MGate 5121 Series User Manual

Version 1.0, June 2023

www.moxa.com/products

MGate 5121 Series User Manual

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

Copyright Notice

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction 4
2. Getting Started 5
Connecting the Power 5
Connecting CAN Devices 5
Connecting to a Network 5
Installing DSU Software 5
Log In to the Web Console 6
microSD 6
3. Web Console Configuration and Troubleshooting 8
System Dashboard 8
System Settings 9
System Settings—General Settings 9
System Settings—Network Settings 11
System Settings—SNMP Settings 12
Protocol Settings 15
Protocol Settings—Protocol Conversion 15
Protocol Settings—CANopen Master Settings 16
Protocol Settings—J1939 Settings 22
Protocol Settings—Modbus TCP Server Settings 25
Protocol Settings—SNMP Mapping Settings 27
Diagnostics 28
Diagnostics—Protocol Diagnostics 28
Diagnostics—Protocol Traffic 31
Diagnostics—Event Log 32
Diagnostics—Tag View 36
Diagnostics—Network Connections 37
Diagnostics—Ping 37
Diagnostics—LLDP 38
Security 39
Security—Account Management 39
Security—Service 42
Security—Allowlist 43
Security—DoS Defense 44
Security—Login Policy 45
Security—Certificate Management 46
Maintenance 47
Maintenance—Configuration Import/Export 47
Maintenance—Firmware Upgrade 48
Maintenance—Load Factory Default 48
Restart 49
Status Monitoring 49
4. Network Management Tool (MXstudio) 50
A. SNMP Agents with MIB II 51
RFC1213 MIB-II Supported SNMP Variables 51

1. Introduction

The MGate 5121 is an industrial Ethernet gateway for converting CANopen or J1939 to Modbus TCP and SNMP network communications. To integrate existing CANopen or J1939 devices into a Modbus TCP or SNMP network, use the MGate 5121 as a CANopen or J1939 master to collect data and exchange data with the Modbus TCP host or SNMP client. All models are protected by a rugged and compact metal housing and are DIN-rail mountable. The rugged design is suitable for industrial applications such as factory automation and other process automation industries.

2. Getting Started

Connecting the Power

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

1. Loosen or remove the screws on the terminal block.
2. Turn off the power source and then connect a 12–48 VDC power line to the terminal block.
3. Tighten the connections, using the screws on the terminal block.
4. Turn on the power source.

Note that the unit does not have an on/off switch. It automatically turns on when it receives power. The PWR LED on the top panel will glow to show that the unit is receiving power. For power terminal block pin assignments, refer to the *Quick Installation Guide,* ***Power Input and Relay Output Pinout*** section.

Connecting CAN Devices

The MGate supports CAN devices. Before connecting or removing the serial connection, first make sure the power is turned off. For the CAN port pin assignments, refer to the *Quick Installation Guide*, ***Pin Assignments*** section.

Connecting to a Network

Connect one end of the Ethernet cable to the MGate's 10/100M Ethernet port and the other end of the cable to the Ethernet network. The MGate will show a valid connection to the Ethernet in the following ways:

- The Ethernet LED maintains a solid green color when connected to a 100 Mbps Ethernet network.
- The Ethernet LED maintains a solid orange color when connected to a 10 Mbps Ethernet network.
- The Ethernet LED will flash when Ethernet packets are being transmitted or received.

Installing DSU Software

If you do not know the MGate gateway's IP address when setting it up for the first time (default IP is *192.168.127.254*); use an Ethernet cable to connect the host PC and MGate gateway directly. If you connect the gateway and host PC through the same Ethernet switch, make sure there is no router between them. You can then use the **Device Search Utility (DSU)** to detect the MGate gateways on your network. You can download DSU (Device Search Utility) from Moxa's website: www.moxa.com.

The following instructions explain how to install the DSU, a utility to search for MGate units on a network.

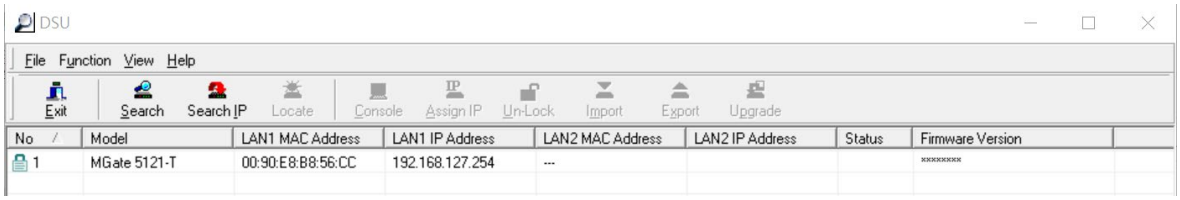
1. Locate and run the following setup program to begin the installation process:

   dsu_setup_[*Version*]**_Build_**[*DateTime*]**.exe**

   This version might be named **dsu_setup_Ver2.x_Build_xxxxxxxx.exe**
2. The Welcome window will greet you. Click **Next** to continue.
3. When the **Select Destination Location** window appears, click **Next** to continue. You may change the destination directory by first clicking on **Browse...**.
4. When the **Select Additional Tasks** window appears, click **Next** to continue. You may select **Create a desktop icon** if you would like a shortcut to the DSU on your desktop.
5. Click **Install** to copy the software files.
6. A progress bar will appear. The procedure should take only a few seconds to complete.
7. A message will show the DSU has been successfully installed. You may choose to run it immediately by selecting **Launch DSU**.

8. You may also open the DSU through **Start > Programs > MOXA > DSU**.

The DSU window should appear as shown below. Click **Search** and a new Search window will pop up.

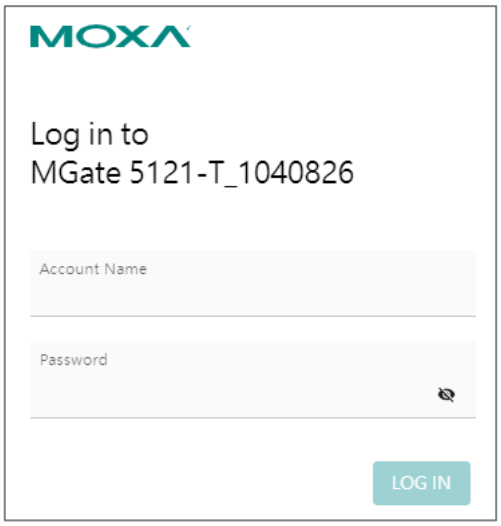


Log In to the Web Console

Use the Web console to configure the MGate through Ethernet or verify the MGate's status. Use a web browser, such as Google Chrome to connect to the MGate, using the HTTPS protocol.

When the MGate gateway appears on the DSU device list, select the gateway and right-click the mouse button to open a web console to configure the gateway.

On the login page, create an account name and set a password when you log in for the first time. Or if you have already an account, log in with your account name and password.



microSD

The MGate provides users with an easy way to back up, copy, replace, or deploy. The MGate is equipped with a microSD card slot. Users can plug in a microSD card to back up data, including the system configuration settings.

First time use of a new microSD card with the MGate gateway

1. Format the microSD card as FAT file system through a PC.
2. Power off the MGate and insert the microSD card (ensure that the microSD card is empty).
3. Power on the MGate. The default settings will be copied to the microSD card.
4. Manually configure the MGate via web console, and all the stored changes will copy to the microSD card for synchronization.

First time use of a microSD card containing a configuration file with the MGate gateway

1. Power off the MGate and insert the microSD card.
2. Power on the MGate.
3. The configuration file stored in the microSD card will automatically copy to the MGate.

Duplicating current configurations to another MGate gateway

1. Power off the MGate and insert a new microSD card.
2. Power on the MGate.
3. The configuration will be copied from the MGate to the microSD card.
4. Power off the MGate and insert the microSD card into the other MGate.
5. Power on the second MGate.
6. The configuration file stored in the microSD card will automatically copy to the MGate.

Malfunctioning MGate replacement

1. Replace the malfunctioning MGate with a new MGate.
2. Insert the microSD card into the new MGate.
3. Power on the MGate.
4. The configuration file stored on the microSD card will automatically copy to the MGate.

microSD card writing failure

The following circumstances may cause the microSD card to experience a writing failure:

1. The microSD card has less than 256 Mbytes of free space remaining.
2. The microSD card is write-protected.
3. The file system is corrupted.
4. The microSD card is damaged.

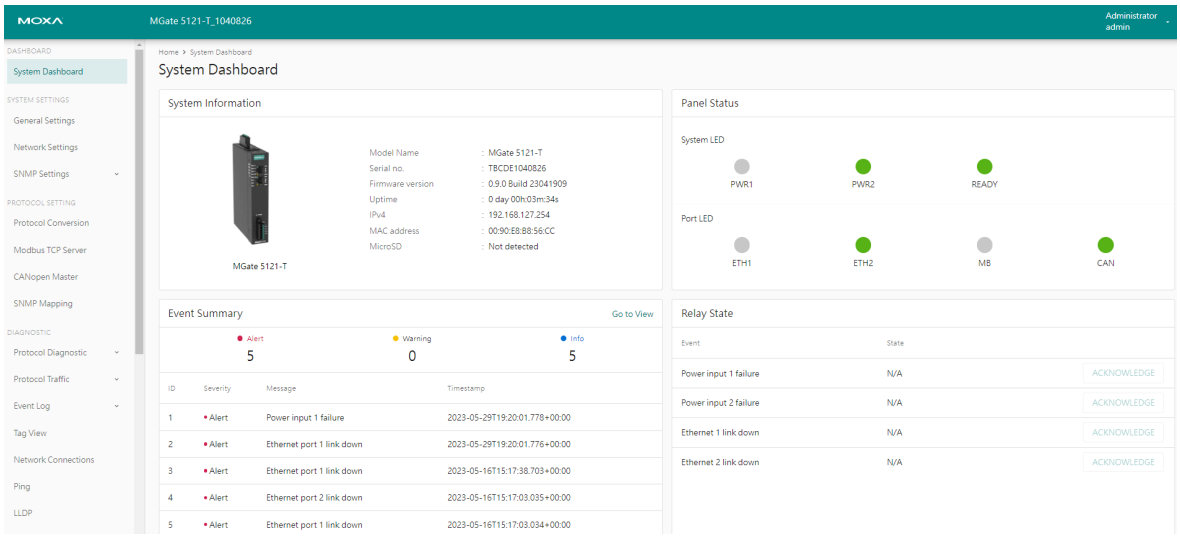
In case of the above events, the MGate will flash Ready LED in red color. When you replace the MGate gateway's microSD card, the microSD card will synchronize the configurations stored on the MGate gateway. Note that the replacement microSD card should not contain any configuration files on it; otherwise, the out-of-date configuration will be copied to the MGate device.

3. Web Console Configuration and Troubleshooting

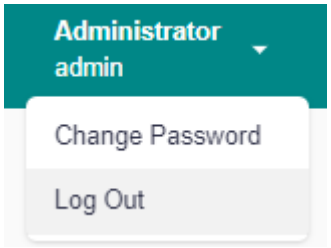
This chapter provides a quick overview of how to configure the MGate 5121 by web console.

System Dashboard

This page gives a system dashboard of the MGate 5121 gateway.



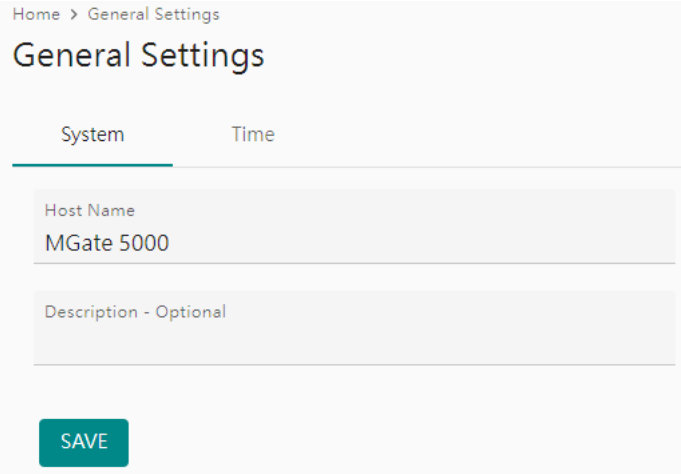
You can change your password or log out using the options on the top-right corner of the page.



System Settings

System Settings—General Settings

On this page, you can change the name of the device and time settings.



System Settings

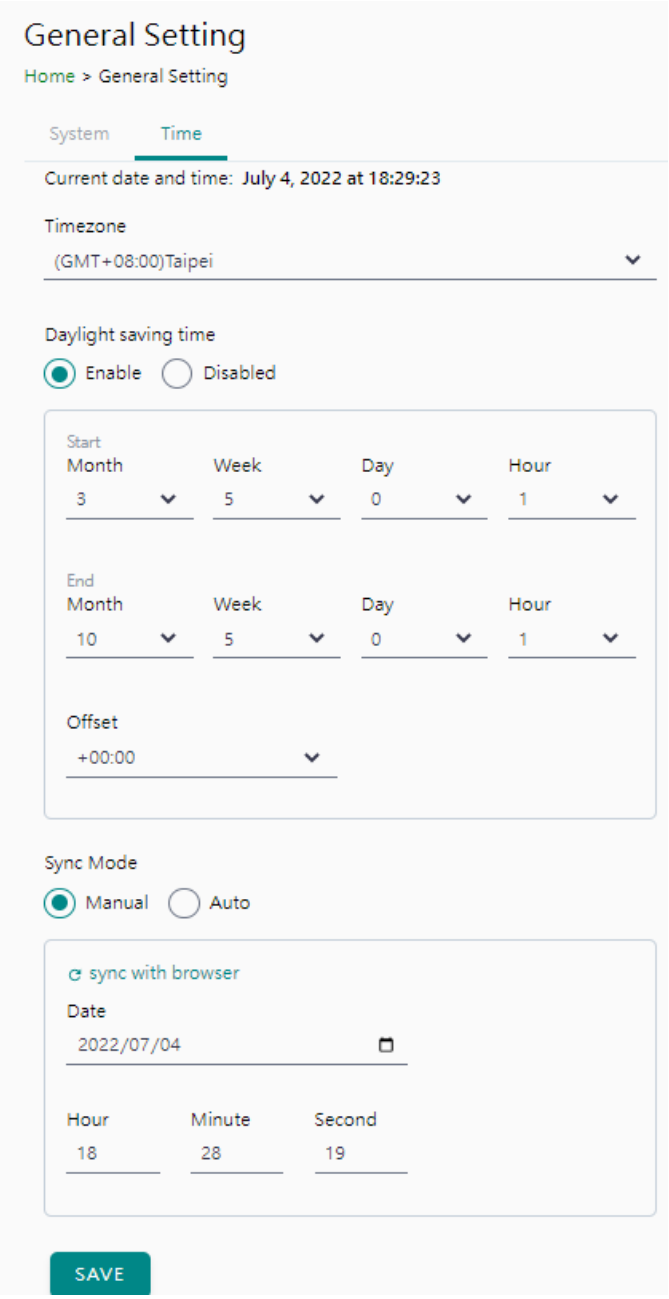
Parameter	Value	Description
Host Name	Alphanumeric string	Enter a name that can help you uniquely identify the device. For example, you can include the name and function of the device.
Description	Alphanumeric string	(optional) You can include additional description about the device such as function and location.

Time Settings

The MGate has a built-in real-time clock for time-calibration functions. Functions such as logs use the real-time clock to add the timestamp to messages.

ATTENTION

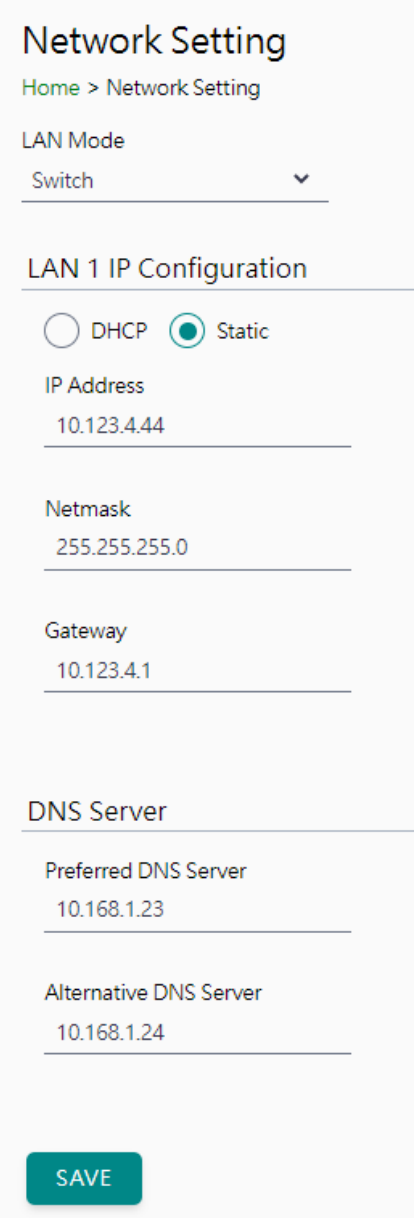
First-time users should select the time zone first. The console will display the actual time in your time zone relative to the GMT. If you would like to change the real-time clock, select Local time. MGate's firmware will change the GMT time according to the Time Zone setting.



Parameter	Value	Description
Time zone	User-selectable time zone	Shows the current time zone selected and allows change to a different time zone.
Daylight saving time	Enable Disable	Enables daylight saving time to automatically adjust the time according to the region.
Sync Mode	Manual	Use this setting to manually adjust the time (1900/1/1-2037/12/31) or sync with the browser time
	Auto	Specify the IP or domain of the time server to sync with (E.g., 192.168.1.1 or time.stdtime.gov.tw). This optional field specifies the IP address or domain name of the time server on your network. The module supports SNTP (RFC-1769) for automatic time calibration. The MGate will request the time information from the specified time server per the set configured time.

System Settings—Network Settings

You can change the IP Configuration, IP Address, Netmask, Default Gateway, and DNS settings on the **Network Settings** page.

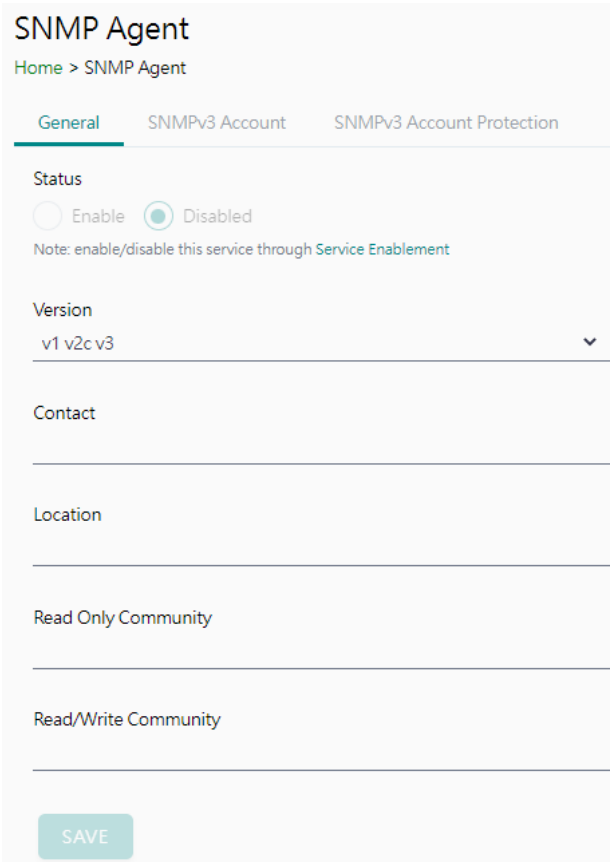


Parameter	Value	Description
LAN Mode	**Switch, Dual IP, Redundant LAN**	The **Switch** mode allows users to install the device with daisy-chain topology. The **Dual IP** mode allows the gateway to have two different IP addresses, each with distinct netmask and gateway settings. The IP addresses can have the same MAC address. The **Redundant LAN** mode allows users to use the same IP address on both Ethernet ports. The default active LAN port is ETH1 after bootup. If the active LAN link is down, the device will automatically switch to the backup LAN ETH2.
IP Configuration	**DHCP, Static IP**	Select **Static IP** if you are using a fixed IP address. Select the DHCP option if you want the IP address to be dynamically assigned.
IP Address	192.168.127.254 (or other 32-bit number)	The **IP Address** identifies the server on the TCP/IP network.

Parameter	Value	Description
Netmask	255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
Gateway	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
Preferred DNS Server	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
Alternative DNS Server	0.0.0.0 (or other 32-bit number)	The IP address of the secondary domain name server.

System Settings—SNMP Settings

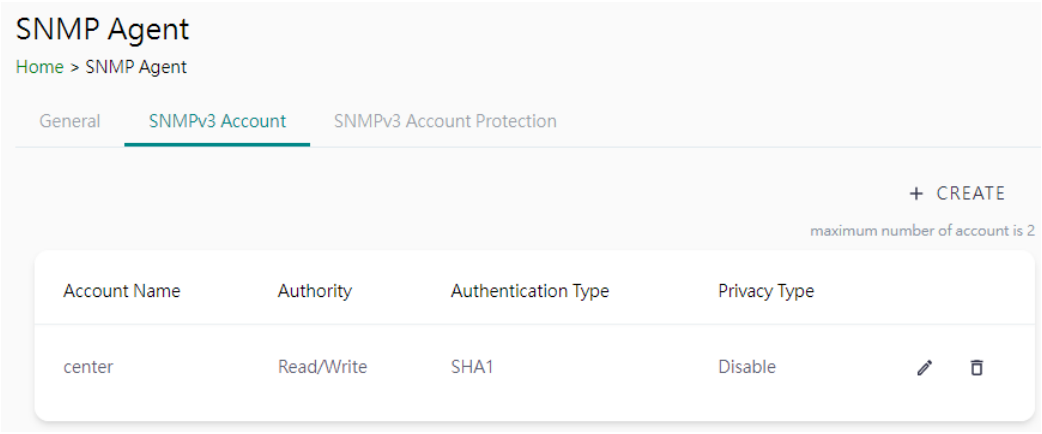
System Settings—SNMP Settings—SNMP Agent

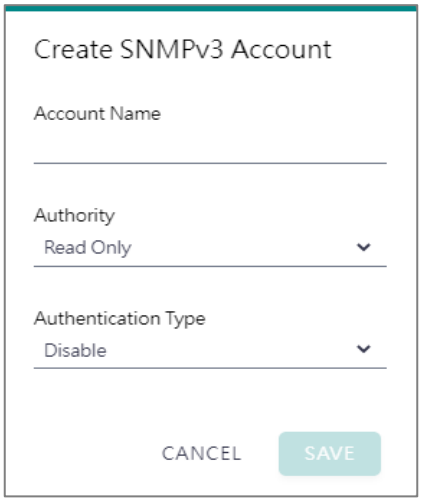


Parameters	Description
Version	The SNMP version; MGate supports SNMP V1, V2c, and V3.
Contact	The optional contact information; usually includes an emergency contact name and telephone number.
Read Only Community	A text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
Read/Write Community	A text password mechanism that is used to weakly authenticate changes to agents of managed network devices.

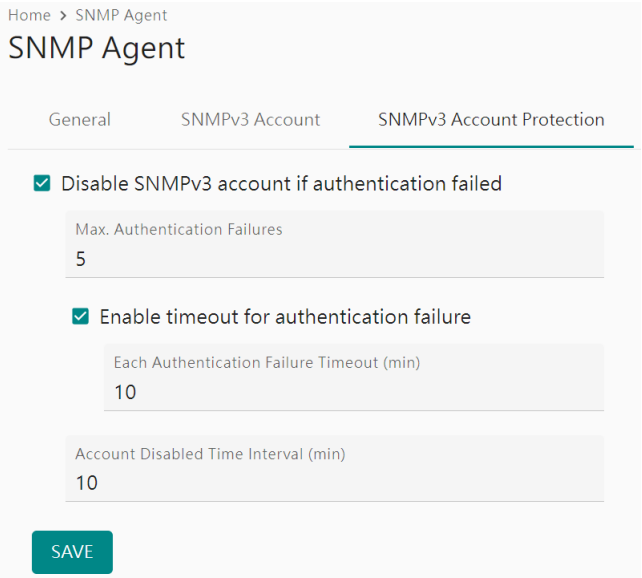
Read-only and Read/write Access Control

You can define usernames, passwords, and authentication parameters in SNMP for two levels of access control: read-only and read/write. The access level is shown in the value of the Authority field. For example, Read-only authentication mode allows you to configure the authentication mode for read-only access, whereas Read/Write authentication mode allows you to configure the authentication mode for read/write access. For each level of access, you may configure the following:



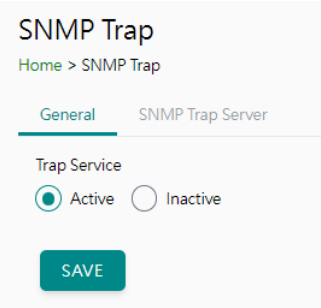


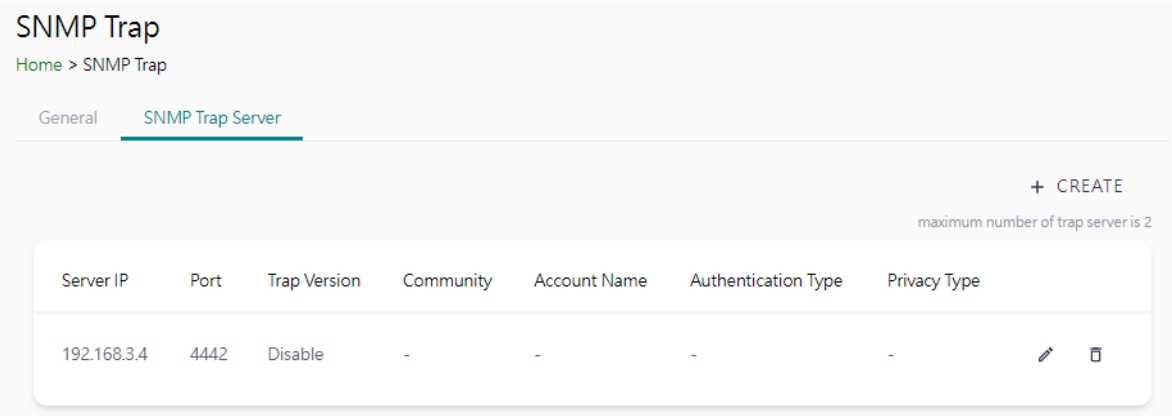
Parameters	Value	Description
Account Name		The username for which the access level is being defined.
Authority	**Read Only** **Read/Write**	The level of access allowed
Authentication Type	**Disable** **MD5** **SHA1** **SHA-224** **SHA-256** **SHA-384** **SHA-512**	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.

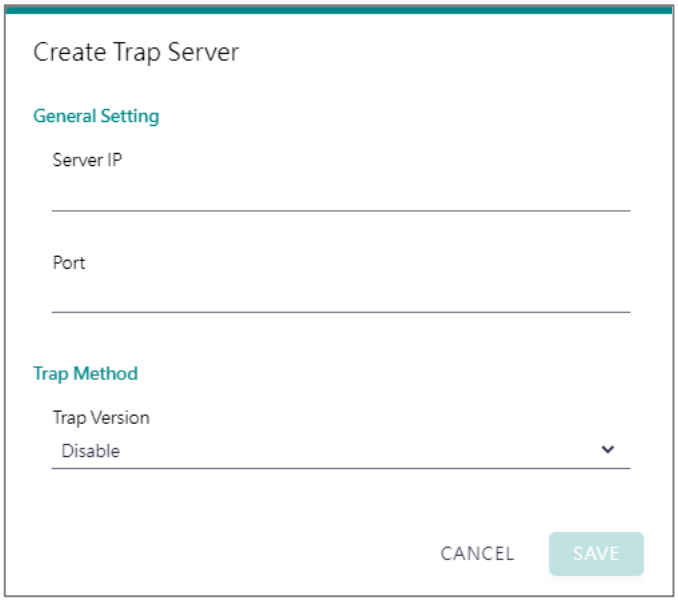


Parameters	Value	Description
Max Authentication Failure	1 to 10 (default 5)	Specifies the maximum number of authentication failures. If this number is exceeded, the MGate will disable SNMPv3.
Each Authentication Failure Timeout (min)	1 to 1440 (default 10)	Specifies a timeout period when enabling the **Timeout for authentication failure** function
Account Disabled Time Interval (min)	1 to 60 (default 10)	When the number of authentication failures exceeds the value set in **Max Authentication Failure Times**, the MGate will disable the SNMPv3 for Account Disabled Time Interval.

System Settings—SNMP Settings—SNMP Trap





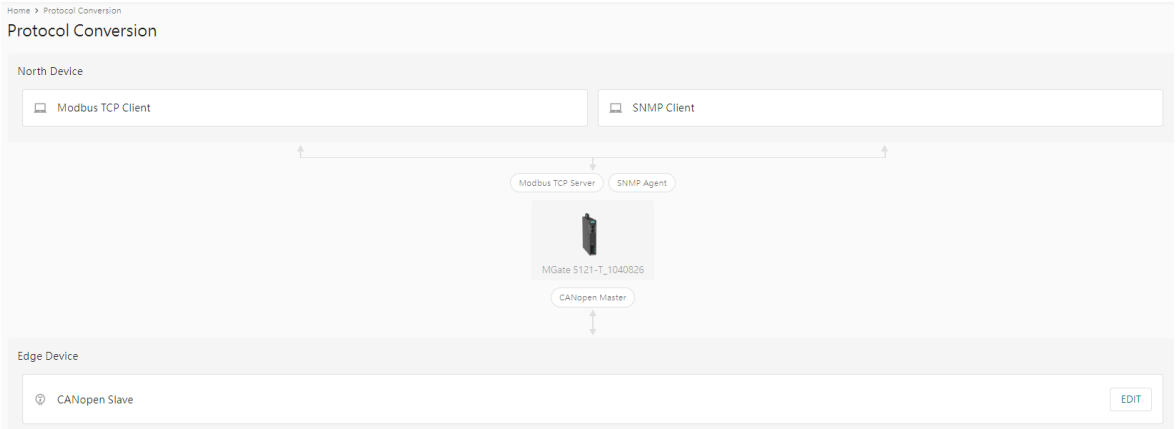


Parameters	Description
Server IP	SNMP server IP address or domain name; the maximum number of trap servers is 2
Port	SNMP server IP Port.
Trap Version	**Disable** **SNMPv1** **SNMPv2** **SNMPv3**

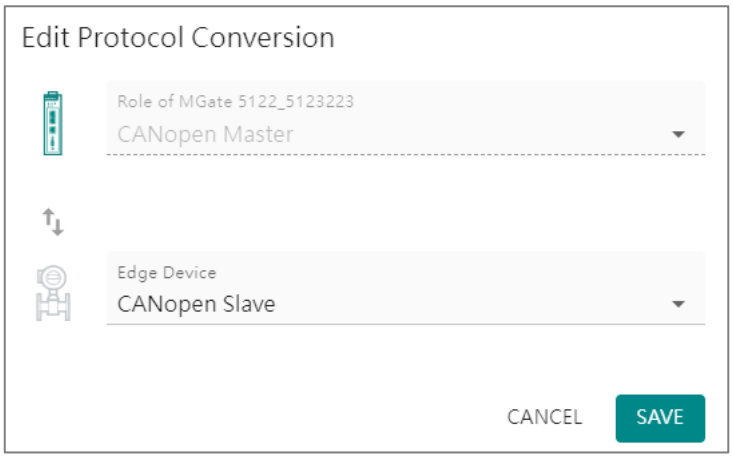
Protocol Settings

Protocol Settings—Protocol Conversion

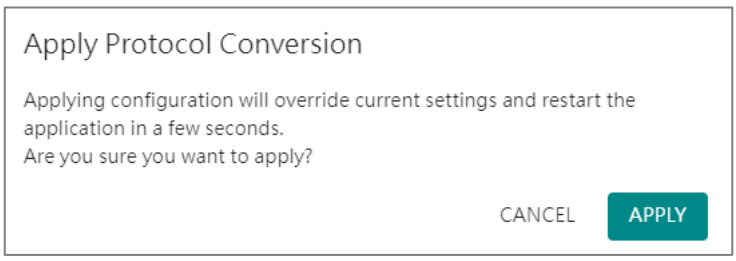
You can select CANopen or J1939 on this page.



Click **Edit** at the "Edge Device" right-hand side and select your device protocol roles.

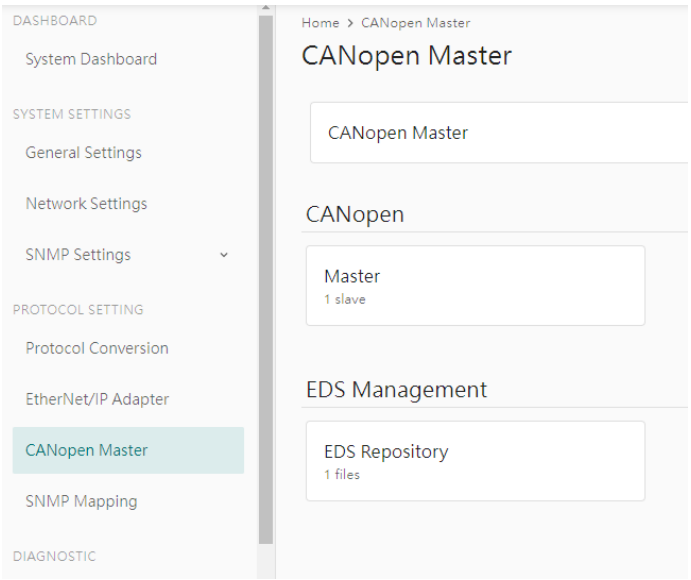


Click **SAVE** then **APPLY** on the warning pop-up window.

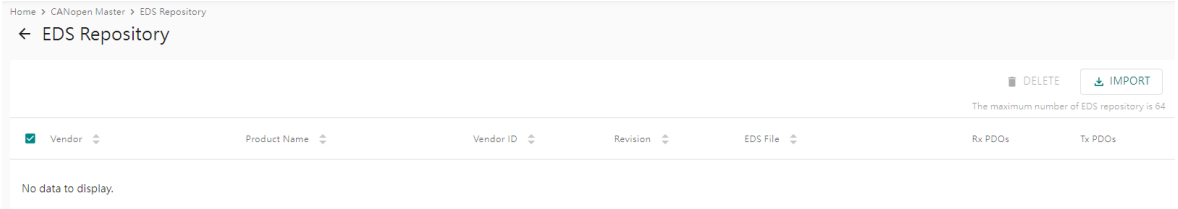


Protocol Settings—CANopen Master Settings

You can manage CANopen devices on this page.

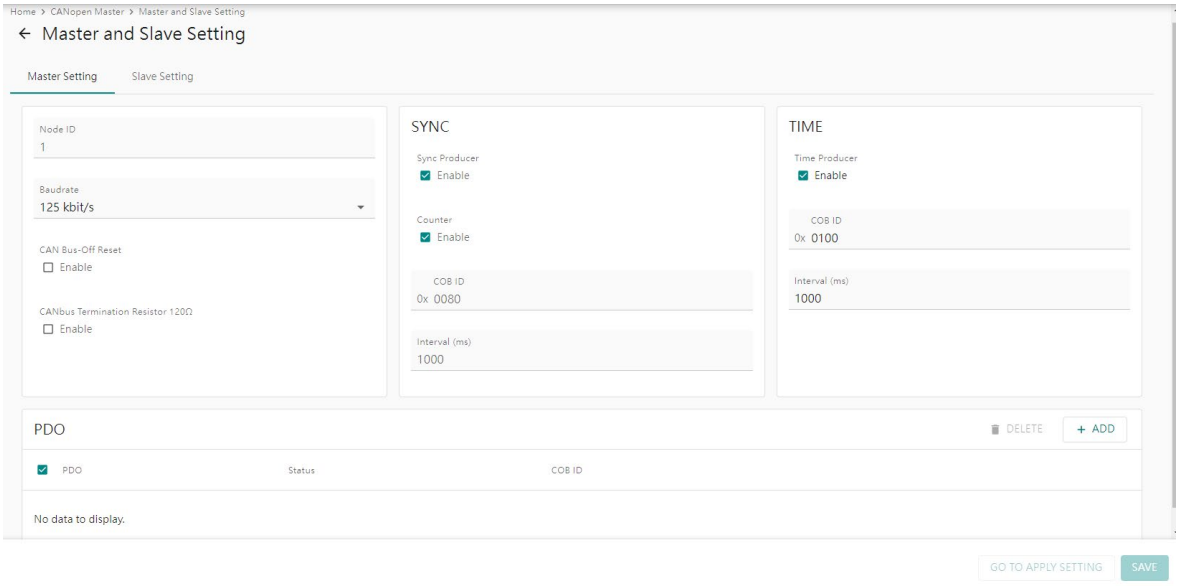


You can manage CANopen slave device EDS files in "EDS Management-EDS Repository". The MGate can store up to 64 different EDS files. Click Import to add the EDS file. Tick the item, then you can delete it.



Parameter	Description
Vendor	Vendor name
Product Name	Product name
Vendor ID	Vendor ID registered in CiA organization
Revision	EDS file revision
EDS file	EDS file name
RxPDOs	Supports number of RxPDO
TxPDOs	Supports number of TxPDO

Click CANopen-Master to config CANopen master and slave settings.

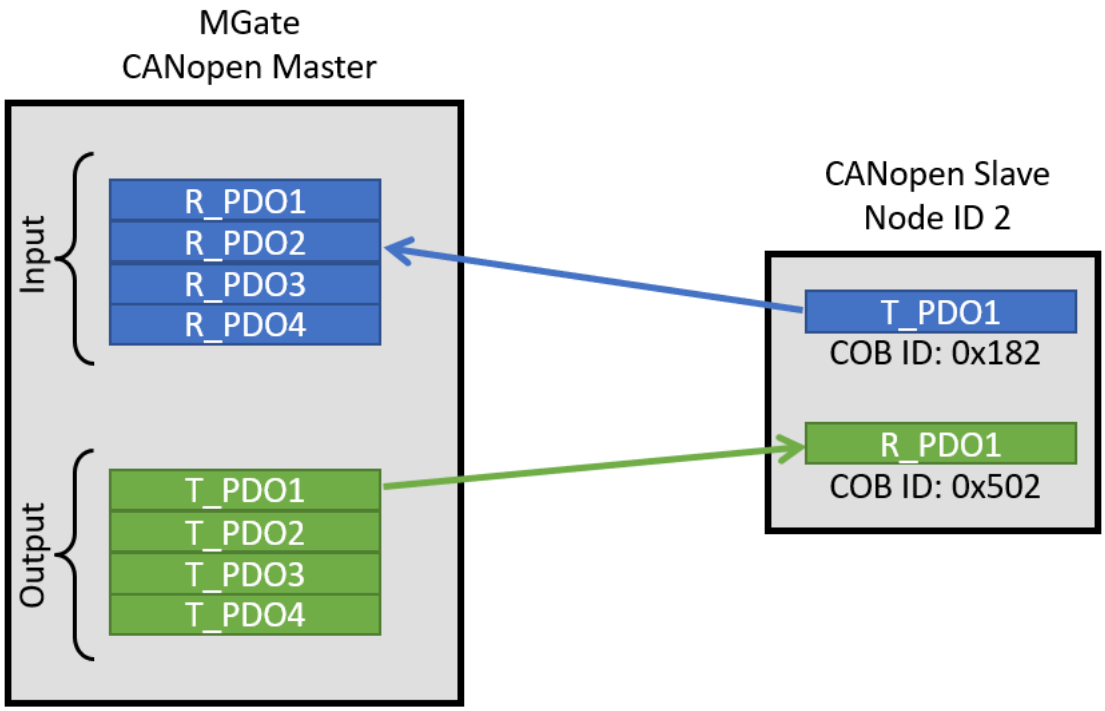


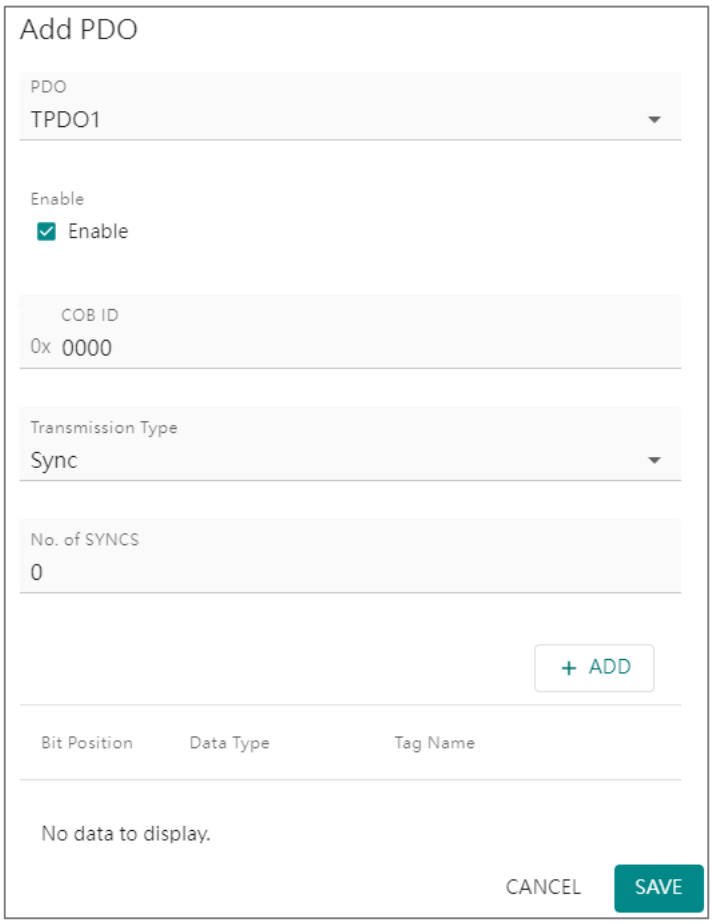
Master Settings

Parameter	Value	Default	Description
Node ID	1~127	1	Master CANopen Node ID
Baudrate	10 kbit/s 20 kbit/s 50 kbit/s 125 kbit/s 250 kbit/s 500 kbit/s 800 kbit/s 1 Mbit/s	125 kbit/s	Set CANopen network baudrate
CAN Bus-OFF Reset	Disable Enable	Disable	When the MGate detects the error count exceed the CAN threshold, the CAN bus will switch to Bus Off mode according the CAN definition. Enable will auto reset the error count and restart the bus. Disable will stay in the Bus Off mode and only can recover by re-power the MGate.
CANbus Termination Resistor 120 ohms	Disable Enable	Disable	

Parameter	Value	Default	Description
SYNC- SYNC Producer	Disable Enable	Enable	Enable the MGate to send out the SYNC signal based on the interval time.
SYNC-Counter	Disable Enable	Enable	Enable to include SYNC counter information in the SYNC message. Counter is a 2 bytes value from 0~65535 with rolling over behavior.
SYNC-COB ID	0x0000 to 0xFFFF	0x0080	Standard SYNC COB ID is 0x0080
SYNC-Interval(ms)	0 to 65535	1000	Interval time for the SYNC message.
Time-Time Producer	Disable Enable	Enable	Enable the MGate to send out the TIME stamp message. TIME is a 6 bytes value with UAT format.
Time-COB ID	0x0000 to 0xFFFF	0x0100	Standard TIME COB ID is 0x0100
Time-Interval (ms)	0 to 65535	1000	Interval time for the TIME message.

MGate CANopen master supports up to 256 TPDO and up to 256 RPDO, Click ADD to edit PDO with slave PDO COB ID. For example, if you want to mapping slave ID 2's RPDO4 to MGate TPDO1, please type in COB ID 0x0502 in the CANopen master TPDO1. If you want to mapping slave ID2's TPDO1 to CANopen master RPDO2, please type in COB ID 0x0182 in RPDO2.



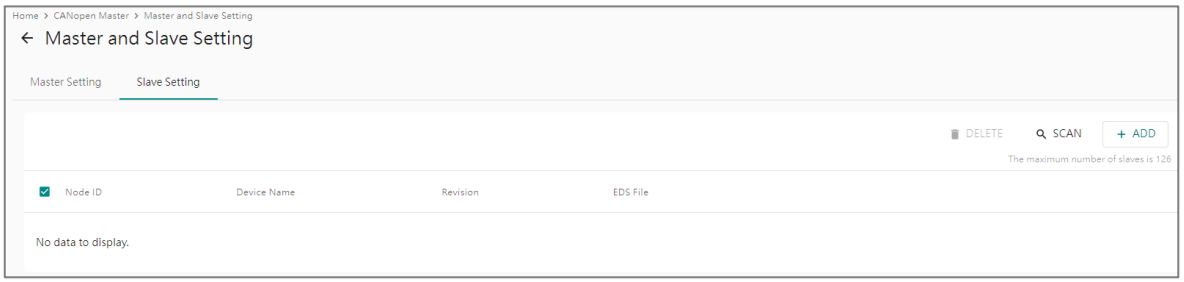


Parameter	Value	Default	Description
PDO	TPDOx RPDOx		Max 256 TPDO, 256 RPTO
Enable	Disable Enable	Enable	
COB ID	0x0000 to 0xFFFF	0x0000	Refer to CANopen COB ID table then type in the slave PDO COB ID number in heximal.
Transmission Type	Sync, RTR, Event	Sync	For TPDO: **Sync.** The MGate will send out TPDO following by the number of SYNC reached which set in the **No. of SYNCS**. **RTR**. The MGate will send out TPDO when received RTR bit ON in the slave RPDO, which COB ID is set in previous setting. **Event.** The MGate will send out TPDO cyclic according to the Event Timer(ms). If Event time is 0, then TPDO will send out when data changed. To use CAN bus loading efficiently, you can set the Inhibit Time(ms) to avoid sending TPDO too frequently. For RPDO: **Sync.** The MGate will update the slave RPDO data into internal memory only when SYNC message occurred. **Event.** The MGate updates the slave RPDO data into internal memory when received the slave RTDO.
No. of SYNCS	0 to 240	0	No. of SYNC messages. Value from 0 to 240.
Bit Position	Automatic generated		Bit offset in the PDO data frame
Data Type	1 to 7 Bit 1 to 8 Byte	1 Bit	Tag data type
Tag Name	Alphanumeric string		Create Tag names. User can select tags in the northbound protocol setting.

CANopen COB ID table

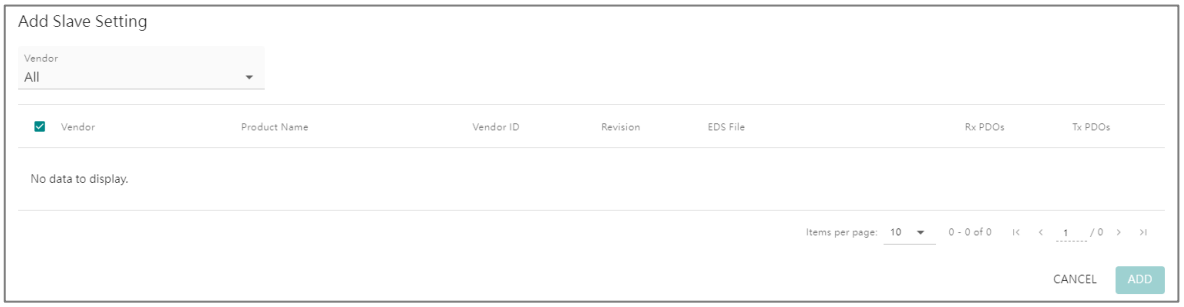
Communication Object	Function Code (4 bit, binary)	Node ID (dec)	COB ID (hex)
NMT	0000	0	0x000
SYNC	0001	0	0x080
EMCY	0001	1~127	0x081~0x0FF
TIME	0010	0	0x100
T_PDO 1	0011	1~127	0x181~1FF
R_PDO 1	0100	1~127	0x201~27F
T_PDO 2	0101	1~127	0x281~2FF
R_PDO 2	0110	1~127	0x301~37F
T_PDO 3	0111	1~127	0x381~3FF
R_PDO 3	1000	1~127	0x401~47F
T_PDO 4	1001	1~127	0x481~4FF
R_PDO 4	1010	1~127	0x501~57F
T_SDO	1011	1~127	0x581~5FF
R_SDO	1100	1~127	0x601~67F
Heartbeat	1110	1~127	0x701~77F

Add CANopen slave device into Slave Setting.

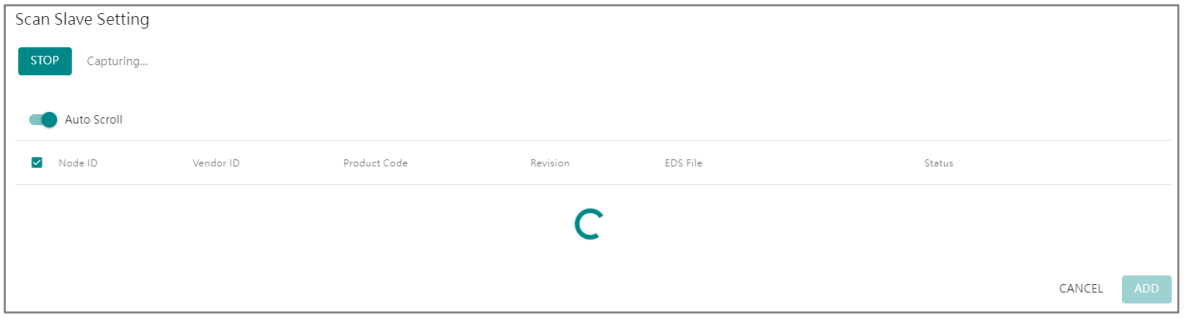


You can ADD slave device manually or SCAN the devices on the CANbus. Please import slave EDS files before adding or scanning the slave devices.

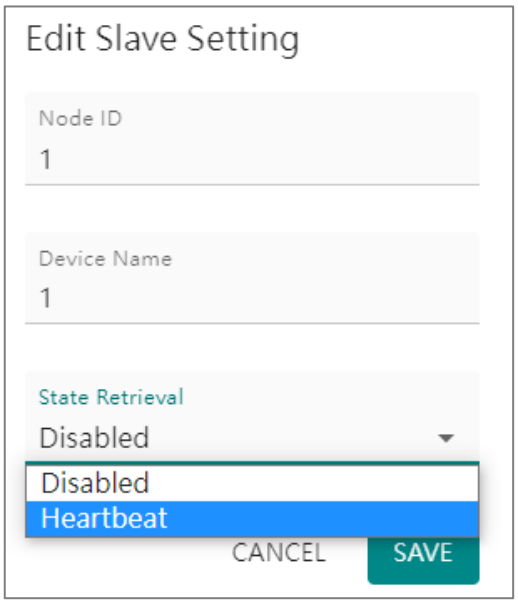
Click the ADD button and select the slave device from the EDS repository.

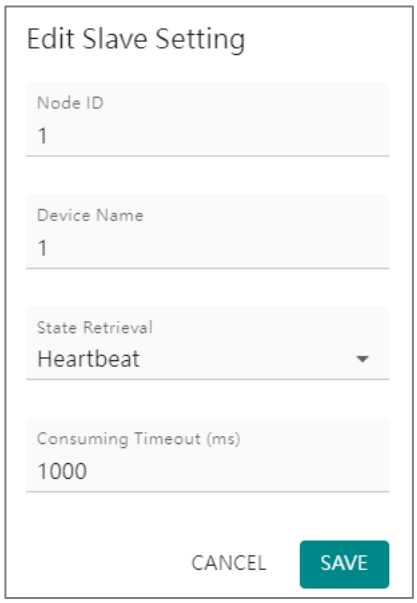


Or click the SCAN button to scan the device on the CAN bus. Only the slave device that matches the EDS file in the EDS Repository will be added to the table.

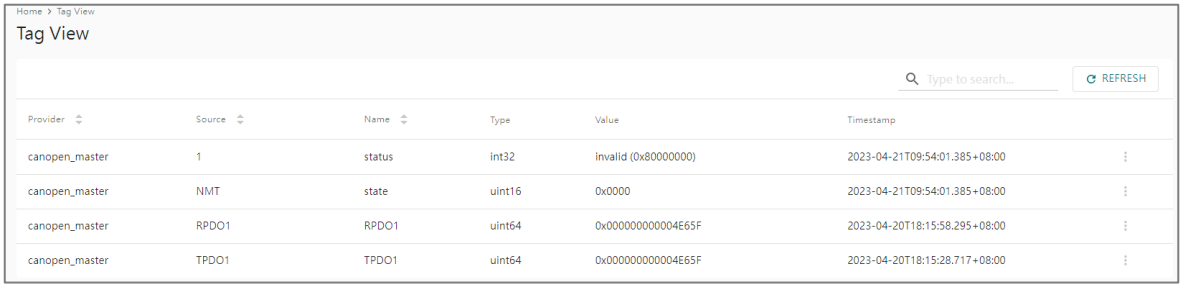


Click the pen icon to edit the slave Node ID and Device Name, and enable Heartbeat with the heartbeat time **Consuming Timeout (ms)**.



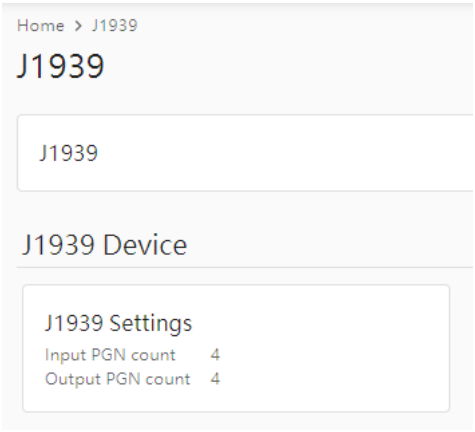


Heartbeat tag view status

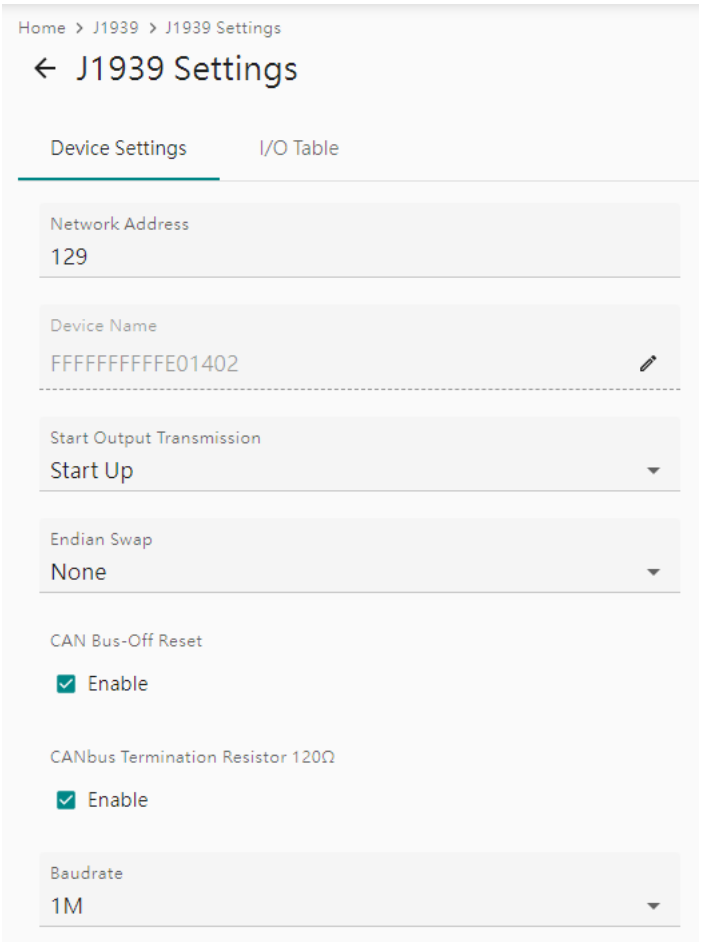


Protocol Settings—J1939 Settings

You can manage J1939 protocol on this page.



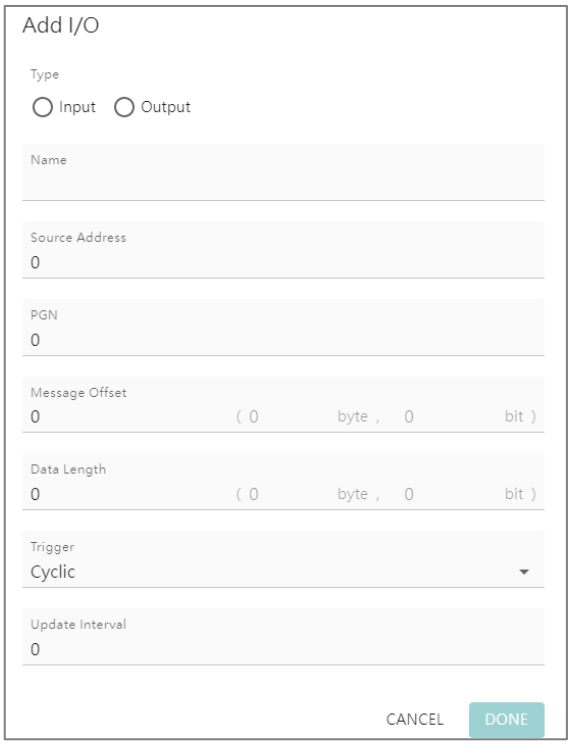
Config J1939 settings in **Device Settings** tab.

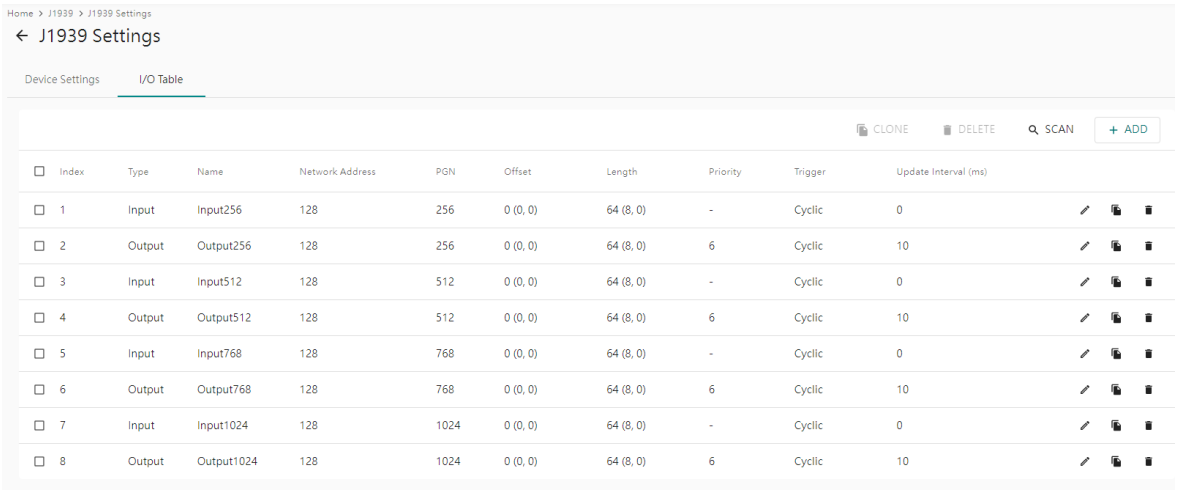


Parameter	Value	Default	Description
Network address	Numerical number	128 to 253	The MGate's network address in the J1939 bus
Device name	The parameters regarding to J1939.	FFFFFFFFFFFFFFFF	A set of J1939 parameter combinations represented in hex value
Start output transmission by	Data update, startup	Data update	To determine the way the transmission starts

Parameter	Value	Default	Description
Endian swap	Data Byte Swapping **None:** Don't need to swap **Byte:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C. **Word:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. **ByteWord:** 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A	None	Swapping the data
CAN bus-off reset	Disable, Enable	Disable	When some kind of J1939 bus error happens, the MGate will automatically stop communication with the J1939 bus. You may choose Enable to have the MGate rejoin the bus.
CANbus termination resistor 120 ohms	Disable, Enable	Disable	To enable 120 ohms termination resistor on CAN bus.
Baudrate	250 kbps, 500 kbps, 1Mbps	250 kbps	The baudrate used in J1939

In the **I/O Table** tab, you can change the input/output commands of J1939. Click **ADD** to add the J1939 commands into the MGate, according to the J1939 device it is attached to.





Parameter	Value	Default	Description
Type	Input, Output	Input	Data type
Name	(An alphanumeric string)	Command1	Max. 32 characters
Source Address	0 to 253, 255	0	Data from which J1939 device. Also listed as Network Address in the IO table.
Destination Address (for output)	0 to 253, 255	0	Data sent to which J1939 device. Also listed as Network Address in the IO table.
PGN	0 to 131071	0	Parameter Group Number
Message Offset	0 to 14279 bits	0 (0, 0)	The location where the data associated with the data point begins. The offset not only can be shown in bits but can be displayed as corresponding bytes and bits (byte, bit).
Data Length	0 to 14280 bits	0 (0, 0)	The length of the data to be transferred between the J1939 devices. The length not only can be shown in bits but also can be displayed as corresponding bytes and bits (byte, bit).
Trigger	Disable, Cyclic, Data Change	Cyclic	Disable: The command has never been sens Cyclic: The command is sent cyclically at the interval specified in the Poll Interval parameter. Data change: The data area is polled for changes at the time interval defined by Poll Interval. A command is issued when a change in data is detected.
Update interval	0 to 65535 ms	0	The desired update interval for the data in milliseconds.
Priority (for output)	0 to 7		Output PGN priority
Fault Protection (for output)	Keep Latest Data Clear All Data Bit to 0 Set To User Defined Value	Keep Latest Data	You can configure the criteria used to determine what to do when the write command is no longer received from the master side. For example, when a cable comes loose accidentally, the most up-to-date write command from the master side will not be received by the gateway. **Keep Latest Data:** The gateway will write the same data to the slave device. **Clear All Data Bit to 0:** The gateway will write zero values to the slave device. **Set To User Defined Value:** A user-defined value will be written to the slave device.

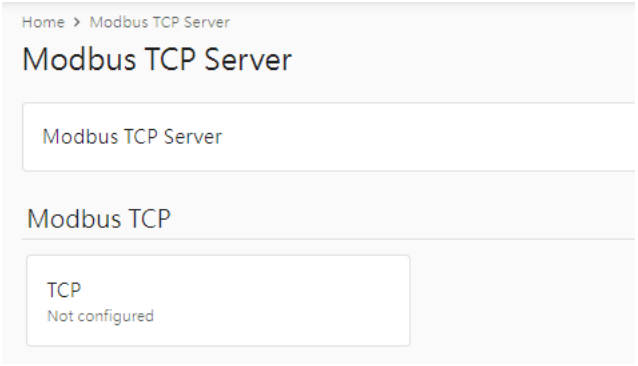
AutoScan:

For users' convenience, the MGate is designed with an innovative command auto-learning function. It can learn all the output commands from the J1939 devices in the same CAN bus. Users don't need to key in the commands one by one. All you have to do is click on the **SCAN** button, and a window will pop up. Click the Start button to learn. Click the pen icon at the right-hand side of the command to edit the command.

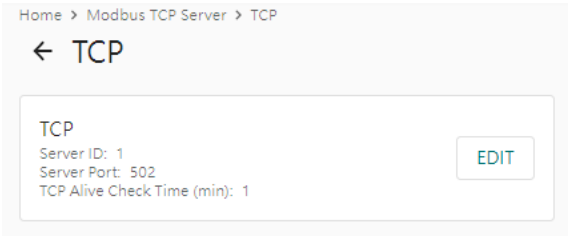
Whenever the commands are set, remember to click the APPLY button to save it.

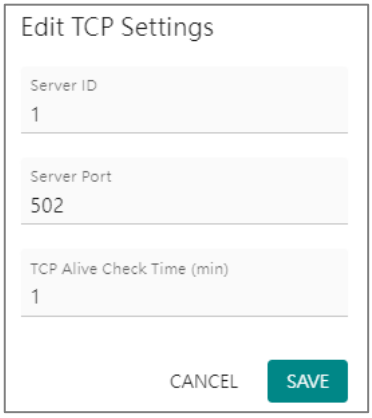
Protocol Settings—Modbus TCP Server Settings

You can configure the Modbus TCP server setting on this page. Click on the TCP button to edit the setting.



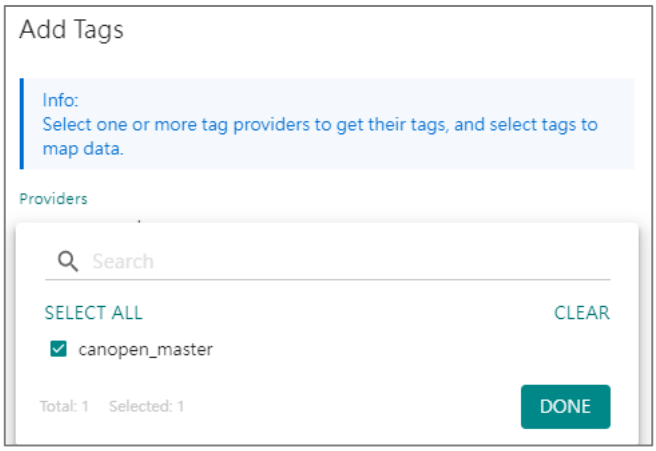
Click **EDIT** to adjust the Modbus TCP basic settings.

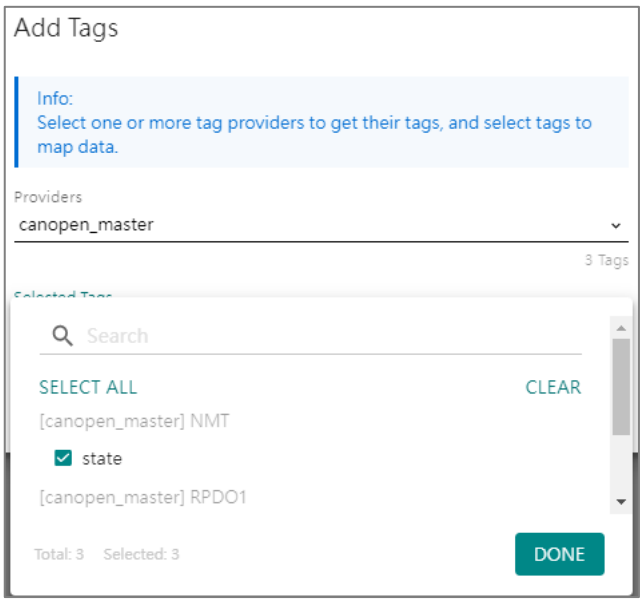




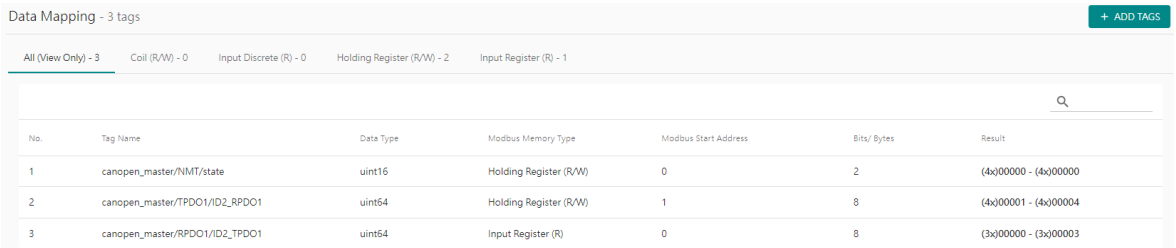
Parameter	Value	Default	Description
Server ID	1 to 255		The Modbus server ID that this slave module will accept.
Server Port	1 to 65535	502	The TCP port number.
TCP Alive Check Time (min)	0 to 99	1	The time to check TCP alive.

Add Tags for Modbus TCP. Notice that the tags must be created in CANopen master or J1939. Click **DONE** after selection. The selection sequence will also decide the sequence in the Modbus TCP register/coil address.



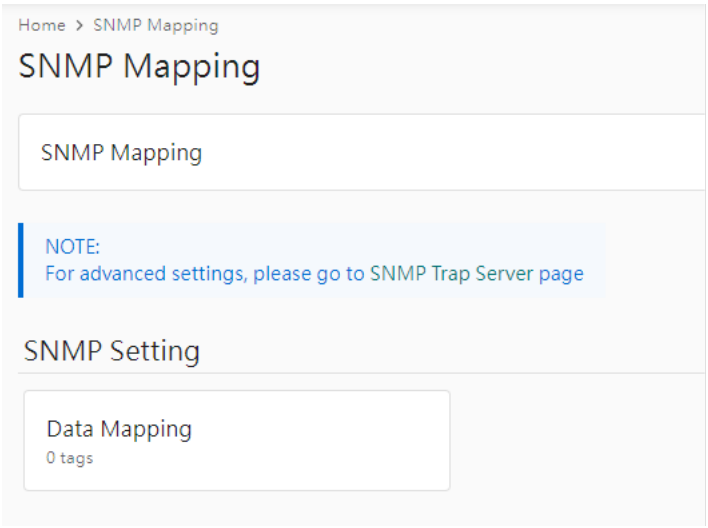


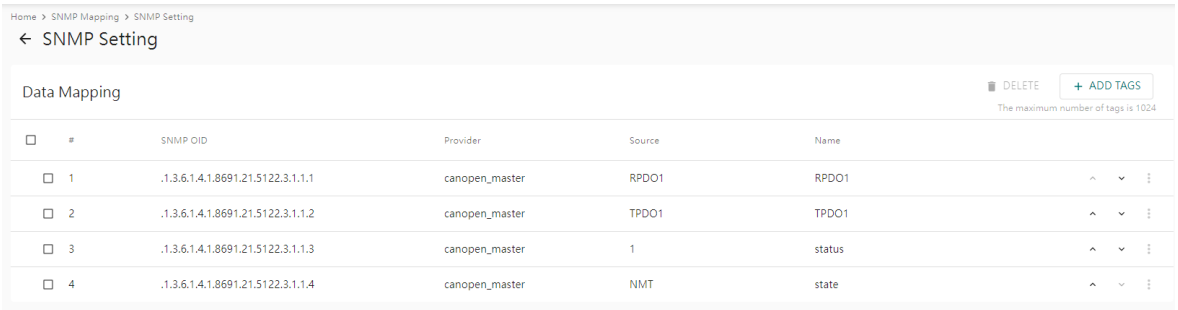
The selected tags will display in the data mapping column by default with register/coil address. You may adjust it manually.



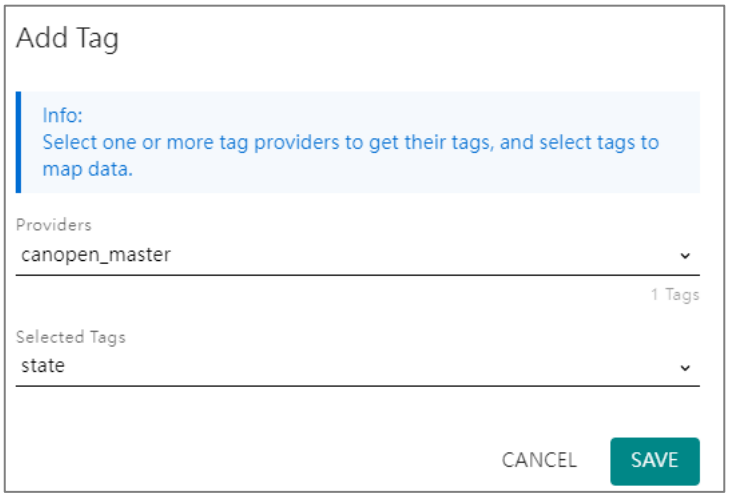
Protocol Settings—SNMP Mapping Settings

You can manage CAN to SNMP mapping data on this page; for detailed SNMP protocol settings, please go to the SNMP Trap Server page.





Click **ADD TAGS** to add tags in the CAN settings.



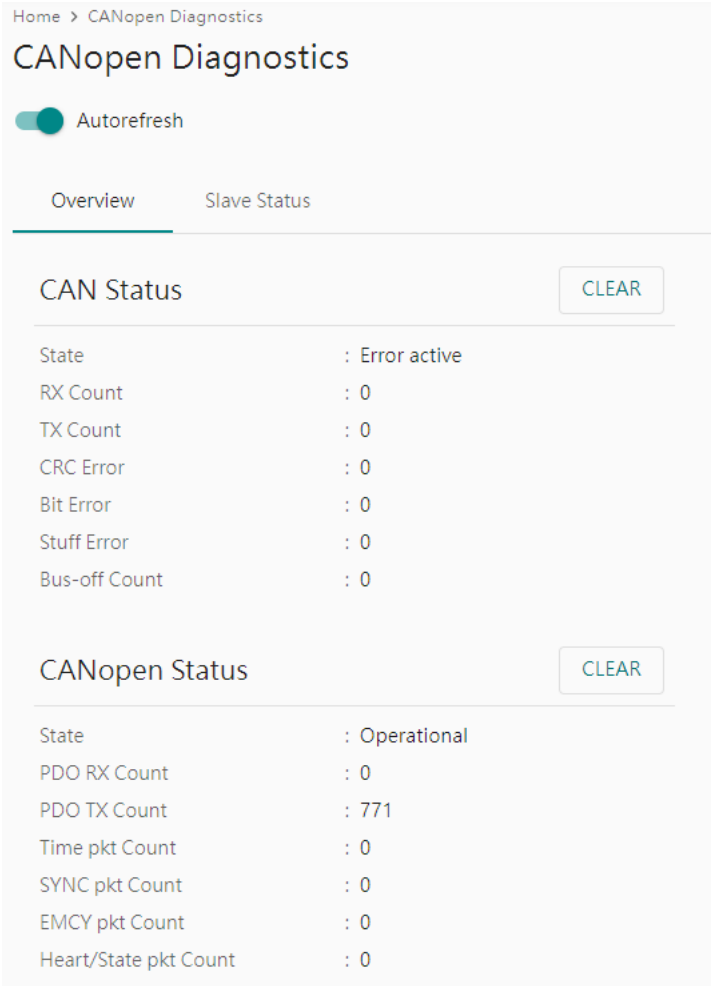
The OID is defined as below:

OID	String	OID (string type)	Description
1.3.6.1.4.1.8691	moxa	1.3.6.1.4.1.8691	
1.3.6.1.4.1.8691.21	mgate	{moxa}.21	MGate Series
1.3.6.1.4.1.8691.21.5121	mgate5121	{mgate}.5121	Model name
1.3.6.1.4.1.8691.21.5121.1	swMgmt	{mgate5121}.1	SNMP management Information
1.3.6.1.4.1.8691.21.5121.2	trap	{mgate5121}.2	SNMP trap
1.3.6.1.4.1.8691.21.5121.3	mapping	{mgate5121}.3	SNMP mapping
1.3.6.1.4.1.8691.21.5121.3.1	tags	{mapping}.1	Tag mapping
1.3.6.1.4.1.8691.21.5121.3.1.1	array of values	{tags}.1	Tag value
1.3.6.1.4.1.8691.21.5121.3.1.2	array of names	{tags}.2	Tag name
1.3.6.1.4.1.8691.21.5121.3.1.1.x	value of array[x]	{array of values}.x	Index of tag value
1.3.6.1.4.1.8691.21.5121.3.1.2.x	name of array[x]	{array of names}.x	Index of tag name

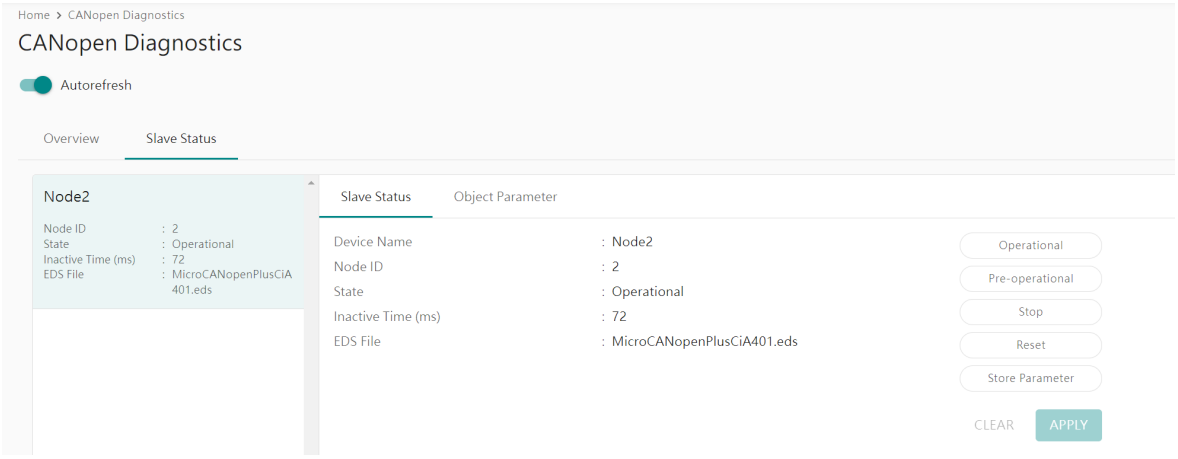
Diagnostics

Diagnostics—Protocol Diagnostics

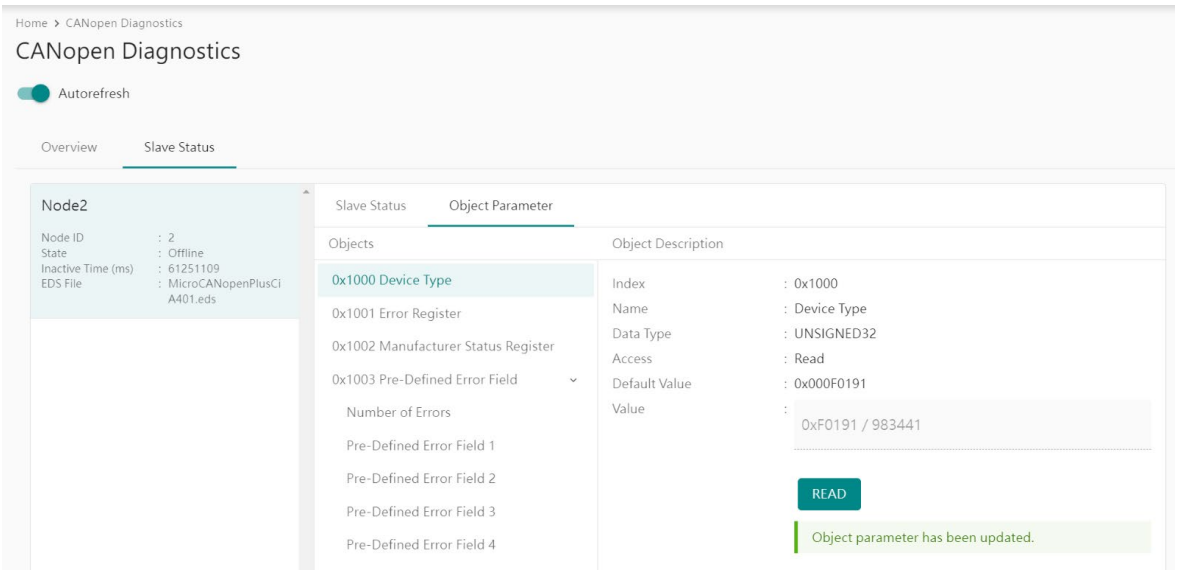
Diagnostics—Protocol Diagnostics—CANopen Diagnostics



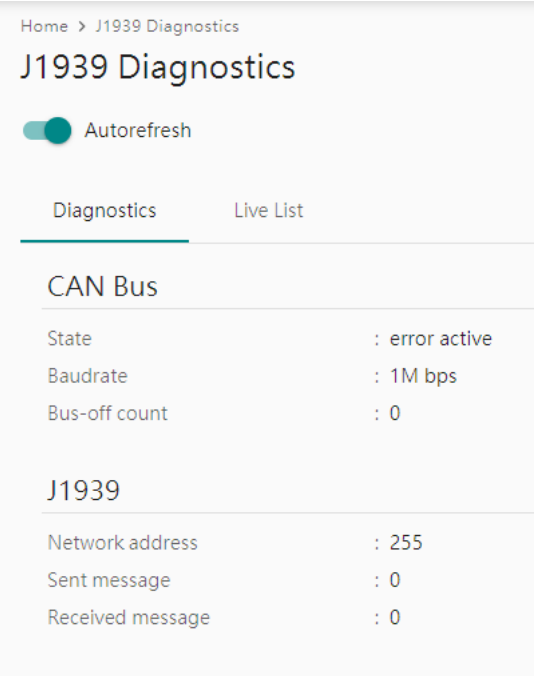
In the Slave Status tab, you can check the detailed information regarding slave status and change CANopen state machine at the right-hand side.



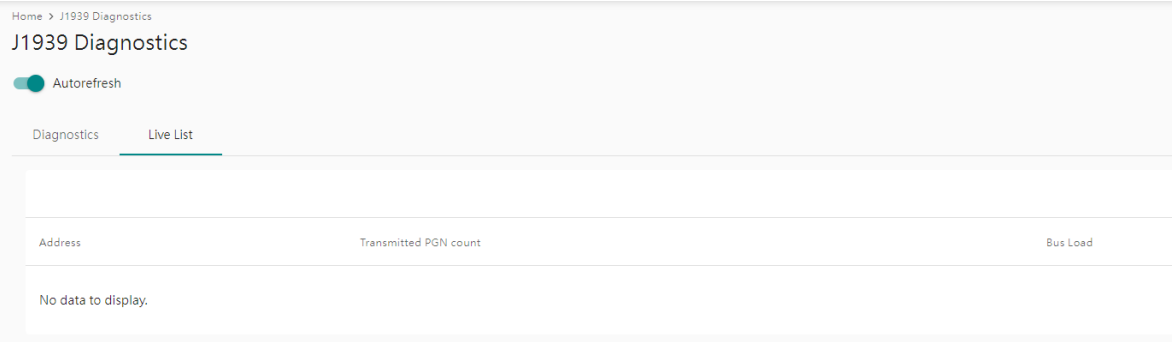
Furthermore, you can open the Object Parameter tab to check and change the slave device's CANopen object value.



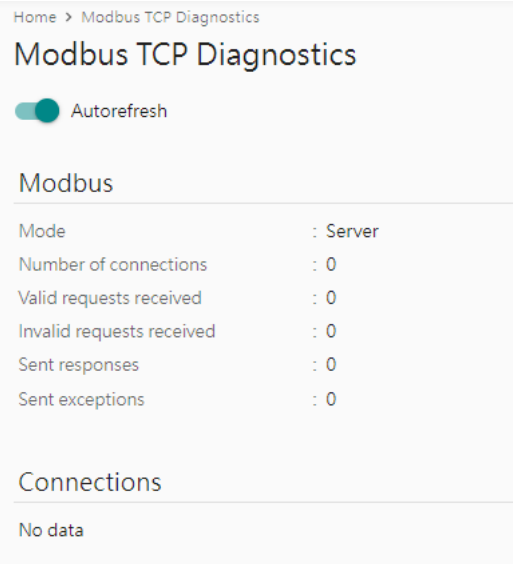
Diagnostics—Protocol Diagnostics—J1939 Diagnostics



The Live List function allows you to check how many live devices are on the same network.



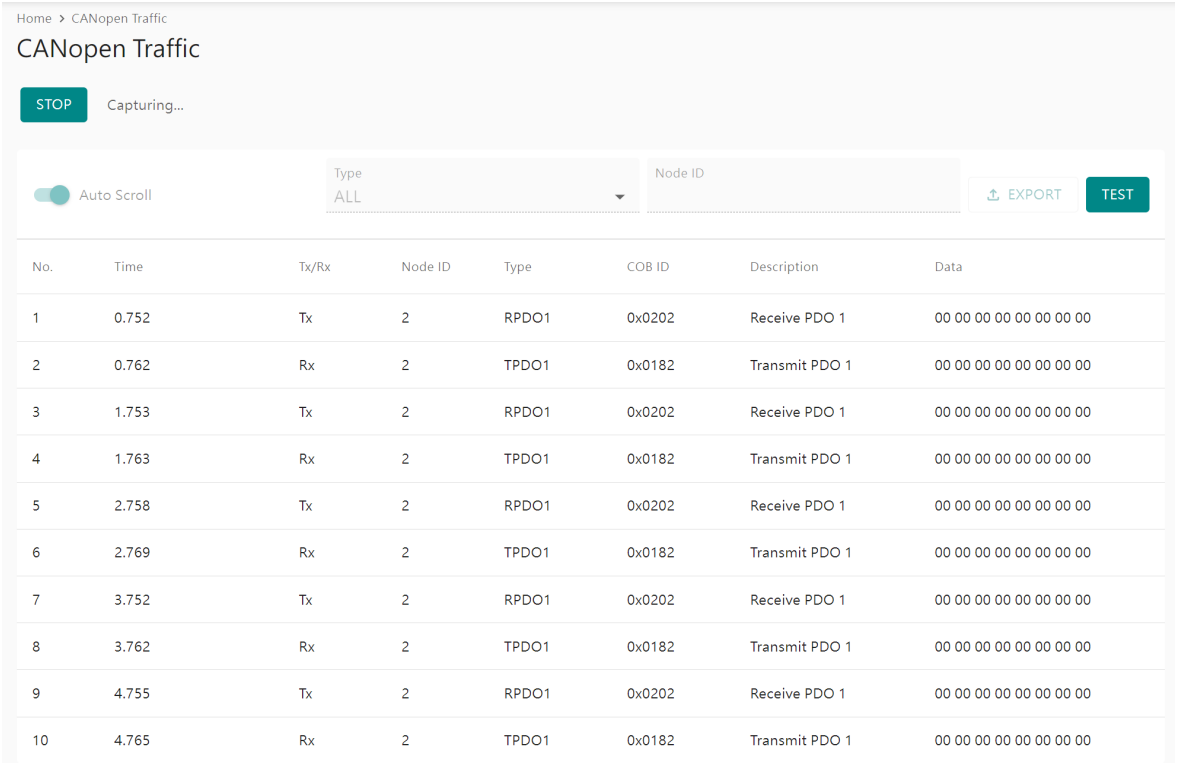
Diagnostics—Protocol Diagnostics—Modbus TCP Diagnostics



Diagnostics—Protocol Traffic

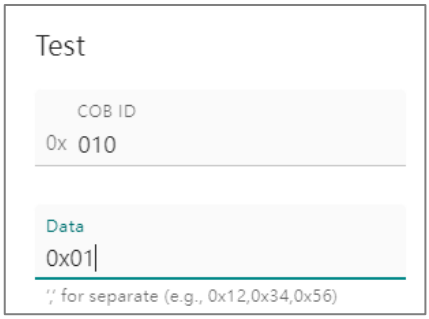
Diagnostics—Protocol Traffic—CANopen Traffic

Click **START** to start traffic log.



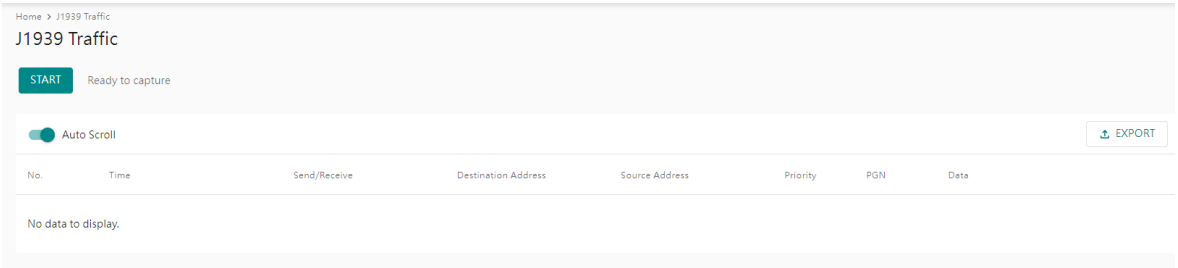
No.	Time	Tx/Rx	Node ID	Type	COB ID	Description	Data
1	0.752	Tx	2	RPDO1	0x0202	Receive PDO 1	00 00 00 00 00 00 00 00
2	0.762	Rx	2	TPDO1	0x0182	Transmit PDO 1	00 00 00 00 00 00 00 00
3	1.753	Tx	2	RPDO1	0x0202	Receive PDO 1	00 00 00 00 00 00 00 00
4	1.763	Rx	2	TPDO1	0x0182	Transmit PDO 1	00 00 00 00 00 00 00 00
5	2.758	Tx	2	RPDO1	0x0202	Receive PDO 1	00 00 00 00 00 00 00 00
6	2.769	Rx	2	TPDO1	0x0182	Transmit PDO 1	00 00 00 00 00 00 00 00
7	3.752	Tx	2	RPDO1	0x0202	Receive PDO 1	00 00 00 00 00 00 00 00
8	3.762	Rx	2	TPDO1	0x0182	Transmit PDO 1	00 00 00 00 00 00 00 00
9	4.755	Tx	2	RPDO1	0x0202	Receive PDO 1	00 00 00 00 00 00 00 00
10	4.765	Rx	2	TPDO1	0x0182	Transmit PDO 1	00 00 00 00 00 00 00 00

You can also read/write CAN data manually by clicking the **TEST** button and type in the CAN data frame.



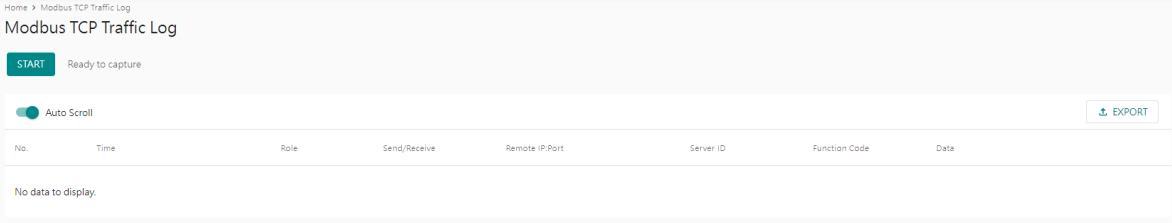
Diagnostics—Protocol Traffic—J1939 Traffic

Click **START** to start J1939 traffic log.



Diagnostics—Protocol Traffic—Modbus TCP Traffic

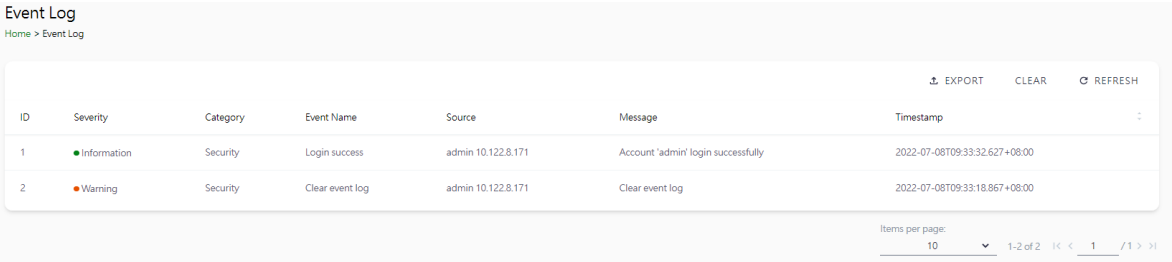
Click START to start Modbus TCP traffic log.



Diagnostics—Event Log

Diagnostics—Event Log—Log View

You can review and export all event information in the event log.

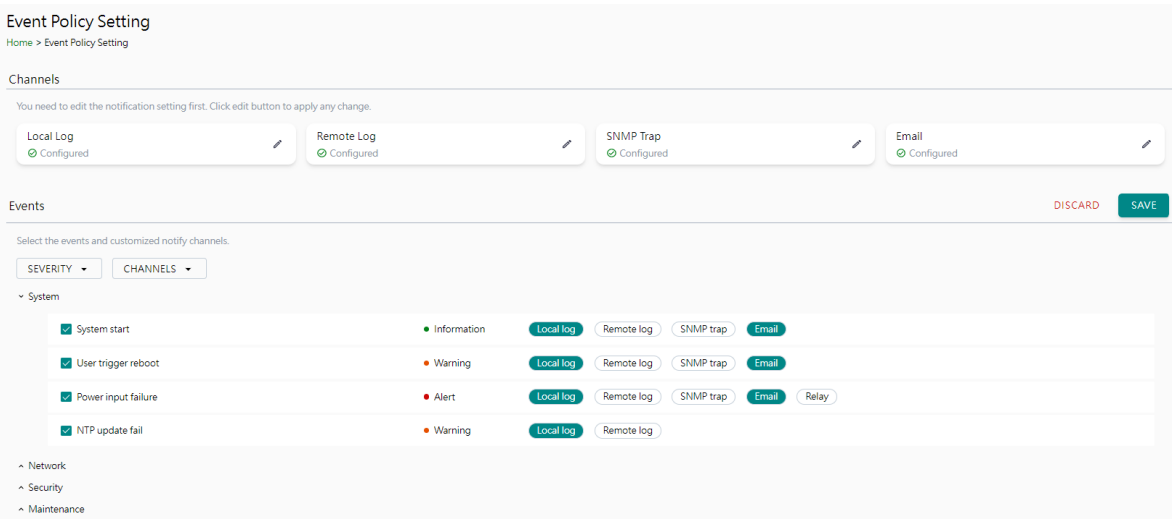


Diagnostics—Event Log—Policy Settings

The event policy settings enable the MGate to record important events, which can be recorded in the Remote Log to Syslog server and Local Log, which will be stored with up to 10,000 events in the MGate.

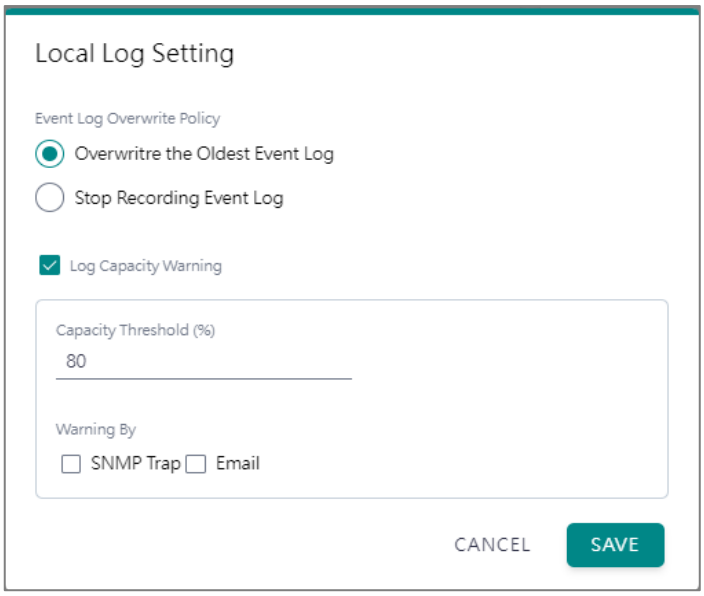
The MGate can also send email alerts, SNMP Trap messages, or open/close the circuit of the relay output when a selected event was triggered.

You can filter events for easy reading or expand by clicking the category, such as System. Tick or untick the events if you want to log it and select which channels you want to use by clicking the channel name. After changing the settings, please remember to SAVE it.



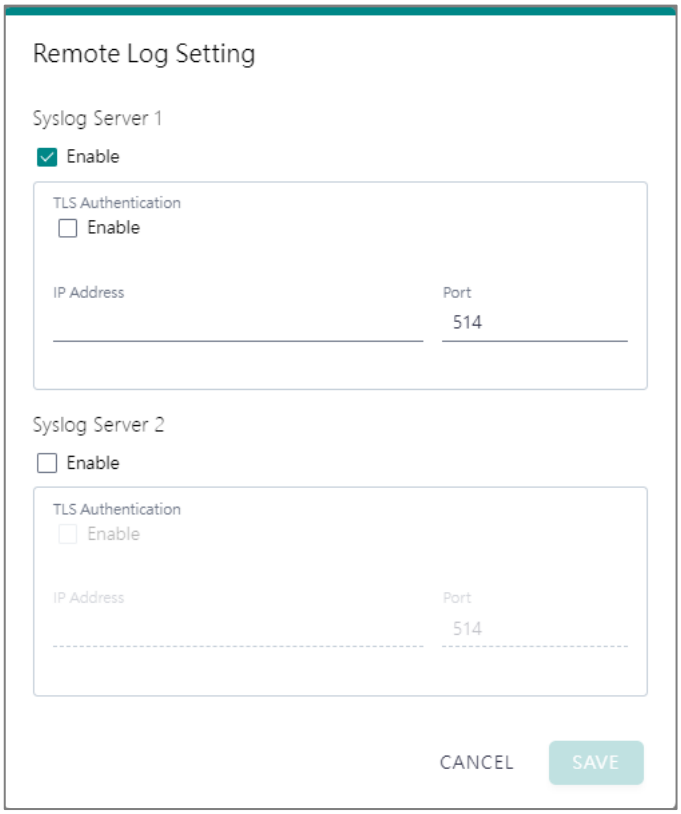
Event Group	Description
System	Start system, User trigger reboot, Power input failure, NTP update failure
Network	IP conflict, DHCP get IP/renew, IP changed, Ethernet link down
Security	Clear event log, Login success, Login failure, Account/group changed, Password reached lifetime, SSL certificate import, Syslog certificate import
Maintenance	Firmware upgrade success, Firmware upgrade failure, Configuration import success, Configuration import failure, Configuration export, Configuration changed, Load factory default
Modbus client	Server connected, Server disconnected, Command recovered, Command fail
Modbus server	Client connected; Client disconnected; Exception function
EtherNet/IP	Adapter connected; Adapter disconnected
PROFINET	I/O Device is connected, I/O Device is disconnected, I/O Controller is running, I/O Controller has stopped
CANopen	Device status changed; CAN bus-off
J1939	CAN bus-off

Local Log Settings



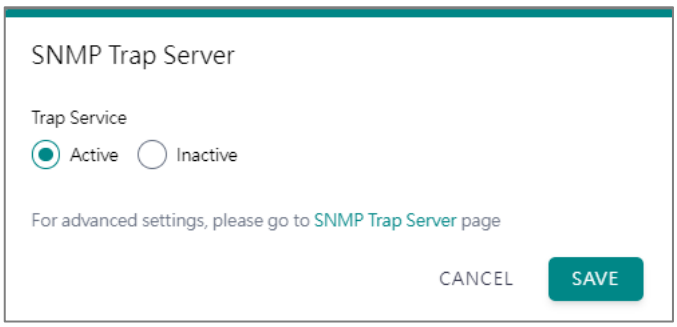
Local Log Settings	Description
Event Log Overwrite Policy	Overwrites the oldest event log Stops recording event log
Log Capacity Warning	When the log amount exceeds the warning
Warning By	SNMP Trap Email

Remote Log Settings

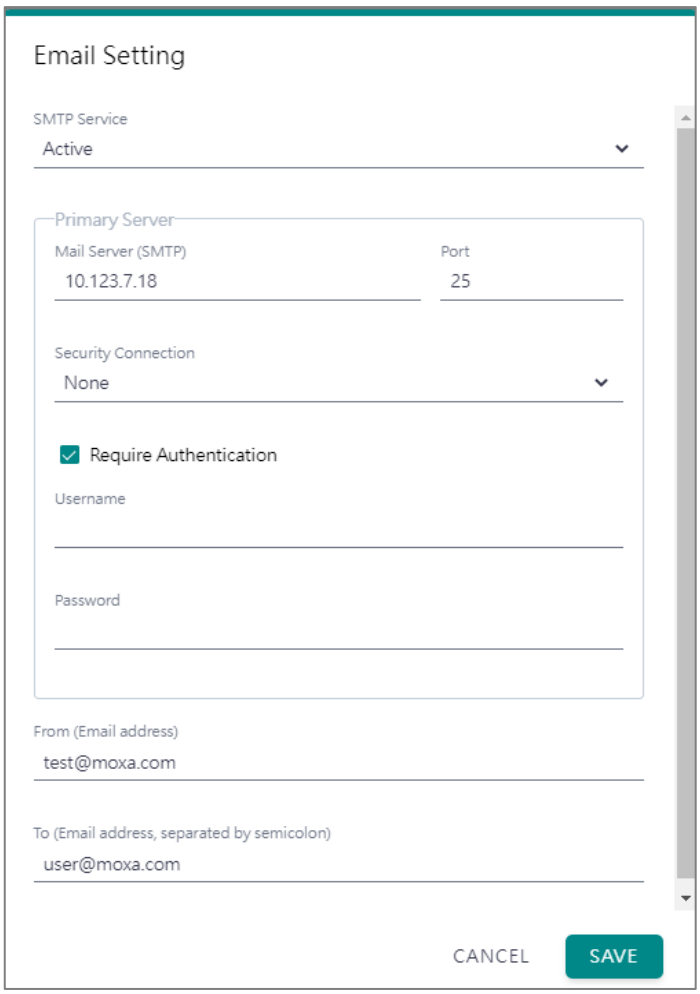


Remote Log Settings	Description
Syslog Server IP	IP address of a server that will record the log data
Syslog Server port	514
TLS Authentication	Enable TLS authentication. Notice TLS files must be uploaded for a successful connection.

SNMP Trap Settings



Email Settings

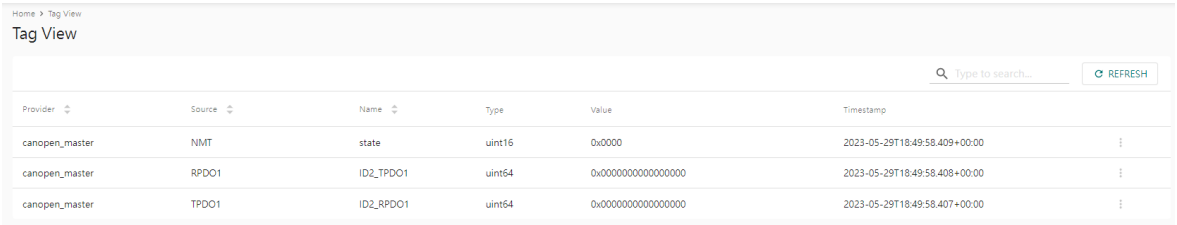


Parameters	Description
Mail Server (SMTP)	The mail server's domain name or IP address.
Port	The mail server's IP port.
Security Connection	TLS STARTTLS STARTTLS-None None
Username	This field is for your mail server's username, if required.
Password	This field is for your mail server's password, if required.
From (Email address)	Email address from which automatic email warnings will be sent.

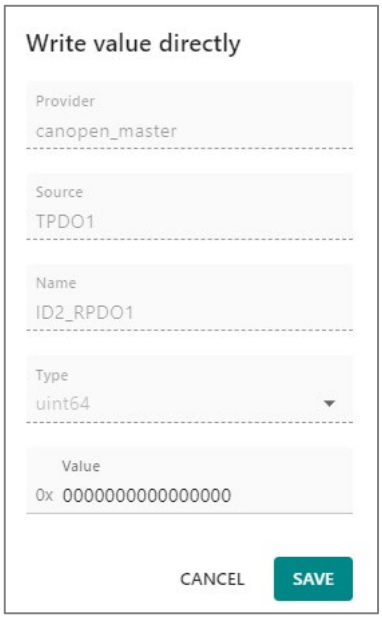
Parameters	Description
To (Email address, separated by semicolon)	Email addresses to which automatic email warnings will be sent.

Diagnostics—Tag View

This page displays the tag live value generated by field devices and updates the values periodically. It is an easy and useful tool if you want to check whether the MGate receives the correct data from field devices. The gateway timestamp shows the time data was updated to the tag.

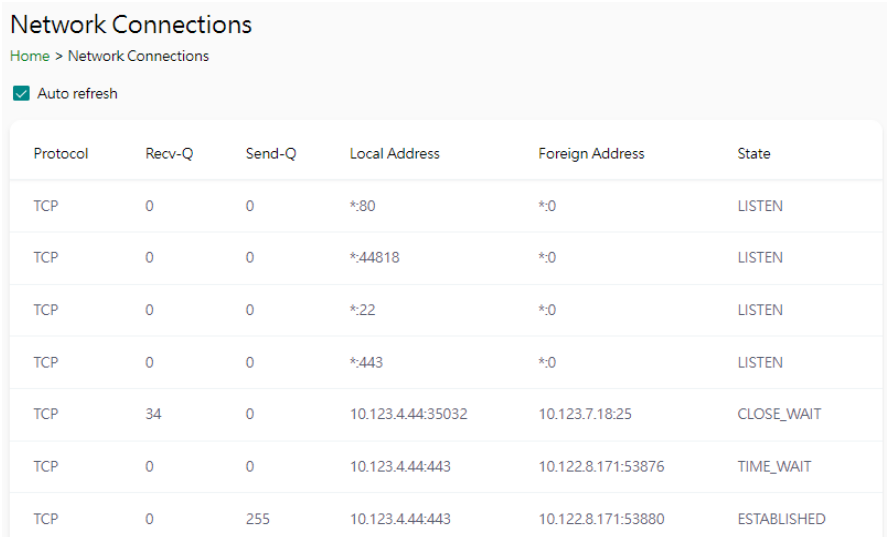


You can write a value to the CAN device via Write value directly to test the communication with CAN device.



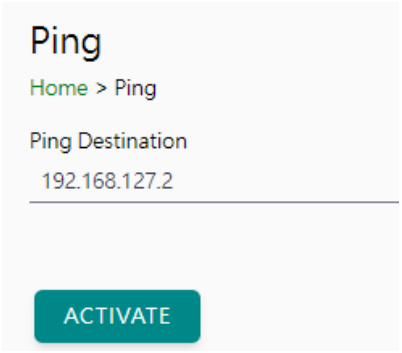
Diagnostics—Network Connections

You can see network-related information, including protocol, address, and state.



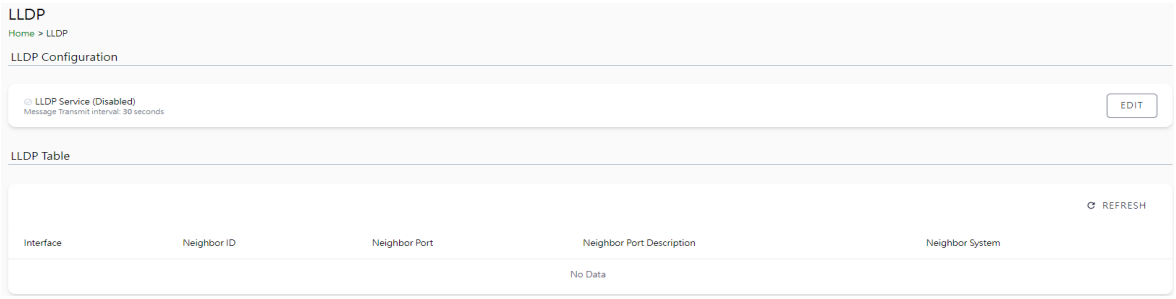
Diagnostics—Ping

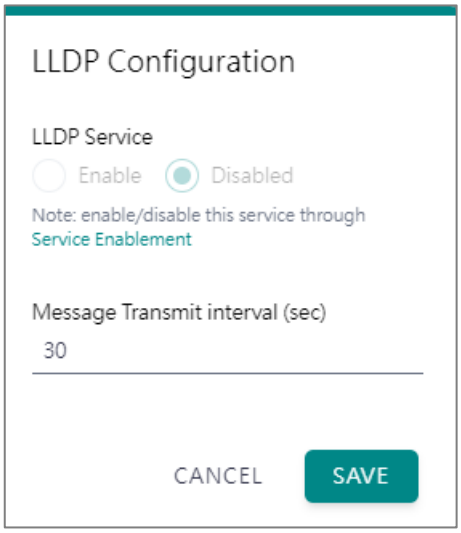
This network testing function is available only in the web console. The MGate gateway will send an ICMP packet through the network to a specified host, and the result can be viewed on the web console immediately.



Diagnostics—LLDP

You can see LLDP related information, including Port, Neighbor ID, Neighbor Port, Neigh Port Description, and Neighbor System. Also, you can adjust the transmit interval for LLDP by clicking the **EDIT** button.

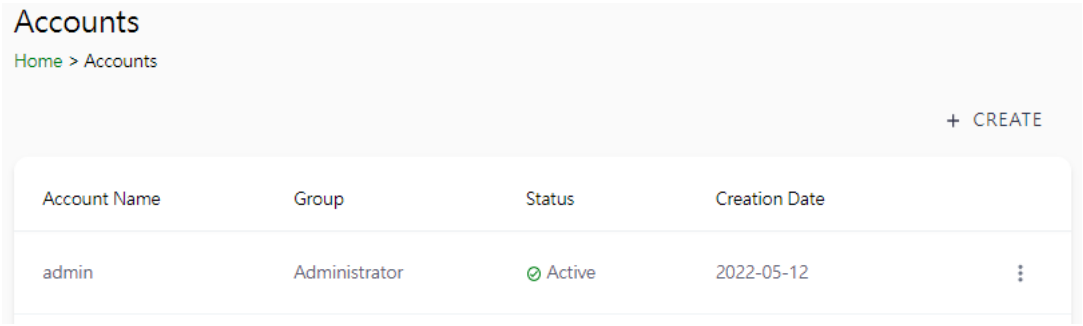




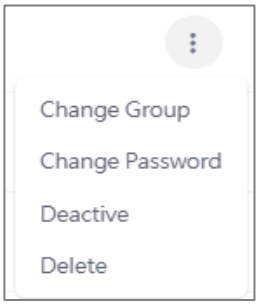
Security

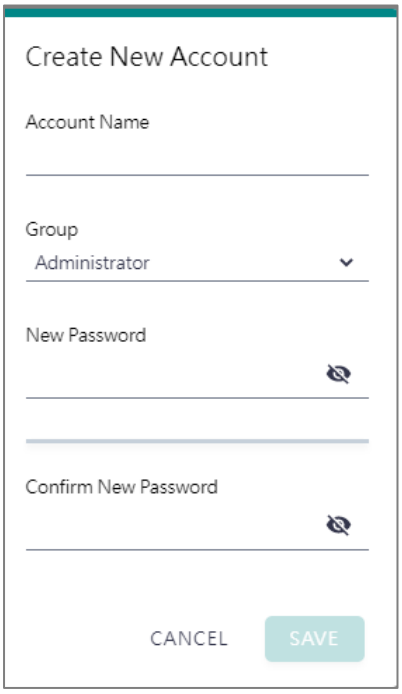
Security—Account Management

Security—Account Management—Accounts



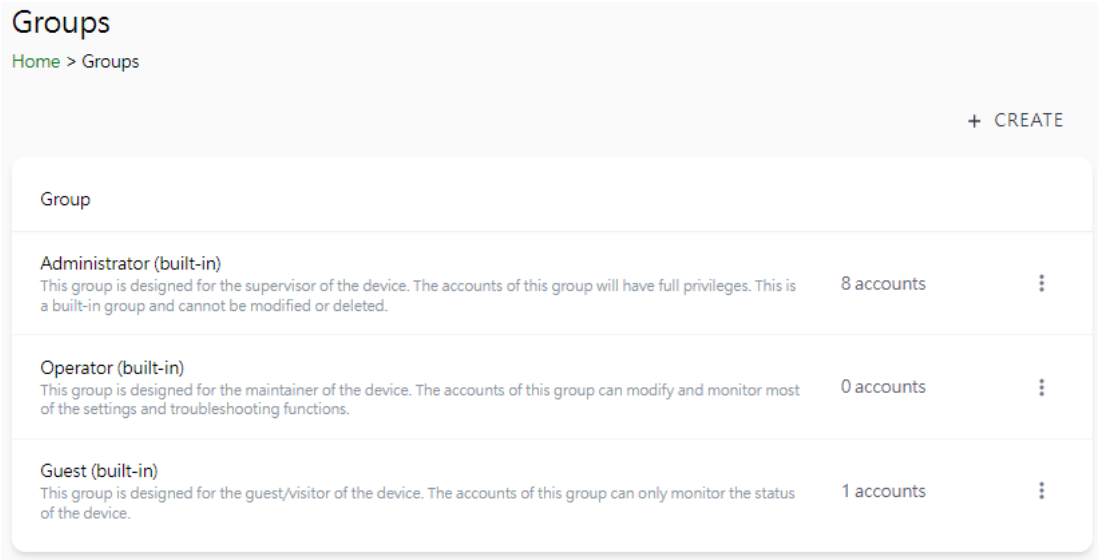
Only Administrator group can create or edit accounts for user management. Click **CREATE** to add new accounts. Click the dot icon to edit the account.



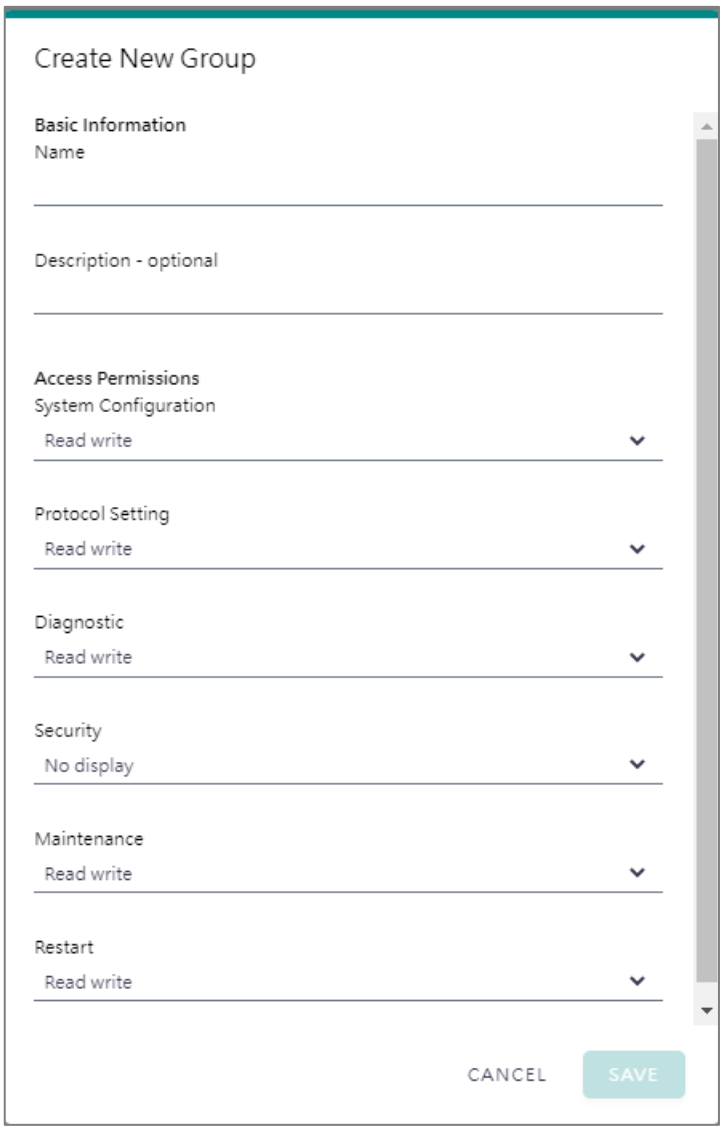


Parameters	Value	Description
Group	Administrator, Operator, Guest	Users can change the password for different accounts. The MGate provides three build-in account groups, administrator, operator and guest. Administrator account can access all settings. Operator accounts can access most settings, except security categories. Guest account can only view the overview page. You can create your own group for account management.

Security—Account Management—Groups

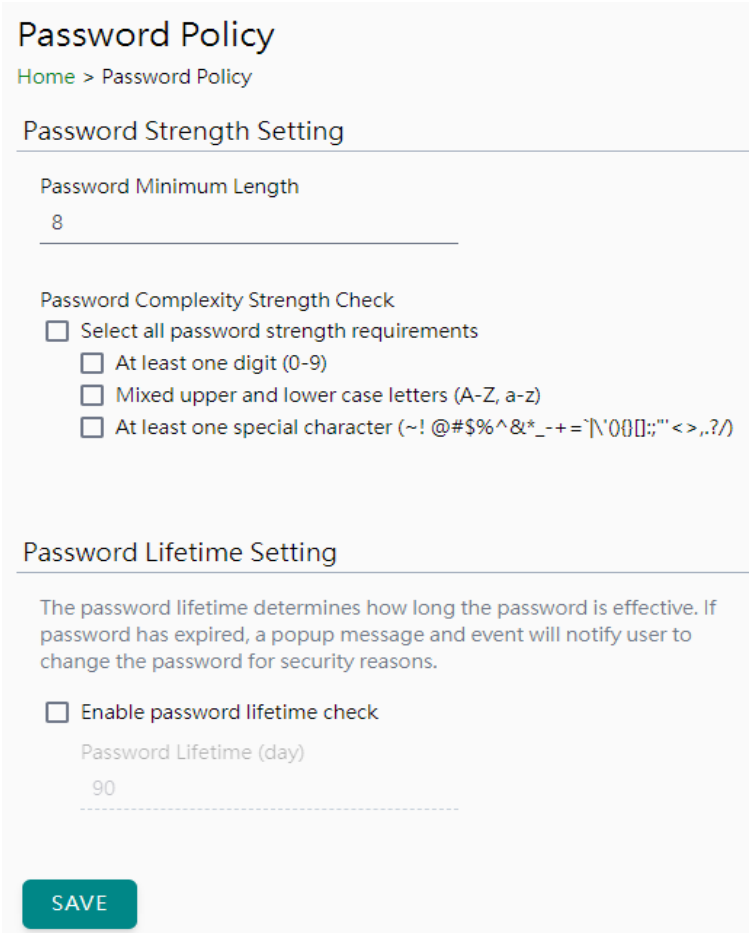


Three MGate build-in types of groups are shown; you can also create your own group by clicking **CREATE.**



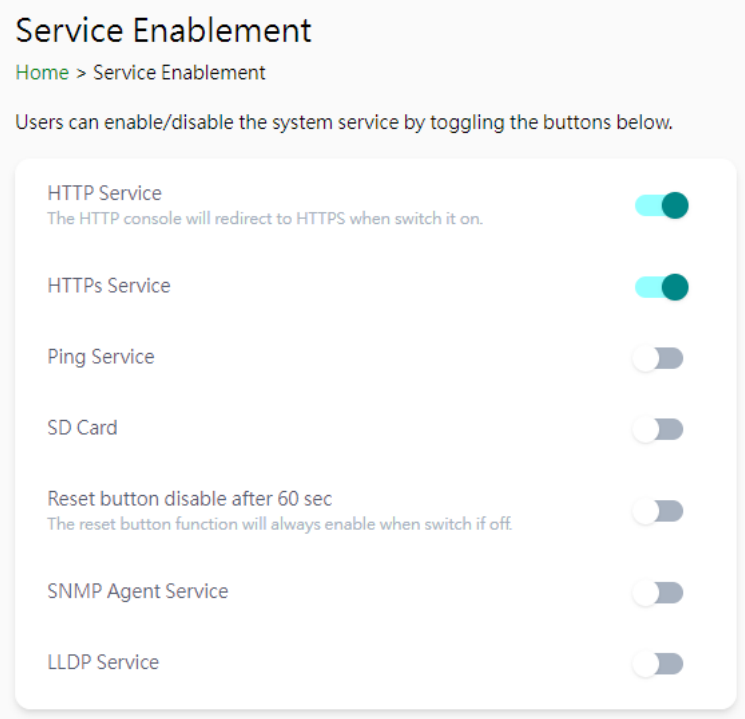
Parameters	Value	Description
Basic Information		Includes Name and Description for the new Group.
Access Permissions	No display Read only Read write	Corresponding to the configuration menu on the left-hand side of the web console, you can select different permissions for a new group. Displays will not show the page on the right-hand side menu.

Security—Account Management—Password Policy



Parameter	Value	Description
Password Minimum Length	8 to 128	The minimum password length
Password Complexity Strength Check		Select how the MGate checks the password's strength
Password lifetime Setting	90 to 180 days	Set the password's lifetime period.

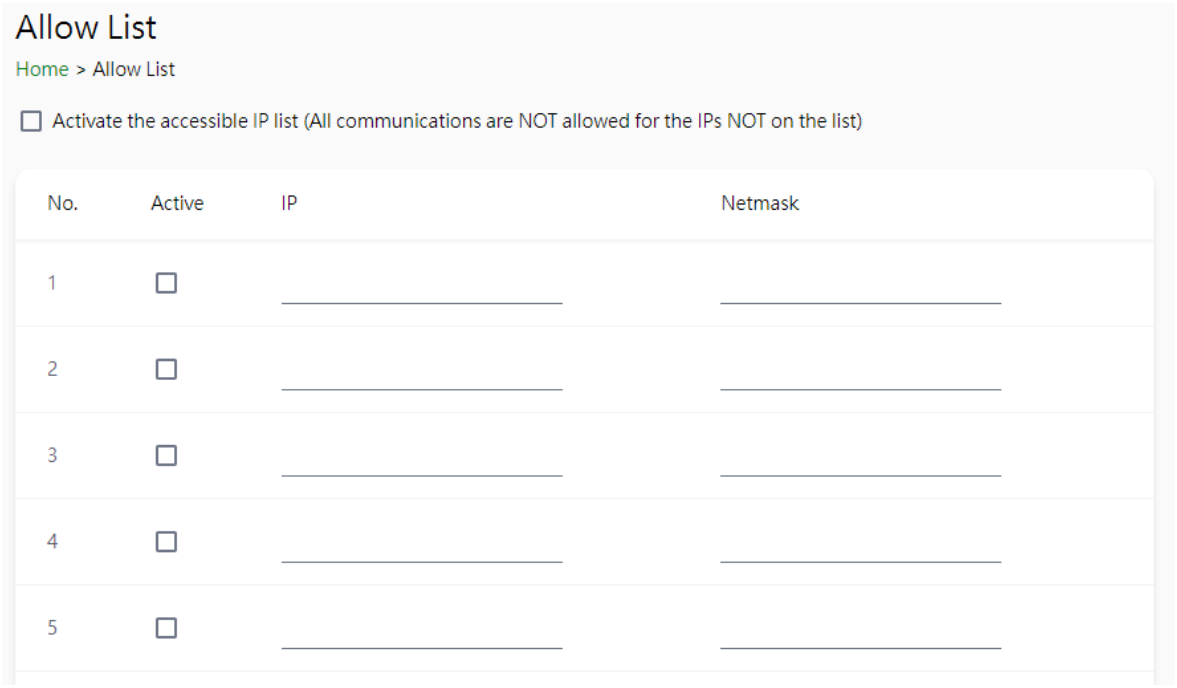
Security—Service



Parameter	Value	Description
HTTP Service	Enable/Disable	To enhance security, all HTTP requests will redirect to HTTPS when the HTTP service is enabled. You can also disable the HTTP service.
HTTPS Service	Enable/Disable	Disabling this service will disable the web console and search utility connections, thus cutting off access to the configuration settings. To re-enable the HTTPS communication, reset to the factory default settings via the hardware Reset button.
Ping Service	Enable/Disable	Disabling this service will block ping requests from other devices.
SD Card	Enable/Disable	Disabling this service will deactivate the SD card function for backup and restore configuration files.
SNMP Agent Service	Enable/Disable	Enable or disable SNMP agent function.
LLDP Service	Enable/Disable	Enable or disable LLDP function.
Reset button disable after 60 sec	Always enable and disable after 60 sec.	The MGate provides a Reset button to load factory default settings. For enhanced security, users can disable this function. In the disabled mode, the MGate will still enable the Reset button for 60 seconds after bootup, just in case you really need to reset the device.

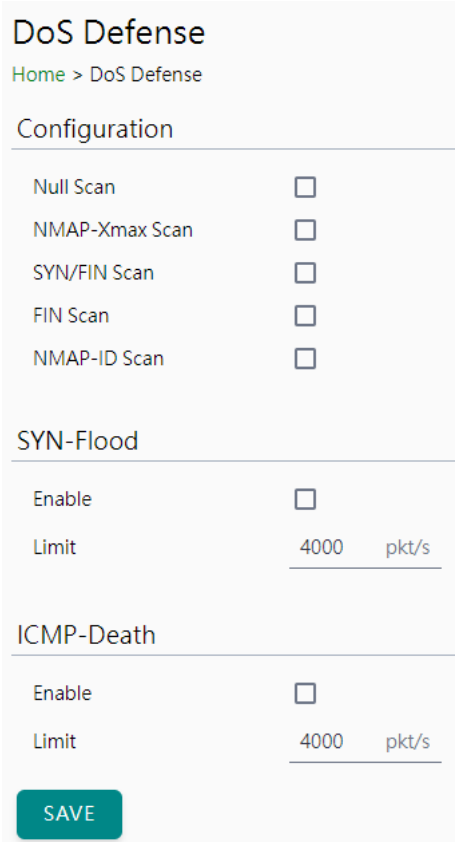
Security—Allowlist

These settings are used to restrict access to the MGate by the IP address. Only IP addresses on the list will be allowed to access the device. Notice the restriction includes configuration and protocol conversion.



Security—DoS Defense

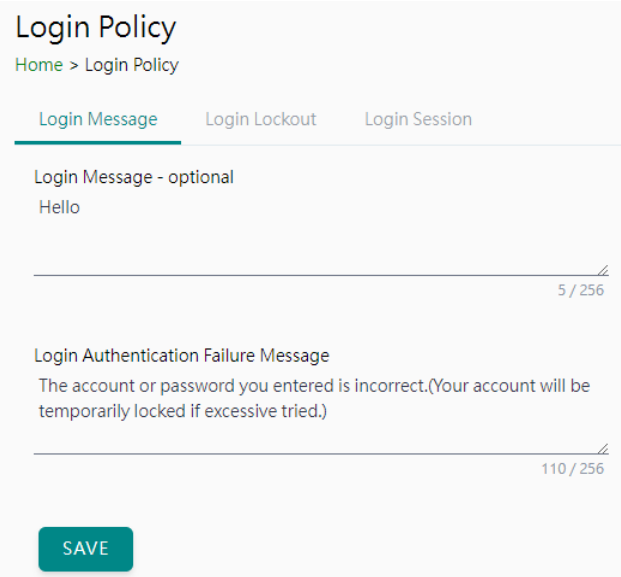
Users can select from several options to enable DoS Defense to fend off cybersecurity attacks. A denial-of-service (DoS) attack is an attempt to make a machine or a network resource unavailable. Users can select from the following options to counter DoS attacks.



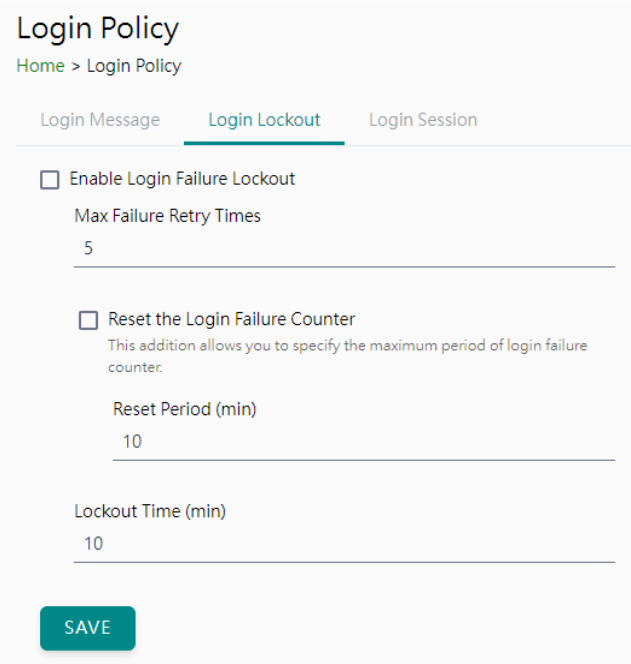
Security—Login Policy

Login Message

You can input a message for Login or for Login authentication failure messages.

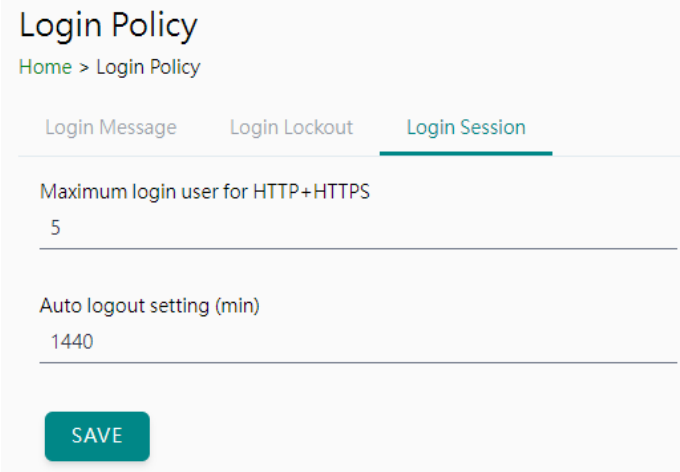


Login Lockout



Parameter	Value	Description
Max Failure Retry Times	1 to 10 (default 5)	You can specify the maximum number of failures reties, if exceed the retry times, MGate will lock out for that account login
Reset Period (min)	1 to 1440 (default 10)	You can specify the reset period time when enabling the "reset the login failure counter" function
Lockout Time(min)	1 to 60 (default 10)	When the number of login failures exceeds the threshold, the MGate will lock out for a period.

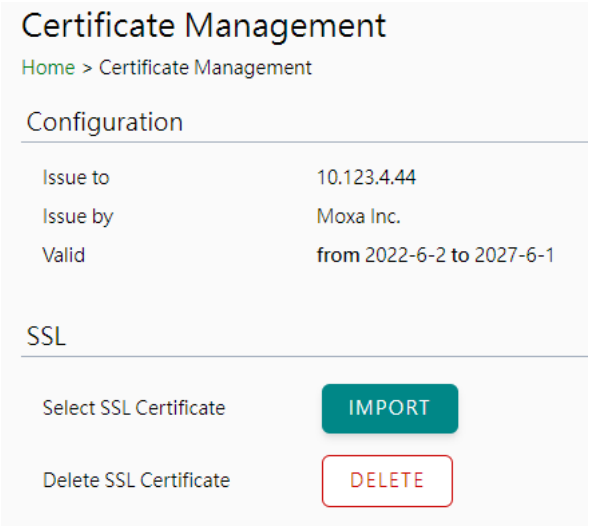
Login Session



Parameter	Value	Description
Maximum login users for HTTP+HTTPS	1 to 10 (default 5)	The number of users that can access the MGate at the same time.
Auto logout setting (min)	1 to 1440 (default 1440)	Sets the auto logout time period.

Security—Certificate Management

Use this function to load the Ethernet SSL certificate. You can import or delete SSL certificate/key files. This function is only available for the web console.



Maintenance

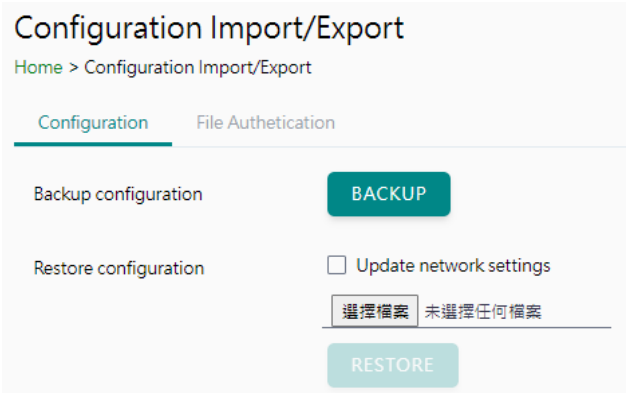
Maintenance—Configuration Import/Export

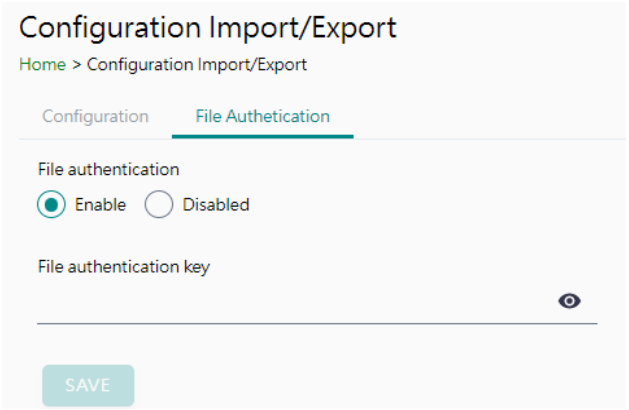
There are three main reasons for using the Import and Export functions:

- Applying the same configuration to multiple units. The Import/Export configuration function is a convenient way to apply the same settings to units in different sites. You can export the configuration as a file and then import the configuration file onto other units.
- Backing up configurations for system recovery. The export function allows you to export configuration files that can be imported onto other gateways to restore malfunctioning systems within minutes.

Troubleshooting. Exported configuration files help administrators to identify system problems that provide useful information for Moxa's Technical Service Team when maintenance visits are requested.

For cybersecurity reason, you can export configuration file with an authentication key, length from 8 to 16 characters. If the key to the imported configuration file differs from the key to the exported file, the import process will fail.





Maintenance—Firmware Upgrade

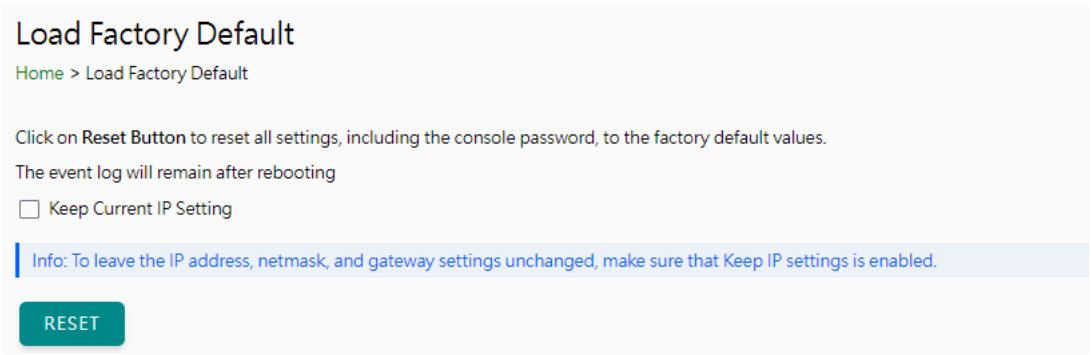
Firmware updates for the MGate are available on the Moxa website. After you have downloaded the new firmware onto your PC, you can use the web console to write it onto your MGate. Select the desired unit from the list in the web console and click **Submit** to begin the process.

ATTENTION

DO NOT turn off the MGate power before the firmware upgrade process is completed. The MGate will erase the old firmware to make room for the new firmware to flash memory. If you power off the MGate and end the progress, the flash memory will contain corrupted firmware, and the MGate will fail to boot. If this happens, contact Moxa RMA services.

Maintenance—Load Factory Default

To clear all the settings on the unit, use the Load Factory Default to reset the unit to its initial factory default values.



ATTENTION

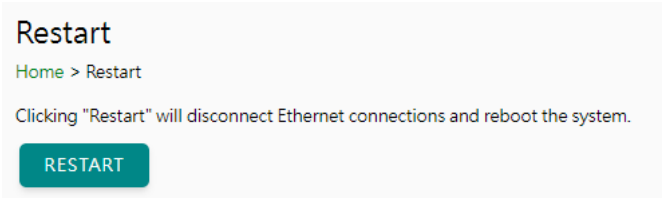
Load Default will completely reset the configuration of the unit, and all the parameters you have saved will be discarded. Do not use this function unless you are sure you want to completely reset your unit.

Restart

You can reboot the MGate by clicking the RESTART button.

ATTENTION

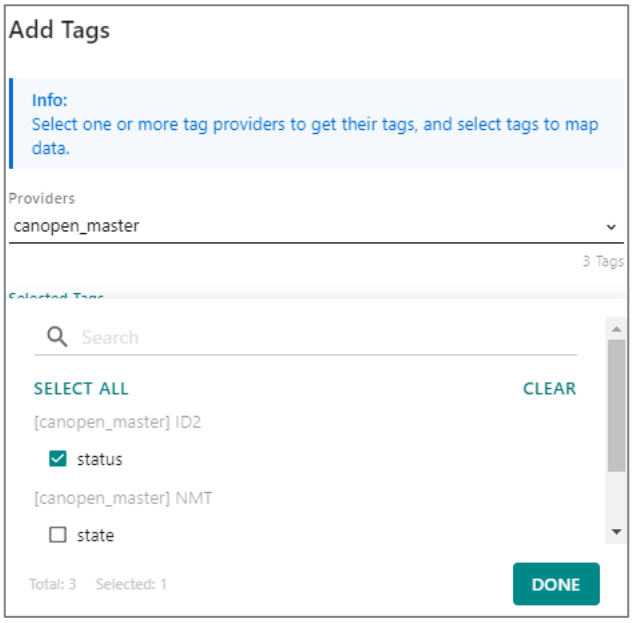
Unsaved configuration files will be discarded during a reboot.



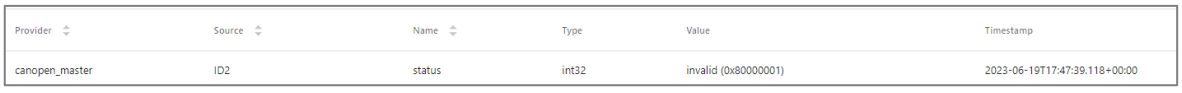
Status Monitoring

The Status Monitoring function provides status information of field devices when the MGate is being used as a CAN client. If a CAN device fails or a cable comes loose, the gateway will not be able to receive up-to-date data from the CAN device. The out-of-date data will be stored in the gateway's memory and will be retrieved by the client (e.g., PLC), which is not aware that the slave device is not providing up-to-date data. To handle this situation, the MGate provides a warning mechanism to report the list of slave devices that are still "alive" through the Status Monitoring function.

The MGate will create a status tag when a CAN device is created. This shows if the CAN device connection is valid or invalid.



The highest significant bit shows the status. 1 is invalid, 0 is valid.



4. Network Management Tool (MXstudio)

Moxa's MXstudio industrial network management suite includes tools such as MXconfig, MXview and N-Snap. MXconfig is for industrial network configuration; MXview is for industrial management software; and N-Snap is for industrial network snapshot. The MXstudio suite in the MGate includes MXconfig and MXview, which are used for the mass configuration of network devices and monitoring network topology, respectively. The following functions are supported:

Tool	Function Support
MXconfig	1. System name and login password modification 2. Network settings 3. Configuration import/export 4. Firmware upgrade
MXview	1. Configuration import/export 2. LLDP for topology analysis 3. Security View**

**Security View can check the security level of devices under the IEC62443-4-2 standard.

A. SNMP Agents with MIB II

The MGate has built-in Simple Network Management Protocol (SNMP) agent software that supports SNMP Trap, and RFC 1213 MIB-II.

RFC1213 MIB-II Supported SNMP Variables

System MIB	Interfaces MIB	IP MIB	ICMP MIB
sysDescr	ifNumber	ipForwarding	icmpInMsgs
sysObjectID	ifIndex	ipDefaultTTL	icmpInErrors
sysUpTime	ifDescr	ipInReceives	icmpInDestUnreachs
sysContact	ifType	ipInHdrErrors	icmpInTimeExcds
sysName	ifMtu	ipInAddrErrors	icmpInParmProbs
sysLocation	ifSpeed	ipForwDatagrams	icmpInSrcQuenchs
sysServices	ifPhysAddress	ipInUnknownProtos	icmpInRedirects
	ifAdminStatus	ipInDiscards	icmpInEchos
	ifOperStatus	ipInDelivers	icmpInEchoReps
	ifLastChange	ipOutRequests	icmpInTimestamps
	ifInOctets	ipOutDiscards	icmpTimestampReps
	ifInUcastPkts	ipOutNoRoutes	icmpInAddrMasks
	ifInNUcastPkts	ipReasmTimeout	icmpInAddrMaskReps
	ifInDiscards	ipReasmReqds	icmpOutMsgs
	ifInErrors	ipReasmOKs	icmpOutErrors
	ifInUnknownProtos	ipReasmFails	icmpOutDestUnreachs
	ifOutOctets	ipFragOKs	icmpOutTimeExcds
	ifOutUcastPkts	ipFragFails	icmpOutParmProbs
	ifOutNUcastPkts	ipFragCreates	icmpOutSrcQuenchs
	ifOutDiscards	ipAdEntAddr	icmpOutRedirects
	ifOutErrors	ipAdEntIfIndex	icmpOutEchos
	ifOutQLen	ipAdEntNetMask	icmpOutEchoReps
	ifSpecific	ipAdEntBcastAddr	icmpOutTimestamps
		ipAdEntReasmMaxSize	icmpOutTimestampReps
		ipRouteDest	icmpOutAddrMasks
		ipRouteIfIndex	icmpOutAddrMaskReps
		ipRouteMetric1	
		ipRouteMetric2	
		ipRouteMetric3	
		ipRouteMetric4	
		ipRouteNextHop	
		ipRouteType	
		ipRouteProto	
		ipRouteAge	
		ipRouteMask	
		ipRouteMetric5	
		ipRouteInfo	
		ipNetToMediaIfIndex	
		ipNetToMediaPhysAddress	
		ipNetToMediaNetAddress	
		ipNetToMediaType	
		ipRoutingDiscards	

Address Translation MIB	TCP MIB	UDP MIB	SNMP MIB
atIfIndex	tcpRtoAlgorithm	udpInDatagrams	snmpInPkts
atPhysAddress	tcpRtoMin	udpNoPorts	snmpOutPkts
atNetAddress	tcpRtoMax	udpInErrors	snmpInBadVersions
	tcpMaxConn	udpOutDatagrams	snmpInBadCommunityNames
	tcpActiveOpens	udpLocalAddress	snmpInBadCommunityUses
	tcpPassiveOpens	udpLocalPort	snmpInASNParseErrs
	tcpAttemptFails		snmpInTooBigs
	tcpEstabResets		snmpInNoSuchNames
	tcpCurrEstab		snmpInBadValues
	tcpInSegs		snmpInReadOnlys
	tcpOutSegs		snmpInGenErrs
	tcpRetransSegs		snmpInTotalReqVars
	tcpConnState		snmpInTotalSetVars
	tcpConnLocalAddress		snmpInGetRequests
	tcpConnLocalPort		snmpInGetNexts
	tcpConnRemAddress		snmpInSetRequests
	tcpConnRemPort		snmpInGetResponses
	tcpInErrs		snmpInTraps
	tcpOutRsts		snmpOutTooBigs
			snmpOutNoSuchNames
			snmpOutBadValues
			snmpOutGenErrs
			snmpOutGetRequests
			snmpOutGetNexts
			snmpOutSetRequests
			snmpOutGetResponses
			snmpOutTraps
			snmpEnableAuthenTraps
			snmpSilentDrops
			snmpProxyDrops