LI-ION TAMER RACK MONITOR USER MANUAL

LI-ION TAMER CONTROL BOX AND SENSORS

May 2022
Doc. No. 35793_A2

Disclaimer

The contents of this document is provided on an "as is" basis. No representation or warranty (either express or implied) is made as to the completeness, accuracy or reliability of the contents of this document. The manufacturer reserves the right to change designs or specifications without obligation and without further notice. Except as otherwise provided, all warranties, express or implied, including without limitation any implied warranties of merchantability and fitness for a particular purpose are expressly excluded.

Intellectual Property and Copyright

General Warning

This product must only be installed, configured and used strictly in accordance with the General Terms and Conditions, User Manual and product documents available from Xtralis. All proper health and safety precautions must be taken during the installation, commissioning and maintenance of the product. The system should not be connected to a power source until all the components have been installed. Proper safety precautions must be taken during tests and maintenance of the products when these are still connected to the power source. Failure to do so or tampering with the electronics inside the products can result in an electric shock causing injury or death and may cause equipment damage. Xtralis is not responsible and cannot be held accountable for any liability that may arise due to improper use of the equipment and/or failure to take proper precautions. Only persons trained through an Xtralis accredited training course can install, test and maintain the system.

Liability

You agree to install, configure and use the products strictly in accordance with the User Manual and product documents available from Xtralis.

Xtralis is not liable to you or any other person for incidental, indirect, or consequential loss, expense or damages of any kind including without limitation, loss of business, loss of profits or loss of data arising out of your use of the products. Without limiting this general disclaimer the following specific warnings and disclaimers also apply:

Fitness for Purpose

You agree that you have been provided with a reasonable opportunity to appraise the products and have made your own independent assessment of the fitness or suitability of the products for your purpose. You acknowledge that you have not relied on any oral or written information, representation or advice given by or on behalf of Xtralis or its representatives.

Total Liability

To the fullest extent permitted by law that any limitation or exclusion cannot apply, the total liability of Xtralis in relation to the products is limited to:
(i) in the case of services, the cost of having the services supplied again; or
(ii) in the case of goods, the lowest cost of replacing the goods, acquiring equivalent goods or having the goods repaired.

Indemnification

You agree to fully indemnify and hold Xtralis harmless for any claim, cost, demand or damage (including legal costs on a full indemnity basis) incurred or which may be incurred arising from your use of the products.

Miscellaneous

If any provision outlined above is found to be invalid or unenforceable by a court of law, such invalidity or unenforceability will not affect the remainder which will continue in full force and effect. All rights not expressly granted are reserved.

Contact Us

UK and Europe +44 1442 242 330 **The Americas** +1 800 229 4434

Middle East +962 6 588 5622 **Asia** +86 21 8038 7825 **Australia and New Zealand** +61 3 9936 7000

www.xtralis.com

Contents

1 General

1.1 Scope

This document provides specification details of the Li-ion Tamer® Rack Monitor system and is intended to aid users in installation, operation, and maintenance.

Notes!

- This device detects the venting of electrolyte solvent vapours from lithium-ion batteries. It does not prevent fires or thermal runaway. This device is not a stand-alone safety device and should be incorporated into a proper safety system. If device responds, there is a risk of battery fault which could lead to thermal runaway. To avoid injury, leave area immediately.
- The Li-ion Tamer system must be powered OFF any time the battery system is being commissioned, tested, maintained, etc. Li-ion Tamer is intended for operating battery systems, so alarms may be activated if exposed to cross-sensitive gases from the environment surrounding the battery system.

1.2 Key Features

- Early warning of lithium-ion battery failures
- Enable thermal runaway prevention with proper mitigation actions
- Single cell failure detection without electrical or mechanical contact of cells
- Extended product lifetime
- Calibration-free product
- Highly reliable output signal
- Low power consumption
- Compatible with all lithium-ion battery form factors and chemistries
- Easy installation
- Independent and redundant perspective on battery health
- Auto diagnostic capabilities
- Reduction/removal of false positive signals
- Configurable communication protocols including digital outputs and serial communication

1.3 Certifications

The Rack Monitor system has been designed and tested to meet the following certifications:

- ETL listed to UL 61010 and CSA 22.2 NO. 61010 for product safety
- EN 61326 for EU Directive (2014/30/EU)
- RoHS 3 EU 2015/863
- UKCA

1.4 Codes, Standards or Regulations

The Rack Monitor system is to be installed in battery systems according to the following codes and regulations:

- Any national or international standards or fire codes that require detection of electrolyte vapours (off gassing phase)
- Local codes and standards

1.5 Quality Assurance

1.5.1 Manufacturer

The manufacturer has an ISO 9001:2015 registered quality system and is committed to achieving the following objectives:

- Development of innovative process and product solutions.
- On-time delivery of products and services to our customers.
- Provide for the safety and empowerment of our team members.
- Continual improvement of operations and our quality system.

1.5.2 Equipment Supplier

- The equipment supplier shall be authorized trained by the manufacturer to calculate/design, install, test and maintain the Li-ion Tamer system.
- The equipment supplier shall be able to produce a certificate of training from the manufacturer.

1.5.3 Installer

- The equipment installer shall be authorized and trained by the manufacturer and shall have the ability to design a system based on code requirements.
- The installer shall be capable of providing calculations, design, and testing documents upon request.

1.5.4 Warranty

- The manufacturer shall guarantee the product by warranty for a period of one year with a target lifetime of more than ten years.
- The installation and dip switch configuration of the Li-ion Tamer Rack Monitor system shall be performed by trained suppliers or commissioning parties.

1.5.5 Training

- The manufacturer or agent of the manufacturer shall train all personnel involved in the supply, installation, commissioning, operation and maintenance of the Rack Monitor system. Contact a Honeywell/ Xtralis or Nexceris representative to arrange training sessions.

1.6 Documentation

The following documentation shall be supplied by the manufacturer:

- Product technical datasheets and site layout drawings for sensor placement, when applicable.
- The manufacturer’s signal integration, operation and maintenance manuals shall be supplied to all installing and purchasing parties.
- The manufacturer’s commissioning manual shall be supplied to all suppliers and commissioning parties.

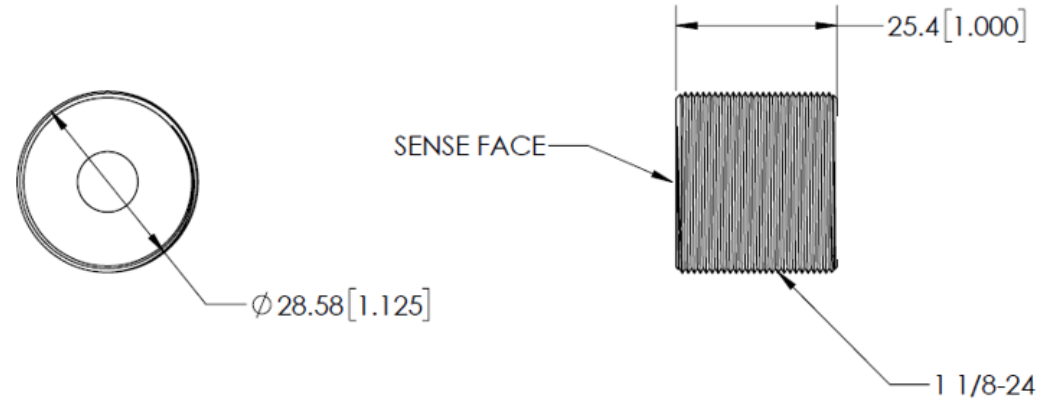
2 System Specifications and Operation

2.1 Off-Gas Monitor Hardware Overview

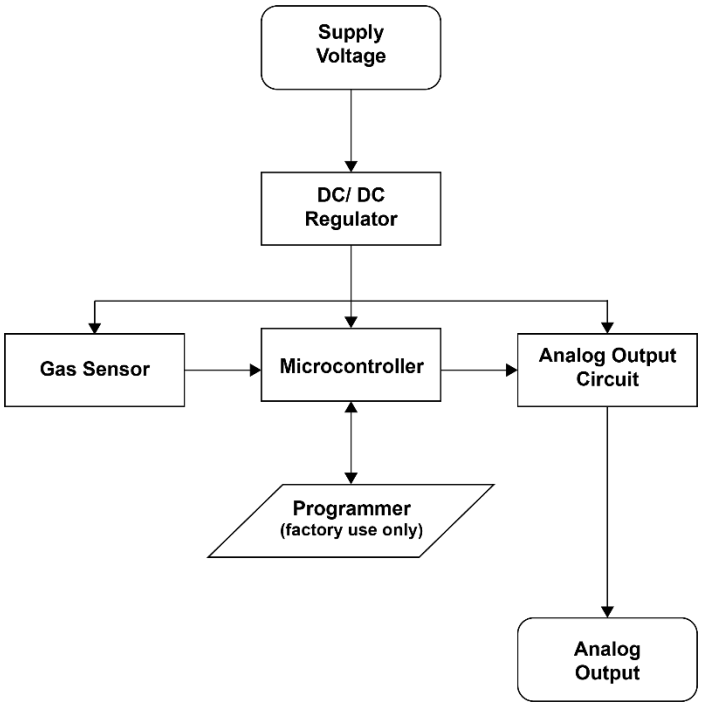
2.1.1 Design Level

The off-gas monitor (OGM) hardware includes the Monitoring Sensors (LT-SEN-M) and Reference Sensors (LT-SEN-R). Monitoring Sensors are indicated by black cables and corresponding controller port labels. Reference Sensors are indicated by blue cables and corresponding controller port labels.

The sensor dimensions are shown below:



A simplified function model of the off-gas monitor is depicted below. Note that all programming and calibration is performed by the manufacturer.



2.1.2 Detection Method and Output

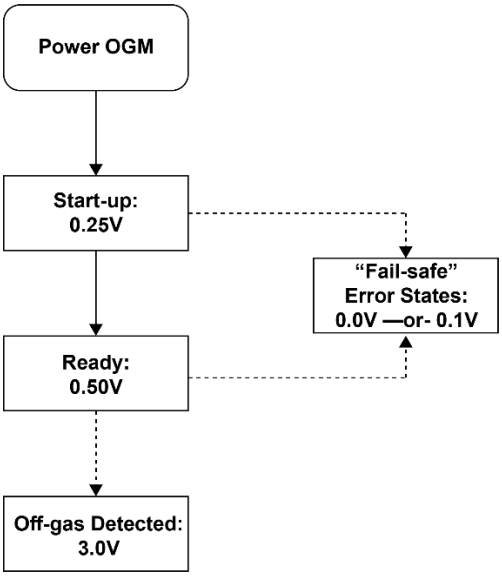
The detection method for all off-gas monitors is as follows:

1. Raw sensor signal is gathered as a continuous function.
2. Li-ion Tamer Event Detection Algorithm processes the signal with a discrete algorithm function indicating event detection.

The gas detection specifications are as follows:

1. Targets lithium ion battery electrolyte solvent vapours (off gassing)
2. Minimum detection threshold of less than 1 [ppm/sec] and response time of 5 seconds
3. Single-cell failure fault detection capabilities

The off-gas monitor expected output signal is depicted below. Note that the individual OGM outputs are not visible when connected to the Li-ion Tamer controller.



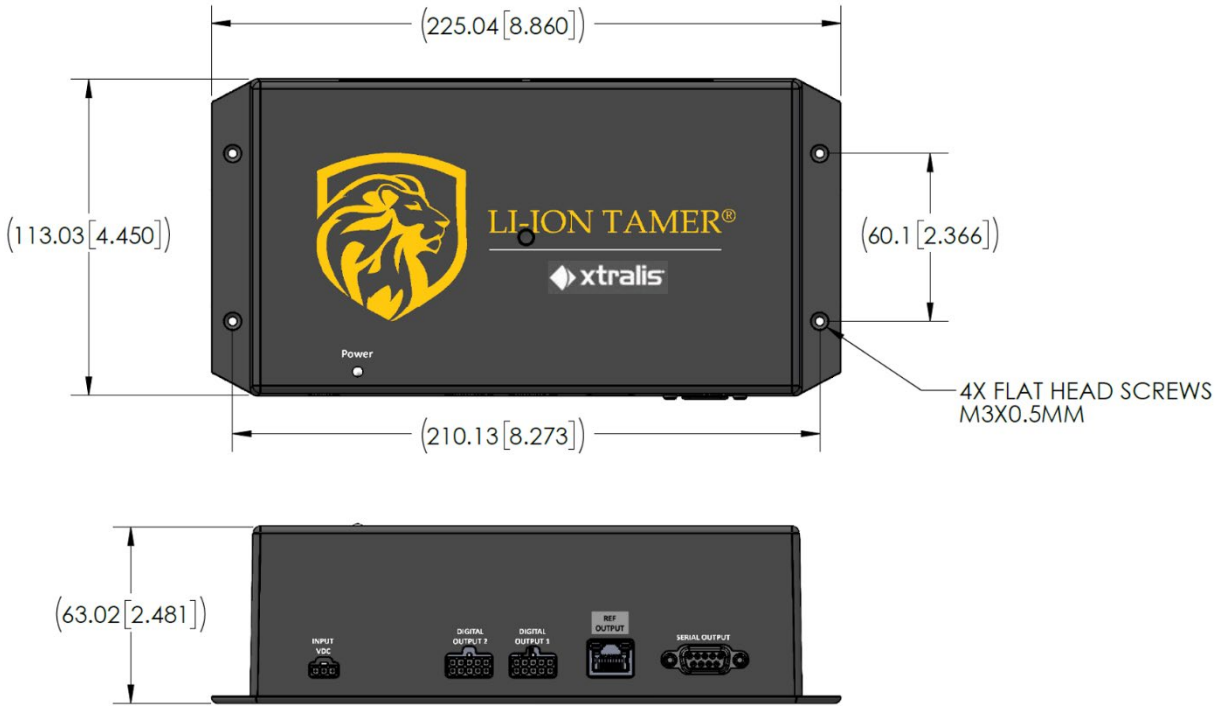
The “fail-safe” error states provide numerous diagnostic capabilities, which are detailed below for both 0.0 VDC and 0.1 VDC outputs.

Li-ion Tamer Output	Condition	Diagnostic Capability
0.0 VDC	Error state – Power failure	• Loss of power to device • Loss of internal DC/DC regulation • Failure of A/D output • Failure of critical component on circuit board • Component failure on output circuit • Provides a “fail-safe” diagnostic state
0.1 VDC	Error state – Signal out of range	Gas sensor signal exceeds max threshold Gas sensor signal resistance below min threshold • Loss of sensor continuity • Failure of sensor heater • Failure of communication between sensor and microcontroller

2.2 Controller Specifications

The Li-ion Tamer controller (LT-CTR-C), detailed in Section 3, has the general specifications as follows:

1. Dimensions: 210 (W) x 113 (L) x 63 (H) [mm]
2. Input power range: 12 – 28 VDC
3. Maximum of fifteen (15) sensors per controller
4. System outputs both digital outputs and MODBUS signal



2.2.1 Power Consumption

The power consumption requirements are detailed below for a variety of conditions.

Power consumption specifications	
Detail	**Specification**
Controller (no sensors)	2.4 W (@ 24 VDC) 1.4 W (@ 12 VDC)
Sensor	275 mW (@ 5 VDC)
Controller (fully populated, 15 sensors)	6.6 W (@ 24 VDC) 5.6 W (@ 12 VDC)
Fuse Rating	3.5 A

2.2.2 Environmental Specifications

The environmental operating conditions are detailed below. Operating outside of the specified ranges may lead to decreased performance and part damage.

Environmental specifications	
Condition	**Specification**
Temperature	-10 to +60˚C
Humidity	5 to 95% RH
Max temperature change	8.6˚C/ min

2.2.3 Digital Outputs

The Combined Controller (LT-CTR-C) provides multiple digital output signals via two (2) 10-pin Molex ports. The Digital Output Cables (LT-ACC-DCL) may be connected to those ports in order to access the outputs listed below via bare-wire connections.

Note!

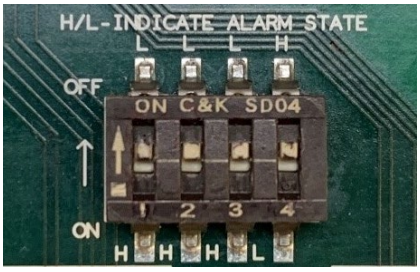
Each digital output conductor has a 100mA maximum current draw.

1. Unique sensor-specific alarms
2. Alarm Any: aggregated output signaling if electrolyte solvent vapours are detected by any Monitoring Sensor connected to the controller
3. System Alarm: aggregated output signaling if electrolyte solvent vapours are detected by any Monitoring Sensor connected to any controller on the daisy-chained network
4. Sensor Error: diagnostic output signaling if any sensor connected to the controller is in an error state (detailed in Section 2.1.2)

Note!

The controller(s) must remain powered ON in the case of a sensor error to ensure proper troubleshooting.

The digital outputs may be configured by removing the controller back-plate and accessing the DIP switch block shown below, with corresponding labels printed directly on the PCB.



Note!

The digital output configuration switches are default set to the OFF position as printed on the PCB.

The table below details the output signals and their corresponding numeric labels on the switch block. Turning the switches ON/OFF will change the HIGH/LOW polarity of the digital output signals.

Output Signal	Switch Label	DIP Switch Position	Digital Output State
Sensor-specific Alarm (Monitoring Sensors 1 through 12)	1	ON	Ready – LOW (0 VDC)
			Alarm – HIGH (12 – 28 VDC)
		OFF	Ready – HIGH
			Alarm – LOW
Alarm Any	2	ON	Ready – LOW
			Alarm Any – HIGH
		OFF	Ready – HIGH
			Alarm Any – LOW
System Alarm	3	ON	Ready – LOW
			System Alarm – HIGH
		OFF	Ready – HIGH
			System Alarm – LOW
Sensor Error	4	ON	Ready – HIGH
			Fault – LOW
		OFF	Ready – LOW
			Fault – HIGH

An example digital output DIP switch configuration and the output signal details are shown below:

1. Sensor-specific outputs (Switch 1 – OFF)
   - Ready: 12 – 28 VDC (Supply Voltage)
   - Alarm State: 0 VDC
2. Alarm Any (Switch 2 – ON)
   - Ready: 0 VDC
   - Alarm State: 12 – 28 VDC (Supply Voltage)
3. System Alarm (Switch 3 – ON)
   - Ready: 0 VDC
   - Alarm State: 12 – 28 VDC (Supply Voltage)
4. Sensor Error (Switch 4 – OFF)
   - Ready: 0 VDC
   - Fault State: 12 – 28 VDC (Supply Voltage)

The wire colors for each signal are detailed below with the corresponding digital output ports labelled on the controller.

Digital Output Connector 1

Pin	Status	Wire Color
1	Monitoring Sensor 1	Blue
2	Monitoring Sensor 2	Orange
3	Monitoring Sensor 3	White
4	Monitoring Sensor 4	Green
5	Monitoring Sensor 5	Red
6	Monitoring Sensor 6	White/ Black
7	Monitoring Sensor 7	Red/ Black
8	Monitoring Sensor 8	Green/ Black
9	Sensor Error	Orange/ Black
10	GND	Black

Digital Output Connector 2

Pin	Status	Wire Color
1	Monitoring Sensor 9	Blue
2	Monitoring Sensor 10	Orange
3	Monitoring Sensor 11	White
4	Monitoring Sensor 12	Green
7	Alarm Any	Red/ Black
8	System Alarm	Green/Black
9	Sensor Error	Orange/ Black
10	GND	Black

Note!

Controllers with Rev A motherboards will have the Alarm Any pinout on the Green/Black conductor. Please contact an Xtralis representative for help identifying the motherboard version.

2.2.4 Modbus Output

The Combined Controller (LT-CTR-C) provides a single Modbus RTU signal over RS-232 3-wire (TX, RX, GND). A standard DB-9 serial cable may be used to obtain the output with the following specifications below.

MODBUS communication specifications	
Detail	**Specification**
Description	Modbus RTU over RS232
Baud rate	9600
Parity	None
Stop bit	One
Hardware	RS232 3-wire (TX, RX, ground)

The outputs are comparable to the digital outputs, where there is an output for each Monitoring Sensor alarm, an Alarm Any output, Sensor Error output and System Alarm output. There are also individual Sensor Error indicators conveyed over the Modbus output. Each bit from the serial string is either a 1 or 0, indicating alarm and normal states, respectively.

The controllers natively have MODBUS RTU and the signal can be converted to TCP/IP with an adapter provided by Xtralis, which is detailed in Section 4.3.

Outputs	Function Code	Bit/ Register Address
Monitoring 1 Alarm	01 (0x01)	1
Monitoring 2 Alarm	01 (0x01)	2
Monitoring 3 Alarm	01 (0x01)	3
Monitoring 4 Alarm	01 (0x01)	4
Monitoring 5 Alarm	01 (0x01)	5
Monitoring 6 Alarm	01 (0x01)	6
Monitoring 7 Alarm	01 (0x01)	7
Monitoring 8 Alarm	01 (0x01)	8
Monitoring 9 Alarm	01 (0x01)	9
Monitoring 10 Alarm	01 (0x01)	10
Monitoring 11 Alarm	01 (0x01)	11
Monitoring 12 Alarm	01 (0x01)	12
Alarm Any	01 (0x01)	16
Sensor Error	01 (0x01)	17
Monitoring 1 Error	01 (0x01)	18
Monitoring 2 Error	01 (0x01)	19
Monitoring 3 Error	01 (0x01)	20
Monitoring 4 Error	01 (0x01)	21
Monitoring 5 Error	01 (0x01)	22
Monitoring 6 Error	01 (0x01)	23
Monitoring 7 Error	01 (0x01)	24
Monitoring 8 Error	01 (0x01)	25
Monitoring 9 Error	01 (0x01)	26
Monitoring 10 Error	01 (0x01)	27
Monitoring 11 Error	01 (0x01)	28
Monitoring 12 Error	01 (0x01)	29
Reference 1 Error	01 (0x01)	30
Reference 2 Error	01 (0x01)	31
Reference 3 Error	01 (0x01)	32
System Alarm	01 (0x01)	59
Heartbeat	04 (0x04)	6

The outputs and their corresponding function codes are shown in the table above. The “Heartbeat” is a watchdog timer that continuously increases every second until 3600, when it resets to 0. It can be used to confirm that the controller is providing live information and has not timed out, frozen, or lost power.

2.3 Li-ion Tamer Part Numbers

The full list of Li-ion Tamer Rack Monitor component part numbers is detailed below.

Part Number	Item	Description
LT-SEN-M	OGM, Monitoring Sensor	Mounted on/near Li-ion battery rack to detect electrolyte solvent vapours from cells
LT-SEN-R	OGM, Reference sensor	Mounted around the ESS
LT-CTR-C	Combined Controller	Controller with 12 ports for monitoring and 3 ports for reference sensors
LT-ACC-PCL	10' Power Cable	Power cable for all Li-ion Tamer controllers
LT-ACC-DCL	10' Digital Output Cable	Digital output cable for all Li-ion Tamer controllers
LT-ACC-MCL-25, -50, -100	25, 50, 100 (ft) Monitoring Sensor Cable (various lengths)	Shielded RJ45 connector cable used with Monitoring sensors, Black
LT-ACC-RCL-25, -50, -100	25, 50, 100 (ft) Reference Sensor Cable (various lengths)	Shielded RJ45 connector cable used with Reference sensors, Blue
LT-ACC-CCL-1, -3, -25, -50, -100	1, 3, 25, 50, 100 (ft) Controller Daisy Chain Cable (various lengths)	Shielded RJ45 connector cable used to daisy-chain reference network signal to other controllers, Grey
LT-ACC-SCL-MF	6' Male-Female Serial Cable	MODBUS DB9 RS232 cable to connect the serial output to the TCP/IP Adapter or customer interface
LT-ACC-IPA	MODBUS TCP/IP Adapter	Adapter for changing the native MODBUS RTU output from the Li-ion Tamer controller to MODBUS TCP/IP
LT-ACC-RLY	Form C Relay	Standard dry-contact Form C relay
LT-ACC-TST	Li-ion Tamer Puff Test DEC Bottle	A plastic bottle with a small amount of DEC for use during bump testing of sensors
LT-ACC-BKT-PK5	Sensor Mount Kit Spare - 5BKT 10NUT	Sensor Mount Kit Spare – 5x brackets 10x nuts
LT-ACC-OEM	OEM Board	A low power device that monitors electrolyte solvent vapours for increased safety

3 Controller Configurations

3.1 Combined Controller

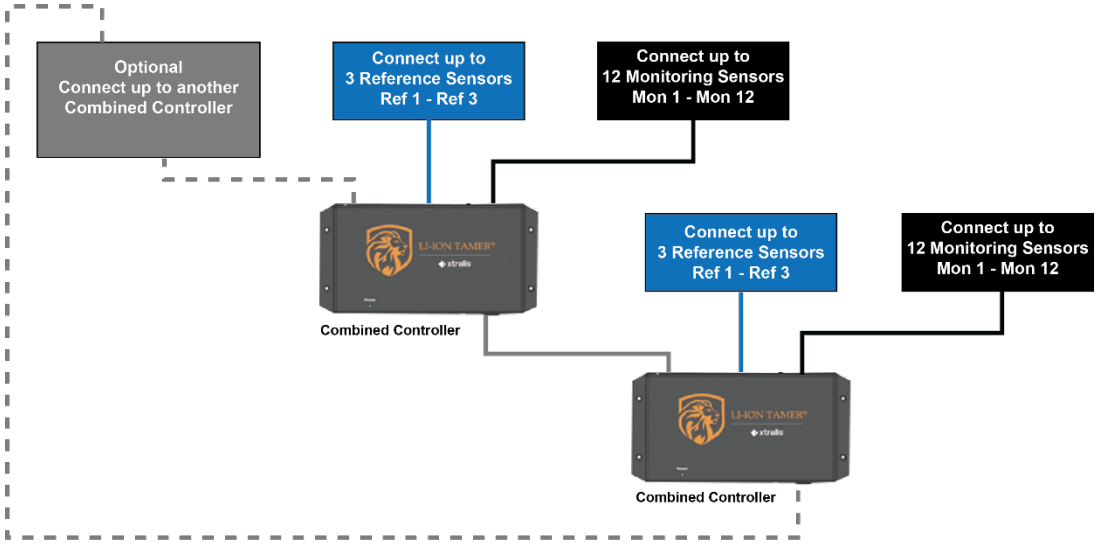
The Combined Controller configuration specifications are as follows:

1. Connect up to 12 Monitoring and 3 Reference Sensors.
2. The input ports, shown below, indicate the sensor states as follows (detailed in Section 2.1.2):
   a. Start-up or Ready states: solid green LED
   b. Alarm state: blinking green LED
   c. Error state: solid amber LED
3. “REF INPUT” is for the input signal from controllers in a network (daisy chain).
4. “REF OUTPUT” is for the output signal to controllers in a network (daisy chain).

3.2 System Configuration

The combined controllers and sensors can be configured in a variety of ways, depending on the application area. Optimized controller configurations are to be determined by the manufacturer or a trained Xtralis representative.

The basic layout for a system utilizing Combined Controllers is shown below. Note that the system may be scaled by daisy-chaining multiple controllers in the manner shown. There is no limitation to the number of controllers that can be daisy-chained.



3.2.1 Controller Daisy-Chaining

In systems requiring multiple controllers, gray Controller Daisy Chain Cables (LT-ACC-CCL) must be used to ensure proper system function. Several important signals are conveyed over the daisy-chain cables, as follows:

> **Note!**
>
> The daisy-chain signals below are specific to Gen 2+ controllers. Gen 2 and Gen 2+ controllers may be daisy-chained together; however, the Gen 2+ controllers in the loop will operate as Gen 2 controllers.
>
> The controller generations are detailed in Section 3.3.

1. Sensor Error – allows all controllers on the network to generate a Sensor Error output if any sensor on the network enters the error state (detailed in Section 2.1.2)
2. System Alarm – aggregating alarm signal indicating if any Monitoring Sensor on the network is alarmed; allows all controllers on the network to generate a System Alarm output and enter the Heightened Alarm State (detailed in Section 3.2.2)
3. Reference Any – aggregating signal indicating if any Reference Sensor on the network is alarmed; allows all controllers on the network to enter the Lockout State (detailed in Section 3.2.2).

> **Note!**
>
> A maximum of two Gen 2+ controllers may be daisy-chained together.

3.2.2 Controller States

The controller undergoes internal logic prior to generating output signals, which are referred to as the “controller states”. These are determined based on which type of sensor is activated first.

1. Heightened Alarm State – activated when a Monitoring Sensor is alarmed prior to a Reference Sensor
   a. Lasts for 10 minutes
   b. Indicates that the venting of electrolyte solvent vapours (off-gassing phase) from battery has been detected
   c. Reference Sensors cannot nullify the alarm at this time
   d. Reference Sensors can no longer activate the Lockout State after the initial activation of the Heightened Alarm State

> **Note!**
>
> Controllers must be power cycled after an alarm is activated on a deployed/ commissioned Li-ion Tamer system. See Section 5.2.6 for more details.

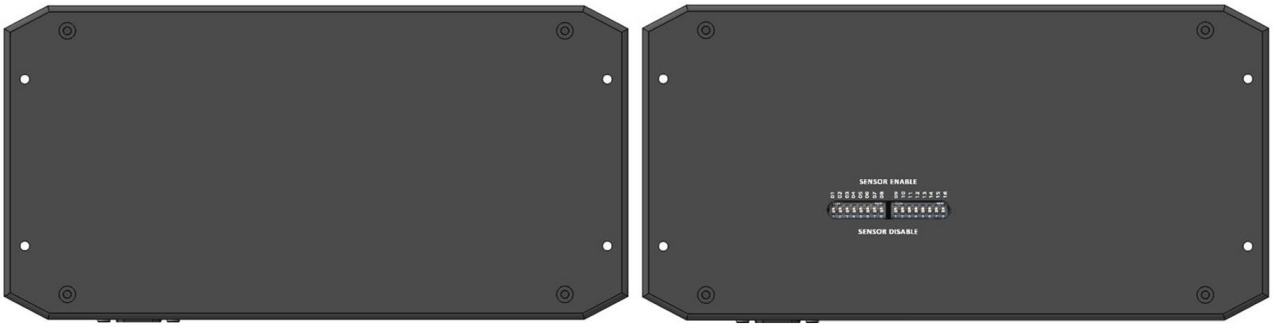
2. Lockout State – activated when a Reference Sensor is alarmed prior to a Monitoring Sensor
   a. Lasts for 3 minutes
   b. Indicates that cross-sensitive gases have been detected that may cause false-positives
   c. Monitoring Sensors cannot activate the Heightened Alarm State during this time

3.3 Controller Generations

There are two versions of the Li-ion Tamer Combined Controller, which are referred to as Gen 2 and Gen 2+. This user manual is specific to the Gen 2+ version and should not be used when working with Gen 2 controllers.

A simple way to distinguish controller versions is to check the backplate.

The Gen 2 controller backplate will not have visible “Sensor Disable” switches, whereas the Gen 2+ controller will have visible switches, as shown below.



Gen 2 **Gen 2+**

3.3.1 Gen 2 Outputs

This section covers the output signals for Gen 2, specifically. The digital outputs are detailed below:

1. Sensor-specific outputs
   - Ready: 12 – 28 VDC (Supply Voltage)
   - Alarm State: 0 VDC
2. Alarm Any
   - Alarm State: 12 – 28 VDC (Supply Voltage)
   - Ready: 0 VDC
3. Sensor Error
   - Ready: 0 VDC
   - Fault State: 12 – 28 VDC (Supply Voltage)

Note!

The controller(s) must remain powered ON in the case of a sensor error to ensure proper troubleshooting.

The wire colors for each signal are detailed below with the corresponding digital output ports labelled on the controller.

Digital Output Connector 1

Pin	Status	Wire Color
1	Monitoring Sensor 1	Blue
2	Monitoring Sensor 2	Orange
3	Monitoring Sensor 3	White
4	Monitoring Sensor 4	Green
5	Monitoring Sensor 5	Red
6	Monitoring Sensor 6	White/ Black
7	Monitoring Sensor 7	Red/ Black
8	Monitoring Sensor 8	Green/ Black

Digital Output Connector 1

Pin	Status	Wire Color
9	Sensor Error	Orange/ Black
10	GND	Black

Digital Output Connector 2

Pin	Status	Wire Color
1	Monitoring Sensor 9	Blue
2	Monitoring Sensor 10	Orange
3	Monitoring Sensor 11	White
4	Monitoring Sensor 12	Green
7	Alarm Any	Red/ Black
9	Sensor Error	Orange/ Black
10	GND	Black

The Modbus output is similar to that of Gen 2+, with the function codes and registers below:

Outputs	Function Code	Bit/ Register Address
Monitoring 1 Alarm	01 (0x01)	1
Monitoring 2 Alarm	01 (0x01)	2
Monitoring 3 Alarm	01 (0x01)	3
Monitoring 4 Alarm	01 (0x01)	4
Monitoring 5 Alarm	01 (0x01)	5
Monitoring 6 Alarm	01 (0x01)	6
Monitoring 7 Alarm	01 (0x01)	7
Monitoring 8 Alarm	01 (0x01)	8
Monitoring 9 Alarm	01 (0x01)	9
Monitoring 10 Alarm	01 (0x01)	10
Monitoring 11 Alarm	01 (0x01)	11
Monitoring 12 Alarm	01 (0x01)	12
Alarm Any	01 (0x01)	16
Sensor Error	01 (0x01)	17
Heartbeat	04 (0x04)	6

For additional details on Gen 2, contact an Xtralis representative.

4 Application

4.1 Sensor Placement

The following sections are general guidelines for sensor placement. Precise location and orientation are to be determined by a trained Xtralis representative upon installation. Refer to the Li-ion Tamer Design Guide (36094) for more design details.

4.1.1 Monitoring Sensor Placement

The Monitoring Sensors are to be placed near or on the battery rack to detect the release of electrolyte solvent vapours from the rack. While airflow is not required for sensor operation, the air flow patterns should be taken into consideration when positioning the Monitoring Sensors. Several examples of potential air-flow patterns and their corresponding sensor placement are shown on the following page.

Example #1

Type: air enters from the back of the rack and exits out the front

Sensor placement: top front of the rack

Sensor orientation: sensing face pointing down (±45˚)

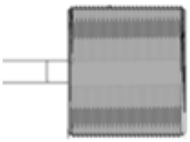
Sensing face
Pointing down

Example #2

Type: air enters from the top of the rack and exits out the bottom

Sensor placement: bottom center of the rack

Sensor orientation: sensing face pointing at 90˚ to vertical (±45˚)



Sensing face
Pointing horizontal

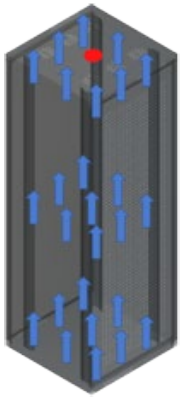
Example #3

Type: air enters from the front of the rack and exits out the back

Sensor placement: top back of the rack

Sensor orientation: sensing face pointing down (±45˚)

Sensing face
Pointing down



Example #4

Type: air enters from the bottom of the rack and exits out the top

Sensor placement: top center of the rack

Sensor orientation: sensing face pointing at 90° to vertical (±45˚)

Sensing face

Pointing horizontal

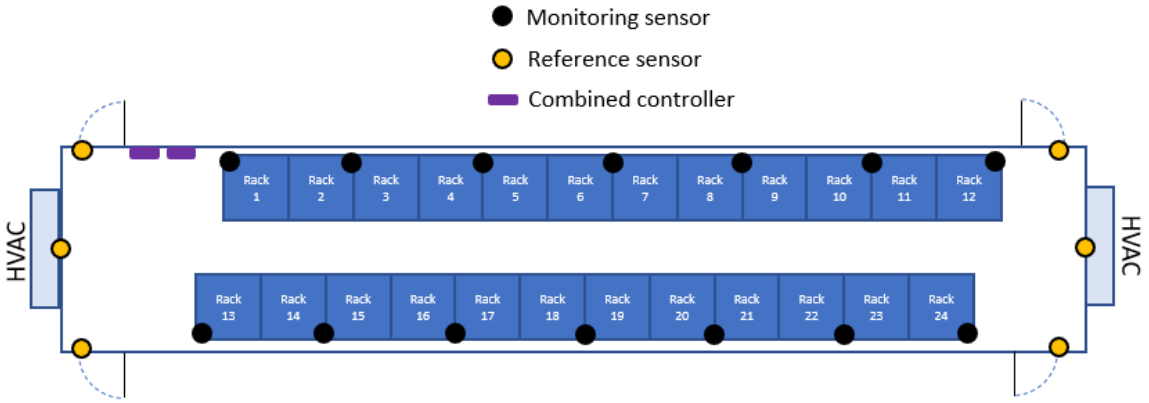
4.1.2 Reference Sensor Placement

The Reference Sensors are to be distributed throughout the ambient environment to monitor air inlets into the system, such as HVAC exchangers, doors, and other media which can serve as air inlets. The following information may be used as guidelines for Reference Sensor placement. Refer to the Li-ion Tamer Design Guide (Doc. No. 36094) for more information.

1. Any entrance or exit locations to the battery space (doors, access points, etc.)
2. Any possible gas entry points to the battery space (forced air or passive vent, unsealed gaps, etc.)
   - Multiple points identified on one surface (i.e. geometric plane) can be monitored with on reference sensor if the separation distance between points is less than 1 meter (3 ft) and not obstructed by a physical barrier or airflow pattern that would prevent a gas entering from a point to be detected by a single monitor.
   - Ensure adequate separation between Monitoring and Reference Sensors. Reference Sensors should never be mounted near battery racks unless they are separated from the hot aisle by a physical barrier (i.e. HVAC barrier, ducting, etc.).
3. Any HVAC entry points into the battery space.

4.1.3 System Layout Example

As an example, a potential installation environment may be a 12-meters (40 ft) shipping container containing 24 battery racks. Additionally, there may be two (2) HVAC units on either ends of the container and four (4) doors for personnel entry. The layout for such a system is shown below.



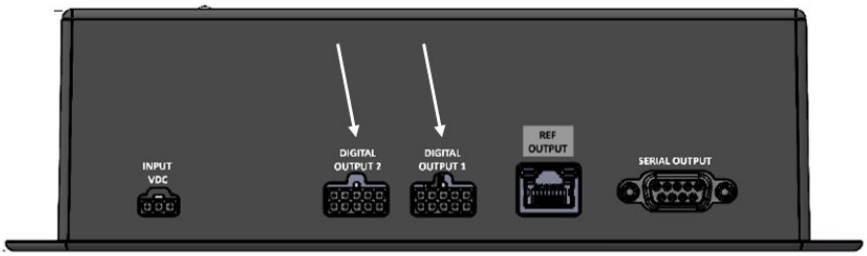
Note that there is a total of fourteen (14) Monitoring Sensors and six (6) Reference Sensors that are aggregated by two (2) Combined Controllers.

4.2 Signal Integration

The Li-ion Tamer controller has two primary outputs, including digital voltage signals and MODBUS serial communications, which are detailed in Sections 2.2.3 and 2.2.4, respectively.

4.2.1 Digital Output Signal Wiring

The digital output signals are generated by the controllers and can be accessed by connecting the Digital Output Cables (LT-ACC-DCL) to the ports indicated below.

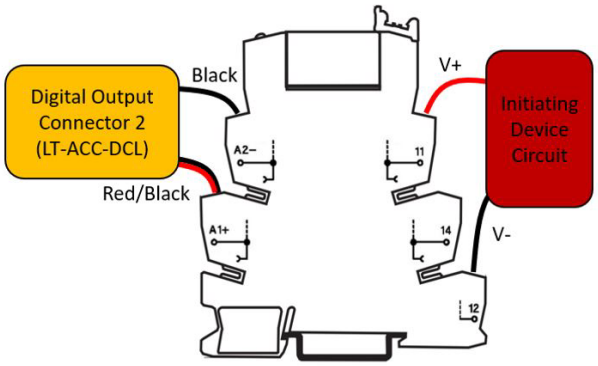


Typically, the digital output signals are wired into relays in order to actuate responses from other systems in the ESS. The correct wiring procedure is shown below for the relay provided by Xtralis (LT-ACC-RLY), which is an SPDT Form C relay. Note that the Initiating Device Circuit (IDC) is wired to a different relay connection depending on which signal is being integrated and whether the relay signal is NO or NC. Additionally, due to the behavior of the signals, the alarm any signal will activate the relay by default whereas the sensor error signal will not – the appropriate wiring is shown for an IDC wired to both NO and NC relay connections.

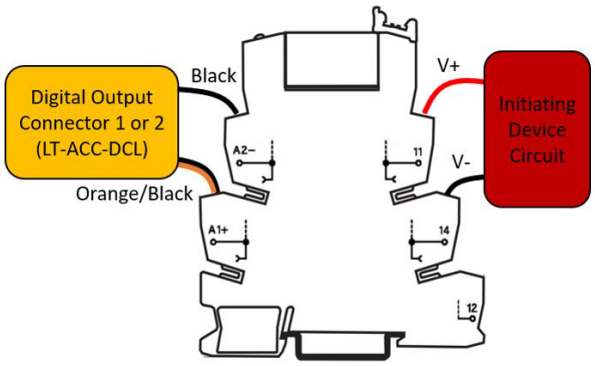
Note!

The sensor error signals should be integrated to indicate required maintenance of the Li-ion Tamer Rack Monitor system.

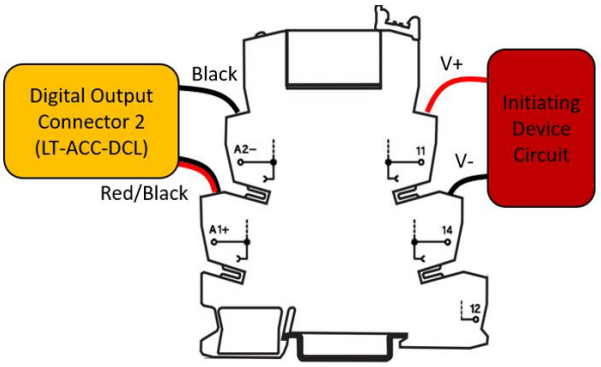
Alternatively, the alarm signals should be integrated to initiate a battery system shutdown, trigger ventilation, increase cooling, or arm pre-action fire suppression.



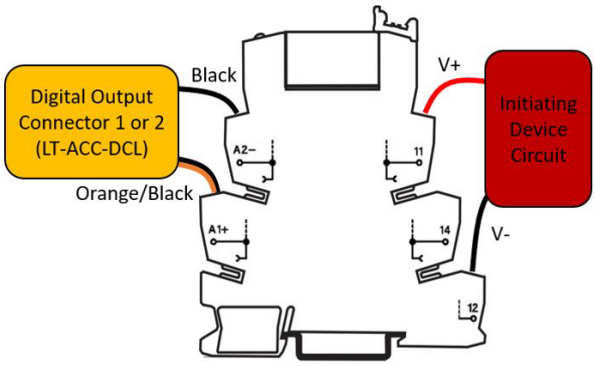
Li-ion Tamer Relay (Form C) alarm any signal wiring diagram for NO connection.



Li-ion Tamer Relay (Form C) sensor error signal wiring diagram for NO connection.



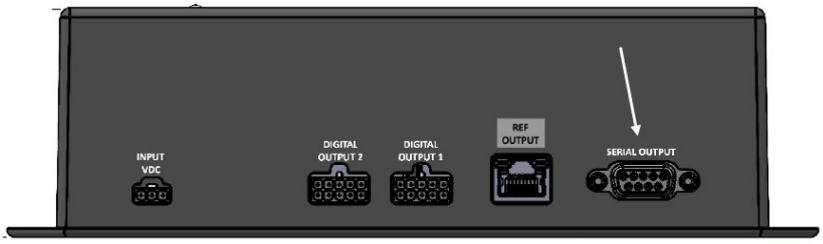
Li-ion Tamer Relay (Form C) alarm any signal wiring diagram for NC connection.



Li-ion Tamer Relay (Form C) sensor error signal wiring diagram for NC connection.

4.2.2 MODBUS Signal Wiring

To access the MODBUS signal, regardless of whether TCP/IP is being utilized, the MODBUS Cable (LT-ACC-SCL-MF) will need to be connected to the controller at the port indicated below.



When integrating the MODBUS signal via a TCP/IP adapter (LT-ACC-IPA), the wiring procedure detailed by the TCP/IP adapter manufacturer should be used to connect to the MODBUS signal. The adapter provided by Xtralis is the MOXA MGate MB3000 Series RTU to TCP/IP adapter. For the MOXA MGate MB3000 Series wiring diagram, please refer to the MOXA MGate MB3000 Series Manual which can be found on www.moxa.com.

The TCP/IP Adapter provided by Xtralis requires external power with the power consumption specifications detailed below:

Power consumption specifications	
Device	**Specification**
MOXA MGate MB3170	12 – 48VDC, 435mA

4.3 TCP/IP Adapter Integration

4.3.1 Accessing the TCP/IP Adapter Configuration Settings

The TCP/IP adapter requires some configuration prior to operation. Please follow the instructions below to properly configure the adapter:

1. Download the MOXA MGate MB3000 Series Manual from (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)
2. Setup a local network by setting your computer to a static IP address in the same subnet as the TCP/IP Adapter (ex. 192.168.0.1)
3. Connect to the device using one of the following methods:
   a. MGate Manager
      i. Download MGate Manager from https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources
      ii. Install the MGate Manager software according to the “Installing the Software” section in the MOXA MGate MB3000 Series Manual
      iii. Launch the MGate Manager according to the “Starting MGate Manager” section in the MOXA MGate MB3000 Series Manual
      iv. Connect to the device according to the “Connecting to the Unit” section in the MOXA MGate MB3000 Series Manual
   b. Web Console
      i. Open a web browser and enter the adapter’s default IP address (192.168.127.254)
4. For security reasons, account and password protection is enabled by default, so you must provide the correct password to unlock the device before configuring the device. Xtralis has pre-configured the initial password as the following:

   Username: admin

   Password: <Production S/N of the device> [See image below for location of Production S/N]

Note!

If the device has been reset or had a firmware upgrade since the device has been received, please refer to Section 4.3.3 for accessing the device.

5. See Section 4.3.2 for instructions on configuring the TCP/IP adapter before commissioning.

4.3.2 Configuring the TCP/IP Adapter

4.3.2.1 Configuration Instructions

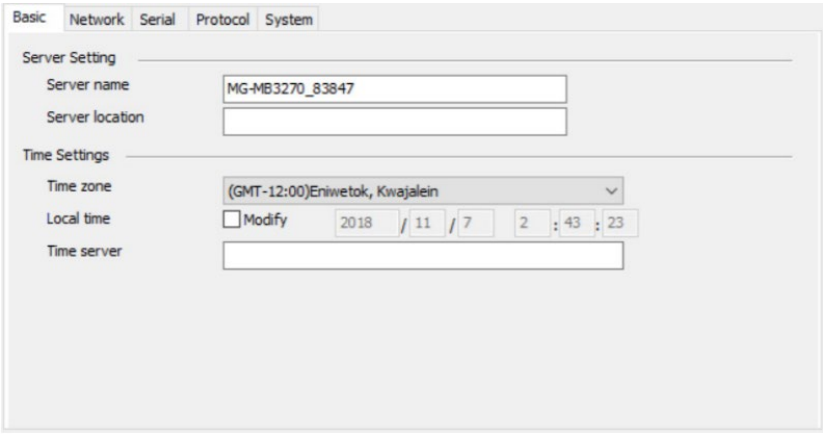
For security reasons, Xtralis has pre-configured the TCP/IP adapter to disable certain communication protocols (See the "Xtralis Pre-Configured Settings" Column in Table 1 in Section 4.3.2.2). However, additional configuration steps outlined in this section are required for setting up and securing the device before commissioning.

For MOXA's Configuration and Hardening Manual, please prefer to Section 7 of this manual.

For a comprehensive configuration manual, please refer to the MOXA MGate MB3000 Series Manual from (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

4.3.2.1.1 Basic Device Settings

Time and date settings – From the Basic tab on the Web console enter the Server and time settings as shown below. For more information on the device name and time zone settings of the device, please refer to Page 10-12 (Modifying the Configuration→ Basic Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

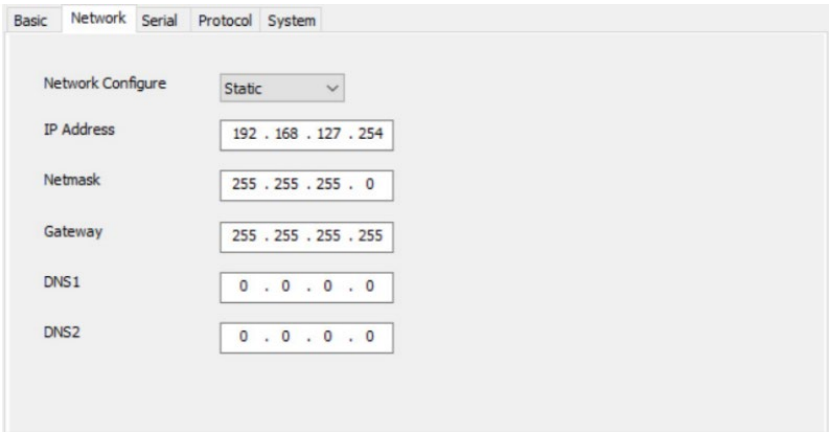


4.3.2.1.2 Network Settings

The Network Settings tab is where the unit's network settings are configured. You can modify the Network, Configuration, IP Address, Netmask, Default Gateway and DNS.

The default IP address of the device is 192.168.127.254. For security reasons, it is not recommended that the device be installed outside of the security firewall network or given a public IP address. Additionally, the Accessible IP List should be configured to prevent unauthorized access to the gateway (See Section 4.3.2.1 for configuration instructions).

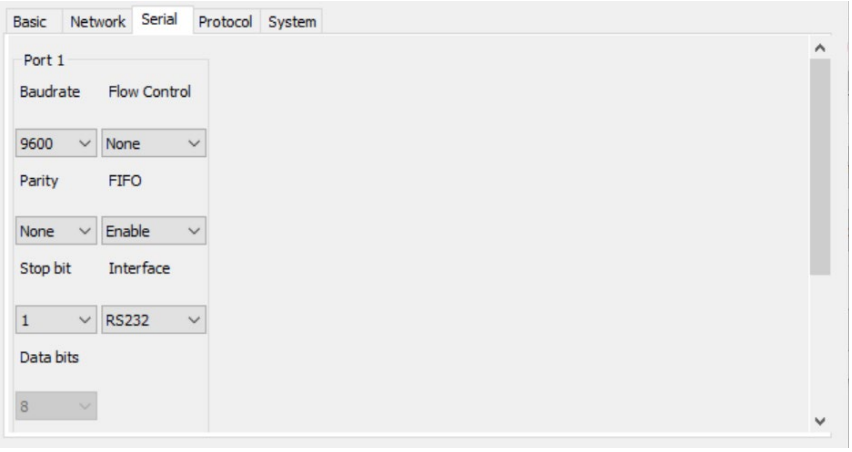
For more information on the network settings of the device, please refer to Page 10-13 (Modifying the Configuration→ Network Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)



4.3.2.1.3 Serial Settings

The Serial Settings interface is used to configure the serial interface of the device, which supports RS-232, 2-wire RS-485, 4-wire RS-485 and RS-422 interfaces. You must configure the baud rate, parity, data bits, and stop bits to match those in the specification table in Section 2.2.4 of this manual. Incorrect settings will result in communication failures.

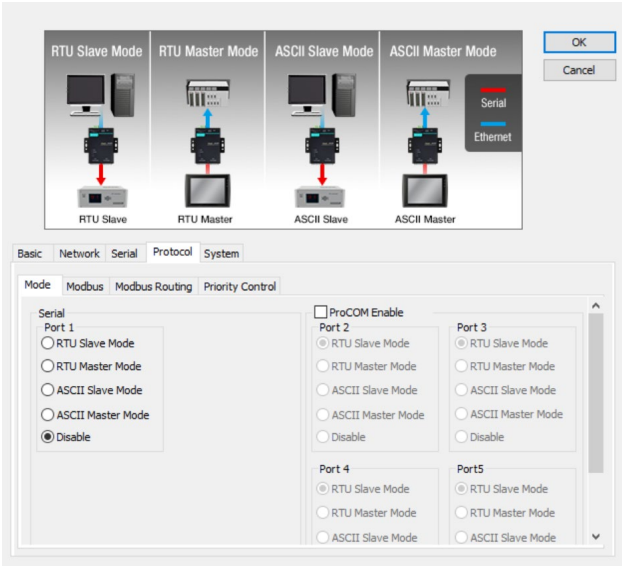
For more information on the network settings of the device, please refer to Page 10-14 (Modifying the Configuration→ Serial Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)



4.3.2.1.4 Protocol Settings

The Protocol Settings is used to configure MODBUS specific settings, each setting group outlined in Table below.

In the “Mode” Settings, there is an option to enable ProCOM, which is a Moxa proprietary function that creates virtual serial ports on the MGate MB3000 Series to mimic to behaviour of native serial ports when transmitting data to the desired destination. Xtralis has pre-configured the device to disable the protocol, and do not recommend enabling it. Additionally, all unused serial ports should be disabled. See Picture below for example of how to disable ProCOM and Serial ports.



Protocol Configuration Settings	Settings Overview
Mode	• Used to determine whether the device(s) that are connected to the serial port will operate as a master or a slave and whether the Modbus RTU or Modbus ASCII protocol will be used. To integrate with the controller, the associated serial port should be set to “RTU Slave Mode”. For security reasons, all unused ports should be set to Disable. • Used to enable/disable the ProCOM proprietary function. For security reasons, ProCOM should be disabled.
Modbus	Used to adjust and fine-tune the communication between different Modbus networks.
Modbus Routing	Used to manage Modbus slave IDs and determine how Modbus requests will be routed to the serial ports by the gateway. This should be changed to match the settings specified in the specification table in Section 2.2.4 of this manual.

Protocol Configuration Settings	Settings Overview
Priority Control	Used to enable and configure emergency requests, and specify which requests are sent to the front of the queue for more immediate response times.

For more information on the protocol settings of the device, please refer to Page 10-15 (Modifying the Configuration→ Protocol Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

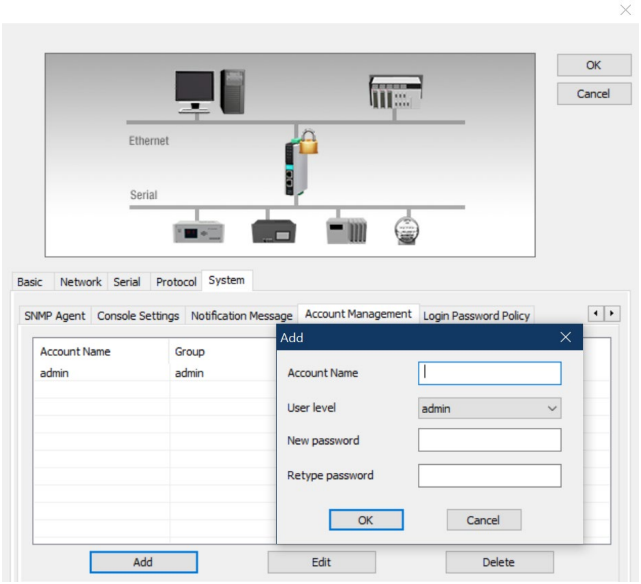
4.3.2.1.5 System Settings

- **Account Management**

  The Account Management Settings is used to manage user accounts. The MGate MB3170/3270 series provides two different user levels: admin and user with maximum 16 accounts. The admin account can access and modify all the settings through the web console. The user account can only view the settings and cannot change anything.

  - At minimum, the “admin” password should be changed before commissioning and after every factory reset and device update.

    However, it is strongly suggested that the TCP/IP adapter should be managed in another “administration level” account instead of using the default “admin” account, as it is commonly used by embedded system. A new account should be created with an “admin” User Level along with a unique username and password. Once the new account is created, the default “admin” account should be deleted. The login details for the “administration level” account should only be shared with authorized individuals who require configuration modification privileges.

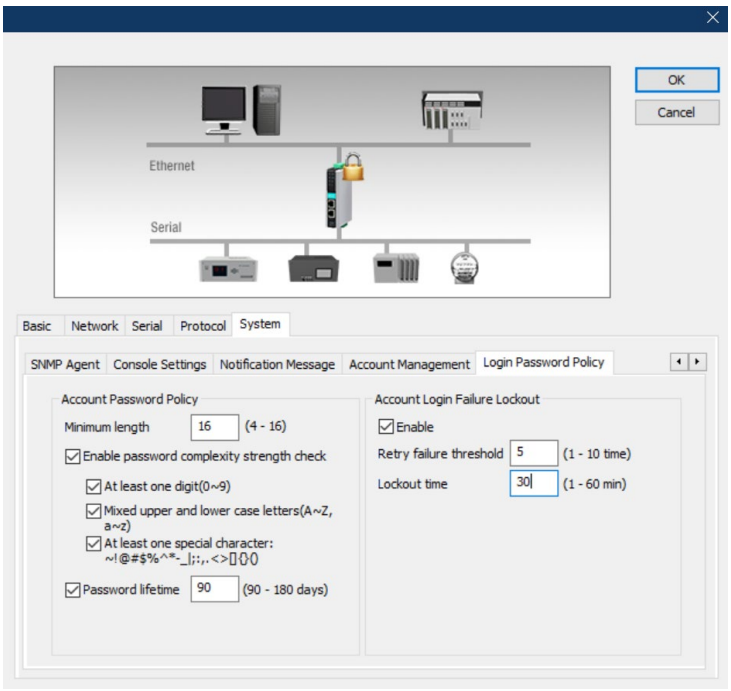


For more information on the account management settings of the device, please refer to Page 10-29 (Modifying the Configuration→ System Settings→ Account Management) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

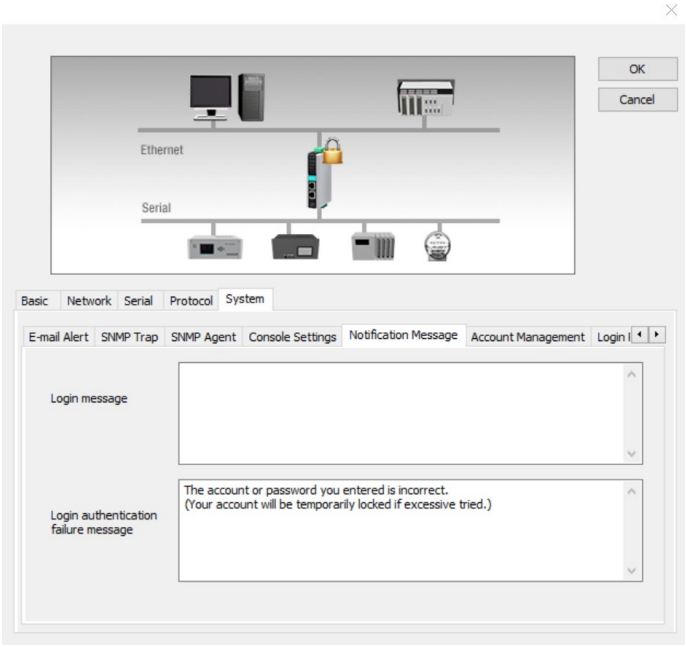
- **Login Password Policy and Notification Message**

  The Login Password Policy settings are used to configure login password policy and failure lockout.

  - The password policy should be set to enable complexity strength check and a password lifetime per the user’s organization requirements.



- In addition to configuring the password policy, the notification messages for Login and Login Authentication Error should be set in the “Notification Message” settings.

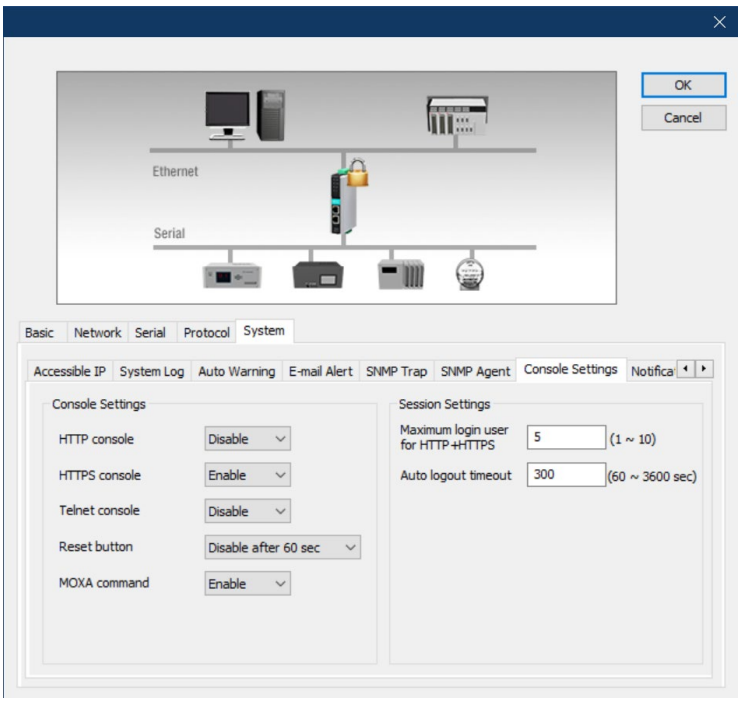


For more information on the login password policy settings of the device, please refer to Page 10-30 (Modifying the Configuration→ System Settings→ Login Password Policy) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- **Console Settings**

  The Console Settings is used to configure the protocols that can be used to communicate with the web console of the TCP/IP Adapter.

  - Xtralis has pre-configured the device with the console settings in the image below.



- Moxa Command is the proprietary protocol used to communicate with Moxa utilities, such as the Device Search Utility and MGate Manager. For security reasons, it is strongly recommended that the user disable the “MOXA command” in the Console Settings if the user does not need to communicate with Moxa utilities after initial configuration. If it is disabled, the device must be factory reset in order for the device to communicate with Moxa utilities.
- The reset button allows users to clear the password and load factory default settings (for a list of the factory default settings, see the “Factory Reset Settings” Column in Table 1 in Section 4.3.2.2 in this manual.) For security reasons, the Reset Button setting should be set to “Disable after 60 sec”. Xtralis has pre-configured the Reset Button setting to “Disable after 60 sec”. For more information on how to reset the device, please refer to Section 4.3.3.
- For security reasons, it is strongly recommended to only use HTTPS to communicate to with the web console. HTTP and Telnet are considered unsecure protocols that are not recommended for use with this device and should remain disabled.
- The TCP/IP Adapter supports TLS 1.0, 1.1 and 1.2 encryption algorithms when HTTPS is in use. TLS 1.1 and lower have been proven to have severe vulnerability and high risks to be hacked. It is strongly recommended that user only enable TLS 1.2 and higher, and disable all other versions of SSL and TLS in the internet properties settings of the web browsers being used to access the web console.
- By default, the HTTPS console in the adapter uses self-sign certificates to communicate with a web browser. For increased security, The HTTPS console supports the use of 3rd party certificates so that web browsers can validate the certificate in the HTTPS connection initialization stage and determine if the certificate could be considered trustworthy. Users should only import a trusted certificate issued by a third-party Certificate Authority. For instructions on how to import a trusted third-party certificate, please see Section 7.2.1 of this manual.

For more information on the console settings of the device, please refer to Page 10-28 (Modifying the Configuration→ System Settings→ Console Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- **Accessible IP List settings**

The Accessible IP List settings is used to add or block remote host IP addresses to prevent unauthorized access to the gateway. In other words, if a host’s IP address is in the accessible IP table, then the host will be allowed to access the TCP/IP Adapter.

By default, the TCP/IP adapter has this feature disabled, meaning that any IP address can communicate with the device. In addition to installing the TCP/IP adapter behind a security firewall, users should enable and configure this feature before commissioning the system to prevent unauthorized access to the gateway.

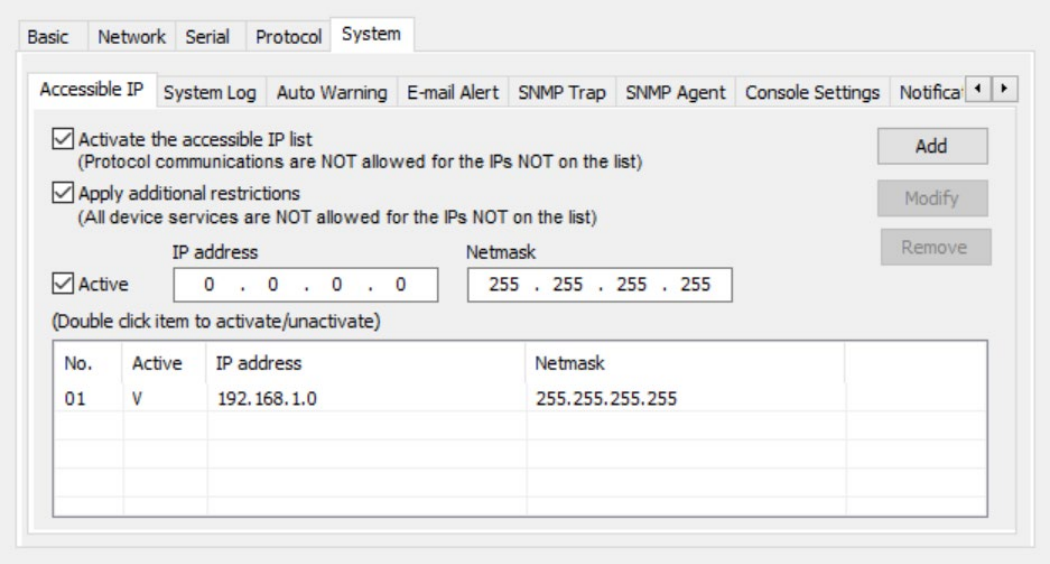
- “Activate the accessible IP list” should be selected to enable the Accessible IP List feature.

Note!

Selecting this feature without having “Apply additional restrictions” selected will not allow protocol communication from IP addresses not on the list, but will allow services from IP addresses not on the list. Services include HTTP, HTTPS, Telnet, SSL, SNMP, SMTP, DNS, NTP, and DSU.

- For security reasons, “Apply additional restrictions” should also be selected in addition to “Activate the accessible IP list” to prevent IP addresses not on the list from communicating with protocol communication or services.
- At minimum, the Accessible IP List setting should be configured to allow access to hosts on a specific subnet. To configure for a specific subnet, for both the IP address and netmask, use 0 for the last digit (e.g., “192.168.1.0” and “255.255.255.0”).

  For increased security, the Accessible IP List setting should be configured to allow access to specific IP addressed. To configure for a specific IP address, Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.



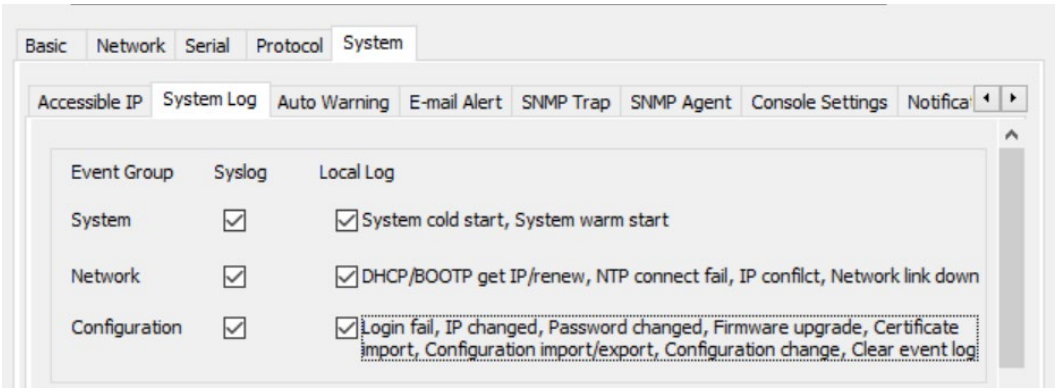
For more information on the Accessible IP List settings of the device, please refer to Page 10-24 (Modifying the Configuration→ System Settings→ Accessible IP) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- **Logging and Auditing**

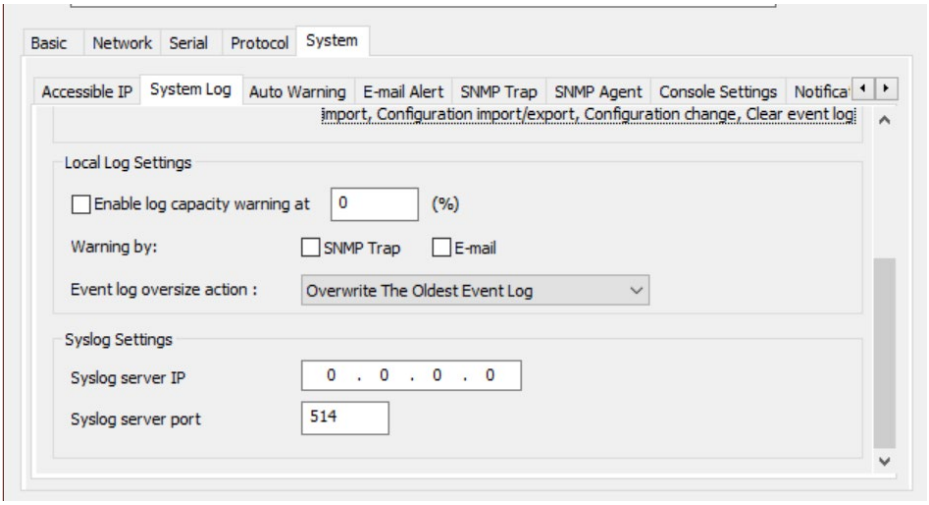
The TCP/IP adapter support system logging, which should be enabled to record all important system events to monitor any security issue of the device status.

- System Logs
  - There are three types of events that can be recorded by the TCP/IP adapter system logs. See Table below for a summary of all the event types

Event Group	Summary
System	System cold start, System warm start
Network	DHCP/BOOTP get IP/renew, NTP connect fail, IP conflict, Network link down
Configuration	Login fail, IP changed, Password changed, Firmware upgrade, Certificate import, Configuration import/export, Configuration change, Clear event log



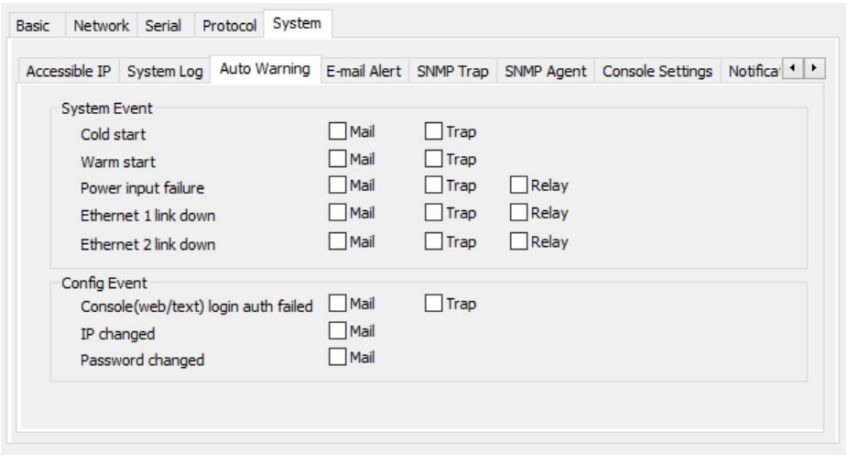
- Syslog – This will enable record keeping on a server over the network. In comparison to the local log, using syslog would allow event logs to be stored for a longer period of time. It is recommended that a syslog server be used to retain log information from the device.



For more information on the System Log settings of the device, please refer to Page 10-25 (Modifying the Configuration→ System Settings→ System Log) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- Auto Warning

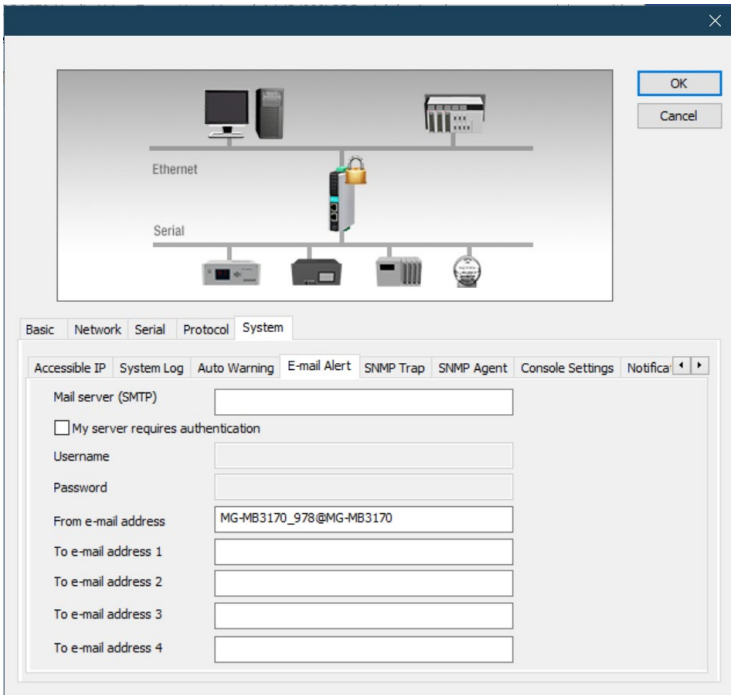
Auto Warning is triggered by different events. When a checked trigger condition occurs, the TCP/IP adapter can send e-mail alters, SNMP Trap messages, or open/close the circuit of the relay output and trigger the Fault LED to start blinking. It is recommended that auto warnings be enabled via Email.



For more information on the Auto Warning settings of the device, please refer to Page 10-26 (Modifying the Configuration→ System Settings→ Auto Warning Settings) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources).

- Email Alert

Email Alerts settings allow users to configure mail server information for email alerts used for event notification. Email alerts should be enabled for the “System Log” and “Auto Warning” events that support email notification.



For more information on the Email Alert settings of the device, please refer to Page 10-26 (Modifying the Configuration→ System Settings→ Email Alert) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- SNMP Trap

  For more information on the SNMP Trap settings of the device, please refer to Page 10-27 (Modifying the Configuration→ System Settings→ SNMP Trap) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

- SNMP Agent

  Xtralis has pre-configured the device with the SNMP Agent disabled.

  For more information on the SNMP Agent settings of the device, please refer to Page 10-27 (Modifying the Configuration→ System Settings→ SNMP Agent) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

4.3.2.2 Pre-Configured and Factory Reset Feature Settings

Table 1, below, provides a list of adapter feature settings pre-configured by Xtralis as well as the Factory Reset settings after a reset or firmware upgrade.

Table 1: Adapter Feature Settings - Pre-Configured and Factory Reset

Process Name	Option	Xtralis Pre-Configured Settings	Factory Reset Settings	Type	Port Number	Description
DSCI (Moxa Command)	Enable/Disable	**Enabled**	Enable	TCP	4900	For Moxa Utility communication
				UDP	4800	
DNS client	Enable/Disable	**Disable**	Disable	UDP	53	Processing DNS & WINS (Client) Data
SNMP agent	Enable/Disable	**Disable**	Enable	UDP	161	SNMP handling routine
HTTP server	Enable/Disable	**Disable**	Enable	TCP	80	Web console
HTTPS server	Enable/Disable	**Enable**	Enable	TCP	443	Secured web console
Telnet server	Enable/Disable	**Disable**	Enable	TCP	23	Telnet console
DHCP client	Enable/Disable	**Disable**	Disable	UDP	67, 68	DHCP client to acquire system IP address from server
Syslog client	Enable/Disable	**Disable**	Disable	UDP	514	Sending system logs to remote syslog server
Email client	Enable/Disable	**Disable**	Disable	UDP/ TCP	25	Sending system/config event notification
SNMP trap client	Enable/Disable	**Enable**	Disable	UDP	162	Sending system/config event notification
NTP client	Enable/Disable	**Disable**	Disable	UDP	123	Network time protocol to synchronize system time from server
Modbus TCP client/server	Enable/Disable	**Enable**	Enable	TCP	502, 7502	502 for Modbus communication;
Reset button protect	Disable after 60 sec, Always Enable	**Disable after 60 sec**	Always Enable	N/A	N/A	The MGate provides the reset button to clear the password or load factory default settings. But for security issues, users can disable this function. In disabled mode, the MGate will still enable this function within 60 seconds after boot-up, just in case users really need to reset this function.

4.3.3 Resetting and Updating the TCP/IP Adapter

In the event the user needs to clear the password or load factory default settings, a factory reset can be performed on the TCP/IP Adapter.

Additionally, MOXA releases version enhancements periodically that may contain important security patches which will require the user to upgrade the TCP/IP Adapter firmware (See sections 7.3.1 and 7.4 of this manual for more information on MOXA's Patch and Vulnerability Management policies).

The following is a guide for factory resetting and updating the firmware for the TCP/IP Adapter:

1. Performing Factory Reset or Firmware Update will reset all configuration and password settings in the device. Before performing a factory reset or firmware update, we recommend exporting the configuration to the local computer and importing the configuration after the reset or update is complete.

   For more information on how to Export the configuration of the device, please refer to Page 10-43 (Export/Import) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

   - **Instructions for Performing a Factory Reset**

     Xtralis has pre-configured the device to only enable the Factory Reset button within the first 60 seconds after power-on. To ensure a successful Factory Reset, press and hold the Reset button within 60 seconds of power-on.

     For more information where to locate the reset button on your MOXA MB3000 Series device, please refer to your device model's Hardware section in the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)

   - **Instructions for Upgrading the Firmware**

     Please refer to Section 7.3.2 of this manual. for more information on how to perform firmware upgrades on the device.

2. After a successful Factory Reset or Firmware Update, the device configuration will reset to the values in the "Factory Reset Settings" column of Table 1 in Section 4.3.2.2.
3. For security reasons, account and password protection is enabled by default, so you must provide the correct password to unlock the device before re-configuring the device. The default username and password after a reset or firmware upgrade is the following:

   Username: admin

   Password: moxa

Notes!

- If the configuration file was exported before the Factory Reset or Firmware Upgrade, import the configuration file to restore all of the TCP/IP adapter settings.

  For more information on how to Export the configuration of the device, please refer to Page 10-43 (Export/Import) of the MOXA MGate MB3000 Series Manual (https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources)
- If the device needs to be configured, please refer to Section 4.3.2 of this manual for how to configure the device.

5 Installation, Operation and Maintenance

5.1 System Installation

All installation should be performed by a trained Xtralis representative. The following steps outline the installation process:

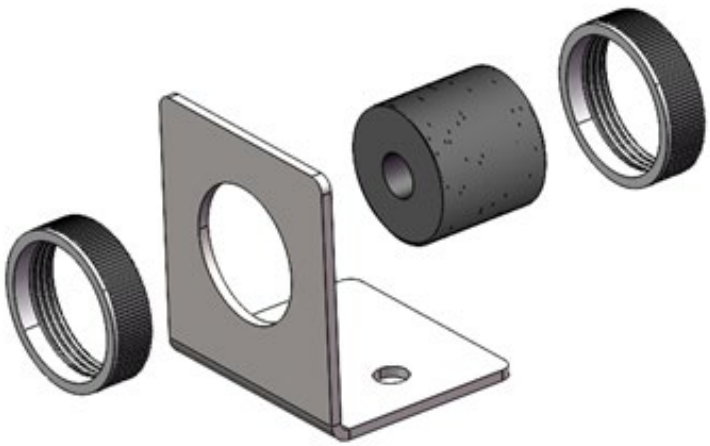
1. Mount sensors (off-gas monitors)
2. Mount controllers
3. Route cables
   - Follow color-coded convention to prevent wiring errors (Black = Monitoring, Blue = Reference, Gray = REF signal daisy-chain)
   - If applicable, locate the main cabling distribution area close to the central region of the installation site to minimize the cable distances
   - Avoid mounting the cabling components in places that block accessibility to other equipment (such as a power strip or fans) in and out of the racks
   - Label the cables with their destination at every termination point (to ensure that both the ends of the cable are labeled for identification and traceability).
   - Test every cable during installation and termination. If a problem occurs, tag the malfunctioning cables and separate them out.
   - Avoid exposing cables to areas of condensation and direct sunlight.
   - Utilize cable trays whenever possible.
   - Provide strain-relief when mounting cables to prevent connection issues.
   - Observe all recommended practices from the cable manufacturer including bend radius, etc.
4. Make all connections to controllers

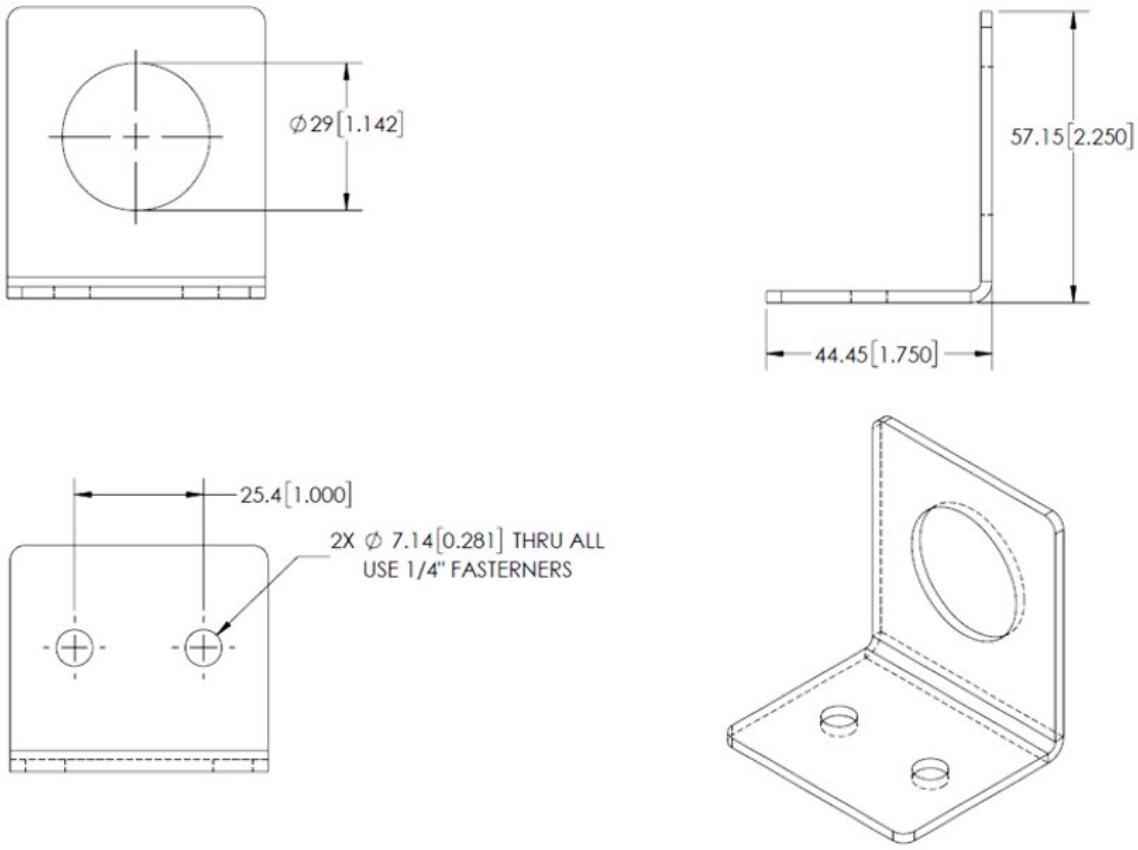
   WARNING: Ensure that cables are not in tension when connected to controller. Make sure to provide enough slack to avoid potential damage.
5. Follow commissioning process.

5.1.1 Sensor Mounting

The Monitoring and Reference Sensors may be mounted using one of two methods. Option 1 is to create a through-hole on the panel the sensor is to be mounted on. Option 2, depicted below, is to use the supplied mounting bracket. The following procedure should be used:

1. Fasten mounting bracket in position determined in the system layout
2. Secure sensor to bracket using the supplied 1 1/8-24 mounting nuts
3. Hand tighten nuts to secure the sensor to the bracket





5.1.2 Controller Mounting and Earth Grounding

The controllers should be mounted according to the procedure below. Additionally, a mounting template is available from Xtralis to locate mounting holes for the controller.

1. Disable any unused sensor ports, detailed in Section 5.2.1.
2. Secure controller to mounting surface using four (4) mounting holes.
3. Connect controller to earth ground and power via Power Cable (LT-ACC-PCL) according to the table below. Earth grounding the controller provides earth ground to the sensor network and reduces signal noise due to EMI.

Earth ground connection points for various DC supplies:

LT-ACC-PCL Conductor Color	DC Supply with Earth Ground Connection	DC Supply without Earth Ground Connection
Red	VDC+	VDC+
Black	GND	GND
Clear (drain wire)	Earth	[Ring terminal to ground location]

4. Make all connections to the controller.

Note!

If required, the power input can be connected to a DC power supply with a battery back-up.

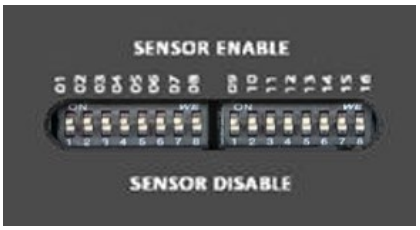
5.2 System Commissioning

5.2.1 Controller Commissioning

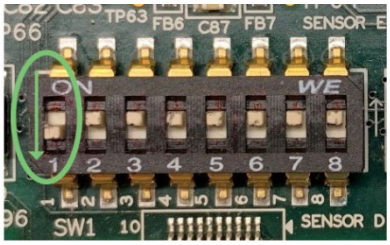
Unused channels on each controller shall be disabled on the controller to prevent the empty ports from being detected as a faulty or missing sensor. Disabling a port will force the LED diagnostic light on the RJ45 port to be ‘green’. The procedure for controller configuration and sensor disabling is as follows:

WARNING: Use proper ESD protection when handling controller motherboard. ESD or anti-static gloves must be worn, or a wrist strap must be worn and connected to an appropriate grounding point.

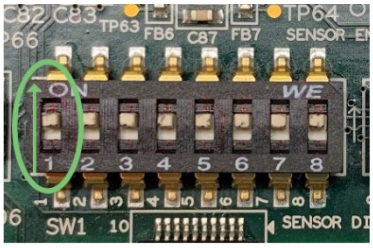
1. The “Sensor Disable” switches are accessible through an opening on the controller backplate with labels on the backplate, as shown below:



2. Locate switch number associated with port – use number printed directly on controller backplate, not the number on the black switch block
3. Disable sensor channel by moving switch to “OFF” position



“Mon 1” Disabled



“Mon 1” Enabled

4. Confirm ‘green’ light on all unused channels

“Mon 1” Disabled

“Mon 1” Enabled

Showing “error” at port because sensor not connected

The table on the following page lists the sensor ports and their corresponding sensor disable switches. Note that if the REF INPUT port is enabled, the LED will be amber when any sensors on the network are in an error state, or if there is a continuity issue between the controllers along the daisy-chain cables.

"Sensor Disable" Switch	Combined Controller
1	"Mon 1"
2	"Mon 2"
3	"Mon 3"
4	"Mon 4"
5	"Mon 5"
6	"Mon 6"
7	"Mon 7"
8	"Mon 8"
9	"Mon 9"
10	"Mon 10"
11	"Mon 11"
12	"Mon 12"
13	"Ref 1"
14	"Ref 2"
15	"Ref 3"
16	"REF INPUT"

5.2.2 Final Tests

The installer shall:

1. Confirm proper earth grounding by measuring resistance between connector block and earth ground
   - Use a multimeter or an equivalent device to check the effectiveness of the connectivity between the different parts of the installed equipment (such as cable shielding at reference and monitoring ports) to the ESS ground.
   - Check at 2 points for each controller installed in the system. Measure earth ground resistance between both of the 4x2 RJ45 connector blocks on the controller.
   - Using IEEE Std 142-2007 "Recommended Practice for Grounding" and IEEE Std 1100-2005 "Recommended Practice for Powering and Grounding Electronic Equipment", the ideal grounding value would be less than 1Ω from the equipment into the Earth.
   - Recommended ground resistance measurements for Li-ion Tamer are **less than 25Ω** from the RJ45 connector block to earth ground.
2. Confirm input conditions at each input port (using port diagnostic lights).
3. Gas bump tests can be conducted to verify tip-to-tail operation of the system with the MODBUS Software. See Section 5.2.3 for testing procedure.
   - Confirm operation of signal connection to the energy storage system. Alarm signals can be generated by bump testing to ensure proper operation of systems connected to the Li-ion Tamer controller.
4. Power cycle each controller and sensor network after installation and testing.

5.2.3 Bump Test Procedure

The Li-ion Tamer DEC Test Bottle (LT-ACC-TST) may be provided by Xtralis upon request. The small bottle, shown on the following page, is filled with a small amount of diethyl carbonate to be used for bump testing of sensors. This liquid must be safely transferred into the larger puff-test bottle prior to testing the sensors. Follow the procedure below to correctly test sensors.

Note!

Use proper personal protective equipment when transferring liquid between bottles. It is important that the puff-test bottle never be turned up-side down during use and is not intended to be refilled.

If the product is being shipped, please transfer the liquid back into the small bottle. To maximize the lifetime of the test kit, store the liquid in the small bottle.

Required Materials for Testing:

- Li-ion Tamer DEC Test Bottle
- Li-ion Tamer MODBUS Software
- Latex gloves (recommended)
- Safety glasses (recommended)

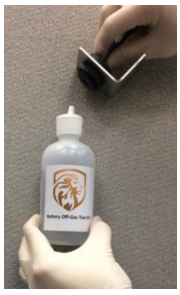
How to Use:

1. Disconnect all Reference Sensors from the system. Visually confirm that the LEDs located on controller's sensor ports are amber for ONLY the disconnected sensors. If any Monitoring Sensor ports display amber LEDs, check the wire connections for the relevant sensors.

   Note!

   If testing Reference Sensors, it is not necessary to disconnect all Monitoring Sensors; however, the controller should be power cycled between each round of bump tests and should be allowed 30 minutes prior to testing.

2. Open and run the included Li-ion Tamer MODBUS Software. See Section 5.2.4 for instructions on connecting controllers to retrieve their serial output. Confirm that all Monitoring Sensor status indicators in the MODBUS Software are OFF and that no sensor RJ45 port is blinking green.
3. Position the bottle relative to the desired Monitoring Sensor, like the example shown below.



4. Open the tab on the cap.

5. Firmly squeeze the bottle to release a puff of headspace gas towards the sensor face.

   WARNING: Avoid ejecting liquid from the bottle, especially onto the sensor. If the sensors were recently powered on, wait at least 30 minutes prior to testing. Additionally, confirm that the heartbeat shown in the MODBUS Software Interface is changing.

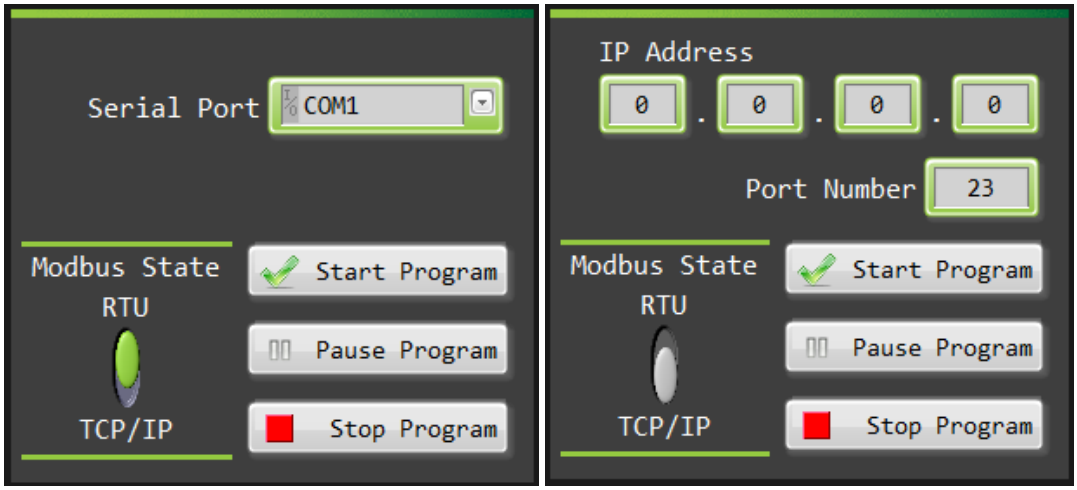
6. Proceed to bump test all Monitoring Sensors, close the tab on the cap, and observe the sensor response. Please see Section 5.2.4 for details on the MODBUS Software.

7. Power cycle each controller and sensor network after testing.

5.2.4 MODBUS Software

The Li-ion Tamer MODBUS Software may be provided by Xtralis upon request. The following steps are intended as a guide to software's user interface:

1. The Modbus State switch, depicted on the following page, may be used to alternate between RTU and TCP/IP connections. When using RTU, simply select the correct serial port. When using TCP/IP, enter the correct IP address and port number.

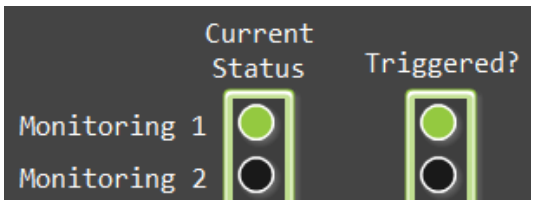


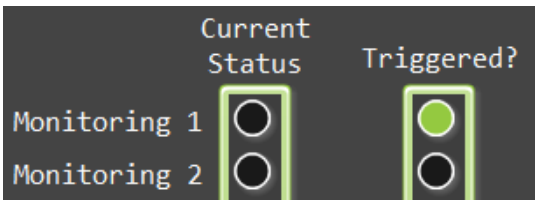
2. Select "Start Program" to begin serial connection with controller. See below for potential error codes and the method for resolving them. If an error code appears that is not listed below, please contact an Xtralis representative.

Error Code	Error Handling
54	• Invalid IP address • Check controller IP address and confirm correct entry
56	• Connection timed out • Check controller IP address or Serial Port and confirm correct entry • Check wire connections

3. Follow the guidelines in Section 5.2.3 for correct bump testing procedure.

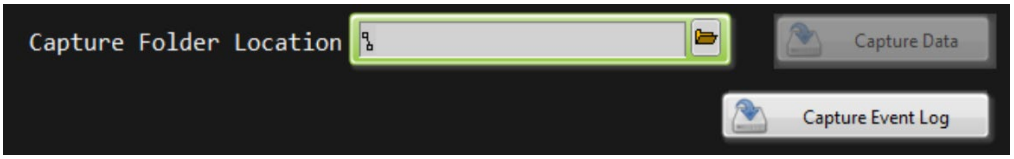
4. When a sensor is activated the "Current Status" and "Triggered?" indicators will be illuminated. After the sensor exits the alarm state, only the "Triggered?" indicator will remain illuminated. Both possible displays are shown below.





5. Confirm that the tested sensors have been "triggered" and verify that the controller generated the correct output, as detailed in Section 2.2.4. See Section 5.2.5 if any sensors are not activated by bump testing.

The Modbus Software also allows users to download the controller's relative time-stamped event log, which tracks sensor error and alarm states during operation. To download the event log, select a file destination in the space below and then select "Capture Event Log".



The event log output can then be transferred to the event log header file, which can be provided by Xtralis upon request.

5.2.5 Error Handling and Diagnostics

The table on the following page details potential system errors and their corresponding diagnostic indicators. Sensor-specific error diagnostics are detailed in Section 2.1.2.

Function	Error Handling	Diagnostic
Sensor Input	Loss of sensor signal Sensor disconnected Loss of continuity on sensor cable	• "Sensor Error" signal on digital output/ Modbus • Port diagnostic light on controller turns amber • Event recorded in relative time-stamped event log • System will continue to operate with remaining sensors
Sensor Input	Sensor gives "Out-of-Range" error state signal, 0.1V	• "Sensor Error" signal on digital output/Modbus • Port diagnostic light on controller turns amber • Event recorded in relative time-stamped event log • System will continue to operate with remaining sensors
Daisy-Chain Input	Loss of continuity on daisy-chain cable Daisy-chain cable disconnected	• Port diagnostic light on controller turns amber • System will continue to operate with remaining sensors/controllers
Digital Output	Loss of output signal Loss of system power Loss of output cable continuity	• Output designed to be "fail-safe" • "Ready" signal is high-state of digital output • "Alarm" signal is low-state of digital output • Loss of signal errors result in alarm state
Serial Output	Loss of output signal Loss of system power Loss of serial cable continuity PLC is frozen	• Modbus handshake communication (i.e. 'heartbeat') will indicate loss of output or if the PLC has frozen • Heartbeat increases every second. Counts 0 – 3600, and roll over to 0

Note!

The controller(s) must remain powered ON in the case of a sensor error to ensure proper troubleshooting.

The following details troubleshooting steps that may be taken if an “Sensor Error” signal is generated:

1. Check input ports for any amber LEDs present and make note of which sensor ports are actively in the error state.
2. Download the event log from the controller using the Modbus Software (Section 5.2.4). Make note of the sensor ports that previously entered the error state (after the most recent power cycle).
3. Perform the following checks on all sensor ports that either are actively in the error state (from Step 1) or were previously in the error state (from Step 2):
   a. If the port is not being used, make sure the “Sensor Disable” switch is ON (Section 5.2.1).
   b. Ensure the cable is connected and has proper continuity. If the cable does not have continuity, replace it.
   c. Swap a known “good” sensor to the port and confirm that the controller output and port LEDs respond accordingly. If the port does not respond correctly, contact an Xtralis representative, as the controller may need to be replaced.

Note!

The controller output and port LED should both indicate a sensor error when the sensor is unplugged, and clear the error when the sensor is plugged in.

   d. If the controller passes Step (c), replace the sensor connected to that port. Be sure to replace the affected part with a device of the same part number.

5.2.6 Alarm Handling

If an alarm occurs on a deployed and commissioned Li-ion Tamer system, the Li-ion Tamer controllers must remain powered ON until technicians are able to visit the site and begin their investigation. The procedure for handling an alarm in the field is as follows:

1. Download the event log from the controller(s) using the Modbus Software (Section 5.2.4).
2. Power cycle the controller(s).

   If any testing is done on the Li-ion Tamer system, power cycle the controller(s) after that is completed.
3. Contact an Xtralis representative for guidance on how to evaluate the controller event log(s) during the investigation of the alarm.

5.3 Maintenance and Service

5.3.1 Maintenance Tests

The Li-ion Tamer Rack Monitor system requires minimal operation and maintenance procedures as the off-gas monitors are designed to be calibration-free and have comparable lifetime to that of the ESS battery system. The general procedure is detailed below and should be performed annually.

1. Immediately attend to any errors generated by the system’s self-diagnostics (detailed in Section 5.2.5).
2. Perform a visual inspection.
   - Confirm that LEDs at all ports are Green. Amber lights indicate an error is present at that port. “Sensor Error” signal communicated over Digital Outputs and Serial Output can be used to remotely monitor the system for errors.
   - Inspect for physical damage to controller, sensor network, cabling, sensor placement, or other visual changes to the original system construction.
   - Inspect sensor for excessive dust build up at the inlet. Sensor inlet is protected by a 40µm breather vent. This prevents diffusion restriction from dust build up from impacting the operation of the off-gas monitor; however, excessive dust should be removed from the inlet of the sensor as a best practice.

Note!

Do not use compressed air dusters as they can alarm and potentially damage sensors.

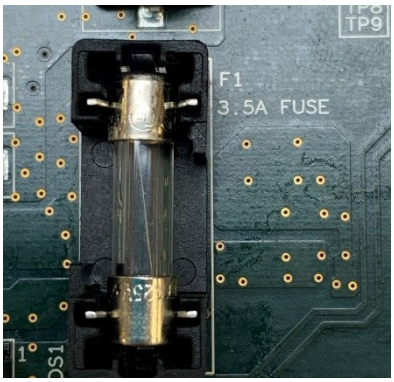
   - Ensure that mounting nuts are tightened to secure sensor to mounting bracket.

3. Bump test the sensors to verify gas response.
    - The sensors can be activated with a bottle of battery electrolyte solvent liquid (LT-ACC-TST), which is supplied by Xtralis.
    - Note that the bump test kit does not simulate the amount of gas released during the venting of electrolyte solvent vapours. It should only be used to release gas into the head of the gas monitor for the purpose of confirming operation of the gas sensor. It should not be used to release electrolyte solvent vapours into the rack or general vicinity to see if a nearby off-gas monitor detects it.
    - When using the bump test kit care needs to be taken not to activate a reference sensor.
    - Bump test kits should be used according to instructions in Section 5.2.3.

5.3.2 Fuse Replacement

The controller and sensor network power is protected by a 3.5A fuse which is located on the printed circuit board inside the controller. Remove the backplate and gently remove the circuit board to access the fuse shown below. Fuses must be replaced with an appropriate substitute 3.5A fuse.

WARNING: Use proper ESD protection when handling controller motherboard. ESD or anti-static gloves must be worn, or a wrist strap must be worn and connected to an appropriate grounding point.



5.3.3 Spare Parts

Spare parts may be provided by Xtralis upon request.

5.3.4 System Decommissioning

Before decommissioning the TCP/IP Adapter, a factory reset should be performed on the device. Please follow Step (1) in Section 4.3.3.

Contact Xtralis representative for guidance on how to decommission the Li-ion Tamer Rack Monitor system.

6 Frequently Asked Questions

1. **How do you know if the Li-ion Tamer monitor is functioning properly?**
   - The output of the Li-ion Tamer off-gas monitors (OGM) is fail-safe and has self-diagnostic capability
   - Errors from sensors are detected at the controller through transmission of the “Sensor Error” signal and diagnostic lights at the port.
2. **What happens if a sensor malfunctions?**
   - The output of the Li-ion Tamer OGM is fail-safe and has self-diagnostic capability
   - Errors from sensors are detected at the controller through transmission of the “Sensor Error” signal and diagnostic lights at the port.
   - The Li-ion Tamer controller will continue to operate using the remaining off-gas monitors
3. **What happens if a sensor is disconnected from the controller?**
   - This is detected by the controller and generates an “Sensor Error” alarm signal at the output.
   - The diagnostic LEDs on the port will indicate that a sensor has been disconnected
   - The Li-ion Tamer controller will continue to operate using the remaining off-gas monitors
4. **What happens if the PLC freezes or becomes unresponsive?**
   - The Modbus communication includes a heartbeat timer that can be used to verify that the PLC is still running.
5. **Can the Li-ion Tamer system be installed with less than one sensor per rack?**
   - Refer to the Li-ion Tamer Design Guide (36094) for details on reducing sensor quantities and designing custom systems for applications.
6. **Can the Li-ion Tamer system be tested with a test-gas to activate the off-gas monitor?**
   - Yes, the sensors can be activated with a bottle of battery electrolyte solvent liquid (LT-ACC-TST), which is supplied by Xtralis.
   - It should be noted that the bump test kit does not simulate the amount of gas released during the venting of electrolyte solvent vapours. It should only be used to release gas into the head of the gas monitor for the purpose of confirming operation of the gas sensor. It should not be used to release electrolyte solvent vapours into the rack or general vicinity to see if a nearby off-gas monitor detects it.
   - When using the bump test kit care needs to be taken not to activate a reference sensor.
   - Bump test kits should be used according to instructions provided by Li-ion Tamer
   - Bump tests should only be performed by appropriately trained and qualified personnel
7. **Are all the off-gas monitors on the system interchangeable?**
   - Off-gas monitors with the same part number are interchangeable
   - Reference (LT-SEN-R) and Monitoring (LT-SEN-M) Sensors are not interchangeable
   - Reference and Monitoring Sensors are color-coded along with their cable and input ports on the controller to ensure proper connection of the system
   - Monitoring Sensors and associated ports are BLACK
   - Reference Sensors and associated ports are BLUE
8. **Does the earth ground connection on the Power Input cable need to be connected to ground?**
   - Yes, the earth ground connection should be connected for all controllers in the system
   - This is propagated throughout the system to connect the cable shielding to earth ground to help protect the system against EMI
9. **Can any RJ45 cable (i.e. Ethernet cable) be used to connect an OGM to the controller?**
   - No, only cables provided by Xtralis are used to maintain minimum requirements and color coding
   - All cables must be shielded with connected drain wires, have 26 AWG conductors or larger and be less than 100 ft.
10. **Does the Li-ion Tamer off-gas monitor need to be tuned for different battery chemistries?**
    - No, the monitor detects the presence of solvents that are common in all lithium-ion battery chemistries; therefore, it is chemistry agnostic.

11. How do we know the parts have not been tampered with between shipping and receival?

- Every sensor and controller package is heat sealed in an ESD bag. If that seal is broken prior to commissioning and installation, please contact an Xtralis representative to request a replacement.

7 Appendix: Configuration Management and Hardening Manual of MGate MB3170_3270 Series_v2

The following is a PDF version of the Configuration Management and Hardening Manual for the MOXA MGate MB3170 adapter. It is highly recommended that this manual be used to harden the configuration settings of the TCP/IP adapter. It also outline's MOXA's management plans for releasing device firmware and software updates, device firmware enhancements, and security advisories.

7.1 General System Information

7.1.1 Basic Information of the Device

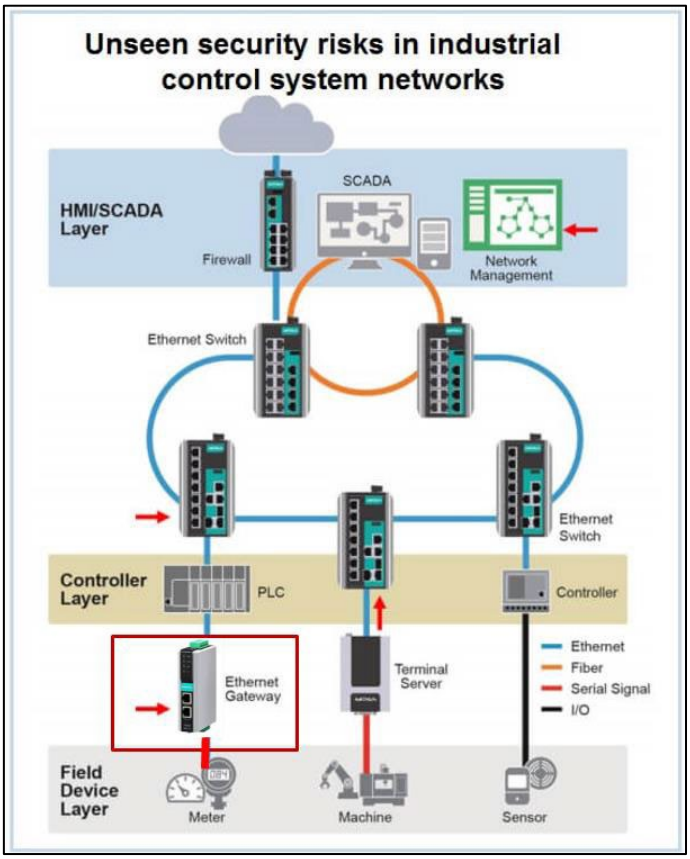
Model	Function	Operating System	Firmware Version
MGate MB3170/3270 Series	Gateway	Moxa Operating System (MOS)	Version 4.1

The MGate MB3170/3270 series is a Modbus protocol gateway specifically designed to allow industrial devices to be directly accessed from the network. Legacy Modbus serial devices can thus be transformed into Ethernet ones, which can be monitored and controlled from any network location or even the Internet.

Moxa Operating System (MOS) is an embedded proprietary operating system, which is only executed in Moxa edge devices. Since the MOS operating system is not openly available, it decreases the chances from malware attack or consistent malicious behavior. To harden the security of proprietary operating system, the open source HTTPS library, mbed TLS v2.7.5, is also included with periodically reviewed for cybersecurity enhancement.

7.1.2 Deployment of the Device

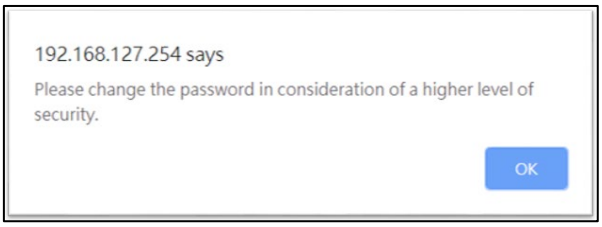
The deployment of the MGate MB3170/3270 series is suggested to allocate behind the security firewall network that have sufficient security features in place and ensure that their networks are safe from internal and external threats.



7.2 Configuration and Hardening Information

For security reasons, account and password protection is enabled by default, so you must provide the correct account and password to unlock the device before entering the web console of the gateway.

Xtralis has pre-configured the device's default account with a unique password. After a factory reset or firmware upgrade, the default account and password are admin and moxa (both in lowercase letters) respectively. Once you successfully log in, the pop-up notification is shown to remind to change the password in consideration of higher level of security. Below snapshot is the GUI for Web Console.



7.2.1 TCP/ UDP Ports Status

Please refer to below table for all the ports, protocols, and services are used to communicate between MGate MB3170/3270 series and other devices.

Process Name	Option	Default Settings	Type	Port Number	Description
DSCI (Moxa Command)	**Enable/Disable**	**Enable**	TCP	4900	For Moxa Utility communication
			UDP	4800	
DNS client	**Enable/Disable**	**Disable**	UDP	53	Processing DNS & WINS (Client) Data
SNMP agent	**Enable/Disable**	**Enable**	UDP	161	SNMP handling routine
HTTP server	**Enable/Disable**	**Enable**	TCP	80	Web console
HTTPS server	**Enable/Disable**	**Enable**	TCP	443	Secured web console
Telnet server	**Enable/Disable**	**Enable**	TCP	23	Telnet console
DHCP client	**Enable/Disable**	**Disable**	UDP	67, 68	DHCP client to acquire system IP address from server
Syslog client	**Enable/Disable**	**Disable**	UDP	514	Sending system logs to remote syslog server
Email client	**Enable/Disable**	**Disable**	UDP/ TCP	25	Sending system/config event notification
SNMP trap client	**Enable/Disable**	**Disable**	UDP	162	Sending system/config event notification
NTP client	**Enable/Disable**	**Disable**	UDP	123	Network time protocol to synchronize system time from server
Modbus TCP client/server	**Enable/Disable**	**Enable**	TCP	502, 7502	502 for Modbus communication; 7502 for priority Modbus communication
ProCOM	**Enable/Disable**	**Enable**	TCP	950~953 966~969	Mapping additional Modbus slave role on Windows platform

For security reason, users can consider disabling unused services and using higher security level of services for data communication. Please refer to the below table of suggested settings.

Process Name	Suggested Settings	Type	Port Number	Security Remark
DSCI (Moxa Command)	**Disable**	TCP	4900	Disable service for not commonly used
		UDP	4800	
DNS client	**Disable**	UDP	53	Disable service for not commonly used
SNMP agent	**Disable**	UDP	161	Suggest managing MGate via HTTPS console
HTTP server	**Disable**	TCP	80	Disable service for HTTP from plain text transmission
HTTPS server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for MGate configuration
Telnet server	**Disable**	TCP	23	Disable service for not commonly used
DHCP client	**Disable**	UDP	67, 68	Suggested to assign system IP in static manner
Syslog client	**Enable**	UDP	514	MGate is the syslog client role to send important system events for the MGate status diagnosis
Email client	**Enable**	UDP/ TCP	25	A service for sending important system events for the MGate status diagnosis
SNMP trap client	**Enable**	UDP	162	A service for sending important system events for the MGate status diagnosis
NTP client	**Disable**	UDP	123	Disable service for not commonly used
Modbus TCP client/server	**Enable**	TCP	502, 7502	Suggested to add communicating Modbus devices IP address to “Accessible IP list”.
ProCOM	**Disable**	TCP	950~953 966~969	Disable ProCOM if users are not using Windows as Modbus client role

The following instructions will guide you to configure the suggested settings of services:

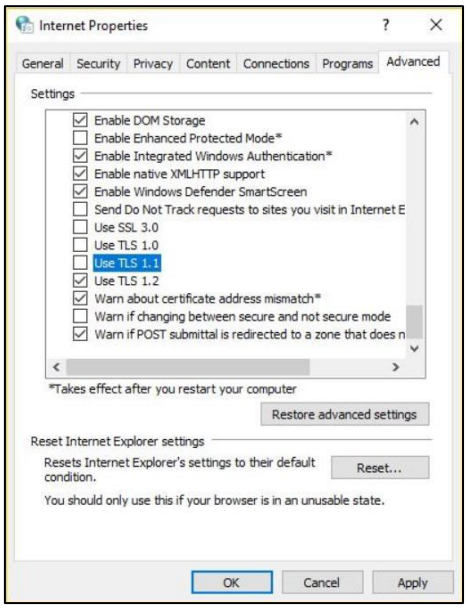
- For the console’s services

HTTP	**Disable**
HTTPS	Enable
Telnet	Disable
Moxa Command	Disable

Login to HTTP/HTTPS consoles, select **System Management→Misc. Settings→Console Settings**, then users can select to enable or disable services as suggested. Below snapshot is the GUI for Web Console.

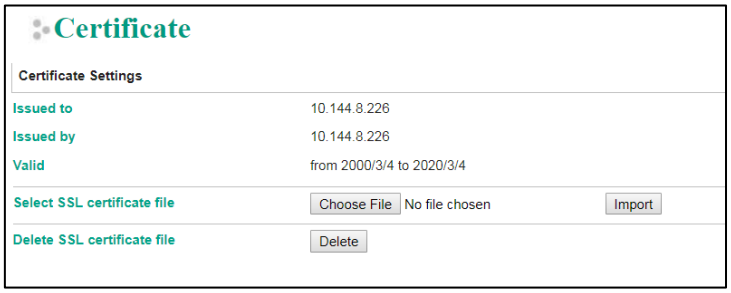
HTTPS is an encrypted communication channel. The encryption algorithm which is lower than TLS v1.1 has been proved to have severe vulnerability and higher risks to be hacked. It is suggested for users to disable the insecure SSL or TLS versions listed below from the Internet properties settings of the web browsers.

- SSL ver1.0
- SSL ver3.0
- SSL ver2.0
- TLS ver1.0
- TLS ver1.1



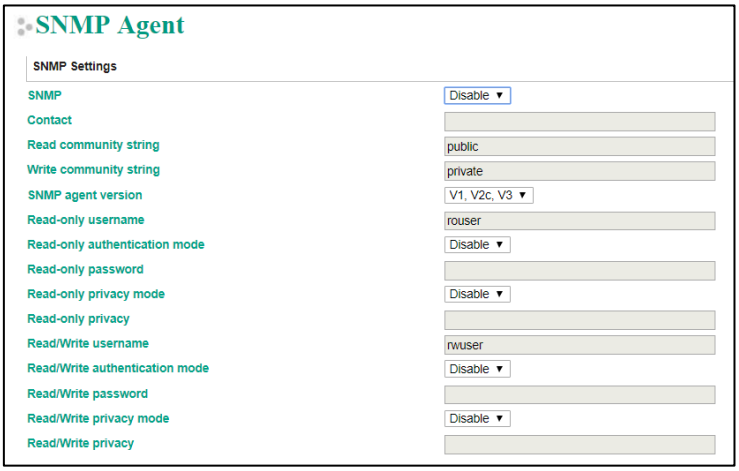
In order to use HTTPS console without certificate warning shown from web browsers, users need to import the trusted certificate issued by 3rd party Certificate Authority. The web browsers would validate the certificate in the HTTPS connection initialization stage and determine if the certificate from MGate MB3170/3270 series server could be considered as trustworthy or not.

Login to HTTP/HTTPS consoles, select **System Management→Certificate**. By importing the 3rd-party trusted SSL certificate, the security level can be enhanced. Below snapshot is the GUI for Web Console.



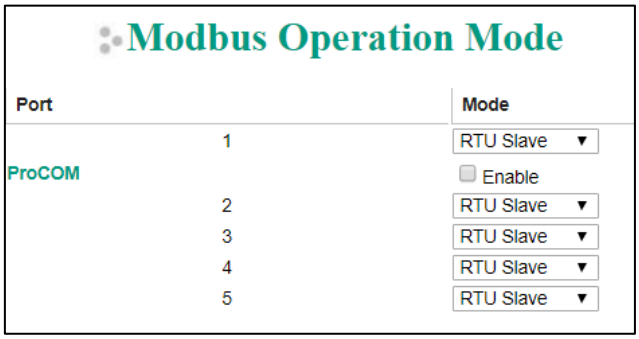
- For the SNMP Agent service

  Login to HTTP/HTTPS consoles, select **System Management→SNMP Agent**. Then, select Disable of the SNMP agent service. Below snapshot is the GUI for Web Console.



- For the ProCOM service

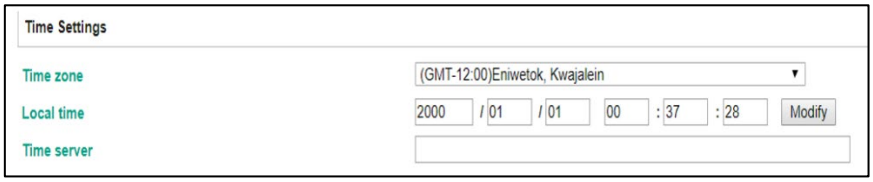
  Login to HTTP/HTTPS consoles, select **Protocol Settings→Mode**. Then, uncheck the Enable service of ProCOM. Below snapshot is the GUI for Web Console.



- For the NTP service

HTTP	Disable

  While entering to HTTP/HTTPS console, select Basic Settings, and then keep the Time server setting empty (which is meant to disable NTP service). Below snapshot is the GUI from the Web Console.

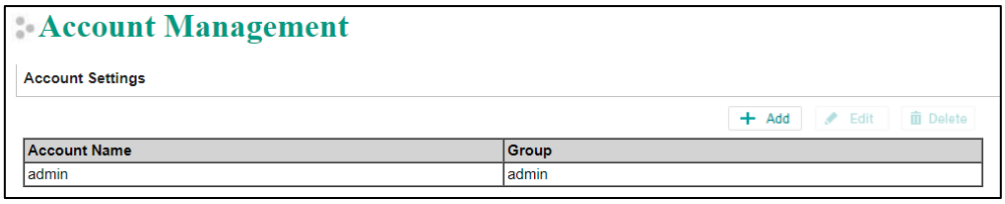


Note!

Every instruction above has to click the Submit button in order to save settings the user has made. Then to restart the MGate MB3170/3270 series to make the new settings effective.

7.2.2 Account Management

- The MGate MB3170/3270 series provides two different user levels: admin and user with maximum 16 accounts. The admin account can access and modify all the settings through the web console. The user account can only view the settings and cannot change anything.
- By default, the administration account, admin, is generated with the password of moxa. To do the account management, please log in to the web consoles, select **System Management→Misc. Settings→ Account Management**. To change the password from existed account, please double click the assigned account, you will then enter to the webpage for changing the password (at least 4 characters by default). The Below snapshots are the GUI for Web Console.



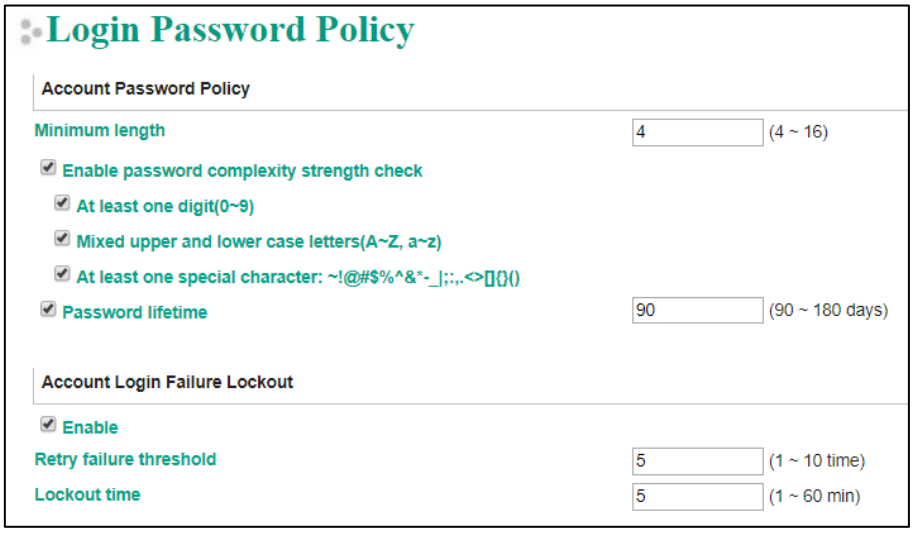
- To add a new account, please log in to HTTP/HTTPS console, and select **System Management→Misc. Settings→Account Management**. By clicking Add button, the account settings interface will be shown for configuration. The Account name, User level, New password, and Retype password are needed to be filled in to generate a new account. The below snapshot is the GUI for Web Console.

Note!

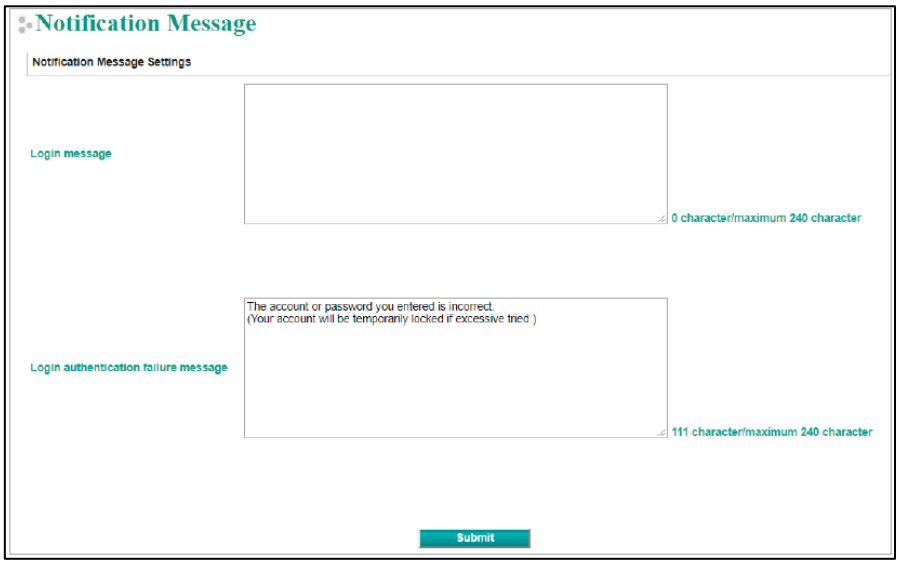
It is suggested to manage MGate MB3170/3270 series in another "administration level" account instead of using the default "admin" account, as it is commonly used by embedded system. Once the new administration level account has been created, the original "admin" account is suggested to be detected for security concern to avoid the brute-force attack.

- Considering security level, the login password policy and failure lockout can be configured. To configure it, please login to HTTP/HTTPS console, and select **System Management→Misc. Settings→Login Password Policy**. Not only the Account Password Policy can be configured, the Account Login Failure Lockout can be further enabled to increase the security level of account management.

  It is suggested to set password policy in higher complexity. For example, set the "Minimum length" to 16; enable all password complexity strength check; enable "Password lifetime" checking mechanism. Also, to avoid brute-force attack, it's suggested to enable Account Login Failure Lockout feature. The below snapshot is the GUI for Web Console.

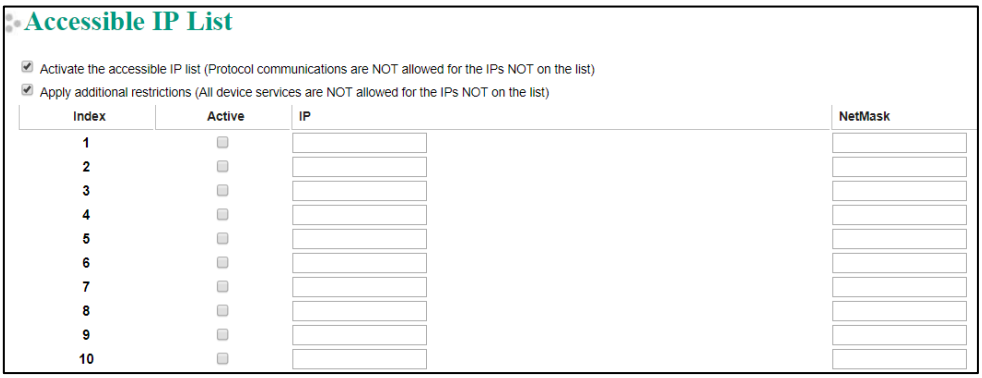


- For some system security requirements, it is needed to display an approved warning banner to all users attempting to access the device. The add up the warning banner please log in to HTTP/HTTPS console, and select **System Management→Misc. Settings→Notification Message**. Users can type in the warning message in the “Login Message” at all access points.



7.2.3 Accessible IP List

The MGate MB3170/3270 series has a feature which can add or block remote host IP addresses to prevent unauthorized access to the gateway. That is, if a host’s IP address is in the accessible IP table, then the host will be allowed to access the MGate MB3170/3270 series. To configure it, please login to HTTP/HTTPS console, select **System Management→Accessible IP List**. The different restrictions are listed in the table below (the checkbox Apply additional restrictions can only be activated if Activate the accessible IP list is activated. The below snapshot is the GUI for Web Console.



Activate the Accessible IP List	Apply Additional Restrictions	IPs on the List (Active Checked)	IPs NOT on the List (Active NOT Checked)
v		All protocol communication and services* are allowed.	Protocol communication is not allowed, but services* are still allowed.
v	v	All protocol communication and services* are allowed.	All services* are not allowed.

* Services indicates HTTP, HTTPS, TELNET, SSL, SNMP, SMTP, DNS, NTP, DSU

You may add a specific address or range of addresses by using a combination of an IP address and a netmask as follows:

- **To allow access to a specific IP address**: Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.
- **To allow access to hosts on a specific subnet**: For both the IP address and netmask, use 0 for the last digit (e.g., “192.168.1.0” and “255.255.255.0”).

- **To allow access to all IP addresses**: Make sure that Enable the accessible IP list is not checked.

Additional configuration examples are shown in the following table:

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	Enable
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.1.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128	255.255.255.128

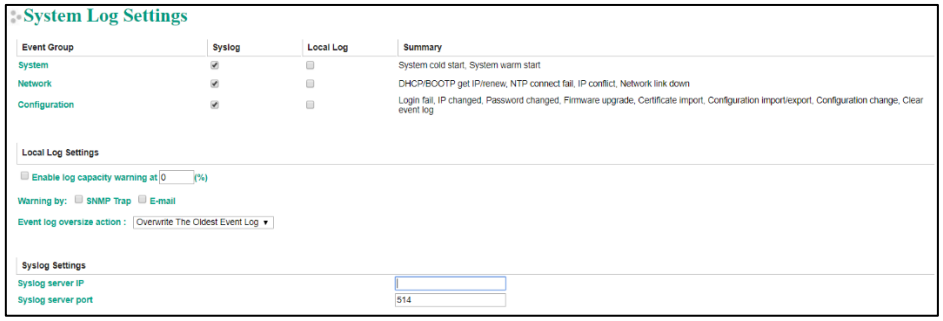
Warning: Ensure the communication peer is listed in the accessible IP list for entering the web console.

7.2.4 Logging and Auditing

- Please refer to below table for all the events that will be recorded by MGate MB3170/3270 series

Event Group	Summary
System	System cold start, System warm start
Network	DHCP/BOOTP get IP/renew, NTP connect fail, IP conflict, Network link down
Configuration	Login fail, IP changed, Password changed, Firmware upgrade, Certificate import, Configuration import/export, Configuration change, Clear event log

- To configure this setting, log in to HTTP/HTTPS console, and select **System Management→System Log Settings**. Then, enable the Local Log for recording on the MGate MB3170 device and/ or Syslog for keeping the records on a server over the network. It is suggested to enable system log settings to record all important system events to monitor any security issue of the device status. The below snapshot is the GUI for Web Console.



- To review above events, login to HTTP/HTTPS console, select **System Monitoring→System Log**. The snapshot in the following page is the GUI for Web Console.

7.3 Patching / Upgrades

7.3.1 Patch Management Plan

Considering to the patch management, Moxa will, in general, release version enhancement with thoroughly release note annually. If there is any security vulnerability issue being identified, Moxa will release the enhanced version within 30 days.

7.3.2 Firmware Upgrades

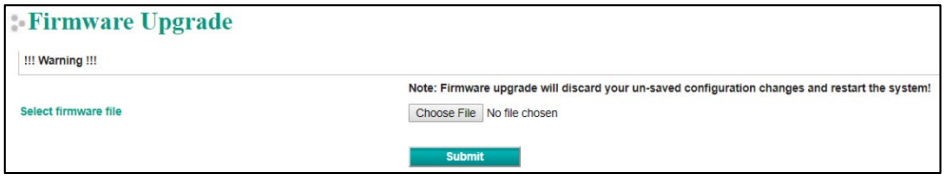
The process of firmware and/or software upgrade is instructed as below.

- Moxa will release the latest firmware and software along with its released notes on our official website. Below linkages are listed for the specified items for MGate

  MB3170/3270 series.

  - Firmware of MGate MB3170/3270 series:

    https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources
- When the user wants to upgrade the firmware of MGate MB3170/3270 series, please download the firmware from website first. Then log in to HTTP/HTTPS console, and select **System Management →Maintenance→Firmware Upgrade**. Click the Choose File button to select the proper firmware and click Submit to upgrade the firmware.



7.4 Security Information/ Vulnerability Feedback

As adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Cyber Security Response Team (CSRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

Please follow the updated Moxa security information from the below linkage:

https://www.moxa.com/en/support/product-support/security-advisory