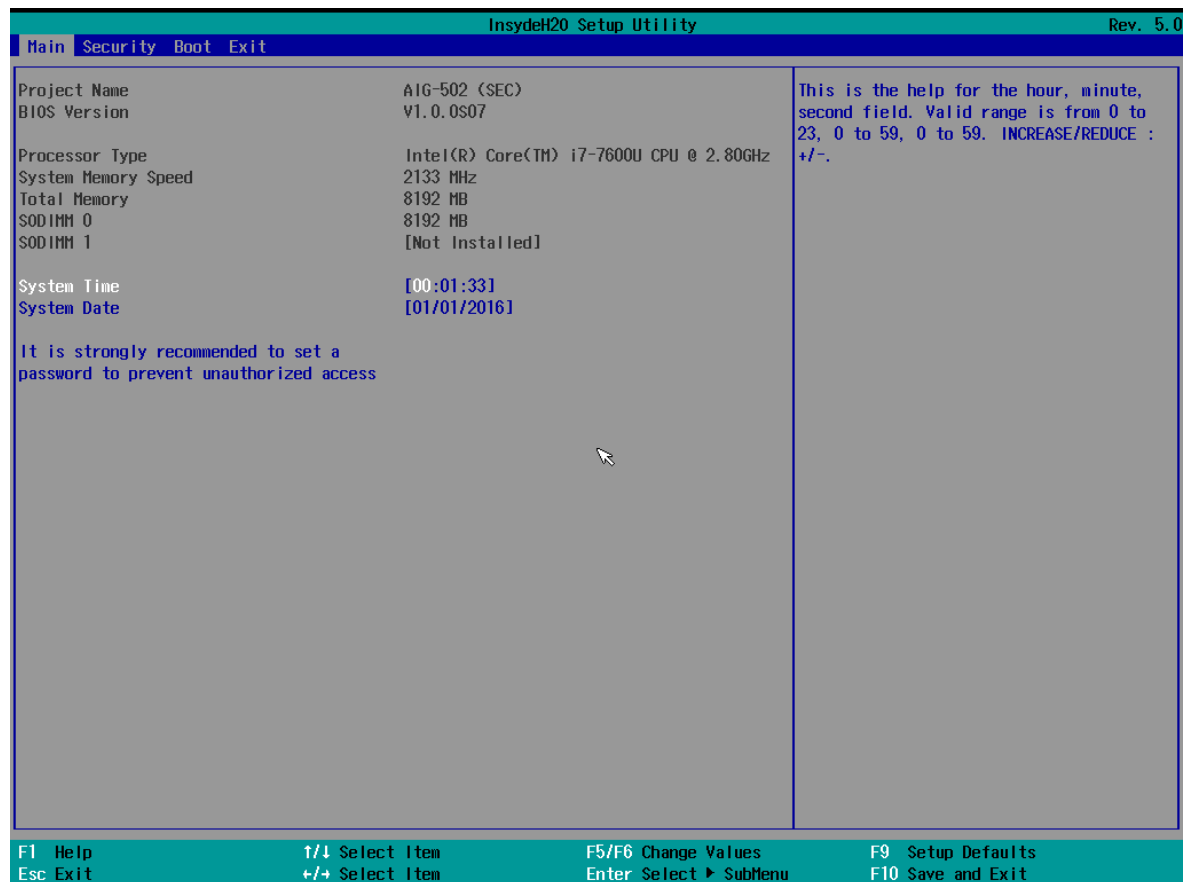


To enter the BIOS setup utility, press the **F2** key while the system is booting up.

# Main Page

The **Main** page displays basic system hardware information, such as model name, BIOS version, and CPU type.

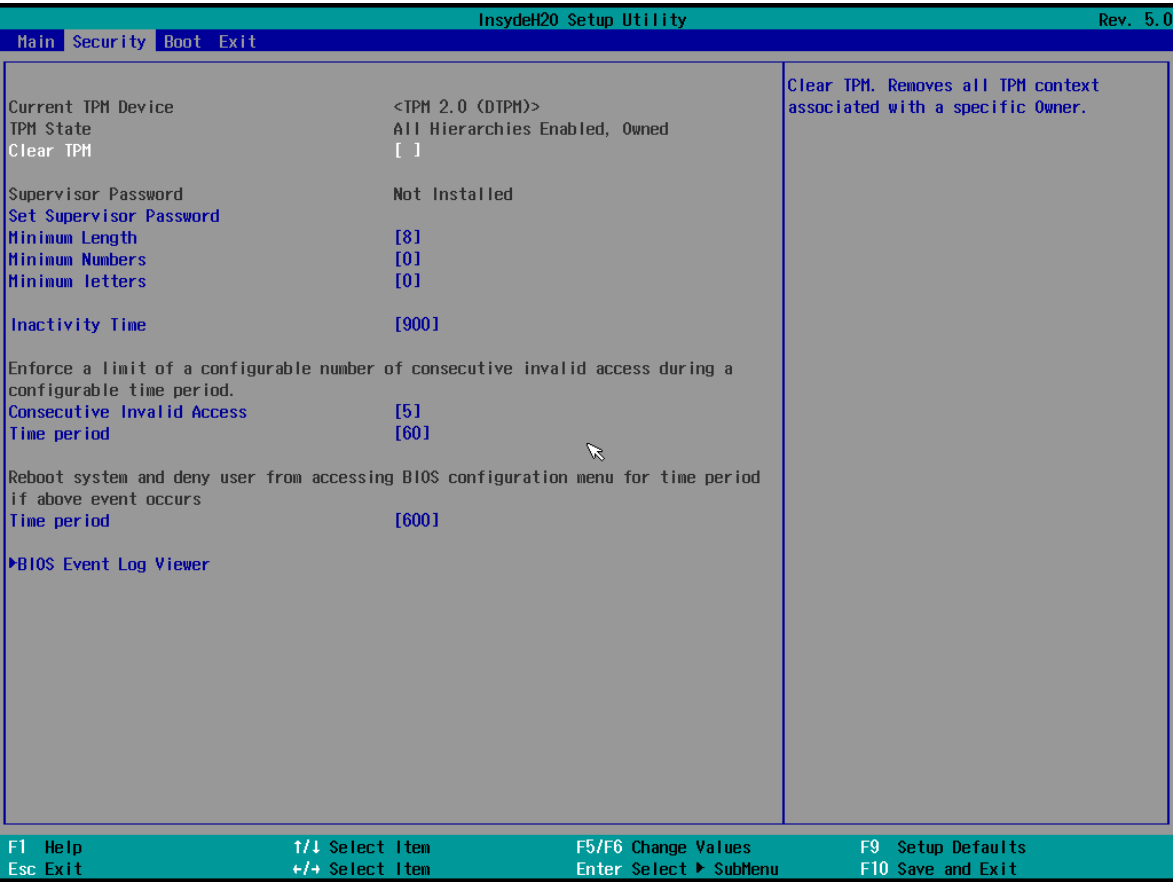
To enter the BIOS, use the default password, which is the product's serial number. You can find the serial number on the product label on the device's cover.



|              |                       |              |                                 |
|--------------|-----------------------|--------------|---------------------------------|
| <b>F1</b>    | <b>General Help</b>   | <b>↑ ↓ .</b> | <b>Select Item</b>              |
| <b>F5/F6</b> | <b>Change Values</b>  | <b>← →</b>   | <b>Select Menu</b>              |
| <b>F9</b>    | <b>Setup Defaults</b> | <b>ESC</b>   | <b>Exit</b>                     |
| <b>F10</b>   | <b>Save and Exit</b>  | <b>ENTER</b> | <b>Select or go to Submenu.</b> |

# Security Settings

This section allows users to configure security-related settings with a supervisor password.



## Current TPM Device

This item shows if the system has TMP device and its type.

## TPM State

This item allows you view the status of current TPM settings.

## Clear TPM

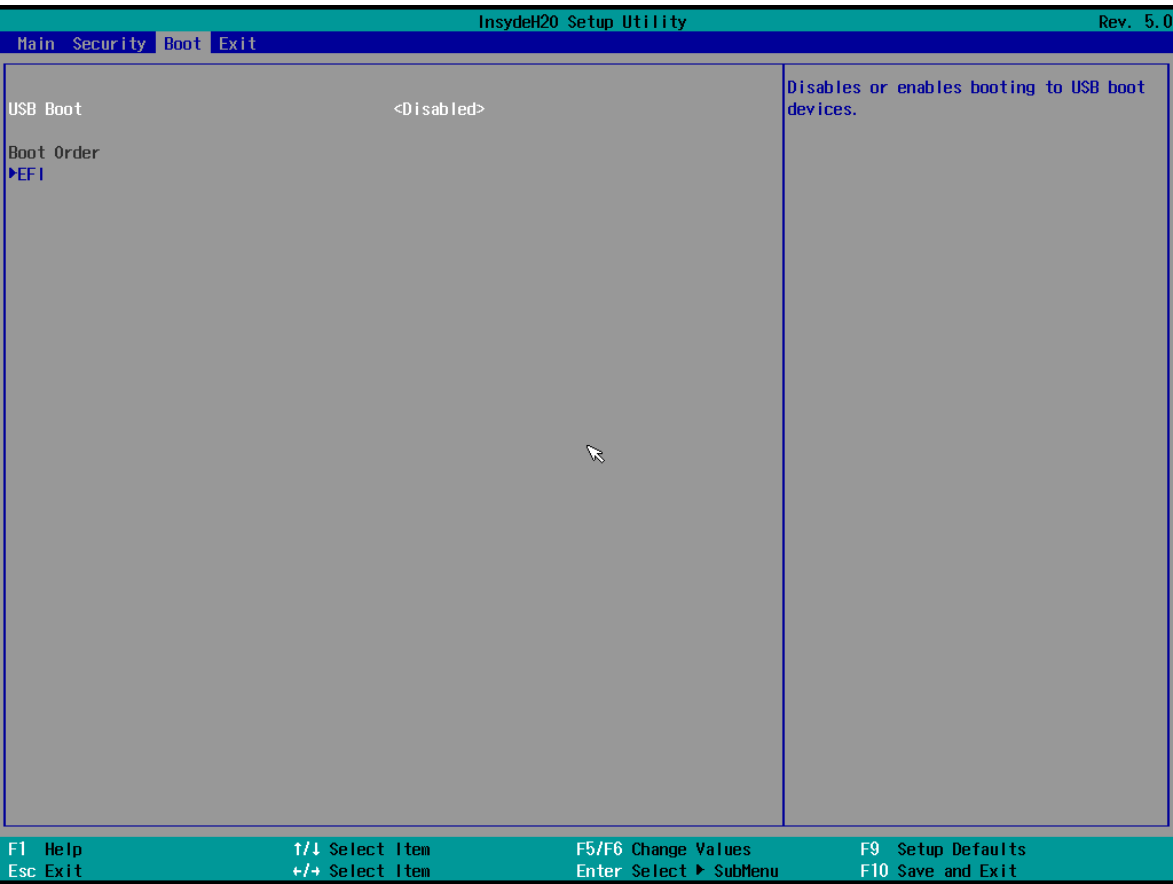
This item allows users to remove all TPM context associated with a specific owner.

## Set Supervisor Password

This item allows you to set the supervisor password. Select the **Set Supervisor Password** option and enter the password and confirm the password again.

# Boot Settings

The section allows users to configure boot settings.



## USB Boot

Set booting to USB boot devices capability.

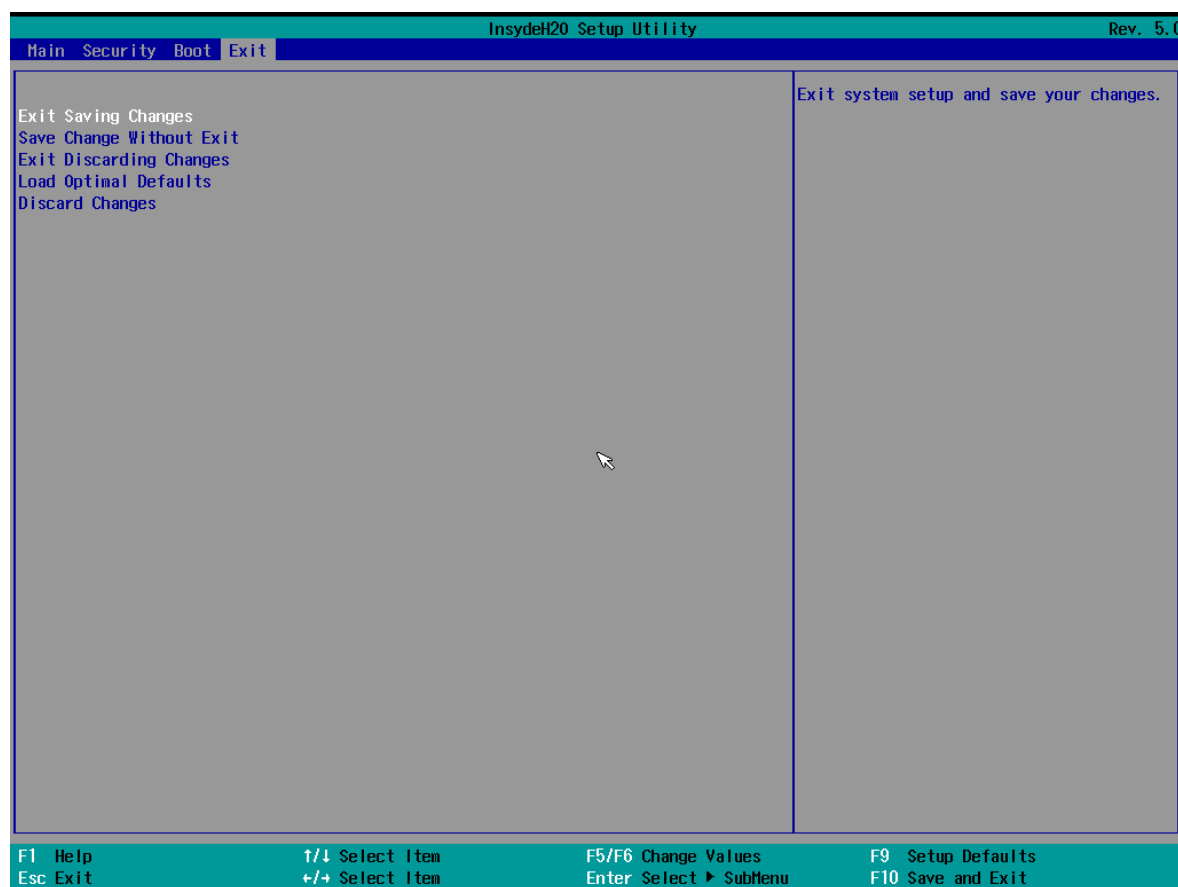
Options: Enabled, Disabled (Default)

## EFI

This item allows users to select the boot order. Use F5 (move down) or F6 (move up) to change the value.

# Exit Settings

The section allows users to exit the BIOS environment.



## Exit Saving Changes

This item allows you to exit the BIOS environment and save the values you have just configured.

Options: Yes (default), No

## Save Change Without Exit

This item allows you to save changes without exiting the BIOS environment.

Options: Yes (default), No

## Exit Discarding Changes

This item allows you to exit without saving any changes that might have been made to the BIOS.

Options: Yes (default), No

## Load Optimal Defaults

This item allows you to revert to the factory default BIOS values.

Options: Yes (default), No

## Discard Changes

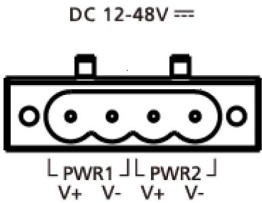
This item allows you to discard all settings you have just configured.

Options: Yes (default), No

# 5. Getting Started

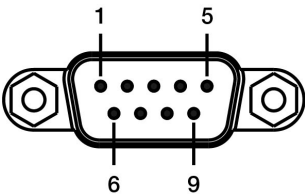
## Connecting the Power

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 are shown in the following table:



| 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-502 Series Quick Installation Guide*.

# Access to the Web Console

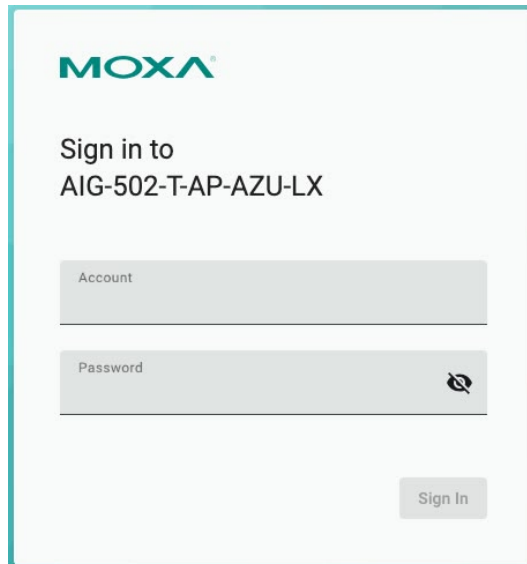
The default LAN2 IP address to access the web console of the AIG is 192.168.4.127.

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

2. 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.
3. Read the system notification and click **Agree and Continue**.
4. Enter the account and password information.

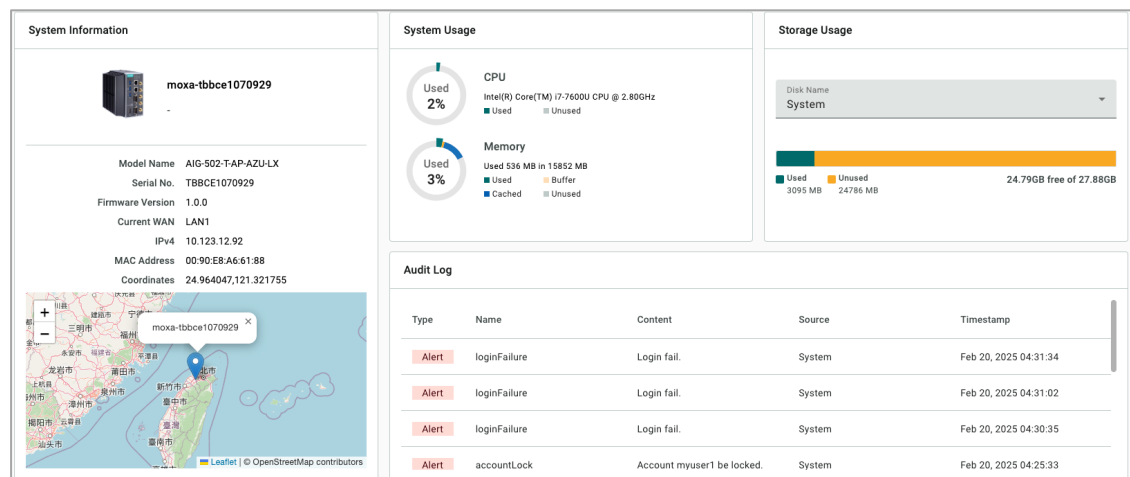
Default account: **admin**

Password: **admin@123**



The image shows the login interface of the MOXA AIG-502-T-AP-AZU-LX. It features the MOXA logo at the top, followed by the text "Sign in to AIG-502-T-AP-AZU-LX". Below this, there are two input fields: "Account" and "Password". The "Password" field has a toggle icon for visibility. At the bottom right, there is a "Sign In" button.

You will see the following homepage after logging in successfully.



## NOTE

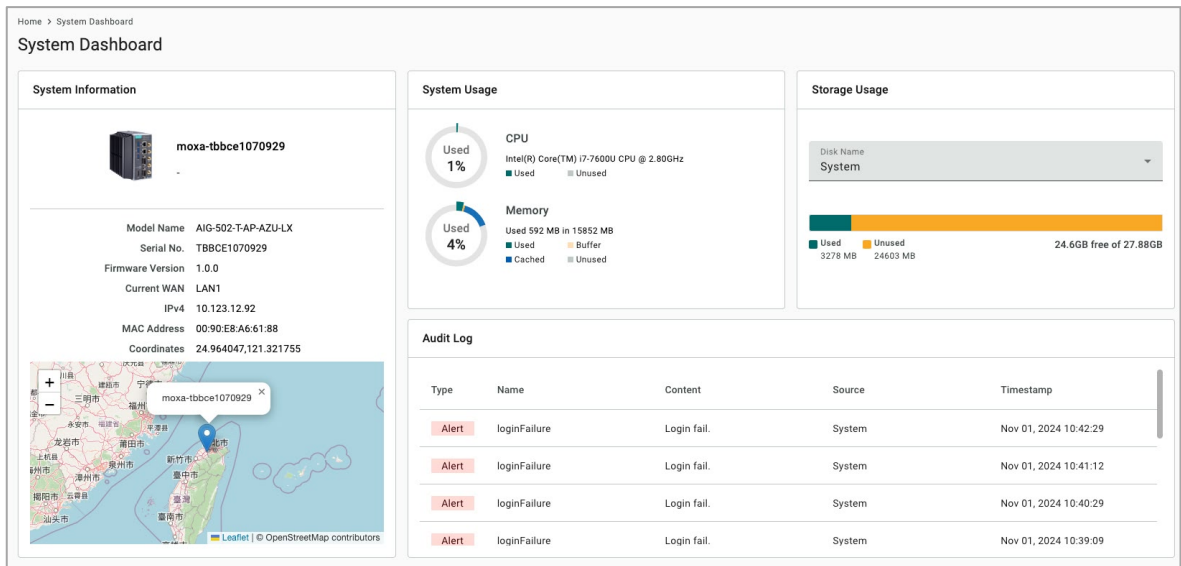
After the first login, we force a password change to comply with general security policies and practices and to increase the security of your device.

## 6. Web Console

### Dashboard

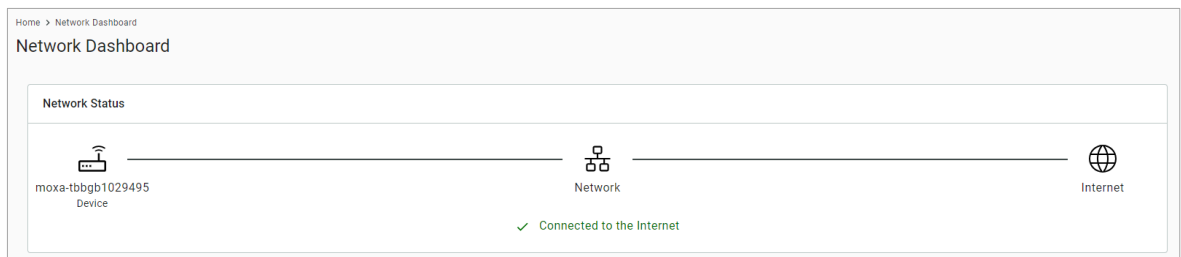
#### System Dashboard

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



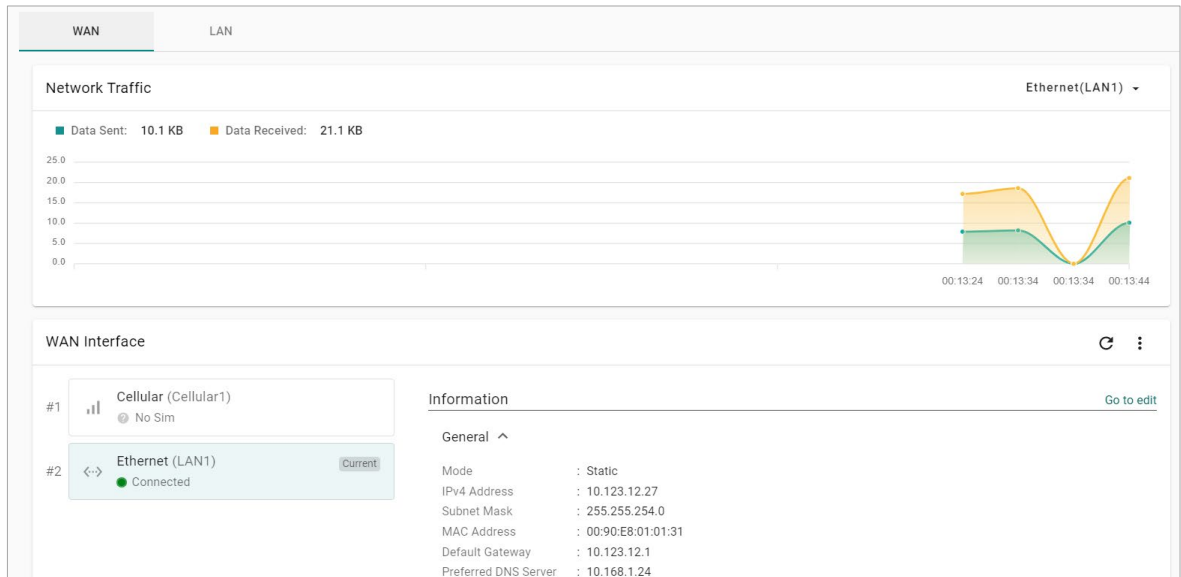
#### Network Dashboard

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.



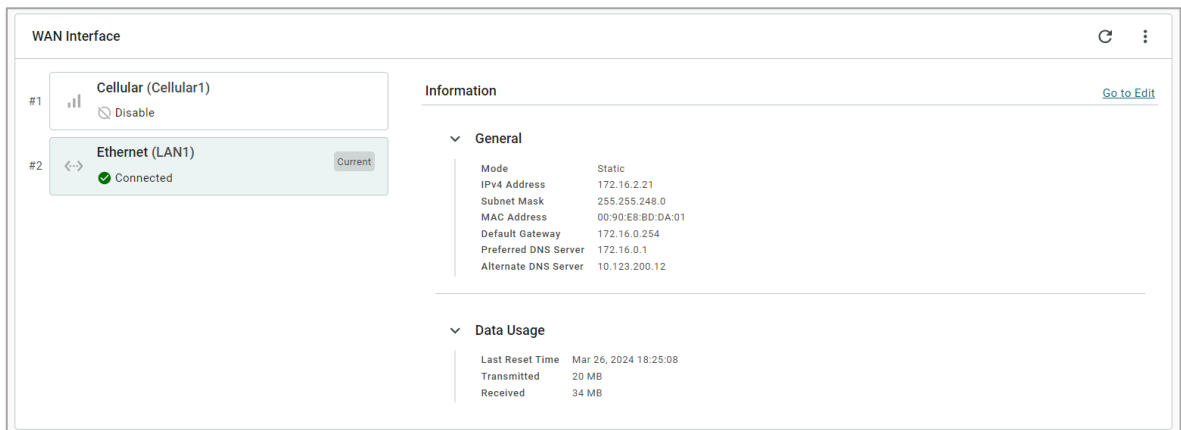
## WAN

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**.

Home > Tag Dashboard

Tag Dashboard

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

Monitoring tags ...

Search

+ Edit Tags

| Provider | Source | Name           | Type   | Value       | Access | Last Update            |   |
|----------|--------|----------------|--------|-------------|--------|------------------------|---|
| system   | status | memoryCached   | uint64 | 2458808320  | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | memoryUsage    | uint64 | 3           | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | gpsLat         | double | 24.964047   | Read   | Nov 01, 2024, 14:41:04 | ⋮ |
| system   | status | cpuUsage       | uint64 | 1           | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | cpuTemperature | uint64 | 39          | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | gpsLong        | double | 121.321755  | Read   | Nov 01, 2024, 14:41:04 | ⋮ |
| system   | status | memoryUnused   | uint64 | 15999623168 | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | memoryBuffers  | uint64 | 138633216   | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | memoryFree     | uint64 | 13402181632 | Read   | Nov 01, 2024, 14:41:09 | ⋮ |
| system   | status | memoryTotal    | uint64 | 16622686208 | Read   | Nov 01, 2024, 14:41:09 | ⋮ |

Items per page: 10 1 - 10 of 56

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

Edit Tags

Select the tags you want to display in the list.

56 item(s) selected

Clear

system

+ Add a filter

| Provider | Source  | Name             | Type   | Access |
|----------|---------|------------------|--------|--------|
| system   | status  | memoryCached     | uint64 | Read   |
| system   | network | Ian1NetworkUsage | uint64 | Read   |
| system   | network | Ian2NetworkRx    | uint64 | Read   |
| system   | status  | memoryUsage      | uint64 | Read   |
| system   | network | networkStatus    | string | Read   |

Items per page: 5 1 - 5 of 33

Cancel Save

3. Select the tags to monitor in the list.

Edit Tags

Select the tags you want to display in the list.

56 item(s) selected

Clear

system

+ Add a filter

| Provider | Source  | Name             | Type   | Access |
|----------|---------|------------------|--------|--------|
| system   | status  | memoryCached     | uint64 | Read   |
| system   | network | Ian1NetworkUsage | uint64 | Read   |
| system   | network | Ian2NetworkRx    | uint64 | Read   |
| system   | status  | memoryUsage      | uint64 | Read   |
| system   | network | networkStatus    | string | Read   |

Items per page: 5 1 - 5 of 33

Cancel Save

4. Click **Save**.

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

Home > Tag Dashboard

### Tag Dashboard

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

Monitoring tags ... Search Edit Tags

| Provider | Source | Name           | Type   | Value       | Access | Last Update            |                                                                                     |
|----------|--------|----------------|--------|-------------|--------|------------------------|-------------------------------------------------------------------------------------|
| system   | status | memoryCached   | uint64 | 2458415104  | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | memoryUsage    | uint64 | 4           | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | gpsLat         | double | 24.964047   | Read   | Nov 01, 2024, 14:43:34 |  |
| system   | status | cpuUsage       | uint64 | 3           | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | cpuTemperature | uint64 | 39          | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | gpsLong        | double | 121.321755  | Read   | Nov 01, 2024, 14:43:34 |  |
| system   | status | memoryUnused   | uint64 | 15938301952 | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | memoryBuffers  | uint64 | 138960896   | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | memoryFree     | uint64 | 13340925952 | Read   | Nov 01, 2024, 14:43:43 |  |
| system   | status | memoryTotal    | uint64 | 16622686208 | Read   | Nov 01, 2024, 14:43:43 |  |

Items per page: 10 1 - 10 of 56

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

Tag Dashboard

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

Monitoring tags ... Search Edit Tags

| Provider          | Source   | Name        | Type    | Value               | Access | Last Update            |                                                                                       |
|-------------------|----------|-------------|---------|---------------------|--------|------------------------|---------------------------------------------------------------------------------------|
| modbus_tcp_master | datatype | int64_30_33 | int64   | -806550705253793... | Read   | Nov 01, 2024, 14:45:52 |  |
| modbus_tcp_master | datatype | boolean_w   | boolean | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | uint16_w    | uint16  | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | int16_w     | int16   | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | float32_w   | float   | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | float64_w   | double  | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | string_w    | string  | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | bytearray_w | raw     | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | uint32_w    | uint32  | --                  | Write  | Jan 01, 1970, 08:00:00 |  |
| modbus_tcp_master | datatype | uint64_w    | uint64  | --                  | Write  | Jan 01, 1970, 08:00:00 |  |

Items per page: 10 11 - 20 of 23

# 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.

Home > Security Dashboard

Security Dashboard

The system's security check is up to date.  
Last scanned: Jan 16, 2024 17:00:47

Generate Report

Scan

Account Setting

Application Networking 1 issue found

Application Resource Usage

Product Certificate Deployment

Service Setting 4 issues found

| Status | Security check                                | Risk   |
|--------|-----------------------------------------------|--------|
|        | Discovery Service should not be enabled.      | High   |
|        | SSH Service should not be enabled.            | High   |
|        | Serial Console Service should not be enabled. | High   |
|        | Account Lock Service should be enabled.       | High   |
|        | System Use Notification should be enabled.    | Medium |

| 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 <b>Account Management &gt; Accounts</b> to change the password.                                                                                                                                       |
|                            | An account should only have one active session at any given time.                                                    | Go to <b>Security &gt; Session Management</b> 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 <b>Security &gt; Firewall</b> 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 <b>/var/run/</b> and <b>/tmp/</b> , 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 <b>Cloud Connectivity &gt; Azure IoT Edge &gt; Module Permission</b> , 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 <b>Cloud Connectivity &gt; Azure IoT Edge &gt; Downstream Certificate</b> 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 <b>Security &gt; Certificate Center</b> to check the status of each certificate.                                                                                                                                 |
|                                | All certificates should not have expired.                                                | If you find that a certificate will expire soon or has already expired, go to <b>Cloud Connectivity &gt; Azure IoT Edge/Azure IoT Device/MQTT Client or Security &gt; HTTPS</b> to check and replace the certificates. |
| Service Settings               | Discovery Service should not be enabled.                                                 | Go to <b>Maintenance &gt; Service</b> to disable the Discovery Service.                                                                                                                                                |
|                                | SSH service should not be enabled.                                                       | Go to <b>Maintenance &gt; Service</b> to disable the Debug Mode.                                                                                                                                                       |
|                                | Serial Console Service should not be enabled.                                            | Go to <b>Security &gt; Service</b> to disable the local console.                                                                                                                                                       |
|                                | Account Lock Service should be enabled.                                                  | Go to <b>Security &gt; Login Lockout</b> to enable the <b>Login Failure Lockout</b> option.                                                                                                                            |
|                                | System Use Notification Service should be enabled.                                       | Go to <b>Security &gt; System Use Notification</b> to enable the System Use Notification Service.                                                                                                                      |
| System Status Check            | Product software packages should be up to date.                                          | Go to <b>Maintenance &gt; Software Upgrade</b> and click <b>Check for Upgrade</b> to retrieve the latest upgrade pack information.                                                                                     |
|                                | System backup should be performed at least once a year.                                  | Go to <b>Maintenance &gt; Backup &amp; Restore</b> and click <b>Manage</b> 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.

| System                                                   | Time | GPS |
|----------------------------------------------------------|------|-----|
| <div>Server/Host Name</div> <div>moxa-tbbgb1029495</div> |      |     |
| <div>Description - optional</div> <div>Factory A1</div>  |      |     |

| 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.

Home > System Settings > General

## General

System **Time** GPS

Current date and time: Jan 16, 2024 17:05:58

Time Zone  
(GMT +08:00) Asia/Taipei

Sync Mode

☒ Manual ☐ Auto

Sync with browser

Date  
Jan 16, 2024

Hour : Minute : Second  
17 : 4 : 9

Save

Home > System Settings > General

## General

System **Time** GPS

Current date and time: Jan 16, 2024 17:10:26

Time Zone  
(GMT +08:00) Asia/Taipei

Sync Mode

☐ Manual ☒ Auto

Interval (sec)  
7200

Source  
NTPsec Server

Time Server  
time.cloudflare.com

Save

| Parameter      | Value                                                           | Description                                                                                                                                                                                                                                                                                            |
|----------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Zone      | User's selectable time zone                                     | The field allows you to select a different time zone.                                                                                                                                                                                                                                                  |
| Sync Mode      | Manual<br>Auto                                                  | Manual: input the time parameters by yourself<br>Auto: it will automatically sync with time source. NTP and GPS can be selected.<br>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<br>NTP Server<br>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.



## CAUTION

For the accuracy of the timestamp on logs, it is critical to ensure the correctness of the system time. Set the system time (if required) during initialization. However, before modifying the time or time zone, you must export the system logs. Also note that, significant time adjustments may require a factory reset. Minor changes can be managed by sorting audit logs based on when the entries were created.

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.

Home > System Settings > General

### General

System   Time   **GPS**

☒ Manually enter coordinates  
☐ Automatically adjust coordinates for GPS changes

Coordinates

Latitude  
24.964047

Longitude  
121.321755



Save

## Serial

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

To configure serial settings, do the following:

1. Choose the COM port to configure.

Home > System Settings > Serial

### Serial

Search Refresh

| Port    | Interface | Baud Rate | Parity, Data Bits, Stop Bits | Flow Control |
|---------|-----------|-----------|------------------------------|--------------|
| #1 COM1 | rs232     | 9600      | none, 8, 1                   | none         |
| #2 COM2 | rs232     | 9600      | none, 8, 1                   | none         |

Items per page: 10 1 ~ 2 of 2

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.

Home > System Settings > Serial > Port #1

← Port#1

Serial Settings

Interface

rs232

Baud Rate

9600

Parity

none

Data Bits

☐ 7

☒ 8

Stop Bits

☒ 1

☐ 2

Flow Control

none

Save

Clone

| Parameter    | Value                        | Description                                                                                                             |
|--------------|------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Interface    | rs232, rs422, rs485-2w       | For RS-485 4-wire mode, select <b>rs422</b> because it shares the same Super I/O UART mode with the RS-485 4-wire mode. |
| Baud Rate    | 50 to 115200                 |                                                                                                                         |
| Parity       | none, odd, even, space, mark |                                                                                                                         |
| Data Bits    | 7, 8                         |                                                                                                                         |
| Stop Bits    | 1, 2                         |                                                                                                                         |
| Flow Control | None, hardware, software     | Hardware: Flow control using the 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**.

External Storage

You can reduce the space occupied on the main system disk by using external storage devices.

Device List

USB\_p1

Refresh



NOTE

LIMITATION

- AIG does not allow the connection of multiple USB devices through a USB hub.
- The external USB formats supported for AIG are FAT32 and ext4.

# 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**.

Home > Network Settings > Ethernet

### Ethernet

LAN1 LAN2

WAN (Wide Area Networks)

Mode

☐ DHCP: Obtain an IP address automatically.

☒ Static: Specify the IP address.

IPv4 Address  
172 . 16 . 2 . 21

Subnet Mask  
255 . 255 . 248 . 0

Gateway  
172 . 16 . 0 . 254

Preferred DNS Server - optional  
172 . 16 . 0 . 1

Alternate DNS Server - optional  
10 . 123 . 200 . 12

| Parameter                     | Value                                                                      | Description                                                                         |
|-------------------------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Types of connectivity         | WAN<br>LAN<br><br>(NOTE: LAN2 does not support WAN.)                       | WAN: Wide Area Networks<br>LAN: Local Area Networks                                 |
| Mode                          | DHCP<br>Static                                                             | DHCP: Gets the IP address automatically.<br>Static: Specify the IP address          |
| IPv4 Address                  | LAN1 default: DHCP<br>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. |

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**.

☒ **Enable DHCP Server**  
 DHCP is a network service that automatically assigns IP addresses and network settings to devices on a local network.

Start IP

192 . 168 . 4 . 200

End IP

192 . 168 . 4 . 250

Lease Time Mode

Customized ▼

Lease Time (hour)

24



## 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.

Home > Network Settings > Cellular

## Cellular

CELLULAR1

☒ Enable cellular data communication

### Profile Settings

Create and manage profiles for a SIM with its data plan.

Connection Retry Timeout (sec)  
120

Profile List + Create

| #  | Profile Name | SIM  | Action |
|----|--------------|------|--------|
| #1 | Profile-1    | SIM1 |        |

### Check-alive

☒ Enable check-alive

Target Host  
8.8.8.8

Ping Interval (sec)  
60

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

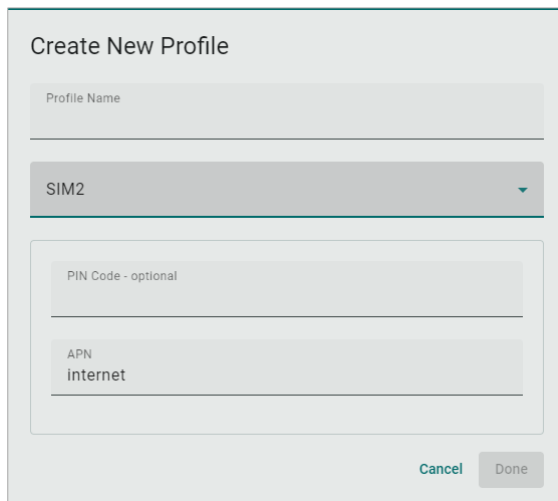
To prevent the SIM from being locked due to three incorrect attempts, a mechanism in the AIG stops attempting to unlock the SIM when the PIN Retry count reaches 2 (only one attempt is remaining). At this point, insert the SIM into another device (e.g., cellphone) and attempt to unlock it. This way, when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



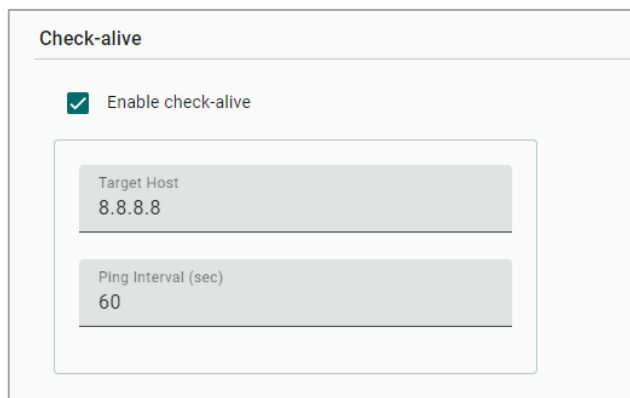
The 'Create New Profile' dialog box contains the following fields and controls:

- Profile Name:** A text input field.
- SIM2:** A dropdown menu with a downward arrow.
- PIN Code - optional:** A text input field.
- APN:** A text input field containing the value 'internet'.
- Buttons:** 'Cancel' and 'Done' buttons at the bottom right.

6. Click **Done**.
7. On the **Cellular** setting page, click **Save**.

When you click **Save** on the Cellular section, the module is restarted 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.



The 'Check-alive' settings dialog box contains the following elements:

- Check-alive:** A section header.
- Enable check-alive:** A checkbox that is checked.
- Target Host:** A text input field containing the value '8.8.8.8'.
- Ping Interval (sec):** A text input field containing the value '60'.

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**.

### Add by SSID

SSID

---

Security Mode

WPA/WPA2 Personal

---

Password

---

CANCEL ADD

### Add by Scan Results

1 Select AP 2 View Details

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

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

CANCEL NEXT >

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

## Wi-Fi Client

WIFI1

☒ Enable Wi-Fi

### AP List

+ Create

|     |                         |  |           |  |
|-----|-------------------------|--|-----------|--|
| # 1 | sqa-iiot-lan-24G-nopass |  | Connected |  |
|-----|-------------------------|--|-----------|--|

### IP Settings

Mode

☒ DHCP: Obtain an IP address automatically

☐ Static: Assign IP address by manual configuration

### Check-alive

☒ Enable check-alive

Target Host

8.8.8.8

Ping Interval (sec)

60

Save

# 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.

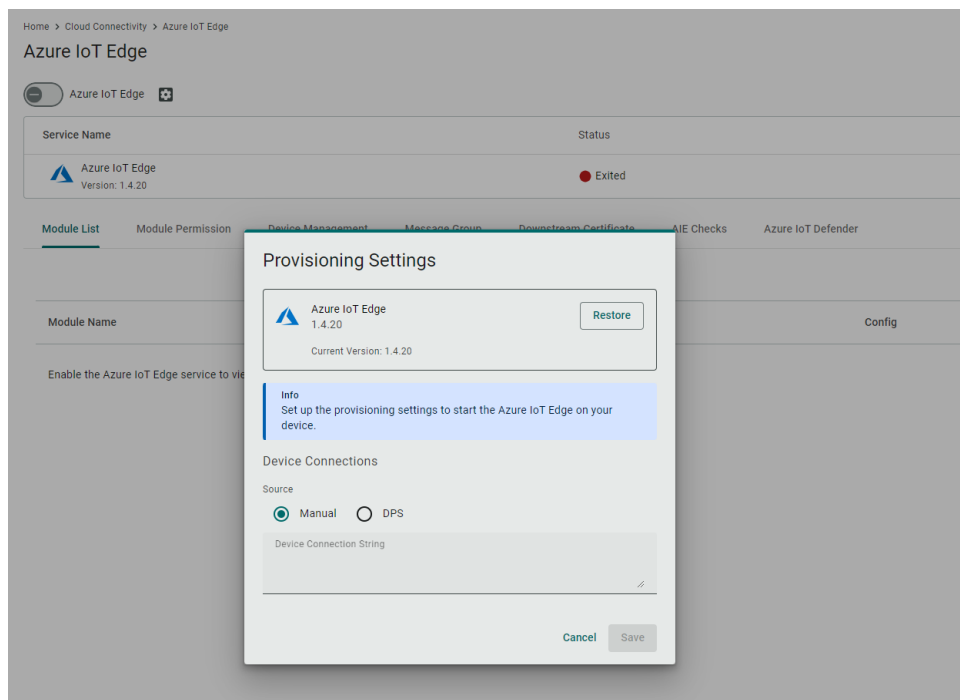


#### NOTE

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**.

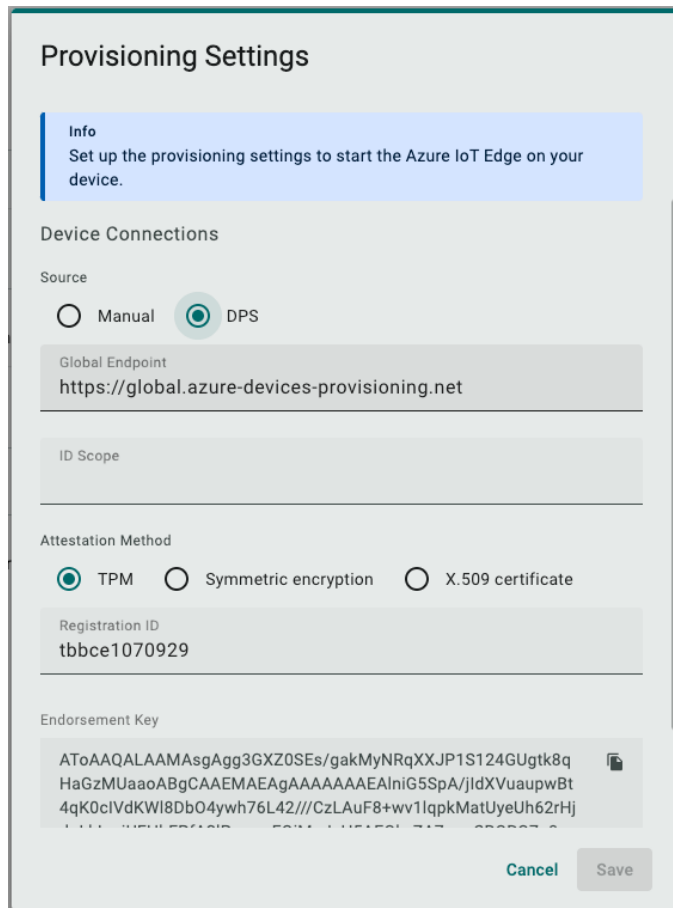
To create an Azure IoT Edge connection for your gateway via DPS, do the following:

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.



The screenshot shows the 'Provisioning Settings' dialog box in the Azure IoT Hub portal. It has a light gray background and a teal header. The 'Info' section at the top states: 'Set up the provisioning settings to start the Azure IoT Edge on your device.' Below this, the 'Device Connections' section shows 'Source' with two radio buttons: 'Manual' (unselected) and 'DPS' (selected). The 'Global Endpoint' field contains 'https://global.azure-devices-provisioning.net'. The 'ID Scope' field is empty. The 'Attestation Method' section has three radio buttons: 'TPM' (selected), 'Symmetric encryption' (unselected), and 'X.509 certificate' (unselected). The 'Registration ID' field contains 'tbbce1070929'. The 'Endorsement Key' field contains a long alphanumeric string: 'AToAAQALAAAMAgg3GXZ0SEs/gakMyNRqXXJP1S124GUgtk8qHaGzMUaa0ABgCAAEMAEAgAAAAAAEAlniG5SpA/jldXVuaupwBt4qK0ciVdKWl8DbO4ywh76L42///CzLAuF8+ww1lqpkMatUyeU62rHj'. At the bottom right are 'Cancel' and 'Save' buttons.

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**.

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

Home > Alfred\_test > Set modules on device: Alfred\_test >

## Add IoT Edge Module

thingspro-IoTHub-newTwin

IoT Edge module settings. [Learn more](#)

Module name \*

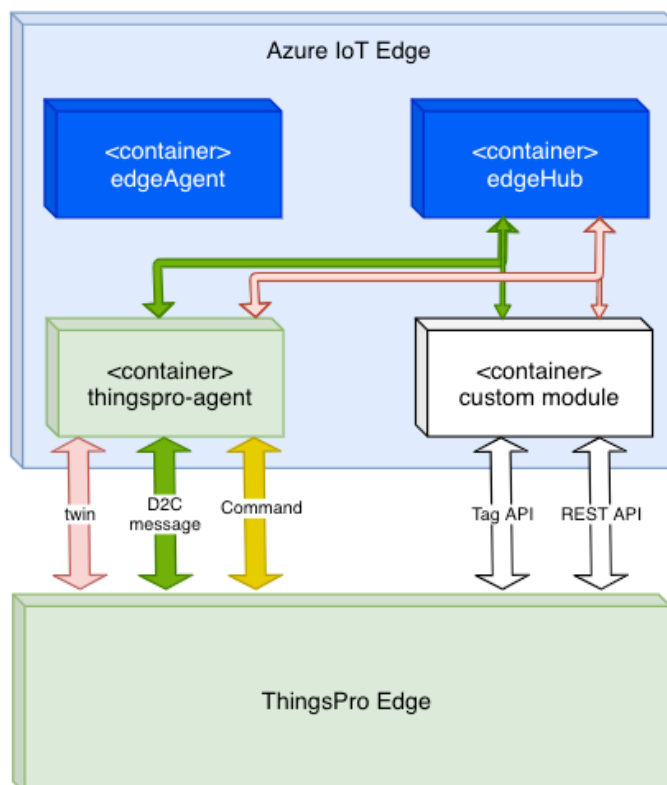
Settings **Environment Variables** Container Create Options Module Twin Settings

Environment variables provide supplemental information to a module facilitating the configuration process.

| NAME                 | TYPE | VALUE                                            |                                                                                     |
|----------------------|------|--------------------------------------------------|-------------------------------------------------------------------------------------|
| SECRET_KEY           | Text | eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJVc2Vy... |  |
| <i>Variable name</i> | Text | <i>Variable value</i>                            |                                                                                     |

## 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:3.0.1-amd64
```

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 | <pre>{   "httpserver": {     "httpPort": 80,     "httpsEnable": true,     "httpsPort": 8443,     "ipv6Enable": true,     "keyFileName": "client_nopassphrase.key",     "certFileName": "client.pem",     "httpEnable": true   } }</pre> |
| discovery  | <pre>{   "discovery": {     "enable": true,     "schedule": {       "enable": true,       "disableAfterSec": 900     }   } }</pre>                                                                                                      |

| Properties | Sample                                                                                                                                                                                                                                                                                          |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wan        | <pre>{   "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"   } }</pre>                                                        |
| route      | <pre>{   "route": {     "defaultRoute": "LAN1",     "priorityList": {       "0": "Cellular1",       "1": "LAN1",       "arraySize": 2     }   } }</pre>                                                                                                                                         |
| serials    | <pre>{   "serials": {     "0": {       "baudRate": 9600,       "dataBits": 8,       "device": "/dev/ttyM0",       "displayName": "PORT 1",       "flowControl": "none",       "id": 1,       "mode": "rs232",       "parity": "none",       "stopBits": 1     },     "arraySize": 1   } }</pre> |
| time       | <pre>{   "time": {     "lastUpdateTime": "2023-05-24T23:22:05+00:00",     "ntp": {       "enable": false,       "interval": 7200,       "server": "time.cloudflare.com",       "source": "timeserver"     },     "timezone": "Asia/Taipei"   } }</pre>                                          |

| Properties      | Sample                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernets       | <pre>{   "ethernets": {     "0": {       "enable": true,       "enableDhcp": false,       "id": 1,       "name": "enp0s31f6",       "status": "connected",       "displayName": "LAN1",       "gateway": "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 }</pre> |
| 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-502-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>                                                                                                                                                                                                                                                                                                                  |

| Properties | Sample                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cellulars  | <pre> {   "cellulars": {     "0": {       "operatorName": "",       "pinRetryRemain": 3,       "profiles": {         "0": {           "name": "Profile-1",           "pdpContext": {             "apn": "internet",             "auth": {               "password": "",               "username": ""             },             "type": "ipv4"           },           "pinCode": "",           "simSlot": 1         },         "1": {           "name": "Profile-2",           "pdpContext": {             "apn": "internet",             "auth": {               "password": "",               "username": ""             },             "type": "ipv4"           },           "pinCode": "",           "simSlot": 2         },         "arraySize": 1       },       "currentProfileName": "Profile-1",       "imsi": "",       "keepalive": {         "enable": true,         "intervalSec": 60,         "targetHost": "8.8.8.8"       },       "mac": "",       "gateway": "",       "id": 1,       "name": "wwan0",       "profileTimeout": 120,       "cellId": "",       "displayName": "Cellular1",       "dns": {         "arraySize": 0       },       "enable": false,       "status": "sim_pin_locked",       "signalStrength": 0,       "capabilities": {         "sim": 2       },       "iccId": "89886972203703305466",       "ip": "",       "mode": "unknown",       "imei": "357575100284579", </pre> |

| Properties | Sample                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | <pre> "lac": "", "netmask": "", "tac": "" }, "arraySize": 1 } } </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| wifi       | <pre> {   "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",             "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         }       },       "arraySize":2     },     "priority":{       "0":"Z3djNkHNR",       "1":"WqOjNzNHRz",       "arraySize":2     }   },   "arraySize":2 }, } </pre> |

| Properties | Sample                                                                                                                |
|------------|-----------------------------------------------------------------------------------------------------------------------|
|            | <pre> "displayName": "WiFi2", "enable": false, "id": 1, "mode": "client", "name": "wlp2s0" }, "arraySize": 1 } </pre> |

Desired Properties:

| Properties | Sample                                                                                                                                                                                                                                                                          |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| httpserver | <pre> {   "desired": {     "httpserver": {       "httpEnable": true,       "httpsEnable": true,       "httpsPort": 8443       "ipv6Enable": true     }   } } </pre>                                                                                                             |
| discovery  | <pre> {   "desired": {     "discovery": {       "enable": true,       "schedule": {         "enable": true,         "disableAfterSec": 900       }     }   } } </pre>                                                                                                           |
| serials    | <pre> {   "desired": {     "serials": {       "0": {         "mode": "rs232",         "stopBits": 1,         "baudRate": 9600,         "dataBits": 8,         "parity": "none",         "flowControl": "none",         "id": 1       },       "arraySize": 1     }   } } </pre> |

| Properties | Sample                                                                                                                                                                                                                                                                                                                                            |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time       | <p>Update NTP Settings:</p> <pre>{   "desired": {     "time": {       "ntp": {         "enable": true,         "interval": 7200,         "server": "time.cloudflare.com",         "source": "timeserver"       }     }   } }</pre> <p>Update Time zone:</p> <pre>{   "desired": {     "time": {       "timezone": "Asia/Taipei"     }   } }</pre> |
| general    | <p>Update gateway host name:</p> <pre>{   "desired": {     "general": {       "hostName": "MyHost"     }   } }</pre> <p>Update gateway description:</p> <pre>{   "desired": {     "general": {       "description": "MyDevice"     }   } }</pre>                                                                                                  |
| gps        | <p>Update GPS latitude and longitude by manual mode:</p> <pre>{   "desired": {     "gps": {       "mode": "manual",       "location": {         "lat": 11,         "lng": 12       }     }   } }</pre> <p>Update GPS by auto mode:</p> <pre>{   "desired": {     "gps": {       "mode": "auto",       "interface": "GPS1"     }   } }</pre>       |

| Properties      | Sample                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ethernets       | <pre> {   "ethernets": {     "0": {       "dns": {         "0": "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   } } </pre>                                                                                                                                                                                                                                                                                             |
| SoftwareUpgrade | <pre> {   "desired": {     "softwareUpgrade": {       "allowUpdate": true,       "allowOverCellular": false,       "snapshotBeforeUpdate": true,       "autoScan": false,       "autoScanExpression": "0 3 * * 1,2,3,4,5"     }   } } </pre>                                                                                                                                                                                                                                                                                                                                                                                        |
| cellulars       | <pre> {   "cellulars": {     "0": {       "enable": false,       "keepalive": {         "enable": false,         "intervalSec": 120,         "targetHost": "8.8.8.8"       },       "profileTimeout": 140,       "profiles": {         "0": {           "name": "SIM1",           "pdpContext": {             "apn": "internet",             "auth": {               "password": "",               "username": ""             },             "type": "ipv4"           },           "pinCode": "0000",           "simSlot": 1         },         "arraySize": 1       },       "arraySize": 1     },     "arraySize": 1   } } </pre> |

| Properties | Sample                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| wifi       | <pre> {   "desired":{     "wifi":{       "0":{         "client":{           "checkalive":{             "enable":false,             "intervalSec":60,             "targetHost":"8.8.8.8"           },           "ipSetting":{             "enableDhcp":true           },           "networks":{             "0":{               "security":{                 "mode":"wpa2-personal",                 "password":"12345678",                 "support":true               },               "ssid":"TESTAP"             },             "1":{               "security":{                 "mode":"wpa2-personal",                 "password":"admin@123",                 "support":true               },               "ssid":"moxa"             },             "arraySize":2           }         },         "enable":true,         "id":1,         "mode":"client"       },       "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 the status of the product packages for available upgrades    |
| 4  | thingspro-software-upgrade       | Performs over-the-air (OTA) software upgrades with product package |
| 5  | message-policy-get               | Retrieves the D2C message policy applied to your gateway           |
| 6  | message-policy-put               | Updates the D2C message policy applied to your gateway             |
| 7  | 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-502 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.

Method name \* ⓘ  
thingspro-api-v1

Payload ⓘ

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

Response timeout ⓘ 30 seconds ▾ Connection timeout ⓘ Module must already be connected ▾

Invoke method

## 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-502-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-502 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-502-tpe"
    ],
    "message": "Successfully trigger"
  }
}
```



### NOTE

AIG-502 allows only one active software upgrade job at a time. We recommend changing the response timeout parameters to 1 minute to prevent system exceptions.

## message-policy-get

Method Name:

message-policy-get

Request Payload:

{}

Response:

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

| Key                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| groups             | Type: array<br>Description: The message group; you can define multiple messages by demand.                                                                                                                                                                                                                                                                                                                                                                                                       |
| id                 | Type: integer<br>Description: The message ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| description        | Type: string<br>Description: The message description.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| enable             | Type: boolean<br>Description: Enable or disable this message policy.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| outputTopic        | Type: string<br>Description: The output topic required by Azure IoT Edge; helps manage the message route in Azure IoT Edge.                                                                                                                                                                                                                                                                                                                                                                      |
| format             | Type: string<br>Description: A <b>jq</b> script to transform a default payload to a custom payload.                                                                                                                                                                                                                                                                                                                                                                                              |
| properties         | Type: string<br>Description: Application properties of the message. This allows cloud applications to access certain messages without deserializing the JSON payload.                                                                                                                                                                                                                                                                                                                            |
| tags               | Type: string<br>Description: The tag data to send in the message. You can retrieve all available tags defined by ThingsPro Edge RESTful API.                                                                                                                                                                                                                                                                                                                                                     |
| sendOutThreshold   | Type: object<br>Define conditions to send out messages to Azure Edge Hub based on:<br>mode<br>Type: string<br>Enum: byTime, bySize immediately<br>size (mode: bySize)<br>Type: integer<br>Unit: bytes<br>time (mode: byTime)<br>Type: integer<br>Unit: second<br>value 0 almost real time<br>sizeIdleTimer (mode: bySize, optional):<br>Description: A fixed publish time between two bySize mode publishes.<br>Type: object<br>enable<br>Type: boolean<br>time<br>Type: integer<br>Unit: second |
| minPublishInterval | Type: integer<br>Unit: second<br>Description: A fixed interval between the two immediately mode publish                                                                                                                                                                                                                                                                                                                                                                                          |
| samplingMode       | Type: string<br>Enum: allValues, latestValues, allChangedValues, latestChangedValues                                                                                                                                                                                                                                                                                                                                                                                                             |
| customSampling     | Type: boolean<br>Description: Enable will use the pollingInterval that user input.                                                                                                                                                                                                                                                                                                                                                                                                               |
| pollingInterval    | Type: integer<br>Description: The interval at which to poll tag data. For example,<br>value 10: Every 10 second<br>value 0: when the data is pushed into the tag (almost real time)                                                                                                                                                                                                                                                                                                              |

## message-policy-put

Method Name:

message-policy-put

Request Payload:

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

The D2C message policy allows you to transform a default payload to your desired payload schema via a **jq** filter. For additional details, refer to the jq website ([jq Manual <development version>](#)).

The AIG Web GUI offers an easy way to apply the jq filter and test the transformed result as shown in the following examples.

## default D2C message schema

Select the tags that you want using the tag selector. The default result for the selected tags will show on the page.

← Create Message Group

✓ Basic Settings

✓ Tag Selection

3 Custom Payload  
Optional

4 Target Settings

☐ Enable JQ filter  
INFO: If the default payload format does not meet your requirement, edit it using the JQ filter.

Message Result

1 {

2 "tags": {

3 "system": {

4 "status": {

5 "cpuUsage": {

6 "values": [

7 {

8 "updateTimeStamp": "2020-02-14T05:53:23Z",

9 "value": 11

10 }

11 ]

12 }

13 }

14 }

15 }

16 }

< Back

Cancel

Next >

Custom payload after transforming the default payload.

Enable custom payload and input the jq Filter to display the custom payload for your selection.

← Create Message Group

✓ Basic Settings

✓ Tag Selection

3 Custom Payload  
Optional

4 Target Settings

☒ Enable JQ filter  
INFO: If the default payload format does not meet your requirement, edit it using the JQ filter.

☒ Basic Editing ☐ Advanced Editing

Tag: Pre-merge Format

1 {device:(.srcName),timestamp:(now|todateiso8601),(.tagName)}

2 }

→

Message Result

1 {

2 "cpuUsage": 11,

3 "device": "status",

4 "timestamp": "2025-02-20T14:04:02Z"

5 }

< Back

Cancel

Next >

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

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

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

Example:

```
{device:(.srcName),timestamp:(now|toDateiso8601),(.tagName):.dataValue}
```

#### Custom Payload Result

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

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

```
{
  "groups": [
    {
      "enable": true,
      "outputTopic": "sample",
      "format": "",
      "properties": [
        { "key": "messageType", "value": "deviceMonitor" }
      ],
      "tags": {
        "system": {
          "status": ["cpuUsage", "memoryUsage"]
        }
      },
      "pollingInterval": 2,
      "sendOutThreshold": { "size": 4096, "time": 5 },
      "format": "{device:(.srcName),timestamp:(now|toDateiso8601),TagName:(.tagName),Value:.dataValue}"
    }
  ]
}
```

## upload-audit-logs

Method Name:

upload-audit-logs

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

```
{
  "connectionString":
  "DefaultEndpointsProtocol=https;AccountName=thingsproedge;AccountKey=hgnYe/08sWqlcGKd7VR8XN
  RvjydebzzSeVZxFvRCmepUqA69LTtNY13UZ5feJgZgcys+jC5B+qf3+AStsEkNzg==;EndpointSuffix=core.w
  indows.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/08sWqlcGKd7VR8XN
  RvjydebzzSeVZxFvRCmepUqA69LTtNY13UZ5feJgZgcys+jC5B+qf3+AStsEkNzg==;EndpointSuffix=core.w
  indows.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

A telemetry message is the simplest message type for sending IoT device data to your IIoT applications. 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.

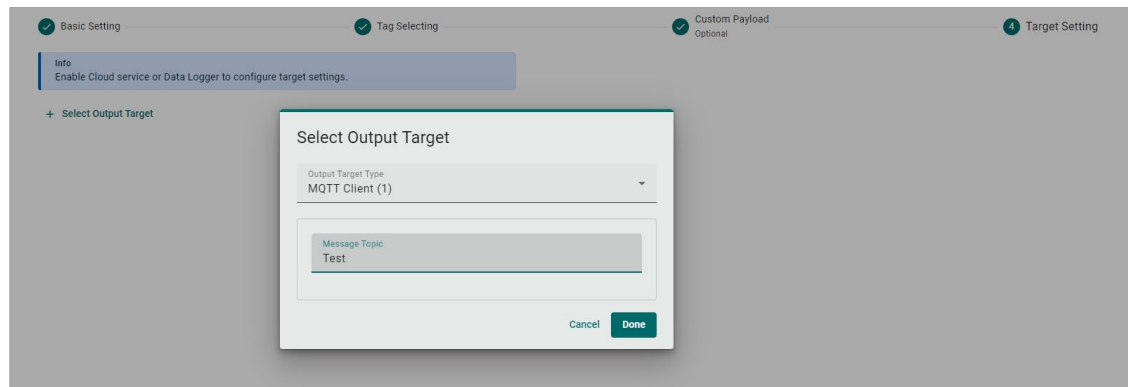
The screenshot shows the 'Create Message Group' dialog with four steps: 1. Basic Setting, 2. Tag Selecting, 3. Custom Payload Optional, and 4. Target Setting. Step 1 is active. The 'Message Group Name' is 'Test123'. Under 'Publish Mode', 'By Interval' is selected. The 'Publish Interval (sec)' is 60. The 'Sampling Mode' is 'All Changed Values'. There is an unchecked checkbox for 'Custom sampling rate from acquired data' and a checked checkbox for 'Enable Message Group by default'. At the bottom right are 'Cancel' and 'Next >' buttons.

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

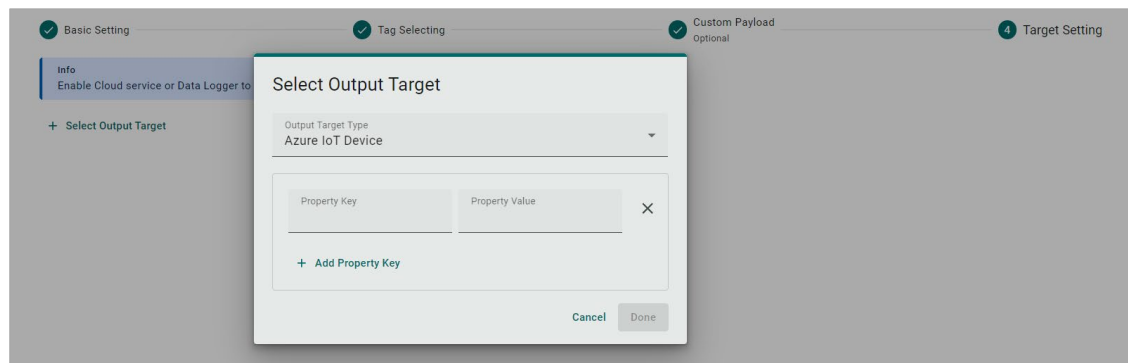
The screenshot shows the 'Create Message Group' dialog at Step 2: Tag Selecting. Step 1 is completed. The 'Select Tags' section has an 'Info' box stating 'Select one or more tag providers and select tags to map data.' The 'Providers' dropdown is set to 'modbus\_tcp\_master'. A search modal is open, showing a search bar, 'Select All', 'Clear', and a list of tags. The tag '[modbus\_tcp\_master] SE\_Meter' is expanded, showing 'Current' and 'status' both checked. At the bottom of the modal, it says 'Total: 2, Selected: 2' and a 'Done' button. The main dialog has a '< Back' button on the bottom left and 'Cancel' and 'Next >' buttons on the bottom right.

- (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 link: <https://stedolan.github.io/jq/manual/>.



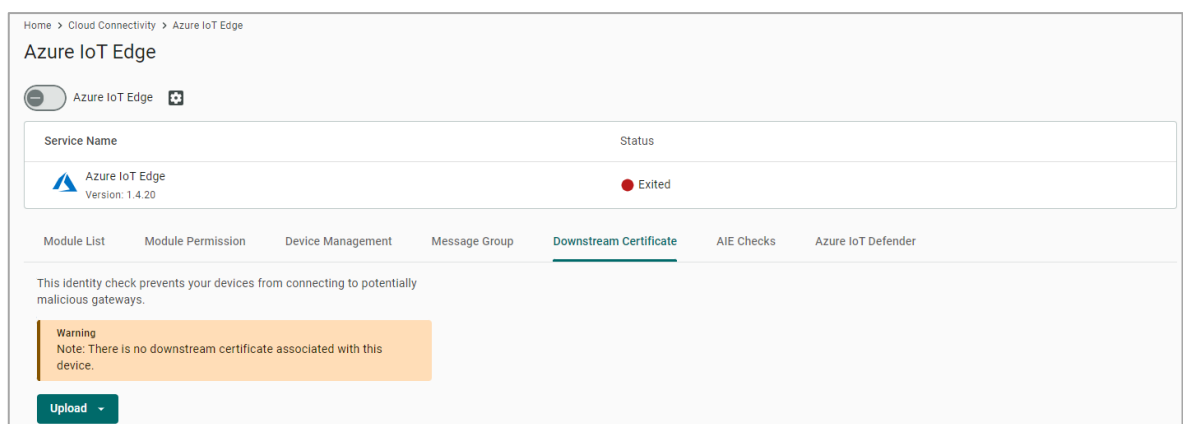
- Click **NEXT**.
- Select **Output Target Type**.
- (Optional) Enter Property Key and Value.



- 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
```

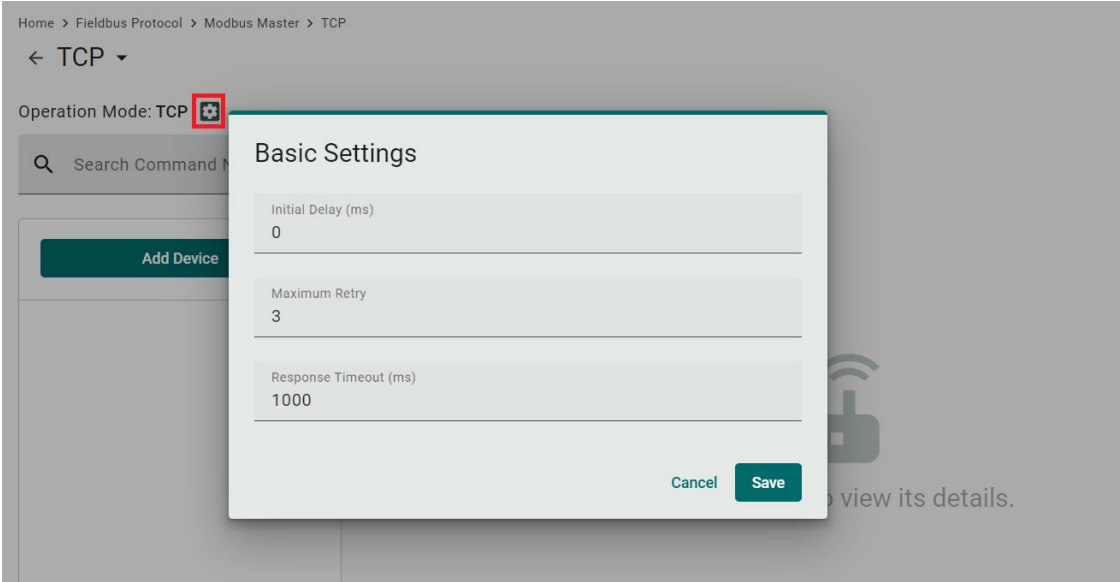
# Fieldbus Protocol

## Modbus Master

### Modbus TCP

#### Basic Settings

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



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

# Modbus Device Settings

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

Home > Fieldbus Protocol > Modbus Master > TCP

← TCP ▾

Operation Mode: TCP ⓘ

Q Search Command Name...

Add Device

GS

Enable

Slave IP: 10.123.21.50

Slave Port: 502

Slave ID: 1

Select a device to view its details.

Editing in progress...

Go to apply settings

## Step 1. Basic Settings

Enter in the basic parameters for the Modbus TCP device.

Home > Fieldbus Protocol > Modbus Master > TCP

← Create New Device

1 Basic Settings

2 Command Optional

3 Confirm

☒ Enable This Device

Device Name

SE\_Meter

Slave IP

192 . 168 . 127 . 50

Slave Port

502

Slave ID

1

The Slave ID should be unique in the set of IP and Port.

Cancel

Next >

| 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 slave device.      |
| Slave Port  | 1 to 65535                                                 | 502     | The TCP port number of a remote slave device. |
| Slave ID    | 1 to 255                                                   | -       | The slave ID of a remote slave device.        |

## Step 2. Command

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

The command settings will pop up.

Home > Fieldbus Protocol > Modbus Master > TCP

← Create New Device

1 Basic Settings 2 Command Optional 3 Confirm

Mode

☒ Manual ☐ Import Configuration

SE\_Meter + Add Command

| No.                                                                                                                                      | Command Name | Function | Address, Quantity | Trigger | Poll Interval (ms) | Enable |
|------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------|-------------------|---------|--------------------|--------|
| There are no commands in this device. Click <span style="color: green;">+ Add Command</span> to create the first command in this device. |              |          |                   |         |                    |        |

Items per page: 10 0 of 0

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

| Parameter                 | Value                                                                                                            | Default | Description                                                                                                                                                                                                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Write quantity</b>     | Write Multiple Coils: 1 to 1968<br>Write Multiple Registers: 1 to 123<br>Read/Write Multiple Registers: 1 to 123 | 1       | Specifying how much data to write.                                                                                                                                                                                                                      |
| <b>Trigger</b>            | Cyclic<br>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. |
| <b>Poll interval (ms)</b> | 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.                       |
| <b>Endian swap</b>        | None<br>Byte<br>Word<br>Byte and Word                                                                            | None    | <b>None:</b> not to swap<br><b>Byte:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C<br><b>Word:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B.<br><b>Byte and Word:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.   |
| <b>Status Term</b>        | Pause<br>Proceed - Clear data to zero<br>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.                                                                                                                                            |
| <b>Tag Type</b>           | boolean<br>int16<br>int32<br>int64<br>uint16<br>uint32<br>uint64<br>float<br>double<br>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.

Home > Fieldbus Protocol > Modbus Master > TCP

← Create New Device

1
Basic Settings

2
Command  
Optional

3
Confirm

Mode

☐ Manual
☒ Import Configuration

Info

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

Command Configuration

Browse

### Step 3. Confirm

Review whether the information of the settings is correct.

Home > Fieldbus Protocol > Modbus Master > TCP

← Create New Device

✓ Basic Settings

✓ Command Optional

3 Confirm

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

|                       |                |
|-----------------------|----------------|
| Device Name           | SE_Meter       |
| Slave ID              | 1              |
| Slave IP              | 192.168.127.50 |
| Slave Port            | 502            |
| Status                | Enable         |
| Number of Commands    | 1              |
| Command Configuration |                |

< Back

Cancel Done

Then, you will see the setting results.

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

Home > Fieldbus Protocol > Modbus Master > TCP

← TCP ▾

Operation Mode: TCP

Search Command Name...

Add Device

SE\_Meter

Enable

Slave IP: 192.168.127.50

Slave Port: 502

Slave ID: 1

SE\_Meter

+ Add Command

Import

Export

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

Items per page: 10 ▾ 1 - 1 of 1 < >

Editing in progress ...

Go to apply settings

Import Command Configuration

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

Command Configuration

Browse

Cancel

Done

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

Home > Fieldbus Protocol > Modbus Master

### Modbus Master

Modbus Master  
Version: 3.5.5  
Device Event: Enable  
Command Event: Enable

Manage

### Modbus TCP

TCP  
1 Device, 1 Command

### Modbus RTU/ASCII

COM1 (RTU)  
Not configured

COM2 (RTU)  
Not configured

Editing in progress...

Discard Apply

## Modbus RTU/ASCII

### Basic Settings

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

Home > Fieldbus Protocol > Modbus Master > COM1

← COM1

Operation Mode: RTU

Search Command Name...

Add Device

### Serial Basic Settings

Mode  
☒ RTU ☐ ASCII

Initial Delay (ms)  
0

Maximum Retry  
3

Response Timeout (ms)  
1000

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

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

Cancel Save

| Parameter          | Value      | Default | Description                                                                                                                                                                                                                                                                                                                 |
|--------------------|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mode               | RTU/ASCII  | RTU     |                                                                                                                                                                                                                                                                                                                             |
| Initial Delay (ms) | 0 to 30000 | 0       | Some Modbus slaves may take more time to boot up than other devices. In some environments, this may cause the entire system to suffer from repeated exceptions during the initial bootup. After booting up, you can force the AIG to wait some time before sending the first request by setting a value for this parameter. |
| Maximum Retry      | 0 to 5     | 3       | Use this to configure how many times AIG will retry to communicate with the Modbus slave when the Modbus command times out.                                                                                                                                                                                                 |

| Parameter                                                | Value                            | Default | Description                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------|----------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Response Timeout (ms)                                    | 10 to 120000                     | 1000    | You can configure a Modbus master to wait a certain amount of time for a slave's response. If no response is received within the configured time, the AIG will disregard the request and continue operation.                                                                                                                                   |
| Automatically determine the inter-frame delay (ms)       | Check<br>unchecked:<br>10 to 500 | check   | Inter-frame delay is the time between the response and the next request. This is to ensure a legacy Modbus slave device can handle packets in a short time.<br><b>Check:</b> The AIG will automatically determine the time interval.<br><b>Unchecked:</b> You can input a time interval.                                                       |
| Automatically determines the intercharacter timeout (ms) | Check<br>unchecked:<br>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.<br><b>Check:</b> The AIG will automatically determine the time out.<br><b>Unchecked:</b> 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.

Home > Fieldbus Protocol > Modbus Master > COM1

← COM1 ▾

Operation Mode: RTU

Add Device

Select a device to view its details.

Editing in progress...

Go to apply settings

## Step 1. Basic Settings

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

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

## Step 2. Command

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

The command settings will pop up.

| Parameter    | Value                                                      | Default | Description      |
|--------------|------------------------------------------------------------|---------|------------------|
| Command Name | Alphanumeric string and characters ( ~ . _ - ) are allowed | -       | Name the command |

| Parameter              | Value                                                                                                                                                                                                                                                                 | Default                     | Description                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Function               | 01 – Read Coils<br>02 – Read Discrete Inputs<br>03 – Read Holding Registers<br>04 – Read Inputs Registers<br>05 – Write Single Coil<br>06 – Write Single Register<br>15 – Write Multiple Coils<br>16 – Write Multiple Registers<br>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<br>Read Discrete Inputs: 1 to 2000<br>Read Inputs Registers: 1 to 125<br>Read Holding Registers: 1 to 125<br>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<br>Write Multiple Registers: 1 to 123<br>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<br>Byte<br>Word<br>Byte and Word                                                                                                                                                                                                                                 | None                        | <b>None:</b> not to swap<br><b>Byte:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C<br><b>Word:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B.<br><b>Byte and Word:</b> 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.   |

| Parameter   | Value                                                                                         | Default | Description                                                                                                    |
|-------------|-----------------------------------------------------------------------------------------------|---------|----------------------------------------------------------------------------------------------------------------|
| Status Term | Pause<br>Proceed - Clear data to zero<br>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<br>int16<br>int32<br>int64<br>uint16<br>uint32<br>uint64<br>float<br>double<br>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.

Home > Fieldbus Protocol > Modbus Master > COM1

← Create New Device

Progress: 1 Basic Settings (checked) 2 Command Optional (active) 3 Confirm (checked)

Mode

☐ Manual ☒ Import Configuration

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

Command Configuration

 Browse

< Back Cancel Next >

### Step 3. Confirm

Review whether the information of the settings is correct.

Home > Fieldbus Protocol > Modbus Master > COM1

← Create New Device

✓ Basic Settings

✓ Command Optional

3 Confirm

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

Device Name

SE\_Meter\_1

Slave ID

1

Status

Enable

Number of Commands

1

Command Configuration

← Back

Cancel

Done

Then, you will see the setting results.

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

Home > Fieldbus Protocol > Modbus Master > COM2

← COM2 ▾

Operation Mode: RTU 

🔍 Search Command Name...

+

 Add Device

 SE\_Meter\_1

✓ Enable

⋮

Slave ID: 1

SE\_Meter\_1

+ Add Command

📄 Import

📄 Export

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

Items per page:

10 ▾

1 - 1 of 1

<< < > >>

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

Home > Fieldbus Protocol > Modbus Master

Modbus Master

Modbus Master

Version: 3.5.5

Device Event: Enable

Command Event: Enable

Manage

Modbus TCP

TCP

1 Device , 1 Command

Modbus RTU/ASCII

COM1 (RTU)

Not configured

COM2 (RTU)

1 Device, 1 Command

Editing in progress ...

Discard

Apply

Manage

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

Home > Fieldbus Protocol > Modbus Master

Modbus Master

Modbus Master

Version: 3.5.5

Device Event: Enable

Command Event: Enable

Manage

Edit General Settings

Import Configuration

Export Configuration

Modbus TCP

TCP

1 Device , 1 Command

Modbus RTU/ASCII

COM1 (RTU)

Not configured

COM2 (RTU)

1 Device, 1 Command

Editing in progress ...

Discard

Apply

# Edit General Settings

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

Edit General Settings

System Event

☒ Enable device event

Send events when the connection status of the device changes.

☒ Enable command event

Send events when the statuses of commands change.

Cancel

Done

| Parameter            | Value            | Default | Description                                                                                                                                                                                                                   |
|----------------------|------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable device event  | Check<br>uncheck | Check   | <b>Check:</b> 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.<br><b>Uncheck:</b> Disable the function |
| Enable command event | Check<br>uncheck | Check   | <b>Check:</b> 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.<br><b>Uncheck:</b> Disable the function.        |

# Import/Export Configuration

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

Home > Fieldbus Protocol > Modbus Master

Modbus Master

Modbus Master

Version: 3.5.5

Device Event: Enable

Command Event: Enable

Manage

Modbus TCP

TCP

1 Device , 1 Command

Modbus RTU/ASCII

COM1 (RTU)

Not configured

COM2 (RTU)

1 Device, 1 Command

Import Configuration

Configuration File

Browse

Cancel

Done

Editing in progress ...

Discard

Apply

|                                                                                                              |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|--------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| @version 3.5.5                                                                                               |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [master-params]                                                                                              |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@masterP:configId                                                                                           | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| enableTcp enableSerial enableDev enableCmdFailEvent                                                          |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [tcp-masters]                                                                                                |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@tcpMast:configId                                                                                           | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| name modbus_tcp_master                                                                                       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [master-tcp-faces]                                                                                           |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@masterT1:tcpMaster]                                                                                        | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| initialDelay retryCount responseTout                                                                         |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 1 0 3 1000                                                                                                 |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [ser-masters]                                                                                                |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@serMast:configId                                                                                           | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| name modbus_serial_master                                                                                    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [master-ser-faces]                                                                                           |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@masterGserMaster]                                                                                          | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| portValue format initialDelay retryCount responseTf frameInter charInterv devPath                            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 1 1 1 0 0 3 1000 0 0 /dev/ttyM0                                                                            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2 1 1 1 0 0 3 1000 0 0 /dev/ttyM1                                                                            |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [remote-devs]                                                                                                |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@remoteCmasterSer]                                                                                          | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| masterTcp name enable slaveId slaveIp add slaveTcpPort                                                       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 1 SE_Meter 1 1 192.168.12 502                                                                              |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2 2 SE_Meter 1 1 0.0.0 502                                                                                   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [mcmds]                                                                                                      |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| [@remoteCName                                                                                                | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| enable mode func readAddr readQunt writeAddr writeQunt pollInterva swap                                      |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1 Current 1 0 3 0 10 0 0 1 1000 0 0 3600                                                                     |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 2 Voltage 1 0 3 0 10 0 1 1000 0 0 3600                                                                       |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| scalingFun interceptSI interceptO pointSource pointTarget pointTargetStFunc stData tagName dataType dataUnit |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 0 0 1 0 0 0 1 0 0 1 0 1 0                                                                                    |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 0 1 0 0 1 0 1 0                                                                                              |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| Current raw Voltage raw                                                                                      |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |

## Certificate Center

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 a root CA certificate to Google Chrome, see:

| Certificate Center                         |              |                                  |              |                                                                |
|--------------------------------------------|--------------|----------------------------------|--------------|----------------------------------------------------------------|
| My Certificates                            |              | Trusted Root CA                  |              |                                                                |
| <div> <div></div> <div>Search</div> </div> |              |                                  |              |                                                                |
| Name ↓                                     | Issued To    | Issued By                        | Source       | Status                                                         |
| > thingspro_https_default.crt              | TBBCE1070929 | ThingsPro Edge Root CA for HTTPS | HTTPS Server | <div> <div>Valid</div> <div>Feb 7, 2027, 01:57:05</div> </div> |
| Items per page: 10                         |              | 1 - 1 of 1                       |              |                                                                |

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

### System Default

| No. | Service/purpose   | Port |
|-----|-------------------|------|
| 1   | HTTP service      | 80   |
| 2   | HTTPS service     | 8443 |
| 3   | SSH server        | 22   |
| 4   | Discovery service | 5353 |



## 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.

| Rule Name         | Gateway Port ↑ | Protocol | Source IP | Source Port |
|-------------------|----------------|----------|-----------|-------------|
| ssh server        | 22             | TCP      | Any       | Any         |
| http service      | 80             | TCP      | Any       | Any         |
| discovery service | 5353           | UDP      | Any       | Any         |
| https service     | 8443           | TCP      | Any       | Any         |

## 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**.

**Create Rule**

Protocol

☒ TCP

☐ UDP

Gateway Port

Rule Name

Port\_

5 / 32

Source IP

Any

Source Port

Any

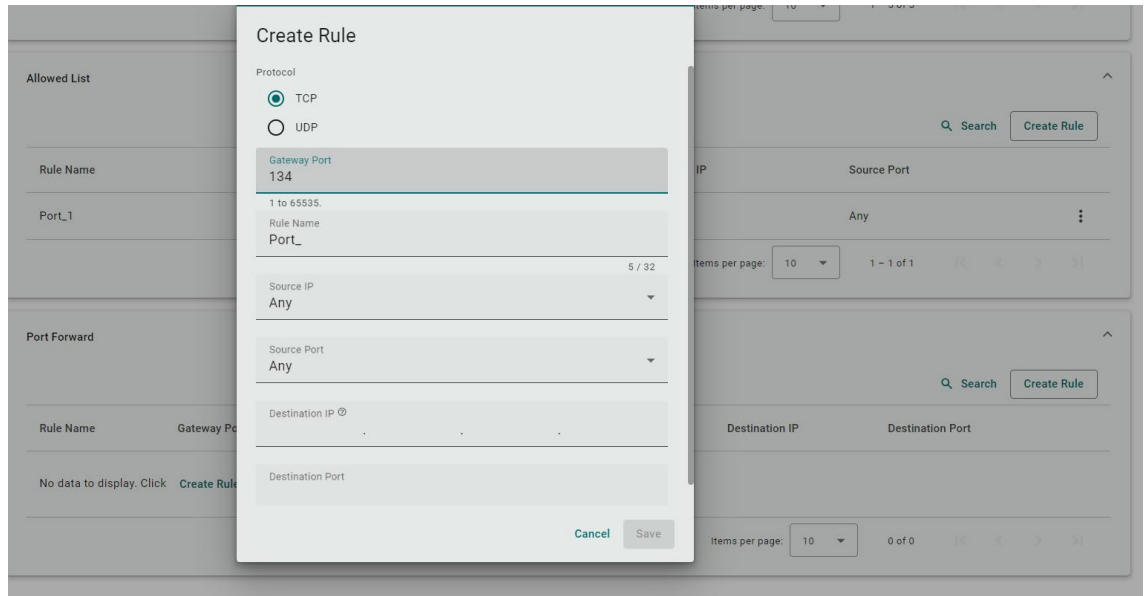
Cancel

Save

## Port Forward

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

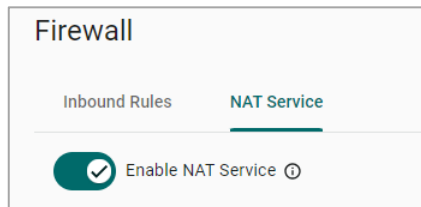
1. Click **+ Create Rule**.
2. Specify the protocol, gateway port, and rule name.
3. Specify a source IP.
4. Specify the destination IP and port.



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.

Home > Security > HTTPS

HTTPS

HTTP Service

☒ Redirect HTTP to HTTPS

HTTPS Service

Port Number  
8443

Import TLS/SSL Certificate

Certificate

 Browse

thingspro\_https\_default.crt

Private Key

 Browse

thingspro\_https\_default.key

Save

## 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.

Login Lockout

To avoid hackers from repeatedly logging in into the account to crack passwords, you can enable the Login Failure Lockout setting and configure related settings.

☒ Enable login failure lockout

Max Failed Retries (times)  
10

Failure Counter Reset Period (min) ⓘ  
15

Lockout Period (min)  
10

Save

| Parameter                          | Value     | Description                                                                                                         |
|------------------------------------|-----------|---------------------------------------------------------------------------------------------------------------------|
| Max Failure Retry (times)          | 3 to 32   | The maximum number of failed retries.                                                                               |
| Failure Counter Reset Period (min) | 1 to 60   | The interval for resetting the login failure counter.                                                               |
| Lockout Time (min)                 | 5 to 1440 | When the number of login failures exceeds the Max Failure Retry, the AIG will lock out the account for this period. |

# Session Management

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

Session Management

You can check the session statuses for all accounts and also perform session management for individual accounts.

Last Updated Jan 24, 2024, 22:15:13

Search

Refresh

| <input type="checkbox"/> | No. | Account | Source IP                 | Created Time           | Last Activity Time ↓   |  |
|--------------------------|-----|---------|---------------------------|------------------------|------------------------|--|
| <input type="checkbox"/> | 1   | admin   | 10.160.122.195 (your web) | Jan 24, 2024, 22:17:42 | Jan 24, 2024, 22:15:11 |  |

Items per page: 10

1 - 1 of 1

<<

<

>

>>

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

Session Management

Home > Security > Session Management

You can check the session statuses for all accounts and also perform session management for individual accounts.

Jan 17, 2024, 07:15:45 Last Updated

SEARCH

REFRESH

| <input type="checkbox"/> | No. | Account | Source IP | Created Time | Last Activity Time ↓   |  |
|--------------------------|-----|---------|-----------|--------------|------------------------|--|
| <input type="checkbox"/> | 1   | admin   |           |              | Jan 17, 2024, 07:02:06 |  |

Items per page: 10

1 - 1 of 1

<<

<

>

>>

Delete Session

Attention: This could be your account session!

This session will be permanently deleted, and the client's next call will receive an "unauthorized" response. Are you sure you want to proceed?

CANCEL

DELETE

AIG-502 Series User Manual

88

# 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.

System Use Notification

The following text will be displayed before the login page. It can be turned off if not necessary.

☐ Enable system use notification

Mode

Default

Text Content

This gateway system is for the use of authorized users only.

Individuals using this gateway system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel.

In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored.

Save

# 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.

Home > Account Management > Accounts

Accounts

Search Create

| Account Name | Role          | Status | Creation Date |  |
|--------------|---------------|--------|---------------|--|
| admin (you)  | Administrator | Active | 22 Jan, 2024  |  |
| user1        | operator      | Active | 23 Jan, 2024  |  |

Items per page: 10 1 - 2 of 2

## 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                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div> <div>Create New Account</div> <div> <div>Account Name</div> <div>Josh</div> <div>4/64</div> </div> <div> <div>Role</div> <div>operator</div> </div> <div> <div>Password</div> <div>*****</div> </div> <div> <div>Confirm Password</div> <div>*****</div> </div> <div> <div>Email - optional</div> <div></div> </div> <div> <div>Cancel</div> <div>Save</div> </div> </div> | <div> <div>Create New Account</div> <div> <div>Account</div> <div>Josh</div> <div>4/16</div> </div> <div> <div>Role</div> <div>Administrator</div> </div> <div> <div>Password</div> <div>*****</div> </div> <div> <div>Confirm Password</div> <div>*****</div> </div> <div> <div>Email - optional</div> <div></div> </div> <div> <div>CANCEL</div> <div>SAVE</div> </div> </div> |

## Managing Existing User Accounts

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

Home > Account Management > Accounts

Accounts

Search Create

| Account Name | Role          | Status | Creation Date |   |
|--------------|---------------|--------|---------------|---|
| admin (you)  | Administrator | Active | 22 Jan, 2024  | ⋮ |
| user1        | operator      | Active | 23 Jan, 2024  | ⋮ |
| Josh         | operator      | Active | 24 Jan, 2024  | ⋮ |

Items per page: 10 1 - 3 of 3

- Edit
- Change Password
- Deactivate
- Delete

| 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.<br><b>(NOTE: This operation is irreversible.)</b> |

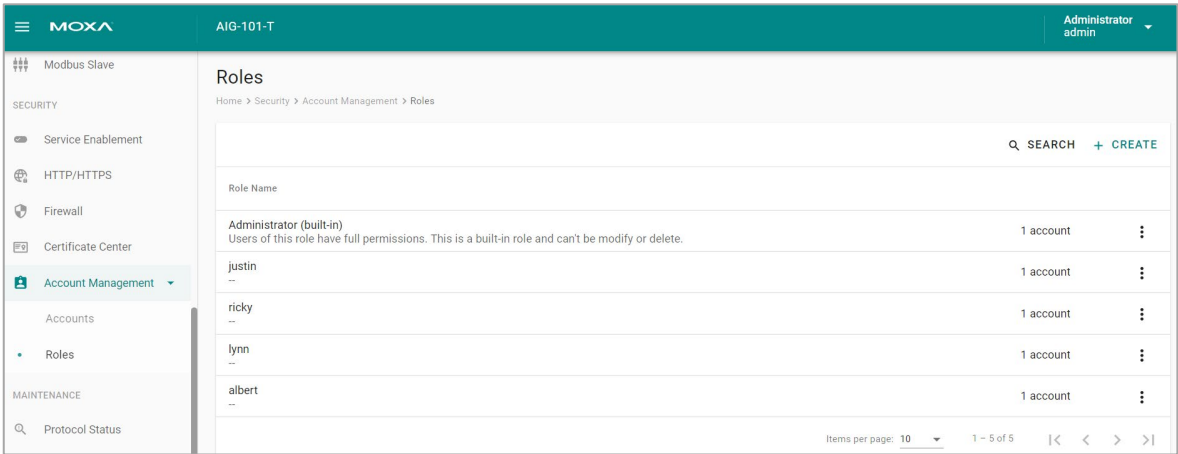


### NOTE

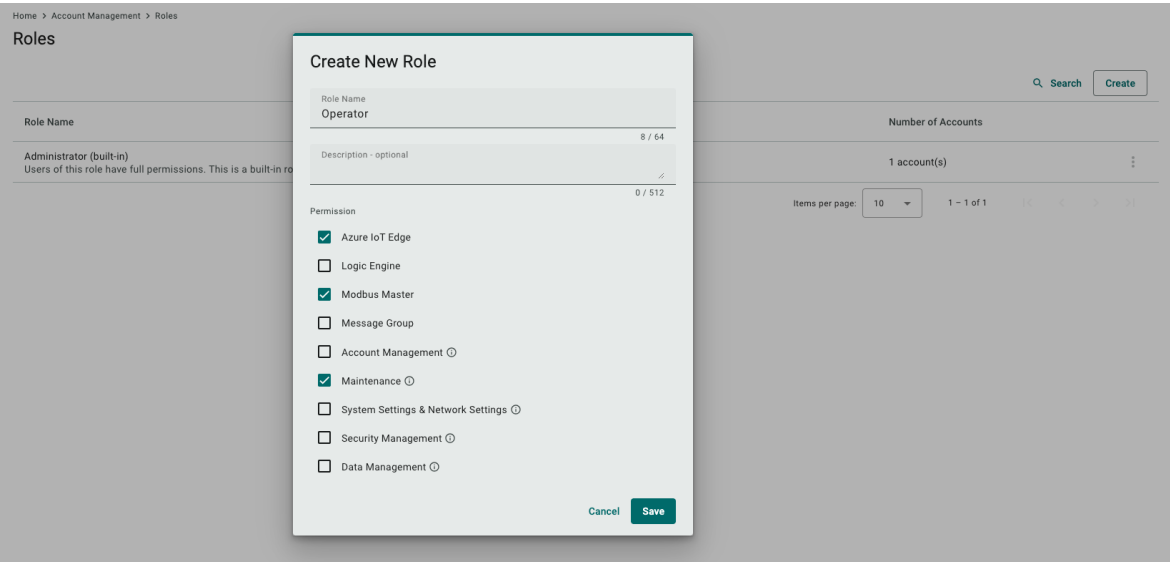
You cannot **Deactivate** or **Delete** the last remaining account with an Administrator role. This is to prevent an unauthorized account from fully managing this system. When the system detects only one active account when the Administrator role is selected, all items in the pop-up menu will be grayed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

# Roles

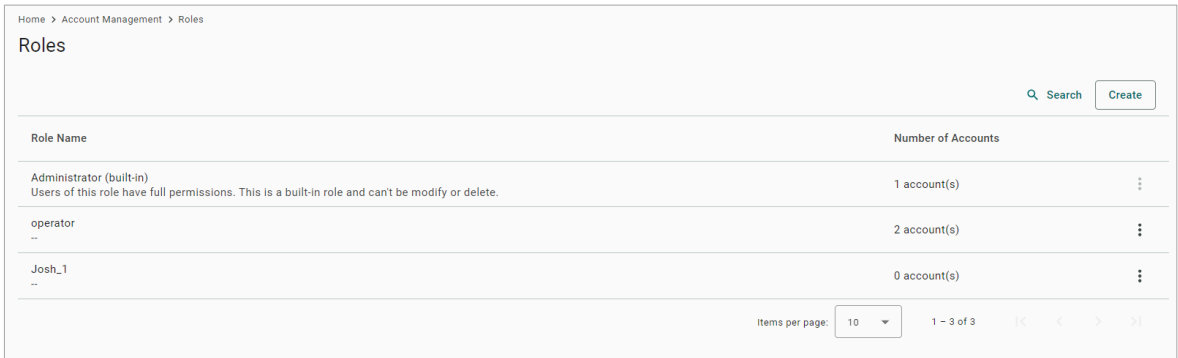
You can **View**, **Create**, **Edit**, and **Delete** user roles on your AIG device.



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 is set up, it will be available for selection under the Account.

To ensure enhanced security for your AIG-502, create user roles with specific permissions for user accounts. For details, see Account Management. In consideration of the security requirements of the AIG-502, we recommend creating the following roles with the specified permissions.

| Role                     | Permissions                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator            | All                                                                                                                                            |
| Monitoring personnel     | (default) Monitoring<br>Data Management                                                                                                        |
| OT-field-site operators  | (default) Monitoring<br>Security Management<br>Device Configuration<br>Device Maintenance<br>Data Management<br>(optional) Add-on Applications |
| IT-maintenance personnel | (default) Monitoring<br>Device Configuration<br>Device Maintenance<br>Data Management<br>(optional) Add-on Applications                        |

## Password Policy

Home > Account Management > Password Policy

### Password Policy

**Info**

This setting will be applied to the password of new accounts or to future password changes. Existing passwords will not be affected.

To enhance the higher security level of your password, you may choose to set the minimum password length and the password strength policy.

Min. Password Length

8

Password Strength Policy

☒ At least one digit (0-9)

☒ Mixed upper and lower case letters (A-Z, a-z)

☒ At least one special character (~`!@#\$%^&\*()\_+={}[]\|.;'<>?,./)

The system will reminder password changes when an account reaches the reminder threshold upon logging in.

☒ Enable password change reminders

Reminder Threshold (day)

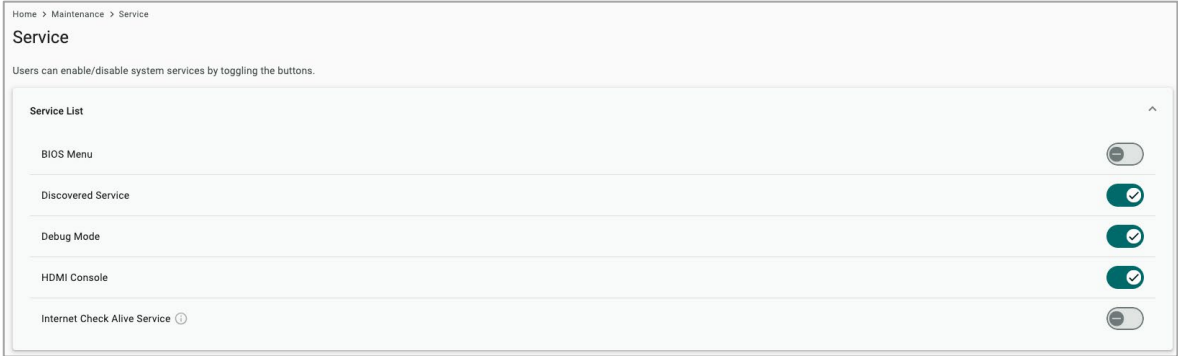
180

Save

| 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.                   |

# Service

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

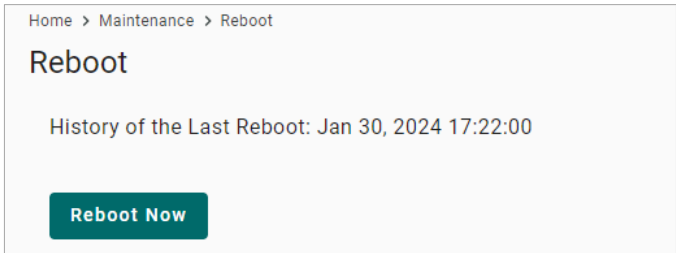


## NOTE

When the HDMI console is disabled, a watchdog service is automatically enabled to allow connection to the system console if the web console is deprecated. The watchdog service uses the `GET /api/_/ping` command to periodically check the availability of the web console.

# 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.

Home > Maintenance > Config. Import/Export

Config. Import/Export

Export

Click "Export" to save your current system log file and export the file.

Export

Import

Click "Browse" to select a previously exported configuration file to upload the file.

Configuration File

 Browse

Upload

## 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.

Backup & Restore

The backup function backs up the data (excluding Audit Log and System Log, which can be manually exported from the relevant page) on AIG devices to a file. Backup files are encrypted and stored in a designated location on the device. You can restore the data from the backups when needed.

 AIG Backup File

 None

Last Backup: --

File Size: --

Manage

Backup

Restore

Delete

# 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-502 and the repository is encrypted for system security.)

Home > Maintenance > Software Upgrades

Software Upgrades

Available Upgrades Upgrade Settings Upgrade History

Allow software upgrade

Over the Air Package Upload

Last checked on Nov 06, 2024 15:12:19

Product Package Patches

Search Check for upgrades

| <input type="checkbox"/> | Name             | Current Version     | New Version         | Size      |  |
|--------------------------|------------------|---------------------|---------------------|-----------|--|
| <input type="checkbox"/> | libcurl3-gnutls  | 7.74.0-1.3+deb11u11 | 7.74.0-1.3+deb11u13 | 772.1 KB  |  |
| <input type="checkbox"/> | libexpat1        | 2.2.10-2+deb11u5    | 2.2.10-2+deb11u6    | 431.1 KB  |  |
| <input type="checkbox"/> | libfdisk1        | 2.36.1-8+deb11u1    | 2.36.1-8+deb11u2    | 578.56 KB |  |
| <input type="checkbox"/> | libglb2-0-0      | 2.66.8-1            | 2.66.8-1+deb11u4    | 4.21 MB   |  |
| <input type="checkbox"/> | libgnutls30      | 3.7.1-5+deb11u3     | 3.7.1-5+deb11u6     | 3.3 MB    |  |
| <input type="checkbox"/> | libgssapi-krb5-2 | 1.18.3-6+deb11u4    | 1.18.3-6+deb11u5    | 473.09 KB |  |
| <input type="checkbox"/> | libk5crypto3     | 1.18.3-6+deb11u4    | 1.18.3-6+deb11u5    | 310.27 KB |  |
| <input type="checkbox"/> | libkrb5-3        | 1.18.3-6+deb11u4    | 1.18.3-6+deb11u5    | 1.16 MB   |  |
| <input type="checkbox"/> | libkrb5support0  | 1.18.3-6+deb11u4    | 1.18.3-6+deb11u5    | 177.15 KB |  |
| <input type="checkbox"/> | libmount1        | 2.36.1-8+deb11u1    | 2.36.1-8+deb11u2    | 499.71 KB |  |

Items per page: 10 1 - 10 of 37

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

Home > Maintenance > Software Upgrade

Software Upgrade

Available Upgrades Upgrade Settings Upgrade History

Allow software upgrade

Over-the-air Upload package

You may upload the product package file or patch file from your local drive.

Local File

Browse

Upload

## Upgrade Settings

Software Upgrade

Home > Maintenance > Software Upgrade

Available Upgrades

Upgrade Settings

Upgrade History

☒ Software upgrade over cellular

☒ Disk Snapshot before upgrade

☐ Check for upgrades automatically (Repeat every 1 week)

SAVE

☒ Check for upgrades automatically (Repeat every 1 week)

Sun.

✓ Mon.

Tue.

Wed.

Thur.

Fri.

Sat.

Time

23:00

Occurs every Mon. 23:00

| 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 to mitigate unexpected system failures.     |
| 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.

Home > Maintenance > Software Upgrade

Software Upgrade

Available Upgrades

Upgrade Settings

Upgrade History

This page shows the latest upgrade record.

Latest History

| Type      | Name             | Version    | Status    | Last Update            |
|-----------|------------------|------------|-----------|------------------------|
| > Package | moxa-aig-302-tpe | 1.0.0+5820 | ● Success | Jan 30, 2024, 17:01:33 |
| Success   |                  |            |           |                        |

Items per page:

10

1 - 1 of 1

## 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**.

[Home](#) > [Maintenance](#) > [Reset to Default](#)

### Reset to Default

#### Configuration Reset

If you wish to revert all configurations to their default settings, please utilize the "configuration default" option. It's important to note that the DLM connection will remain active (excludes **EULA agreement**).

> [Show details on storage location of log files](#)

☐ Reserve network settings

**Reset**

#### Factory Reset

If you want to reset the device back to the factory default use the **Factory Reset** function. It's important to note that the DLM connection will remain active.

**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 thorough lower-level formatting of the memory that is required to erase the data, it may take approximately 1.5 hours to complete.

### Device Retirement

You can initiate a process to securely erase a device, including all software, settings, and data on its internal disk. With this, the device will be restored to the factory default settings and all log files cleared, thereby preventing any potential data recovery from the device.

**Retire**

The AIG-502 comes with encrypted mSATA system storage for the highest level of data protection. Even if the storage is physically removed or stolen, your sensitive data remains completely unreadable, safeguarding your information until the device's retirement and beyond.

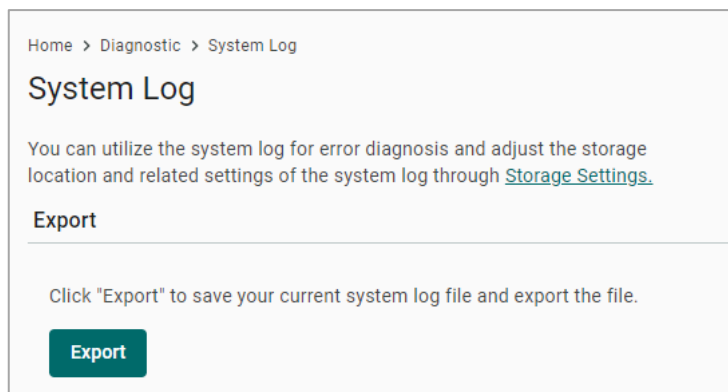
# Diagnostics

## 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.

The screenshot shows the 'Audit Log' page. At the top, there is a breadcrumb trail: 'Home > Diagnostic > Audit Log'. Below this, the title 'Audit Log' is displayed. There are two tabs: 'Log View' (active) and 'Log Settings'. In the top right corner, there is a search icon and a button labeled 'Export'. The main content is a table with the following columns: Type, Name, Content, Source, and Timestamp ↓. The table contains 10 rows of log entries. The first 9 rows are 'Notice' type, and the 10th row is an 'Alert' type. At the bottom right, there is a pagination control showing 'Items per page: 10' and '1 - 10 of 4531'.

| Type     | Name                | Content                       | Source | Timestamp ↓            |
|----------|---------------------|-------------------------------|--------|------------------------|
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 14:51:02 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 14:41:42 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 14:05:48 |
| > Notice | configurationExport | Configuration export success. | admin  | Feb 01, 2024, 13:49:14 |
| > Notice | configurationExport | Configuration export success. | admin  | Feb 01, 2024, 13:48:49 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 13:44:07 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 13:40:18 |
| > Alert  | loginFailure        | Login fail.                   | System | Feb 01, 2024, 13:39:13 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 13:36:45 |
| > Notice | loginSuccess        | Account admin login success.  | System | Feb 01, 2024, 13:26:53 |

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.

Home > Diagnostic > Audit Log

Audit Log

Log View   **Log Settings**

Reserved Storage Size (MB) ⓘ

100

Notification Threshold (%) ⓘ

80

☐ Enable time to live

Save

## 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 Fieldbus Protocol.

For Modbus troubleshooting, do the following:

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

← Modbus Master - TCP ▾

Home > Maintenance > Protocol Status > modbus master - TCP

Status Check provides diagnostic tool to help you identify connection issues. For editing the configuration, please go to **Modbus Master TCP**.

Diagnostic   Traffic Monitoring

Modbus Overview (Auto-refresh after 3s)

| Number of Connections | Send Requests | Received Valid Responses | Received Invalid Responses | Received Exceptions | Timeout |
|-----------------------|---------------|--------------------------|----------------------------|---------------------|---------|
| 1                     | 47537         | 47537                    | 0                          | 0                   | 0       |

Connections (Auto-refresh after 3s)

| Slave ID | Status | Remote IP/Port   | Send Requests | Received Valid Responses | Received Invalid Responses | Received Exceptions | Timeout |
|----------|--------|------------------|---------------|--------------------------|----------------------------|---------------------|---------|
| 1        | OK     | 10.123.12.59:502 | 47537         | 47537                    | 0                          | 0                   | 0       |

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

[illegible]

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

## 7. Security Capability

In this chapter, we will introduce the key security functions of the AIG-502 and a security hardening guide to deploy and operate the AIG-502 in a secure manner.

### Communication Integrity and Authentication

Below is a list of network communication services and protocols available in the AIG-502.

| Communication Interface          | Protocol             | TCP/ UDP Port | Authenticator                    | Default Configuration |
|----------------------------------|----------------------|---------------|----------------------------------|-----------------------|
| WEB                              | HTTP                 | TCP 80        | password                         | Disabled              |
|                                  | HTTPS                | TCP 443       | password                         | Enabled               |
| NTP client                       | NTP                  | UDP 123       | Key string                       | Disabled              |
| DHCP client                      | DHCP                 | UDP 67, 68    | N/A                              | Enabled (LAN1)        |
| DHCP server                      | DHCP                 | UDP 67, 68    | N/A                              | Disabled              |
| DNS client                       | DNS                  | TCP 53        | N/A                              | Disabled              |
| Azure IoT Edge                   | MQTT                 | TCP 8883      | 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              |
|                                  | HTTPS                | TCP 443       | Symmetric Key, X.509 certificate | Disabled              |
| Modbus Master                    | TCP                  | TCP 502       | N/A                              | Disabled              |
|                                  | RTU                  | RS232         | N/A                              | Disabled              |
| openssh-server (Debug mode used) | SSH                  | TCP 22        | password                         | Disabled              |
| mDNS                             | mDNS                 | UDP 5353      | N/A                              | Enabled               |

### Account Management

- **Permissions**
  - (Default) Monitoring – system and network status monitoring
  - Account Management – user access and permission allocation
  - Security Management – management for certification, Firewall settings, session monitoring etc.
  - Device Configuration – system configurations such as protocol settings, network settings etc.
  - Device Maintenance – software upgrade, backup & restore, etc.
  - Data Management – tag service and monitoring
  - Add-on Applications – Azure IoT Edge, Modbus Master

- **Role-based design:**

Considering the security context of AIG-502, we suggest creating roles with allocated permissions.

| Role                       | Permissions                                                                                                                                    |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrator              | All                                                                                                                                            |
| Monitoring personnel       | (Default) Monitoring<br>Data Management                                                                                                        |
| OT – Field site operator   | (Default) Monitoring<br>Security Management<br>Device Configuration<br>Device Maintenance<br>Data Management<br>(Optional) Add-on Applications |
| IT – maintenance personnel | (Default) Monitoring<br>Device Configuration<br>Device Maintenance<br>Data Management<br>(Optional) Add-on Applications                        |

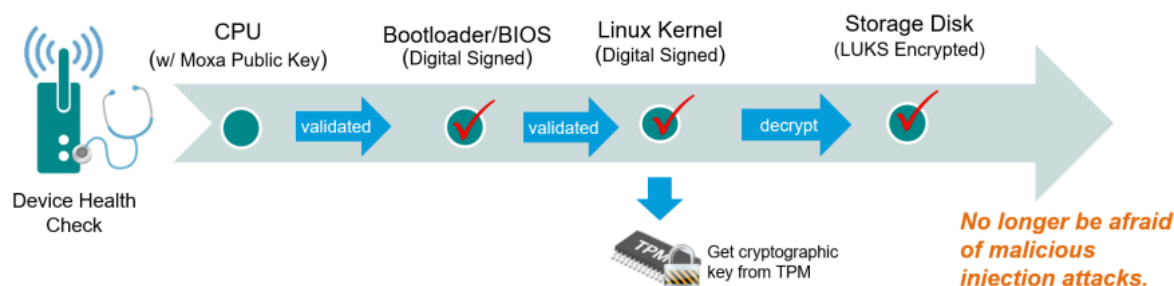
## Login Policy

To avoid unauthorized users repeatedly login the account to crack the passwords, AIG-502 is capable of configuring a login policy including the max. amount of the failure retry, failure counter reset period and the lockout time. To configure it, please refer to the chapter 6 Web Console > Security > Login Lockout.

## Secure Boot and Disk Encryption

Moxa's Secure Boot process begins from CPU as hardware root-of-trust to ensure integrity and authenticity of bootloaders and Linux kernels are validated with Moxa digital signature before execution, preventing malicious or unauthenticated bootloaders and kernels to run on Moxa Arm-based computer.

Next, only after BIOS and kernel have been validated, the LUKS (Linux Unified Key Setup) encrypted root file system (rtfs) will be decrypted by a key provisioned in TPM during factory production. The disk encryption prevents confidential data from being read without authorization when the device is stolen or lost.



- **Public Key Infrastructure (PKI)**

Moxa Secure Boot uses X.509 public key infrastructure (PKI) to validate authenticity and integrity of BIOS and Linux kernel.

- **Private Keys Protection**

Private keys used to digitally sign Moxa software are stored in an on-premises tamper and intrusion-resistant hardware security module (HSM), where strict access authorization and 24-hour video surveillance are applied.

- **Key lifecycle and revocation**

In an unlikely scenario where the private key stored in HSM is compromised, Moxa will announce the news on [Moxa Security Advisory](#), including instructions to revoke the compromised public key burned in the CPU via a utility downloadable from Moxa APT repository. Then update the BIOS and system image signed by a new private key.



# Managing Resources

- Core service protection: Grants higher privileges to elevate CPU priority and Block IO, preventing OOM killer incidents.
- Limit IoT Edge module resources: Sets maximum CPU and memory allocations at 90% and 70%, respectively.

## Audit Logs

AIG-502 provides the capability to generate security-related audit records for the following:

| IEC 62443 requirement    | AIG-502 audit log's categories                                                                                                                                                                                                                                                          |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access control           | <ul style="list-style-type: none"><li>• <b>Account &amp; Access</b></li></ul>                                                                                                                                                                                                           |
| request errors           | <ul style="list-style-type: none"><li>• <b>Command &amp; Message</b><ul style="list-style-type: none"><li>➢ commandRequestError</li></ul></li></ul>                                                                                                                                     |
| control system events    | <ul style="list-style-type: none"><li>• <b>Maintenance</b></li><li>• <b>Connection &amp; Interface</b></li><li>• <b>Performance &amp; Health</b></li></ul>                                                                                                                              |
| backup and restore event | <ul style="list-style-type: none"><li>• <b>Maintenance</b><ul style="list-style-type: none"><li>➢ systemBackup</li><li>➢ systemRestore</li><li>➢ configurationExport</li><li>➢ configurationImport</li></ul></li></ul>                                                                  |
| configuration changes    | <ul style="list-style-type: none"><li>• <b>Configuration Update</b></li></ul>                                                                                                                                                                                                           |
| audit log events         | <ul style="list-style-type: none"><li>• <b>Maintenance</b><ul style="list-style-type: none"><li>➢ auditLogExport</li></ul></li><li>• <b>Performance &amp; Health</b><ul style="list-style-type: none"><li>➢ auditLogOutOfSpace</li><li>➢ auditLogSizeReachThreshold</li></ul></li></ul> |

For details of the audit logs list, refer to the [Appendix C. Audit Log Index](#).

- The audit process (auditd) is an independent system service that doesn't impact other essential services, even if the audit process unexpectedly crashes.
- A dedicated system partition is allocated for audit logs, ensuring read-only access.
- Capable of configuring the desired storage and retention policy. You may refer to the Chapter 6 Web Console > Diagnostics > Audit Log.

# Security Advisories

AIG-502 offers a comprehensive list of security check items. To swiftly assess security, utilize the Security Dashboard for system scanning and aid in configuring your gateway securely. To configure it, please refer to the chapter 6 Web Console > Security Dashboard

| Category                       | Security Check                                                                           | Threat mitigated/ handled                                                                                                                                                                                  | Risk   |
|--------------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Account Setting                | Password not changed within the set time.                                                | To ensure there is no default password to access the gateway.                                                                                                                                              | Medium |
|                                | More than one session is active for the same account.                                    | To monitor the sessions, go to Security > Session Management to manage concurrent sessions.                                                                                                                | Medium |
|                                | More than one session is active for the same account with different source IP address.   |                                                                                                                                                                                                            | Medium |
| Application Networking         | System has open network port                                                             | Go to Security > Firewall and check the allow list.                                                                                                                                                        | Low    |
| Application Resource Usage     | IoT Edge modules utilize system disk's configurable space.                               | To ensure the IoT Edge modules are deployed in the specific path /var/run/ and /tmp/ in the system storage.                                                                                                | Low    |
|                                | IoT Edge modules utilize system disk's non-configurable space.                           |                                                                                                                                                                                                            | Medium |
|                                | IoT Edge module MODULE_NAME has been granted privilege.                                  | To grant permissions to the IoT Edge module, go to Cloud Connectivity > Azure IoT Edge > Module Permission and create a service account with the granted permission to the IoT Edge module.                | High   |
| Product Certificate Deployment | Production Certificate hasn't been configured for Azure IoT Edge Downstream Certificate. | For enhanced security robustness, it is recommended to use your own certificate instead of the default one. Go to Cloud Connectivity> Azure IoT Edge > Downstream Certificate, and upload the certificate. | Medium |
|                                | Azure IoT Edge is using connection string for provisioning.                              | For enhanced security robustness, it is recommended to use TPM or X.509 certificate.                                                                                                                       | Medium |
|                                | Any certificates have expired within the last three months.                              | Go to Cloud Connectivity > Azure IoT Edge or Security > HTTPS to check the certificates.                                                                                                                   | Medium |
|                                | Any certificates have expired.                                                           |                                                                                                                                                                                                            | High   |
| Service Setting                | Discover Service is enabled.                                                             | Go to Maintenance > Service to disable Discovered Service.                                                                                                                                                 | High   |
|                                | SSH Service is enabled.                                                                  | Go to Maintenance > Service to disable Debug Mode.                                                                                                                                                         | High   |
|                                | Account Lock Service is disabled.                                                        | Go to Security > Login Lockout to enable login failure lockout.                                                                                                                                            | High   |
|                                | System Use Notification is disabled.                                                     | Go to Security > System Use Notification to enable system use notification.                                                                                                                                | Medium |
| System Status Check            | New package updates are available for product software upgrade.                          | Go to Maintenance > Software Upgrade and click CHECK FOR UPGRADE to retrieve the latest upgrade pack information.                                                                                          | Medium |
|                                | No system backup performed in over a year or never.                                      | Go to Maintenance > Backup & Restore and click Manage to back up the system.                                                                                                                               | Medium |

## 8. Security Hardening Guide

In this chapter, we have included some recommendations to guide you on securely operating the AIG-502.

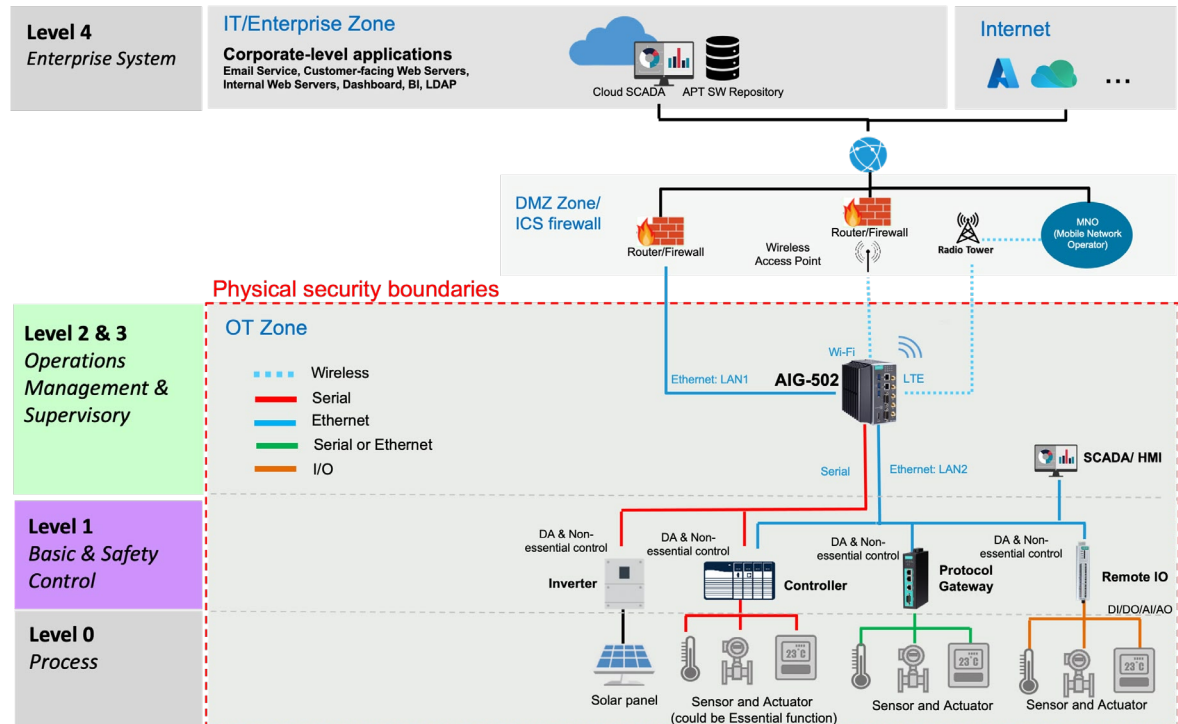
### Communication Integrity and Authentication

Below is a list of network communication services and protocols available in the AIG-502.

| Communication Interface          | Protocol             | TCP/ UDP Port | Authenticator                    | Default Configuration |
|----------------------------------|----------------------|---------------|----------------------------------|-----------------------|
| WEB                              | HTTP                 | TCP 80        | password                         | Disabled              |
|                                  | HTTPS                | TCP 443       | password                         | Enabled               |
| NTP client                       | NTP                  | UDP 123       | Key string                       | Disabled              |
| DHCP client                      | DHCP                 | UDP 67, 68    | N/A                              | Enabled (LAN1)        |
| DHCP server                      | DHCP                 | UDP 67, 68    | N/A                              | Disabled              |
| DNS client                       | DNS                  | TCP 53        | N/A                              | Disabled              |
| Azure IoT Edge                   | MQTT                 | TCP 8883      | 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              |
|                                  | HTTPS                | TCP 443       | Symmetric Key, X.509 certificate | Disabled              |
| Modbus Master                    | TCP                  | TCP 502       | N/A                              | Disabled              |
|                                  | RTU                  | RS232         | N/A                              | Disabled              |
| openssh-server (Debug mode used) | SSH                  | TCP 22        | password                         | Disabled              |
| mDNS                             | mDNS                 | UDP 5353      | N/A                              | Enabled               |

# Potential Threats and Corresponding Security Measures

A list of potential security threats that can harm AIG-502 and the corresponding security measures that need to be taken by the asset owner to mitigate the threats is illustrated in the following diagram.



| 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                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 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. | <ul style="list-style-type: none"> <li>Configure maximum storage capacity for individual Azure IoT Edge modules.</li> <li>Secure crucial data, like telemetry messages, on encrypted external storage (e.g., USB).</li> <li>Utilize the IoT Edge device metrics monitor on Azure IoT Hub for monitoring Azure IoT modules. See <a href="https://learn.microsoft.com/en-us/azure/iot-edge/how-to-collect-and-transport-metrics?view=iotedge-1.5&amp;tabs=iothub">https://learn.microsoft.com/en-us/azure/iot-edge/how-to-collect-and-transport-metrics?view=iotedge-1.5&amp;tabs=iothub</a>.</li> </ul> |

| Threat ID | Threat mitigated/handled                                                                                                                                                     | Security measures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. | <ul style="list-style-type: none"> <li>Back up the logs to Azure Blob storage for safekeeping.</li> <li>Store system logs on external storage, freeing the log partition for audit logs exclusively.</li> </ul> <p>AIG-502 originally supports:</p> <ul style="list-style-type: none"> <li>A reserved partition in the primary system for audit/system logs is provided.</li> <li>Logs don't override each other.</li> <li>A log generation mechanism to reduce redundancy, capturing crucial logs.</li> </ul> |
| 8         | Network data flow could be potentially interrupted, crashed or stopped by DOS attack.                                                                                        | <ul style="list-style-type: none"> <li>Configure an alternative WAN interface for connection failover, like Ethernet or Wi-Fi</li> <li>Configure keep-alive for cellular connections</li> </ul>                                                                                                                                                                                                                                                                                                                |
| 9         | Excessive write-tag requests from an IoT Edge module affect Modbus data acquisition.                                                                                         | <p>Restrict internal HTTPS API server usage to 10 requests per second maximum.</p> <ul style="list-style-type: none"> <li>Find the corresponding API "limit_req". See <a href="https://github.com/TPE-TIGER/TPE-TIGER.github.io">https://github.com/TPE-TIGER/TPE-TIGER.github.io</a>.</li> </ul> <p>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.</p>                                                   |
| 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-502 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-502 has anti-tamper labels on the enclosures. This allows the administrator to tell whether the device has been tampered with.
  - AIG-502 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-502 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 lost.
- Environmental Requirement
  - If AIG-502 connects to an untrusted network (e.g., Internet) via Ethernet or Wi-Fi, it MUST NOT directly connected to the untrusted network, which means a firewall must be setup between Ethernet and Wi-Fi connections from AIG-502 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.
  - BIOS 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 BIOS 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
  - a. Disabled communication interfaces that are not in use.
  - b. Make sure only trusted and reliable people are registered to access the AIG-502.
  - c. Frequently run the scan from the Security Dashboard, and execute the corresponding configuration or actions.
  - d. We recommend you reset AIG-502 to factory default upon receiving it to avoid the risk of potential software tampering before the AIG-502 reaches your hand.
- Maintenance
  - a. Perform software upgrade frequently to enhance features, security patches or fix bugs.
  - b. Perform backup of system on timely manner.
  - c. Examine audit logs frequently to detect any anomalies.
  - d. 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 Retire to reset the AIG-502 to factory default and further wipe out all user data, including logs, in an unrecoverable manner before removing the AIG-502 from.

## Publish Modes

| 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<br>Latest Values<br>All Changed Values<br>Latest Changed Values | All Values: All values recorded within a specified interval will be sent to the cloud.<br>Latest Values: Only the most recent value will be sent to the cloud.<br>All Changed Values: All values that have changed within the configured interval will be sent to the cloud.<br>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.<br>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<br>All Changed Values                                           | All Values: All values recorded within the specified size will be sent to the cloud.<br>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 can be set to ensure that the data is sent out as soon as it reaches the specified timer setting.                                                                                                                                                                                 |

### 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 here.

#### **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**.

## C. Audit Log Index

---

### Account & Access

| ID   | Name           | Content                                | Source (Operator)                           | Type   |
|------|----------------|----------------------------------------|---------------------------------------------|--------|
| AA01 | roleCreate     | Role:\$roleName be created             | \$Account Name                              | NOTICE |
| AA02 | roleDelete     | Role:\$roleName be deleted             | \$Account Name                              | NOTICE |
| AA03 | roleUpdate     | Role:\$roleName be updated             | \$Account Name                              | NOTICE |
| AA04 | accountCreate  | Account:\$accountName be created       | user: \$Account Name<br>service: \$APP Name | NOTICE |
| AA05 | accountDelete  | Account:\$accountName be deleted       | user: \$Account Name<br>service: \$APP Name | NOTICE |
| AA06 | accountUpdate  | Account:\$accountName be updated       | user: \$Account Name<br>service: \$APP Name | NOTICE |
| AA07 | passwordChange | Account:\$accountName password changed | \$Account Name                              | NOTICE |
| AA08 | loginSuccess   | Account:\$accountName login success    | System                                      | NOTICE |
| AA09 | loginFailure   | Login Fail                             | System                                      | ALERT  |
| AA10 | accountLock    | Account:\$accountName be locked        | System                                      | ALERT  |
| AA11 | accountUnlock  | Account:\$accountName unlocked         | System                                      | NOTICE |

### Configuration Update

| ID   | Name                | Content                             | Source (Operator)                           | Type   |
|------|---------------------|-------------------------------------|---------------------------------------------|--------|
| CU01 | configurationChange | \$serviceName configuration changed | user: \$Account Name<br>service: \$APP Name | NOTICE |

## Connection & Interface

| ID   | Name                           | Content                                                       | Source (Operator) | Type   |
|------|--------------------------------|---------------------------------------------------------------|-------------------|--------|
| CI01 | ipRenew                        | IP renew on interface:\$interfaceName                         | System            | NOTICE |
| CI02 | connectionStatusConnect        | Interface:\$interfaceName connected                           | System            | NOTICE |
| CI03 | connectionStatusDisconnect     | Interface:\$interfaceName disconnected                        | System            | NOTICE |
| CI04 | appServerConnectionEstablish   | Service:\$serviceName accepted connection request from client | \$APP Name        | NOTICE |
| CI05 | appServerConnectionDrop        | Service:\$serviceName drop connection from client             | \$APP Name        | NOTICE |
| CI06 | appClientConnectionConnect     | Service:\$serviceName connected                               | \$APP Name        | NOTICE |
| CI07 | appClientConnectionDisconnect  | Service:\$serviceName disconnected                            | \$APP Name        | NOTICE |
| CI11 | ethernetPortPlugIn             | Ethernet port:\$interfaceName plugged-in                      | System            | NOTICE |
| CI12 | ethernetPortPlugOut            | Ethernet port:\$interfaceName plugged-out                     | System            | NOTICE |
| CI13 | externalStoragePlugIn          | External storage:\$interfaceName plugged-in                   | System            | NOTICE |
| CI14 | externalStoragePlugOut         | External storage:\$interfaceName plugged-out                  | System            | NOTICE |
| CI15 | internetConnectionStatusChange | Internet Connection changed to \$status                       | System            | NOTICE |
| CI16 | externalStorageEncrypted       | New External storage \$status                                 | \$Account Name    | NOTICE |
| CI17 | appOpenPortSuccess             | Service:\$serviceName port opened                             | \$APP Name        | NOTICE |
| CI18 | appOpenPortFailure             | Service:\$serviceName failed to open port                     | \$APP Name        | ALERT  |

## Command & Message

| ID   | Name                  | Content                                | Source (Operator) | Type   |
|------|-----------------------|----------------------------------------|-------------------|--------|
| CM01 | commandReceive        | Service received command:\$commandName | \$APP Name        | NOTICE |
| CM02 | commandRequestError   | Service request failed                 | \$APP Name        | ALERT  |
| CM03 | commandRequestRecover | Service request recover                | \$APP Name        | NOTICE |

# Maintenance

| ID   | Name                        | Content                             | Source (Operator)                          | Type   |
|------|-----------------------------|-------------------------------------|--------------------------------------------|--------|
| MA01 | systemBackup                | System backup success               | \$Account Name                             | NOTICE |
| MA02 | systemRestore               | System restore success              | \$Account Name                             | NOTICE |
| MA03 | configurationExport         | Configuration export success        | \$Account Name                             | NOTICE |
| MA04 | configuraitonImport         | Configuration import success        | \$Account Name                             | NOTICE |
| MA05 | deviceReboot                | Device reboot                       | manual: \$Account Name<br>schedule: System | NOTICE |
| MA06 | softwarePackageUpdate       | Software package update<br>\$status | \$Account Name                             | NOTICE |
| MA07 | newSoftwareAvailable        | New software package available      | System                                     | NOTICE |
| MA08 | auditLogExport              | Audit log export success            | \$Account Name                             | NOTICE |
| MA09 | systemLogExport             | System log export success           | \$Account Name                             | NOTICE |
| MA10 | resetToFactoryDefault       | Reset to Factory Default            | \$Account Name                             | NOTICE |
| MA11 | resetToConfigurationDefault | Reset to configuration Default      | \$Account Name                             | NOTICE |
| MA12 | timeUpdate                  | System Time update success.         | manual: \$Account Name<br>NTP: System      | NOTICE |
| MA13 | timeUpdateFailure           | System Time update failure.         | manual: \$Account Name<br>NTP/GPS: System  | ALERT  |
| MA14 | systemBackupFailure         | System backup failure.              | \$Account Name                             | ALERT  |
| MA15 | systemRestoreFailure        | System restore failure.             | \$Account Name                             | ALERT  |

# Performance & Health

| ID   | Name                        | Content                                                                                                                                      | Source (Operator) | Type   |
|------|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------|--------|
| PH01 | untrustExecutionEnvironment | ThingsPro Edge is running on an untrusted execution environment.                                                                             | System            | ALERT  |
| PH02 | storageUsageAlarm           | System detects \$diskName storage usage reach 95%. You must take necessary actions immediately, before allocated disk space runs out.        | System            | ALERT  |
| PH03 | storageUsageNotice          | System detects \$diskName storage usage reach 80%. You must take necessary actions before allocated disk space runs out.                     | System            | NOTICE |
| PH04 | systemLoadingAlarm          | System detects unexpected system loading. You may upgrade device hardware spec or reduce unnecessary processes, to avoid system outage risk. | System            | NOTICE |
| PH05 | auditLogReachThreshold      | Audit log ran out of space, log rotation triggered.                                                                                          | System            | ALERT  |
| PH06 | httpMaxSessionExceeded      | Reach max HTTP/HTTPS session limit                                                                                                           | System            | ALERT  |
| PH07 | certificateExpired          | Certificate:\$certDisplayName is going to expired                                                                                            | System            | NOTICE |
| PH08 | certificateAdd              | Certificate(\$certDisplayName) be added                                                                                                      | \$APP Name        | NOTICE |
| PH09 | certificateRemove           | Certificate(\$certDisplayName) be removed                                                                                                    | \$APP Name        | NOTICE |
| PH11 | auditLogReachAlertThreshold | System detects audit log storage usage reach \$configurePercentage%                                                                          | System            | ALERT  |
| PH12 | systemInitialize            | System initialized                                                                                                                           | System            | NOTICE |
| PH13 | unlockPinFailure            | Failed to unlock SIM card's PIN code on interface:\$interfaceName                                                                            | System            | ALERT  |
| PH14 | certificateUpdate           | Certificate(\$certDisplayName) be updated                                                                                                    | \$APP Name        | NOTICE |
| PH15 | secretsAdd                  | Secrets(\$secretsDisplayName) be added                                                                                                       | \$APP Name        | NOTICE |
| PH16 | secretsUpdate               | Secrets(\$secretsDisplayName) be updated                                                                                                     | \$APP Name        | NOTICE |
| PH17 | secretsRemove               | Secrets(\$secretsDisplayName) be removed                                                                                                     | \$APP Name        | NOTICE |
| PH18 | auditLogReachTTL            | Audit logs have exceeded the configured live time, log rotate triggered.                                                                     | System            | ALERT  |

## D. System Tag List

---

| Provider Name | Source Name | Tag Name             | Data Type | Publish Interval |
|---------------|-------------|----------------------|-----------|------------------|
| system        | status      | cpuUsage             | unit64    | 1                |
| system        | status      | cpuTemperature       | unit64    | 1                |
| system        | status      | memoryBuffers        | unit64    | 1                |
| system        | status      | memoryUsed           | unit64    | 1                |
| system        | status      | memoryUnused         | unit64    | 1                |
| system        | status      | memoryCached         | unit64    | 1                |
| system        | status      | memoryUsage          | unit64    | 1                |
| system        | status      | memoryFree           | unit64    | 1                |
| system        | status      | memoryTotal          | unit64    | 1                |
| system        | status      | gpsLat               | double    | 1                |
| system        | status      | gpsLong              | double    | 1                |
| system        | network     | netowrkStatus        | string    | 10               |
| system        | network     | networkTx            | unit64    | 10               |
| system        | network     | networkRx            | unit64    | 10               |
| system        | network     | networkUsage         | unit64    | 10               |
| system        | network     | \$(name)NetworkUsage | unit64    | 10               |
| system        | network     | \$(name)NetworkRx    | unit64    | 10               |
| system        | network     | \$(name)NetworkTx    | unit64    | 10               |
| system        | network     | \$(name)Signal       | double    | 60               |
| system        | network     | \$(name)SignalLevel  | int32     | 60               |
| system        | storage     | systemDiskUsed       | uint64    | 1                |
| system        | storage     | systemDiskFree       | uint64    | 1                |
| system        | storage     | systemDiskPercent    | double    | 1                |
| system        | storage     | \$(storage)Used      | uint64    | 1                |
| system        | storage     | \$(storage)Free      | uint64    | 1                |
| system        | storage     | \$(storage)Percent   | double    | 1                |

## E. Regulatory Approval Statement

---

### FCC Statement

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 minimum distance 20cm 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.

### IC Statement

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

This device has also been evaluated and shown compliant with the ISED RF Exposure limits under mobile exposure conditions. (antennas are greater than 20cm 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).