MGate 5122 Series User Manual

Version 1.1, January 2025

www.moxa.com/products

MGate 5122 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

The MGate 5122 is an industrial Ethernet gateway for converting CANopen, J1939 or CAN proprietary (CAN 2.0A/B) to EtherNet/IP and SNMP network communications. To integrate existing CAN-based devices into an EtherNet/IP or SNMP network, use the MGate 5122 as a CAN master to collect data and exchange data with the EtherNet/IP 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.

NOTE

CAN proprietary (CAN 2.0 A/B) is supported in firmware version V2.0 and later.

2. Getting Started

Connecting the Power

Power the unit by connecting a power source to the terminal block.

1. Connect the 12 to 48 VDC power line or DIN-rail power supply to the MGate’s power terminal block.
2. Tighten the screws on both sides of the terminal block.
3. 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. Always turn off the power before connecting or disconnecting the serial connection. 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.

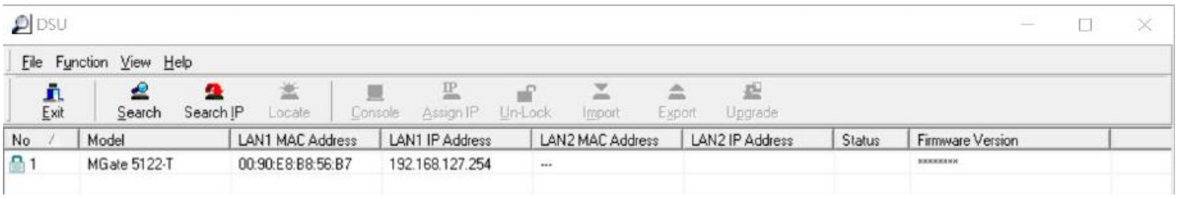
The following instructions explain how to install the DSU, a utility to search for MGate units on a network.

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.



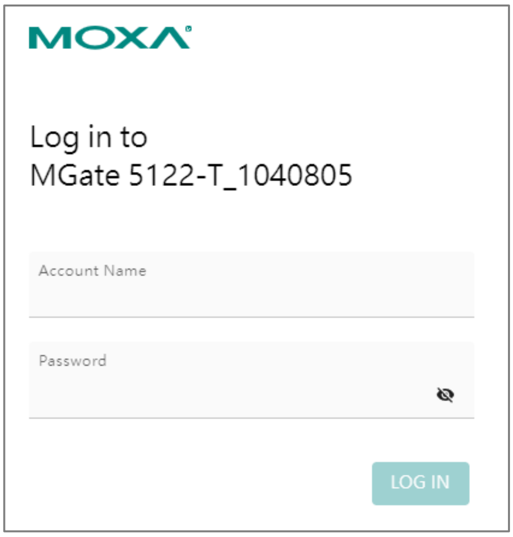
No	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status	Firmware Version
1	MGate 5122-T	00:90:E8:B8:56:B7	192.168.127.254	---			xxxxxxxx

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 that is at least eight characters long when you log in for the first time. Or if you have already an account, log in with your account name and password. If you change the MGate's IP and other related network settings, click SAVE, and the MGate will reboot.



Log in to
MGate 5122-T_1040805

microSD

The MGate provides you with an easy way to back up, copy, replace, or deploy. The MGate has a microSD card slot. 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.

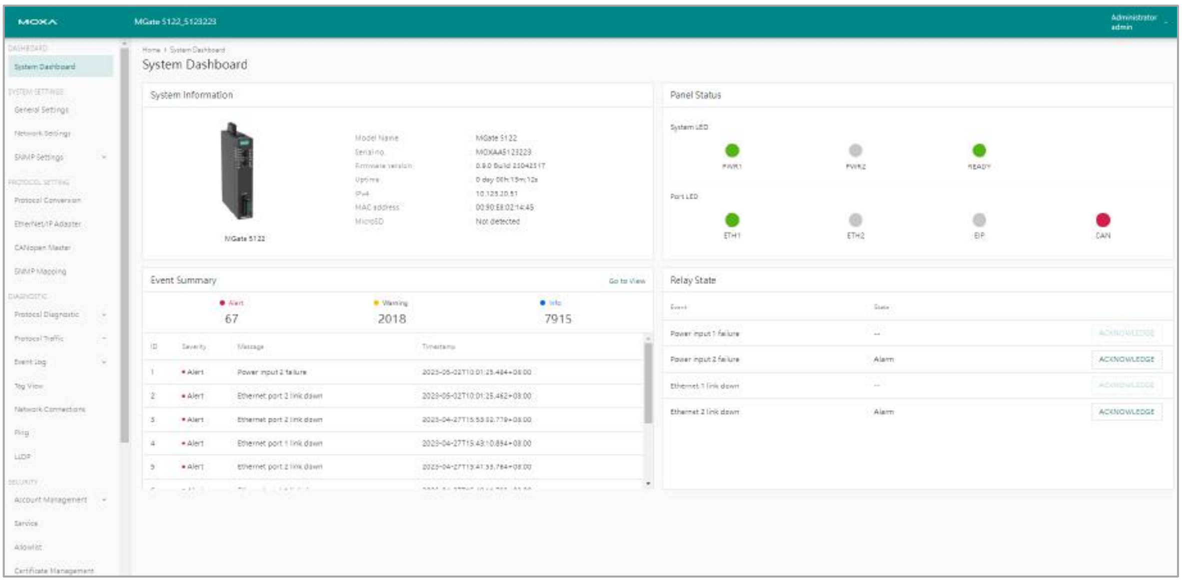
In case of the above events, the MGate will flash Ready LED in red color. When you replace the MGate gateway's microSD card, the microSD card will synchronize the configurations stored on the MGate gateway. Note that the replacement microSD card should not contain any configuration files on it; otherwise,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

3. Web Console Configuration and Troubleshooting

This chapter provides a quick overview of how to configure the MGate 5122 by web console.

System Dashboard

This page gives a system dashboard of the MGate 5122 gateway.



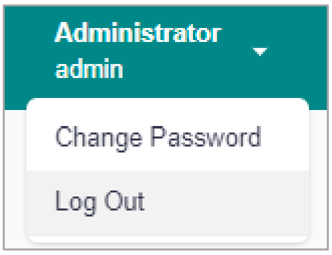
Model Name	MGate 5122
Serial no.	MOXAA5123223
Firmware version	0.9.0 Build 23042517
Uptime	0 day 00h:15m:12s
IPv4	10.123.20.51
MAC address	00:90:E8:02:14:45
MicroSD	Not detected

● Alert	● Warning	● Info
67	2018	7915

ID	Severity	Message	Timestamp
1	• Alert	Power input 2 failure	2023-05-02T10:01:25.484+08:00
2	• Alert	Ethernet port 2 link down	2023-05-02T10:01:25.462+08:00
3	• Alert	Ethernet port 2 link down	2023-04-27T15:53:02.779+08:00
4	• Alert	Ethernet port 1 link down	2023-04-27T15:43:10.894+08:00
5	• Alert	Ethernet port 2 link down	2023-04-27T15:41:35.784+08:00

Event	State	
Power input 1 failure	--	ACKNOWLEDGE
Power input 2 failure	Alarm	ACKNOWLEDGE
Ethernet 1 link down	--	ACKNOWLEDGE
Ethernet 2 link down	Alarm	ACKNOWLEDGE

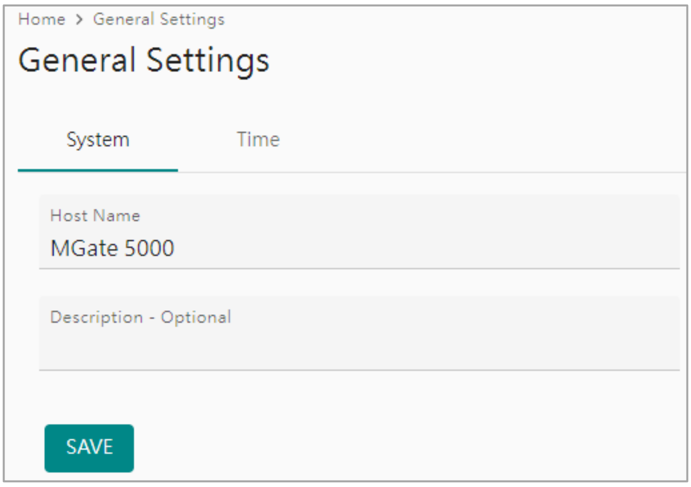
Change your password or log out using the options on the top-right corner of the page.



System Settings

System Settings—General Settings

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



Host Name: MGate 5000

Description - Optional

System Settings

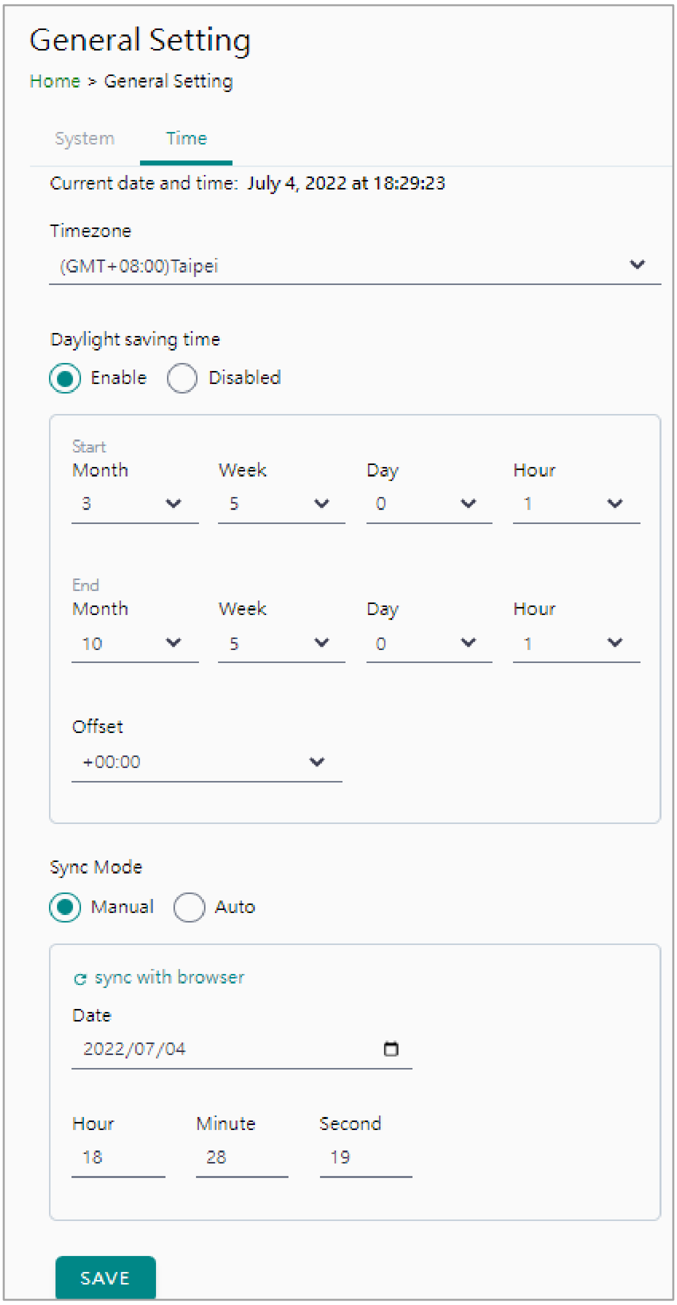
Parameter	Value	Description
Host Name	Alphanumeric string	Enter a name that can help you uniquely identify the device. For example, you can include the name and function of the device.
Description	Alphanumeric string	(optional) You can include additional description about the device such as function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



General Setting

Home > General Setting

System Time

Current date and time: July 4, 2022 at 18:29:23

Timezone: (GMT+08:00)Taipei

Daylight saving time: ● Enable ○ Disabled

Start: Month 3, Week 5, Day 0, Hour 1

End: Month 10, Week 5, Day 0, Hour 1

Offset: +00:00

Sync Mode: ● Manual ○ Auto

sync with browser

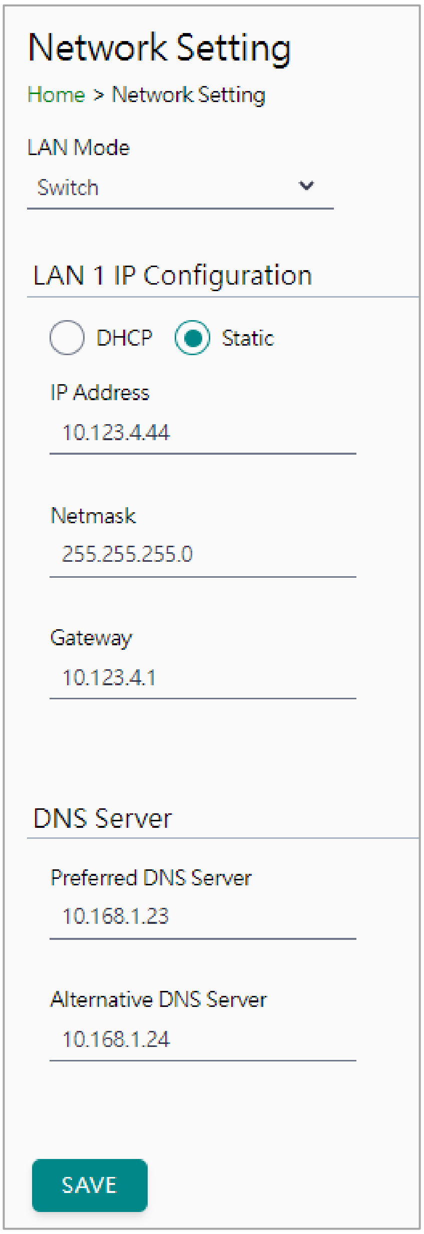
Date: 2022/07/04

Hour 18, Minute 28, Second 19

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/disables 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

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



Network Setting

Home > Network Setting

LAN Mode: Switch

LAN 1 IP Configuration

○ DHCP ● Static

IP Address: 10.123.4.44

Netmask: 255.255.255.0

Gateway: 10.123.4.1

DNS Server

Preferred DNS Server: 10.168.1.23

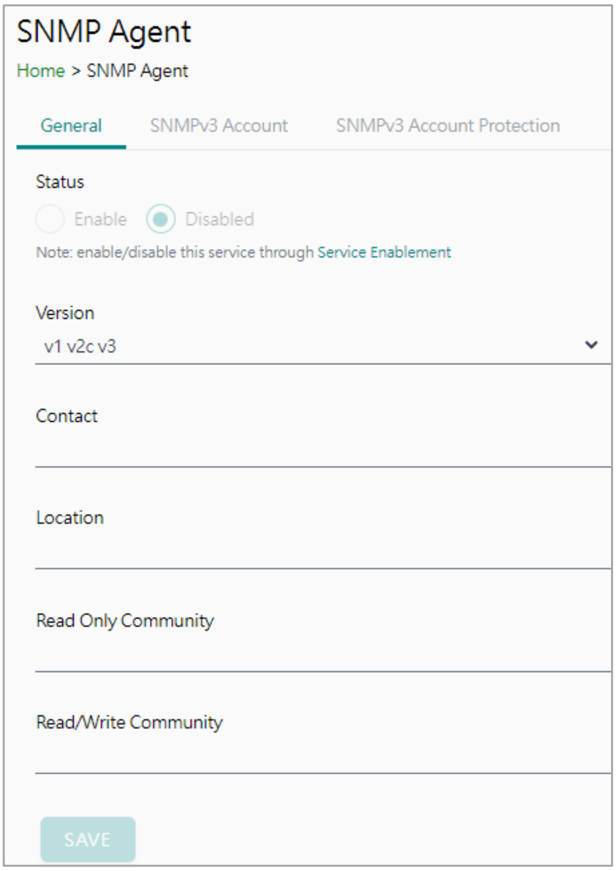
Alternative DNS Server: 10.168.1.24

Parameter	Value	Description
LAN Mode	**Switch, Dual IP, Redundant LAN**	The **Switch** mode allows you 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 you 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



SNMP Agent

Home > SNMP Agent

General | SNMPv3 Account | SNMPv3 Account Protection

Status

○ Enable ● Disabled

Note: enable/disable this service through Service Enablement

Version: v1 v2c v3

Contact

Location

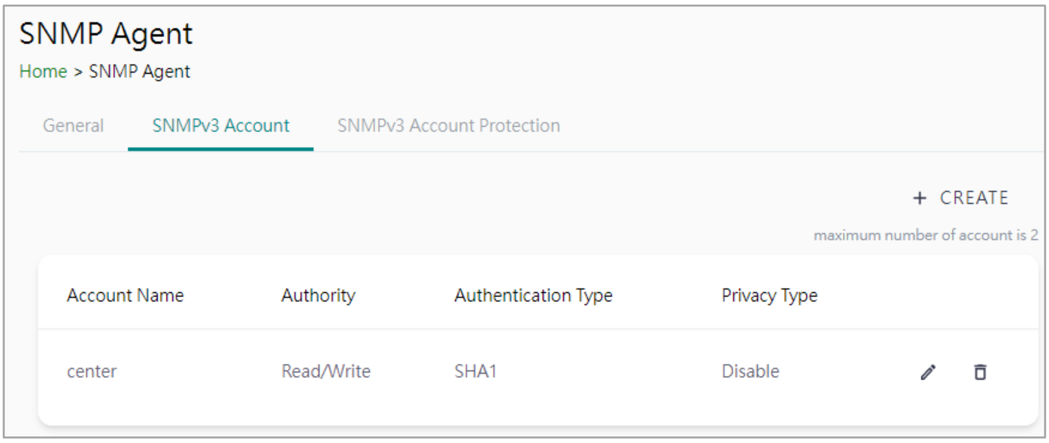
Read Only Community

Read/Write Community

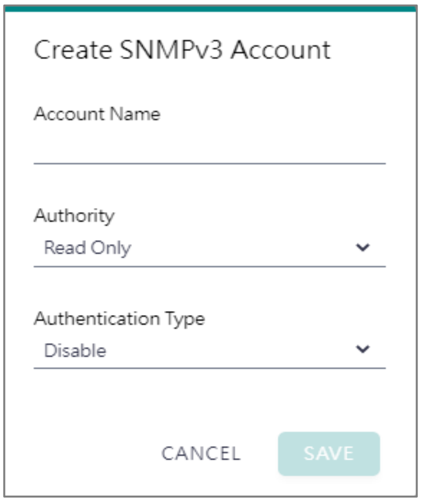
Parameters	Description
Version	The SNMP version; the MGate supports SNMP v1, v2c, and v3.
Contact	The optional contact information; it usually includes an emergency contact name and telephone number.
Location	The location information. This string is usually set to the street address where the MGate is physically located.
Read-only Community	A text password mechanism that is used to weakly authenticate queries to agents of managed network devices. Default is empty. Type in the community string when selecting v1 v2c or v1 v2c v3 version.
Read/Write Community	A text password mechanism that is used to weakly authenticate changes to agents of managed network devices. Default is empty. Type in the community string when selecting v1 v2c or v1 v2c v3 version.
Minimum Authentication/Privacy Password Length	Minimum Authentication/Privacy Password Length must be between 8 and 64.

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 value in the Authority field indicates the access level. 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, configure the following:



Account Name	Authority	Authentication Type	Privacy Type
center	Read/Write	SHA1	Disable



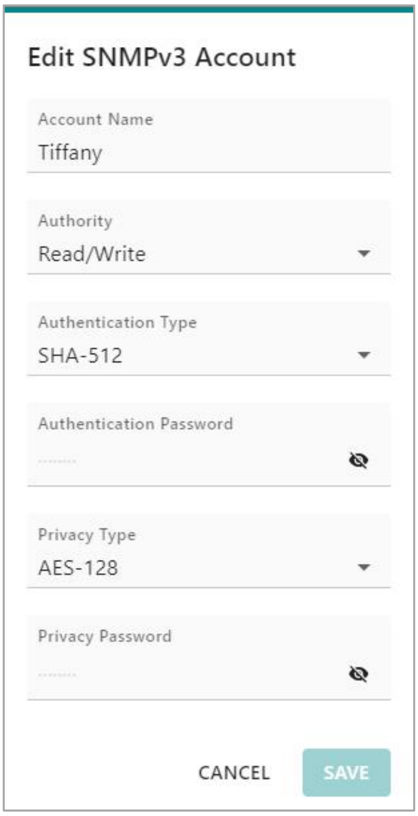
Account Name

Authority: Read Only

Authentication Type: Disable

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.
Privacy Type	**Disable (Default)** **DES-CBC** **AES-128**	Use this field to enable or disable data encryption for the specified level of access. If you enable a privacy type, also configure the privacy password.

If you need to change the SNMP Account settings created previously, click on the button on the right of the configured SNMP item to change settings, such as Authentication Type or Privacy Type.



Edit SNMPv3 Account

Account Name: Tiffany

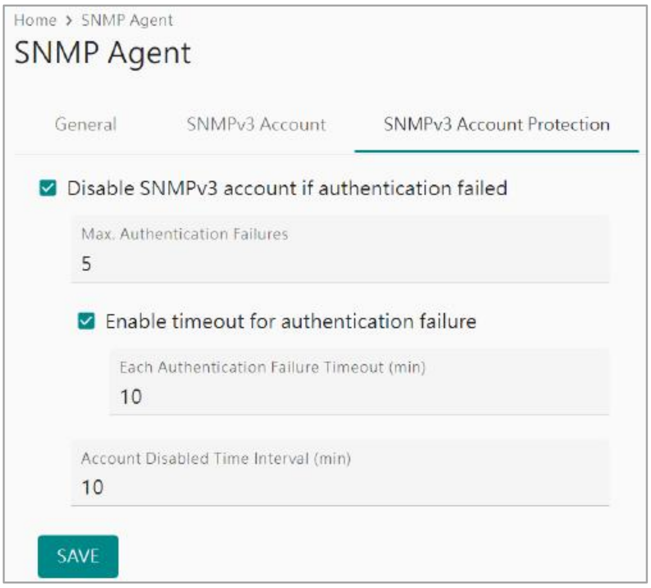
Authority: Read/Write

Authentication Type: SHA-512

Authentication Password: ········

Privacy Type: AES-128

Privacy Password: ········



SNMP Agent

☑ Disable SNMPv3 account if authentication failed

Max. Authentication Failures: 5

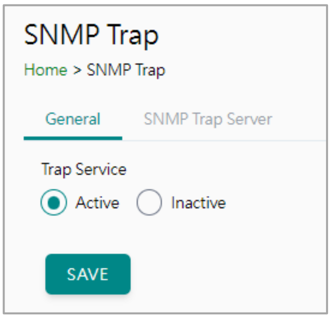
☑ Enable timeout for authentication failure

Each Authentication Failure Timeout (min): 10

Account Disabled Time Interval (min): 10

Parameters	Value	Description
Max Authentication Failure	1 to 10 (default 5)	Specifies the maximum number of authentication failures. The MGate disables SNMPv3 when this number is exceeded.
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



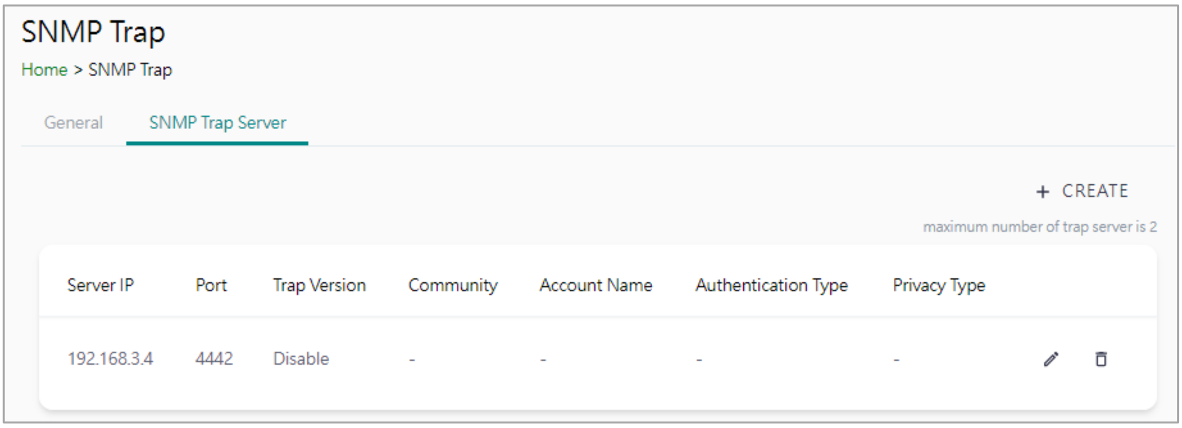
SNMP Trap

Home > SNMP Trap

Trap Service

● Active ○ Inactive

Set up the SNMP trap server to send the trap events, such as warning messages.

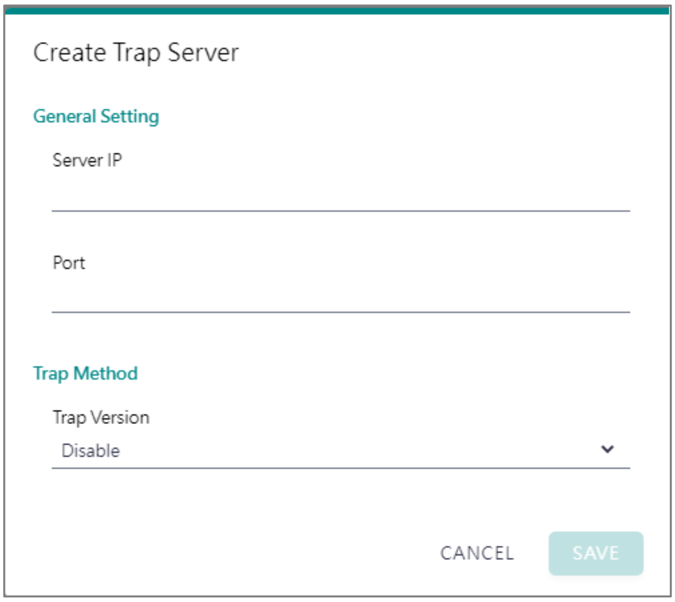


SNMP Trap

Home > SNMP Trap

maximum number of trap server is 2

Server IP	Port	Trap Version	Community	Account Name	Authentication Type	Privacy Type
192.168.3.4	4442	Disable	-	-	-	-



Create Trap Server

General Setting

Server IP

Port

Trap Method

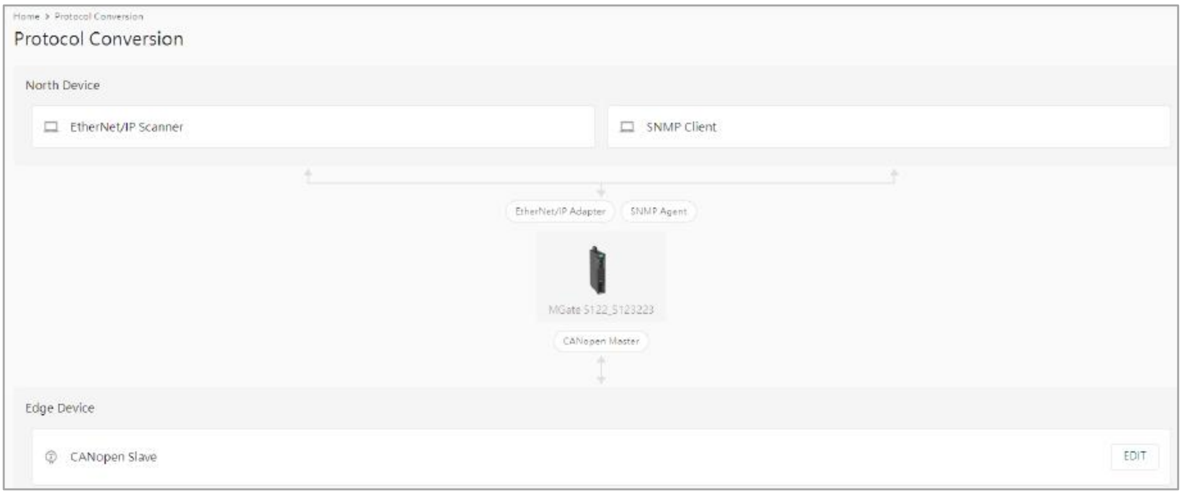
Trap Version: Disable

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** **SNMPv2c** **SNMPv3**

Protocol Settings

Protocol Settings—Protocol Conversion

Select CANopen, J1939, or CAN proprietary on this page.



Home > Protocol Conversion

Protocol Conversion

North Device

EtherNet/IP Scanner

SNMP Client

EtherNet/IP Adapter

SNMP Agent

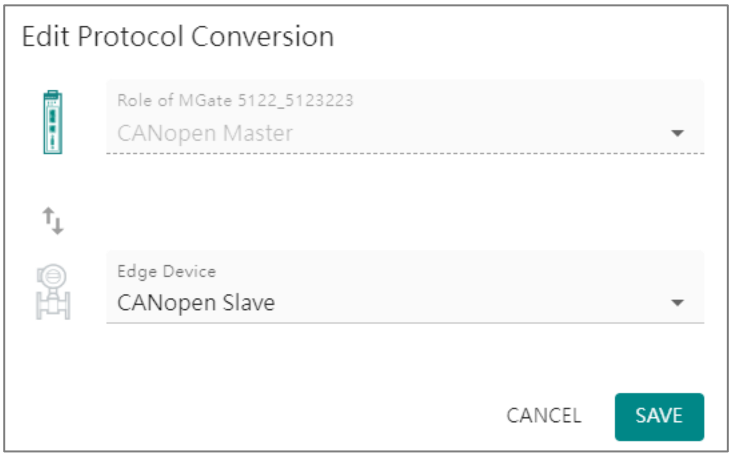
MGate 5122_5123223

CANopen Master

Edge Device

CANopen Slave

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

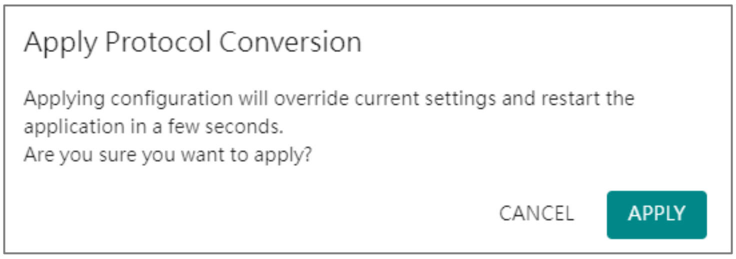


Edit Protocol Conversion

Role of MGate 5122_5123223: CANopen Master

Edge Device: CANopen Slave

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

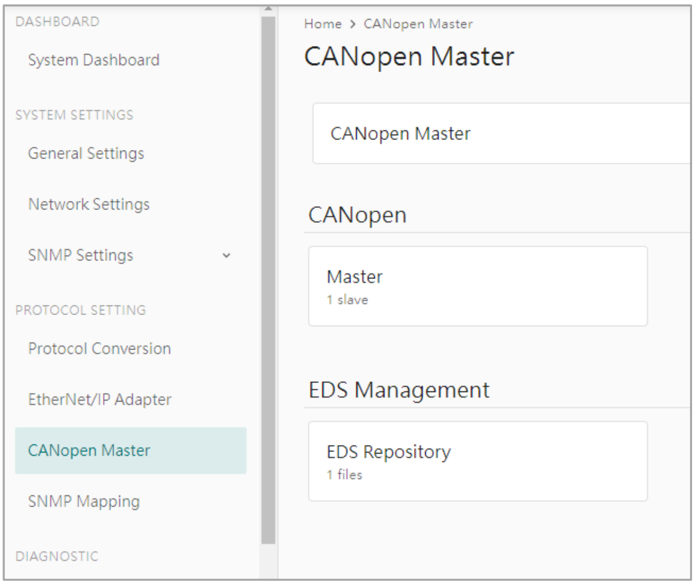


Apply Protocol Conversion

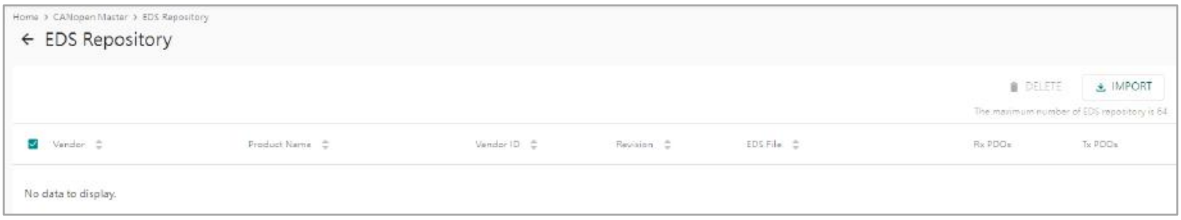
Applying configuration will override current settings and restart the application in a few seconds.
Are you sure you want to apply?

Protocol Settings—CANopen Master Settings

Manage CANopen devices on this page.



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

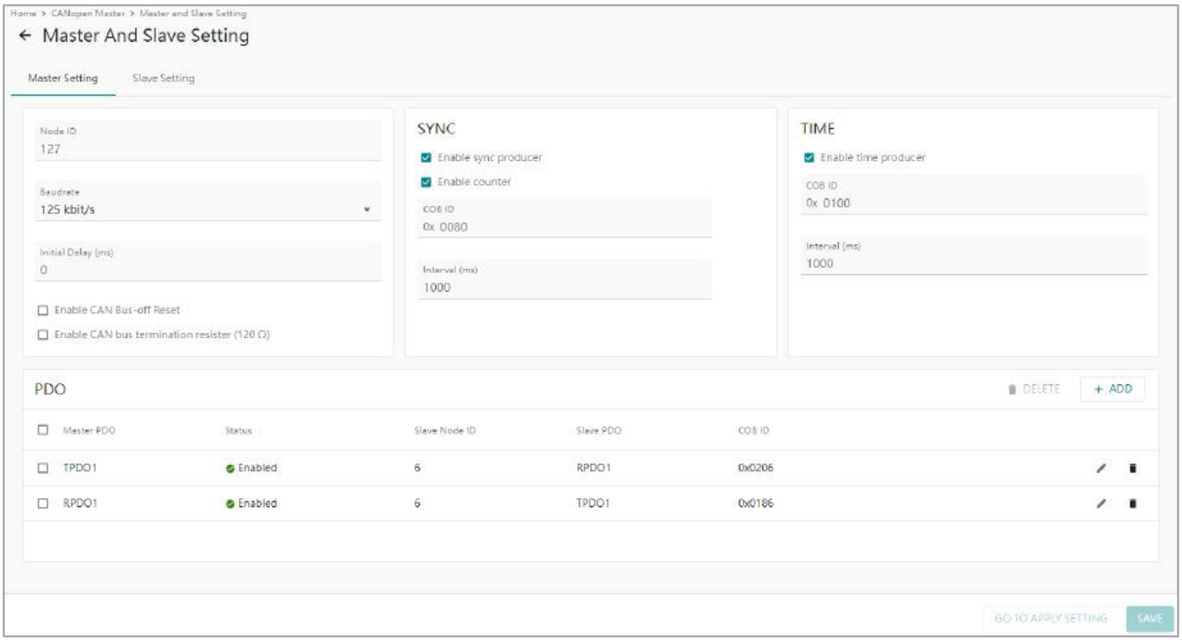


The maximum number of EDS repository is 64.

No data to display.

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 configure CANopen master and slave settings.



Home > CANopen Master > Master and Slave Setting

← Master And Slave Setting

Master Setting | Slave Setting

Node ID: 127

Baudrate: 125 kbit/s

Initial Delay (ms): 0

□ Enable CAN Bus-off Reset

□ Enable CAN bus termination resister (120 Ω)

SYNC

☑ Enable sync producer

☑ Enable counter

COB ID: 0x 0080

Interval (ms): 1000

TIME

☑ Enable time producer

COB ID: 0x 0100

Interval (ms): 1000

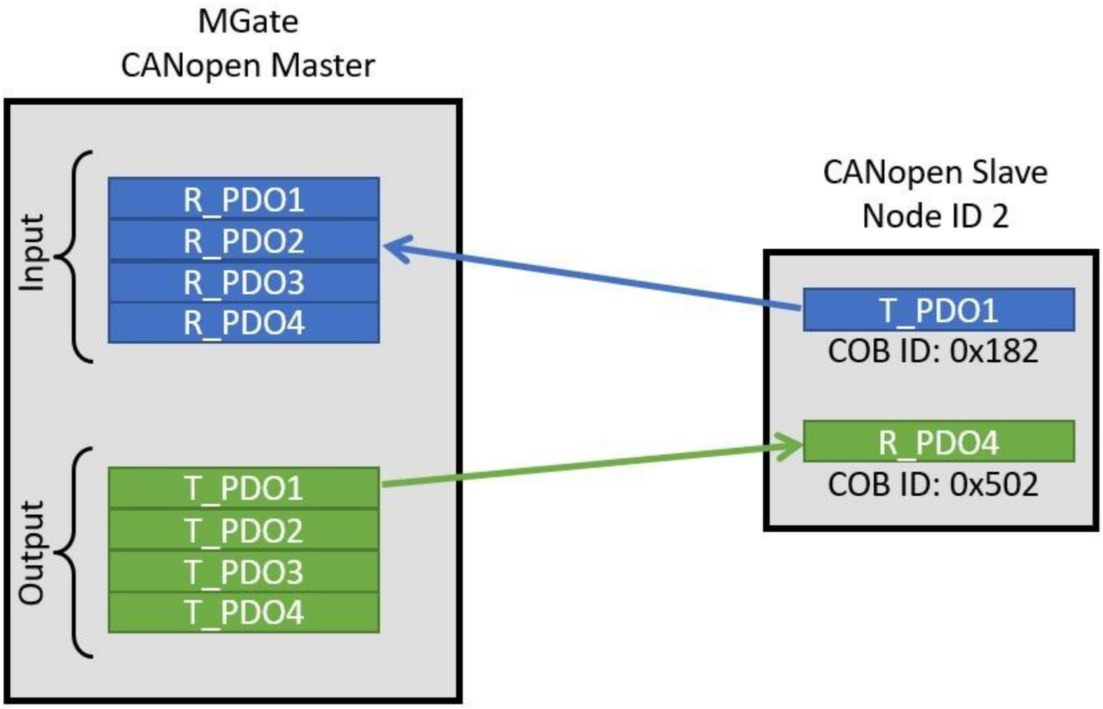
PDO

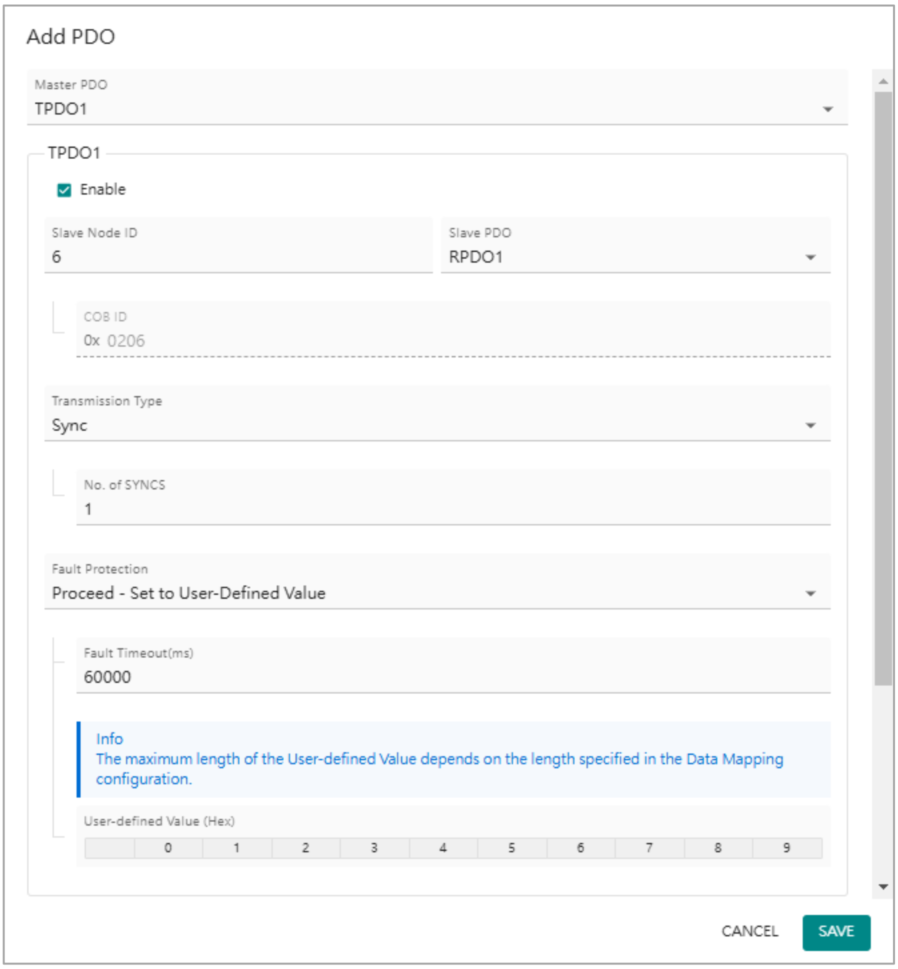
□ Master PDO	Status	Slave Node ID	Slave PDO	COB ID
□ TPDO1	● Enabled	6	RPDO1	0x0206
□ RPDO1	● Enabled	6	TPDO1	0x0186

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
Initial Delay (ms)	0 to 120000	0	For those CAN devices that need longer time to boot up, the MGate needs to wait until the device is ready for communication. Set the initial delay time to wait for the device to boot up.
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 to 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	
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, type in COB ID 0x0502 in the CANopen master TPDO1. If you want to mapping slave ID2's TPDO1 to CANopen master RPDO2, type in COB ID 0x0182 in RPDO2.





Add PDO

Master PDO: TPDO1

TPDO1

☑ Enable

Slave Node ID: 6

Slave PDO: RPDO1

COB ID: 0x 0206

Transmission Type: Sync

No. of SYNCS: 1

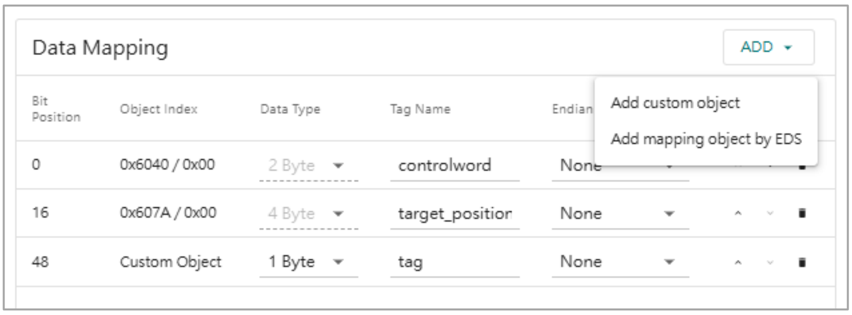
Fault Protection: Proceed - Set to User-Defined Value

Fault Timeout(ms): 60000

Info
The maximum length of the User-defined Value depends on the length specified in the Data Mapping configuration.

User-defined Value (Hex)

	0	1	2	3	4	5	6	7	8	9



Bit Position	Object Index	Data Type	Tag Name	Endian
0	0x6040 / 0x00	2 Byte	controlword	None
16	0x607A / 0x00	4 Byte	target_positior	None
48	Custom Object	1 Byte	tag	None

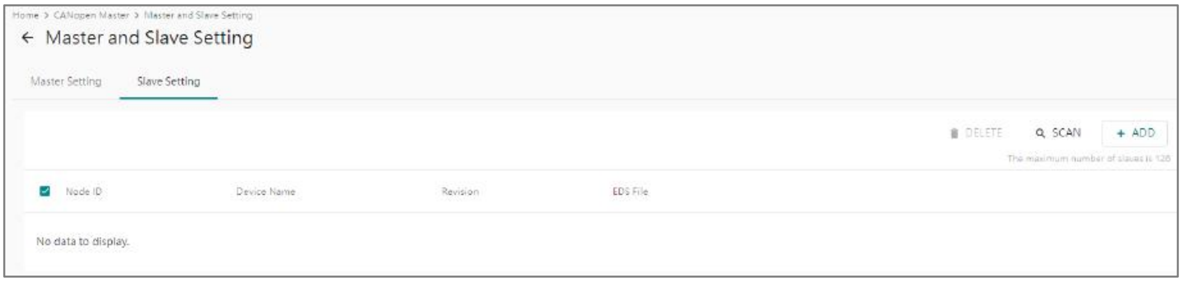
Parameter	Value	Default	Description
PDO	TPDOx RPDOx		Max 256 TPDO, 256 RPTO
Enable	Disable Enable	Enable	
COB ID	0x0000 to 0xFFFF	0x0000	There are two methods to create COB ID. Automatic generate COB ID by Slave Node ID and choose PDOx from Slave PDO. Alternatively, you can manually enter the COB ID when Slave PDO is set to "-- Select One --".
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 the previous setting. **Event.** The MGate will send out TPDO cyclic according to the Event Timer(ms). If the 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 TPDO data into internal memory only when SYNC message occurred. **Event.** The MGate updates the slave TPDO data into internal memory when received from the slave TPDO.
No. of SYNCS (for Sync Type)	0 to 240	0	No. of SYNC messages. Value from 0 to 240.
Inhibit Time (ms) (for Event Type))	0 to 65535	0	This can be used to set a time that must wait after the sending of a PDO
Event Timer (ms)	0 to 65535	0	This time can be used to trigger an event which handles the sending of the PDO.
Fault Protection	Pause Proceed-Clear data to zero Proceed – Set to User Defined Value	Pause	**Pause:** The gateway will write the same data to the slave device. **Proceed—Clear data to zero:** The gateway will write zero values to the slave device. **Proceed—Set to User Defined Value:** A user-defined value will be written to the slave device.
Fault Timeout (ms)	100 to 65535	60000	Defines the communication timeout on the opposite side.
Bit Position	Automatic generated		Bit offset in the PDO data frame
Object index	Customer Object index/ sub-index		Add customer object or add quickly with index/sub-index from slave EDS parameter.
Data Type	1 to 7 Bit 1 to 8 Byte	1 Bit	Tag data type
Tag Name	Alphanumeric string		Create Tag names. Select tags in the northbound protocol setting.

Parameter	Value	Default	Description
Endian Swap	None Byte swap Reverse Reverse with byte swap	None	Swapping the data. The item may change with different tag type or length for raw data type. **None:** No swap **Byte swap:** Switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x22 11 44 33 66 55 88 77 **Reverse:** Reverse the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x88 77 66 55 44 33 22 11 **Reverse with byte swap:** Reverse the order of bytes first, then switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x77 88 55 66 33 44 11 22

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 to 127	0x081 to 0x0FF
TIME	0010	0	0x100
T_PDO 1	0011	1 to 127	0x181 to 1FF
R_PDO 1	0100	1 to 127	0x201 to 27F
T_PDO 2	0101	1 to 127	0x281 to 2FF
R_PDO 2	0110	1 to 127	0x301 to 37F
T_PDO 3	0111	1 to 127	0x381 to 3FF
R_PDO 3	1000	1 to 127	0x401 to 47F
T_PDO 4	1001	1 to 127	0x481 to 4FF
R_PDO 4	1010	1 to 127	0x501 to 57F
T_SDO	1011	1 to 127	0x581 to 5FF
R_SDO	1100	1 to 127	0x601 to 67F
Heartbeat	1110	1 to 127	0x701 to 77F

Add CANopen slave device into Slave Setting.


Home > CANopen Master > Master and Slave Setting
← Master and Slave Setting
Master Setting
Slave Setting
DELETE
SCAN
+ ADD

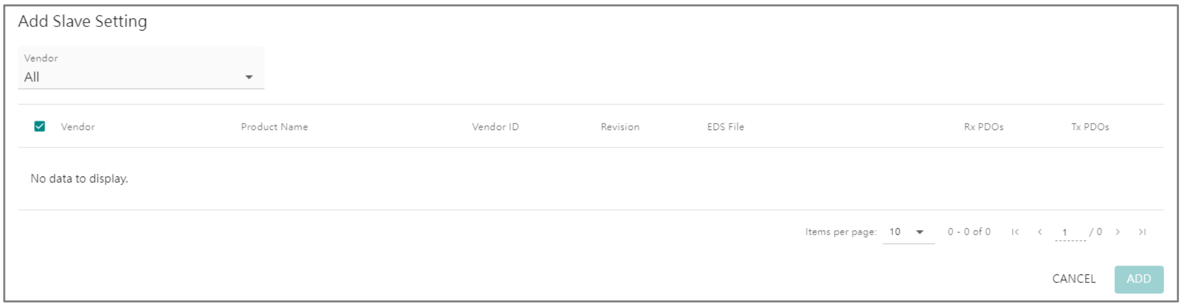
The maximum number of slaves is 126

☑ Node ID	Device Name	Revision	EDS File

No data to display.

ADD the slave device manually or SCAN the devices on the CANbus. Import slave EDS files before adding or scanning the slave devices.

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


Add Slave Setting

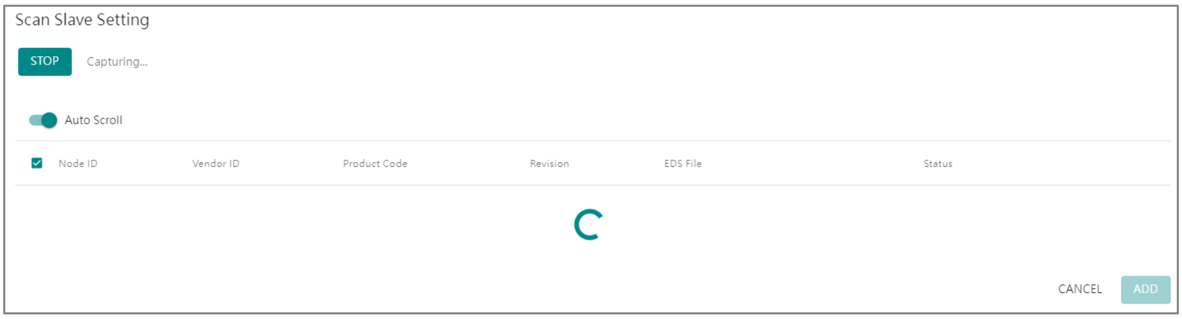
Vendor: All

☑ Vendor	Product Name	Vendor ID	Revision	EDS File	Rx PDOs	Tx PDOs

No data to display.

Items per page: 10   0 - 0 of 0   1 / 0

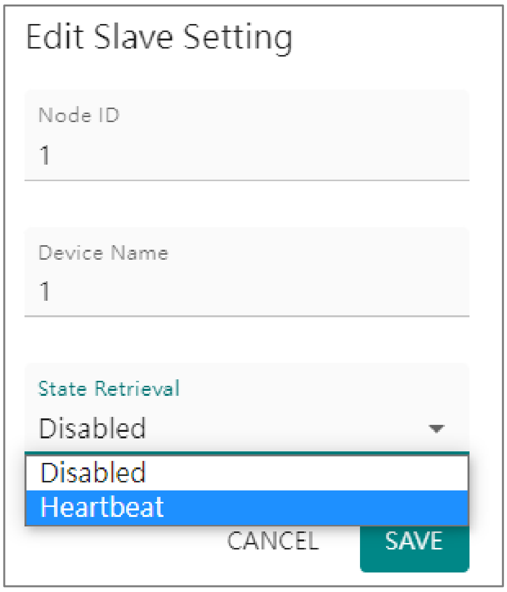
Or, click the SCAN button to scan the device on the CAN bus. Only the slave device that matches the EDS file in the EDS Repository will be added to the table.



Scan Slave Setting

☑ Node ID	Vendor ID	Product Code	Revision	EDS File	Status

Click the pen icon to edit the slave Node ID and Device Name. Enable the **Enable device parameters initialization** setting. The MGate will send SDO requests to set the slave's communication parameters when the CANopen bus is ready. Select **Heartbeat** to retrieve the slave's status and set **Master Heartbeat Consuming Timeout** time for the CANopen slave parameter.

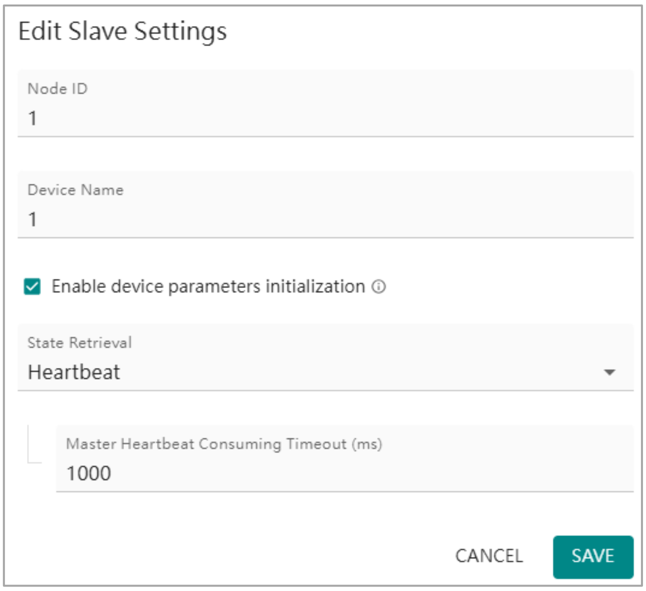


Edit Slave Setting

Node ID: 1

Device Name: 1

State Retrieval: Disabled



Edit Slave Settings

Node ID: 1

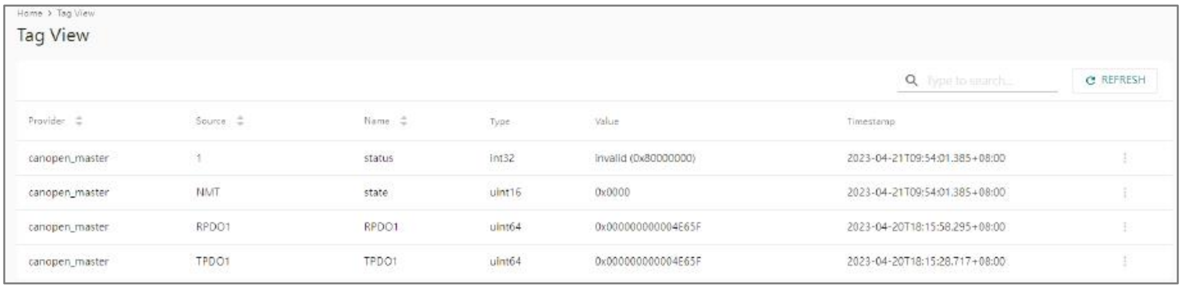
Device Name: 1

☑ Enable device parameters initialization ⓘ

State Retrieval: Heartbeat

Master Heartbeat Consuming Timeout (ms): 1000

Heartbeat tag view status

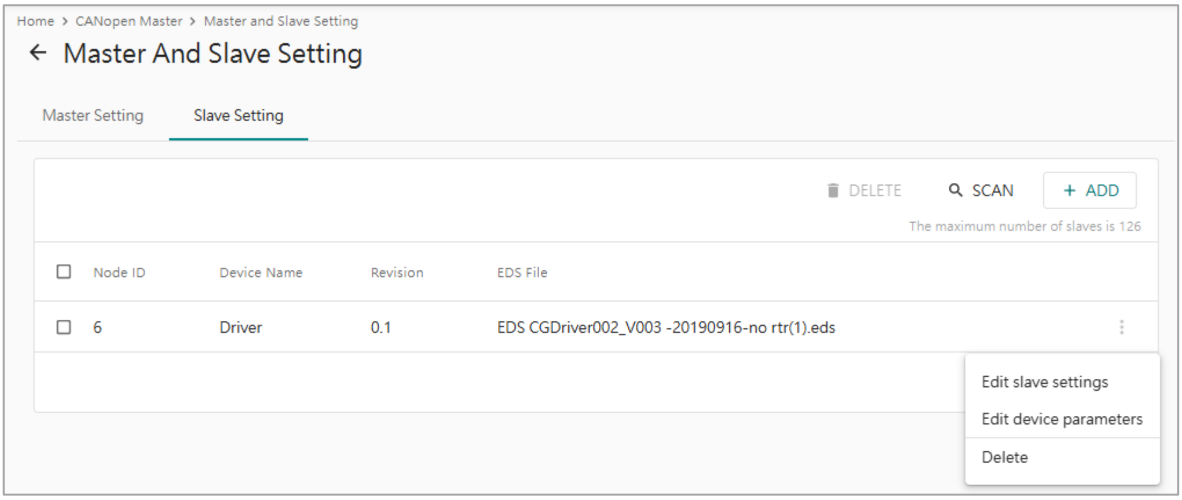


Home > Tag View

Tag View

Provider	Source	Name	Type	Value	Timestamp
canopen_master	1	status	int32	invalid (0x80000000)	2023-04-21T09:54:01.385+08:00
canopen_master	NMT	state	uint16	0x0000	2023-04-21T09:54:01.385+08:00
canopen_master	RPDO1	RPDO1	uint64	0x000000000004E65F	2023-04-20T18:15:58.295+08:00
canopen_master	TPDO1	TPDO1	uint64	0x000000000004E65F	2023-04-20T18:15:28.717+08:00

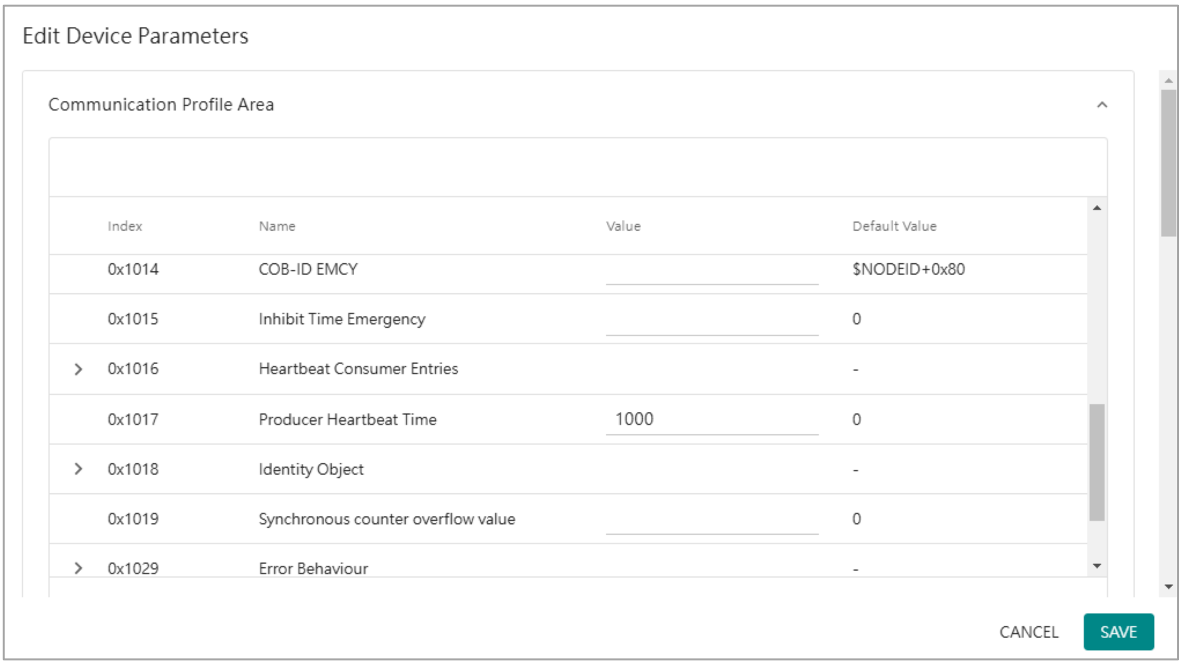
If you would like to initialize or change parameters default value of slave device when CAN bus ID is ready to send SDOs. Click the Edit device parameters.



The maximum number of slaves is 126

	Node ID	Device Name	Revision	EDS File
□	6	Driver	0.1	EDS CGDriver002_V003 -20190916-no rtr(1).eds

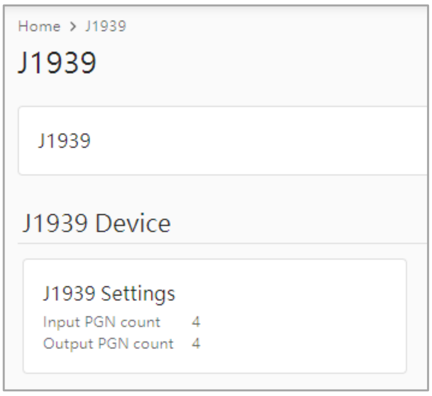
In the following window, you can see the default value from the EDS file, and you may type in the new value in the value column, and then click the SAVE button.



	Index	Name	Value	Default Value
	0x1014	COB-ID EMCY		$NODEID+0x80
	0x1015	Inhibit Time Emergency		0
>	0x1016	Heartbeat Consumer Entries		-
	0x1017	Producer Heartbeat Time	1000	0
>	0x1018	Identity Object		-
	0x1019	Synchronous counter overflow value		0
>	0x1029	Error Behaviour		-

Protocol Settings—J1939 Settings

Manage the J1939 protocol on this page.



Home > J1939

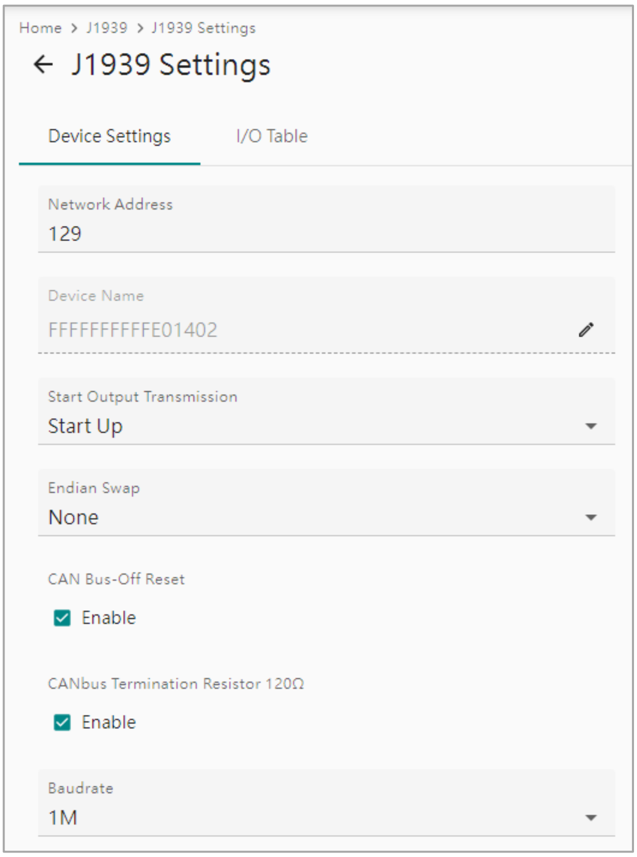
J1939

J1939

J1939 Device

J1939 Settings
Input PGN count 4
Output PGN count 4

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



Home > J1939 > J1939 Settings

J1939 Settings

Network Address: 129

Device Name: FFFFFFFFFFE01402

Start Output Transmission: Start Up

Endian Swap: None

CAN Bus-Off Reset: ☑ Enable

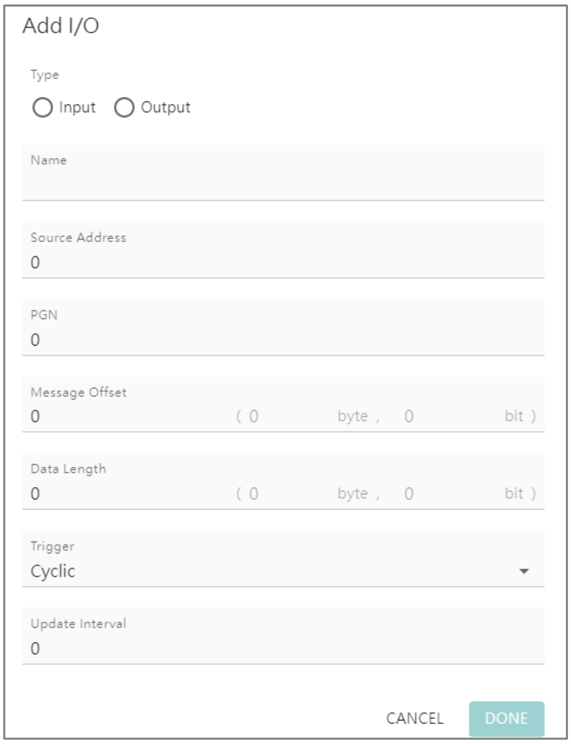
CANbus Termination Resistor 120Ω: ☑ Enable

Baudrate: 1M

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	None Byte swap Reverse Reverse with byte swap	None	Swapping the data. The item may change with different tag type or length for raw data type. **None:** Don't need to swap **Byte swap:** Switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x22 11 44 33 66 55 88 77 **Reverse:** Reverse the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x88 77 66 55 44 33 22 11 **Reverse with byte swap:** Reverse the order of bytes first, then switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x77 88 55 66 33 44 11 22
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. Choose Enable to have the MGate rejoin the bus.
CANbus termination resistor 120 ohms	Disable, Enable	Disable	To enable 120 ohms termination resistor on the CAN bus.
Baudrate	250 kbps, 500 kbps, 1Mbps	250 kbps	The baudrate used in J1939

Under the **I/O Table** tab, 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.


Add I/O

Type
○ Input ○ Output

Name

Source Address
0

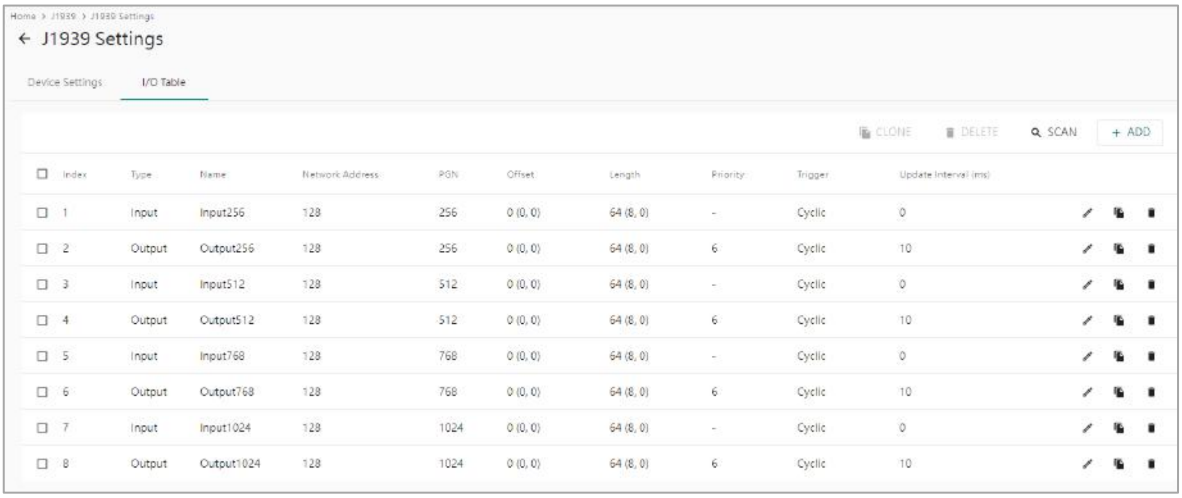
PGN
0

Message Offset
0 (0 byte , 0 bit)

Data Length
0 (0 byte , 0 bit)

Trigger
Cyclic

Update Interval
0



□	Index	Type	Name	Network Address	PGN	Offset	Length	Priority	Trigger	Update Interval (ms)
□	1	Input	Input256	128	256	0 (0, 0)	64 (8, 0)	-	Cyclic	0
□	2	Output	Output256	128	256	0 (0, 0)	64 (8, 0)	6	Cyclic	10
□	3	Input	Input512	128	512	0 (0, 0)	64 (8, 0)	-	Cyclic	0
□	4	Output	Output512	128	512	0 (0, 0)	64 (8, 0)	6	Cyclic	10
□	5	Input	Input768	128	768	0 (0, 0)	64 (8, 0)	-	Cyclic	0
□	6	Output	Output768	128	768	0 (0, 0)	64 (8, 0)	6	Cyclic	10
□	7	Input	Input1024	128	1024	0 (0, 0)	64 (8, 0)	-	Cyclic	0
□	8	Output	Output1024	128	1024	0 (0, 0)	64 (8, 0)	6	Cyclic	10

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 sent **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)	Pause Proceed—Clear data to zero Proceed—Set to User-defined Value	Keep Latest Data	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. **Pause:** The gateway will write the same data to the slave device. **Proceed—Clear data to zero:** The gateway will write zero values to the slave device. **Proceed—Set to User Defined Value:** A user-defined value will be written to the slave device.

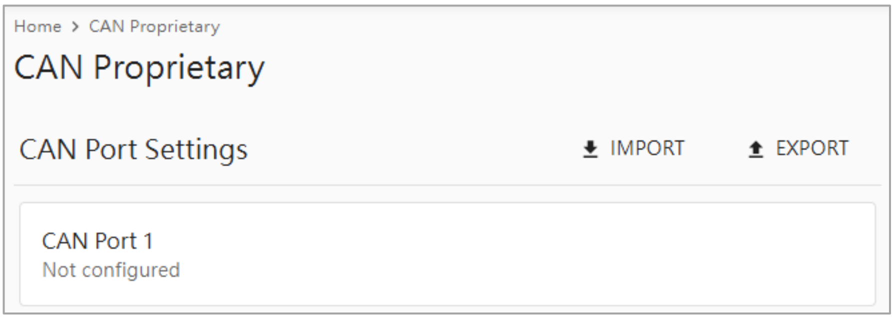
AutoScan:

For your convenience, the MGate is designed with an innovative command auto-learning function. It learns all the output commands from the J1939 devices on the same CAN bus. You don’t need to key in the commands one by one. All you must 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—CAN Proprietary Settings

Import or export offline excel CAN data frame configuration by clicking the IMPORT or EXPORT button on the right-hand side. Or, click CAN Port 1 to configure manually.



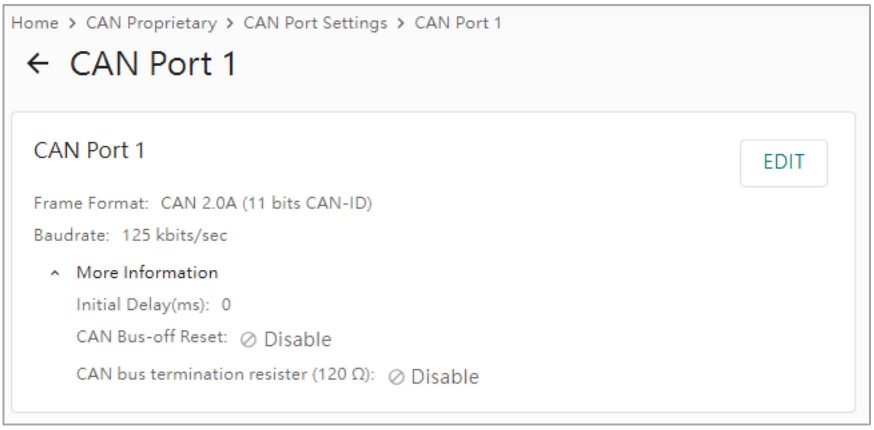
Home > CAN Proprietary

CAN Proprietary

CAN Port Settings

CAN Port 1
Not configured

Click the EDIT button to set the CAN proprietary settings.



Home > CAN Proprietary > CAN Port Settings > CAN Port 1

← CAN Port 1

CAN Port 1

Frame Format: CAN 2.0A (11 bits CAN-ID)

Baudrate: 125 kbits/sec

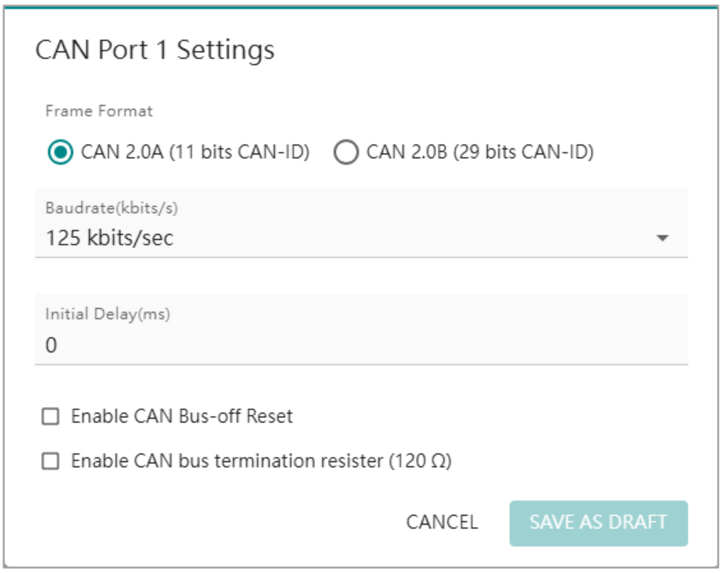
More Information

Initial Delay(ms): 0

CAN Bus-off Reset: ⊘ Disable

CAN bus termination resister (120 Ω): ⊘ Disable

Select the CAN settings for CAN port 1. Click SAVE AS DRAFT button.



CAN Port 1 Settings

Frame Format

● CAN 2.0A (11 bits CAN-ID) ○ CAN 2.0B (29 bits CAN-ID)

Baudrate(kbits/s)
125 kbits/sec

Initial Delay(ms)
0

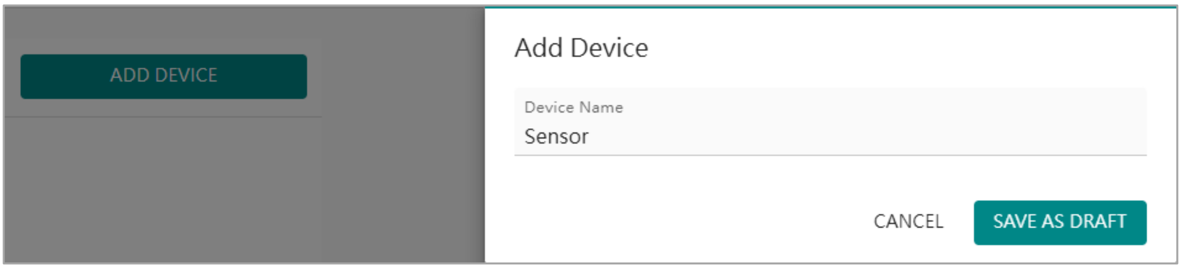
□ Enable CAN Bus-off Reset

□ Enable CAN bus termination resister (120 Ω)

CAN Port 1 Settings

Parameter	Value	Default	Description
Frame Format	CAN 2.0A CAN 2.0B	CAN 2.0A	According to your CAN proprietary device, select either CAN 2.0A or 2.0B CAN data frame format.
Baudrate(kbits/s)	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
Initial Delay(ms)	0 to 120000	0	For some CAN devices which need longer boot up time, the MGate needs to wait until the device is ready for communication. Set the initial delay time to wait the device boot-up.
CAN Bus-OFF Reset	Disable Enable	Disable	When the MGate detects the error count exceeding the CAN threshold, the CAN bus will switch to Bus Off mode, according to the CAN definition. Enable will auto reset the error count and restart the bus. Disable will stay in the Bus Off mode and only recovers when re-powering the MGate.
CAN bus termination resistor 120 ohms	Disable Enable	Disable	Software configurable CAN bus termination resistor.

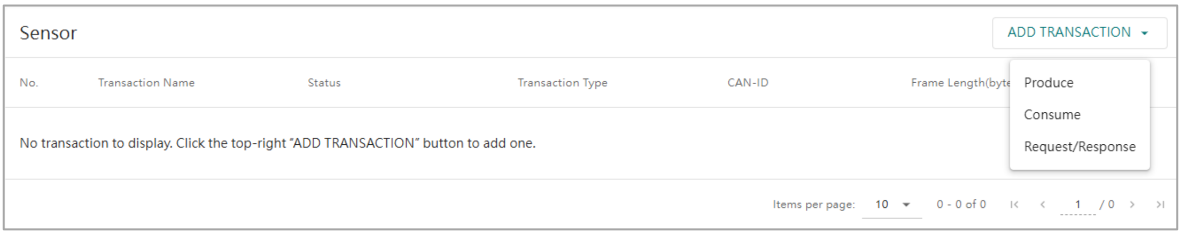
Click ADD DEVICE to add the CAN devices, type in a 1- to 64-character device name. Click SAVE AS DRAFT to save the configuration temporarily.



Add Device

Device Name: Sensor

Click ADD TRANSACTION button to select the CAN data frame type Produce, Consume, or Request/Response.



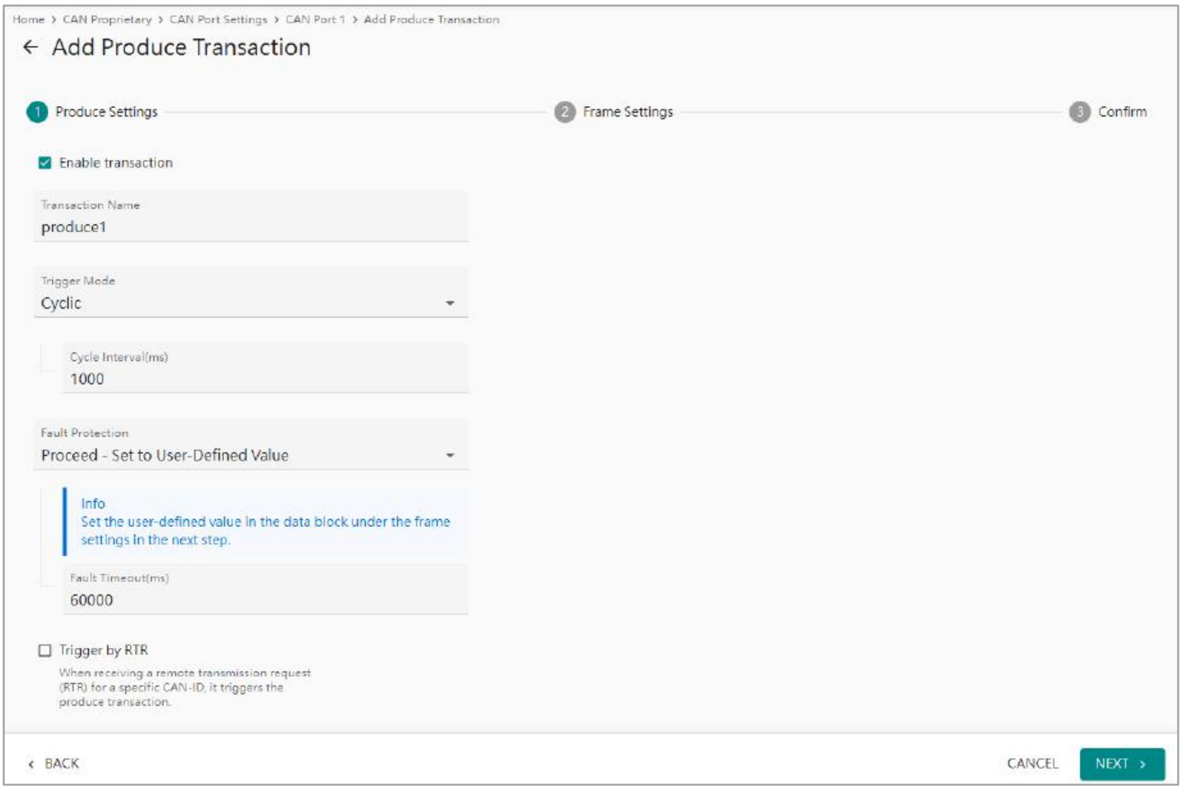
Sensor

No.	Transaction Name	Status	Transaction Type	CAN-ID	Frame Length(byte

No transaction to display. Click the top-right “ADD TRANSACTION” button to add one.

Items per page: 10 0 - 0 of 0 1 / 0

Follow a 3-step configuration for Produce Transaction, which the MGate will send CAN data to slave devices.



Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Produce Transaction

← Add Produce Transaction

1 Produce Settings — 2 Frame Settings — 3 Confirm

☑ Enable transaction

Transaction Name: produce1

Trigger Mode: Cyclic

Cycle Interval(ms): 1000

Fault Protection: Proceed - Set to User-Defined Value

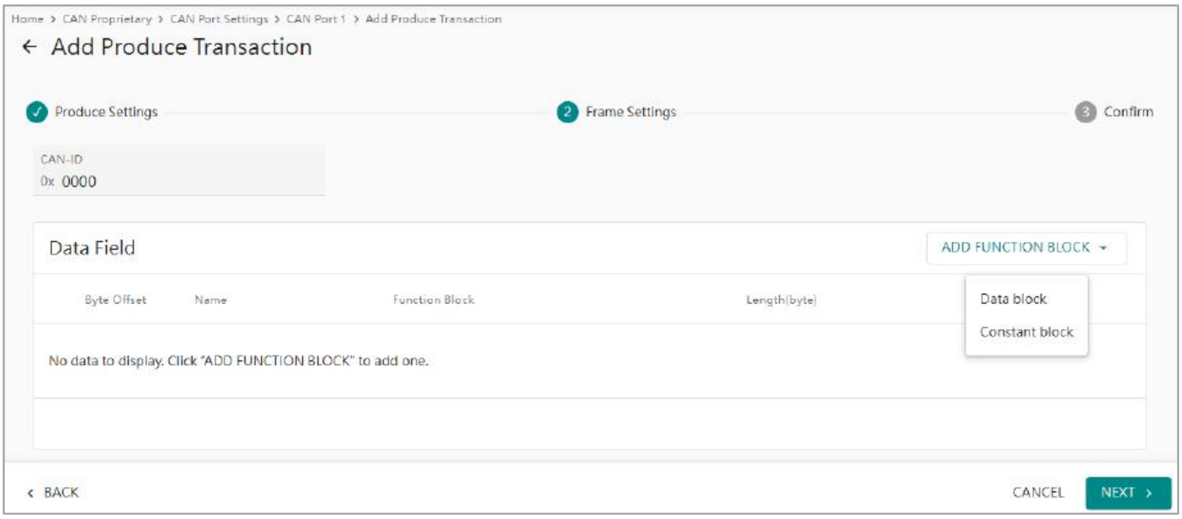
Info
Set the user-defined value in the data block under the frame settings in the next step.

Fault Timeout(ms): 60000

☐ Trigger by RTR
When receiving a remote transmission request (RTR) for a specific CAN-ID, it triggers the produce transaction.

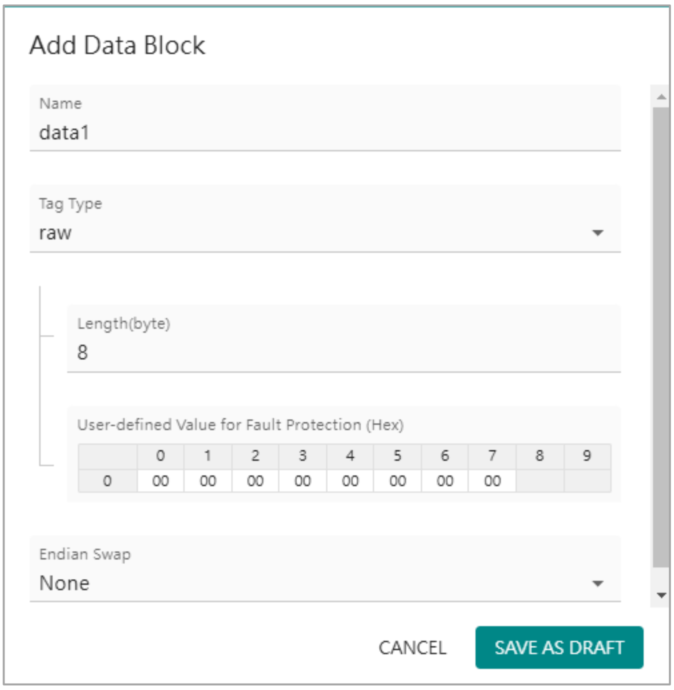
Parameter	Value	Default	Description
Transaction Name	(An alphanumeric string)		1 to 64 characters.
Trigger Mode	Cyclic Data Change Boot-up	Cyclic	**Cyclic:** The transaction is sent cyclically at the interval specified in the Cyclic Interval parameter. **Data change:** The transaction is sent when a change in data is detected. **Boot-up:** The transaction is sent once the CAN bus boots up
Cyclic Interval (ms)	10 to 65535	1000	The desired cyclic interval in milliseconds.
Fault Protection	Pause Proceed—Clear data to zero Proceed—Set to User Defined Value	Pause	**Pause:** The gateway will write the same data to the slave device. **Proceed—Clear data to zero:** The gateway will write zero values to the slave device. **Proceed—Set to User Defined Value:** A user-defined value will be written to the slave device.
Fault Timeout (ms)	100 to 65535	60000	Defines the communication timeout on the opposite side.
Tigger by RTR	Disable Enable	Disable	When receiving a remote transmission request (RTR) for a specific CAN-ID, it triggers the produce transaction.

In the Frame Settings, type the CAN-ID according to the CAN device user manual first. Then click ADD FUNCTION BLOCK to add Data blocks or Constant blocks.



CAN-ID
0x 0000

No data to display. Click "ADD FUNCTION BLOCK" to add one.



Name: data1

Tag Type: raw

Length(byte): 8

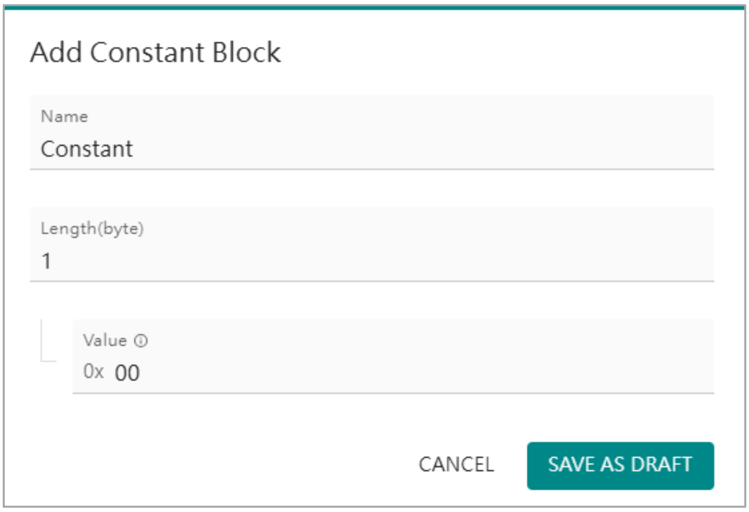
User-defined Value for Fault Protection (Hex)

	0	1	2	3	4	5	6	7	8	9
0	00	00	00	00	00	00	00	00		

Endian Swap: None

Parameter	Value	Default	Description
Name	(An alphanumeric string)		1 to 64 characters
Tag Type	raw, int 8, int 16, int 32, int 64, uint 8, uint 16, uint 32, uint 64, float, double	raw	Tag data type
Length(byte)	1 to 8	1	The default length for raw type is 1. The value is fixed for other data type, except raw type.
User-defined Value for Fault Protection (Hex)		00	Set the user-defined value in the data block when you activate Fault Protection in the Produce Settings step and select "Proceed—Set to User-defined Value"

Parameter	Value	Default	Description
Endian Swap	None Byte swap Reverse Reverse with byte swap	None	Swapping the data. The item may change with different tag type or length for raw data type. **None:** Don't need to swap **Byte swap:** Switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x22 11 44 33 66 55 88 77 **Reverse:** Reverse the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x88 77 66 55 44 33 22 11 **Reverse with byte swap:** Reverse the order of bytes first, then switch the order of bytes. 0x11 22 33 44 55 66 77 88 → 0x77 88 55 66 33 44 11 22



Add Constant Block

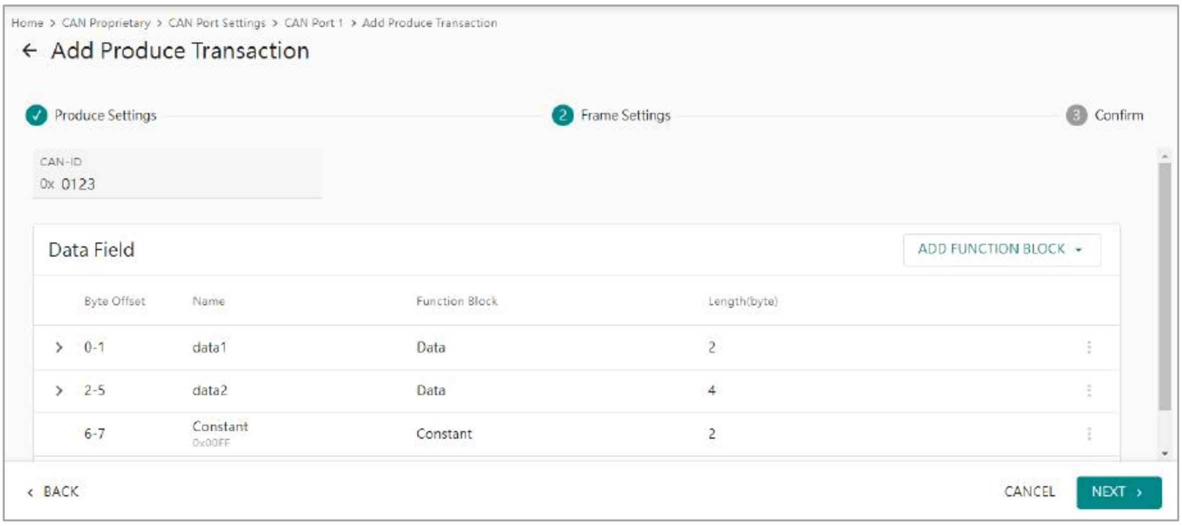
Name: Constant

Length(byte): 1

Value: 0x 00

Parameter	Value	Default	Description
Name	(An alphanumeric string)		1 to 32 characters.
Length (byte)	1 to 8	1	Data length of constant value.
Value	0x0000000000000000 to 0xFFFFFFFFFFFFFFFF	0x0000000000000000	Set the constant value in Hex.

The configuration will display the Frame Settings below.



Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Produce Transaction

Add Produce Transaction

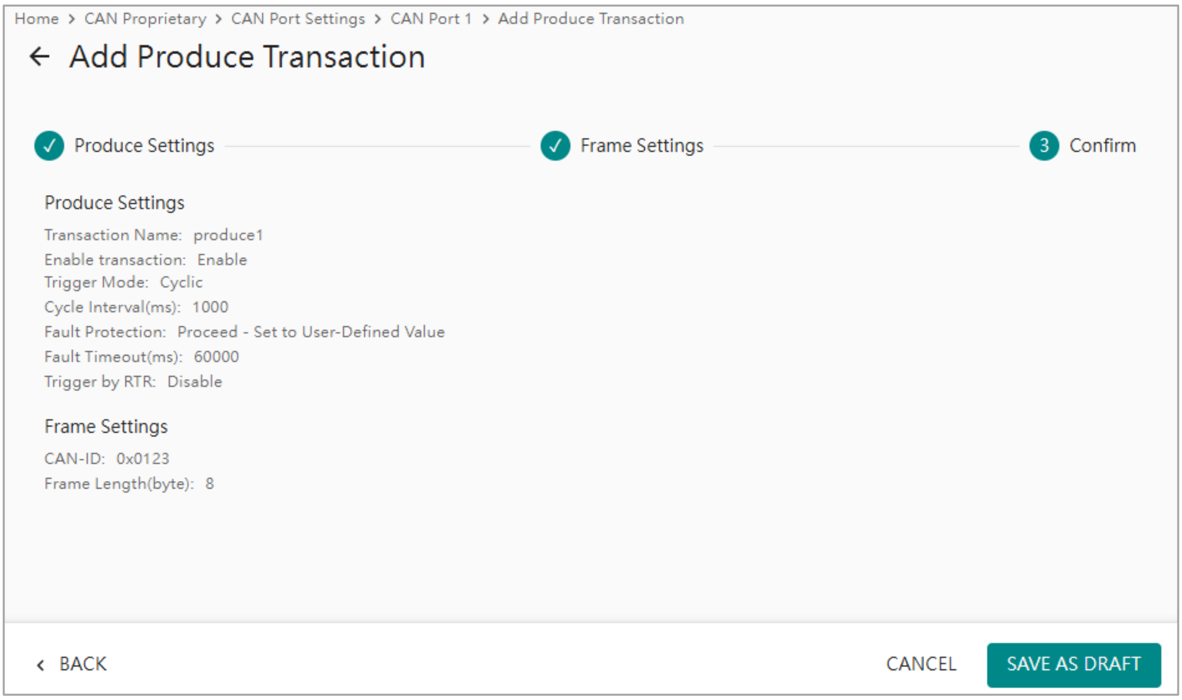
✓ Produce Settings
2 Frame Settings
3 Confirm

CAN-ID: 0x 0123

Data Field

Byte Offset	Name	Function Block	Length(byte)
0-1	data1	Data	2
2-5	data2	Data	4
6-7	Constant 0x00FF	Constant	2

Finally, confirm the transaction settings. Then, click SAVE AS DRAFT.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Produce Transaction
← Add Produce Transaction
✓ Produce Settings
✓ Frame Settings
3 Confirm

Produce Settings

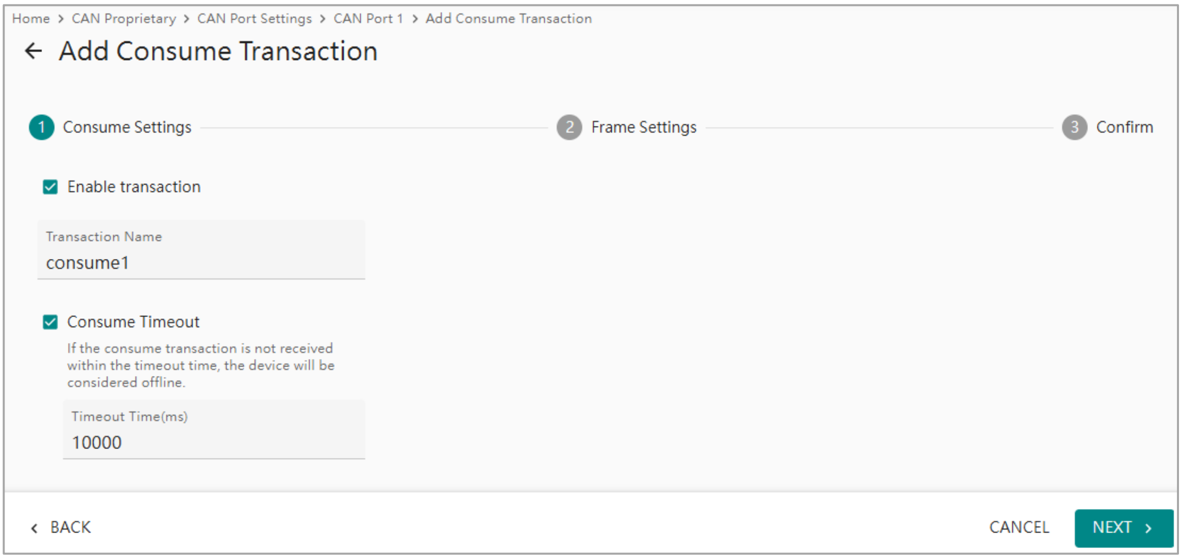
Transaction Name: produce1
Enable transaction: Enable
Trigger Mode: Cyclic
Cycle Interval(ms): 1000
Fault Protection: Proceed - Set to User-Defined Value
Fault Timeout(ms): 60000
Trigger by RTR: Disable

Frame Settings

CAN-ID: 0x0123
Frame Length(byte): 8

‹ BACK
CANCEL
SAVE AS DRAFT

Follow 3 steps configuration for Consume Transaction which MGate will receive data from CAN slave devices.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Consume Transaction
← Add Consume Transaction
1 Consume Settings
2 Frame Settings
3 Confirm

☑ Enable transaction

Transaction Name
consume1

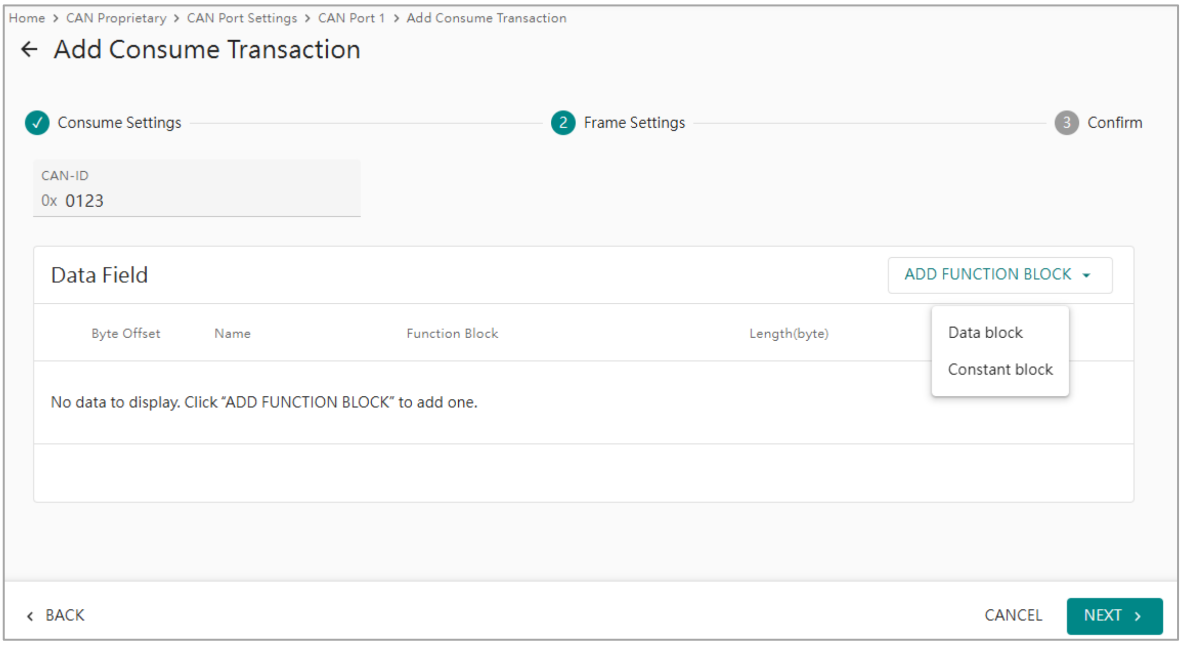
☑ Consume Timeout

If the consume transaction is not received within the timeout time, the device will be considered offline.

Timeout Time(ms)
10000

Parameter	Value	Default	Description
Transaction Name	(An alphanumeric string)		1 to 64 characters.
Consume Timeout (ms)	10 to 65535	10000	The timeout value in milliseconds. If the consume transaction is not received within the timeout time, the device will be considered offline.

Type in the CAN-ID, according to the CAN device user manual. Click the ADD FUNCTION BLOCK button to add Data blocks or Constant blocks. The block setting is the same as the producer. Refer to the Produce Frame Settings' description.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Consume Transaction
← Add Consume Transaction
✓ Consume Settings
2 Frame Settings
3 Confirm
ADD FUNCTION BLOCK
Data block
Constant block
BACK
CANCEL
NEXT

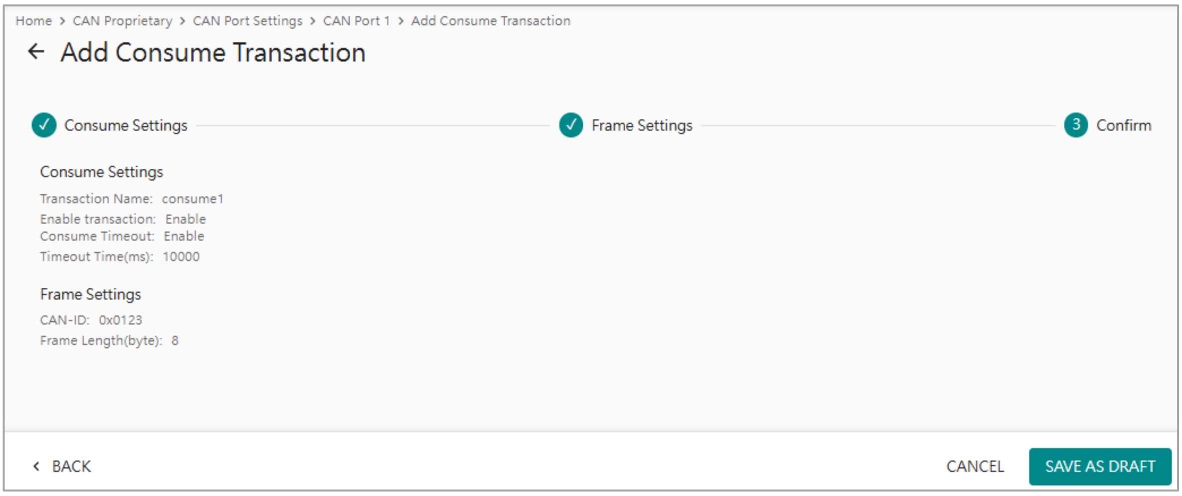
CAN-ID
0x 0123

Data Field

Byte Offset	Name	Function Block	Length(byte)

No data to display. Click "ADD FUNCTION BLOCK" to add one.

Confirm the transaction settings. Click SAVE AS DRAFT.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Consume Transaction
← Add Consume Transaction
✓ Consume Settings
✓ Frame Settings
3 Confirm
BACK
CANCEL
SAVE AS DRAFT

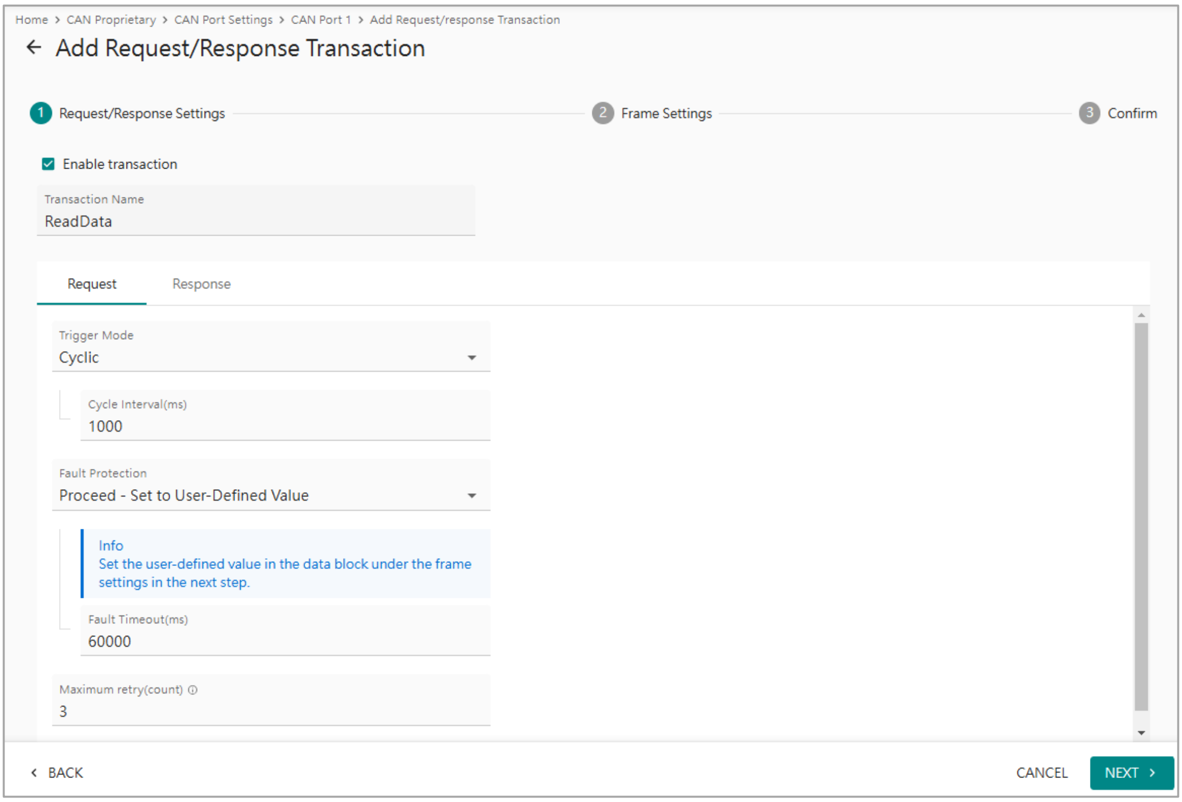
Consume Settings

Transaction Name: consume1
Enable transaction: Enable
Consume Timeout: Enable
Timeout Time(ms): 10000

Frame Settings

CAN-ID: 0x0123
Frame Length(byte): 8

Regarding Request/Response Transaction, the MGate will send a request to the CAN device to query a data, and then wait for its response.



Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Request/response Transaction
← Add Request/Response Transaction
1 Request/Response Settings
2 Frame Settings
3 Confirm
Request
Response
< BACK
CANCEL
NEXT >

☑ Enable transaction

Transaction Name
ReadData

Trigger Mode
Cyclic

Cycle Interval(ms)
1000

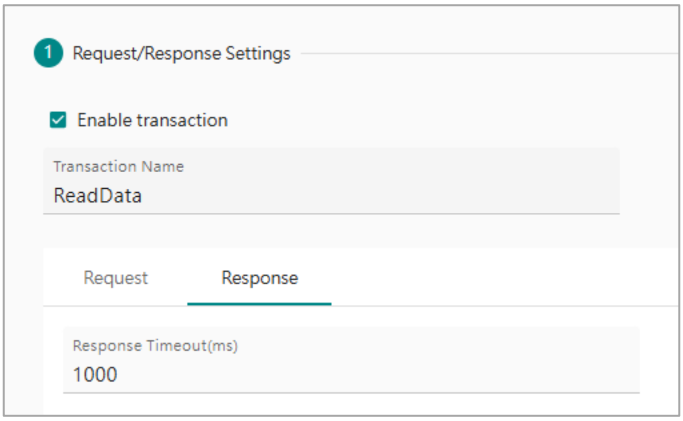
Fault Protection
Proceed - Set to User-Defined Value

Info
Set the user-defined value in the data block under the frame settings in the next step.

Fault Timeout(ms)
60000

Maximum retry(count)
3

Parameter	Value	Default	Description
Transaction Name	(An alphanumeric string)		1 to 64 characters.
Trigger Mode	Cyclic Data Change Boot-up	Cyclic	**Cyclic:** The transaction is sent cyclically at the interval specified in the Cyclic Interval parameter. **Data change:** The transaction is sent when a change in data is detected. **Boot-up:** The transaction is sent once the CAN bus boots up
Cyclic Interval (ms)	10 to 65535	1000	The desired cyclic interval in milliseconds.
Fault Protection	Pause Proceed—Clear data to zero Proceed—Set to User Defined Value	Pause	**Pause:** The gateway will write the same data to the slave device. **Proceed—Clear data to zero:** The gateway will write zero values to the slave device. **Proceed—Set to User Defined Value:** A user-defined value will be written to the slave device.
Fault Timeout (ms)	100 to 65535	60000	Defines the communication timeout on the opposite side.
Maximum retry (count)	0 to 5	0	The request retries counts when a timeout occurred without receiving a response. The response timeout value is set in the Response tab.



1 Request/Response Settings

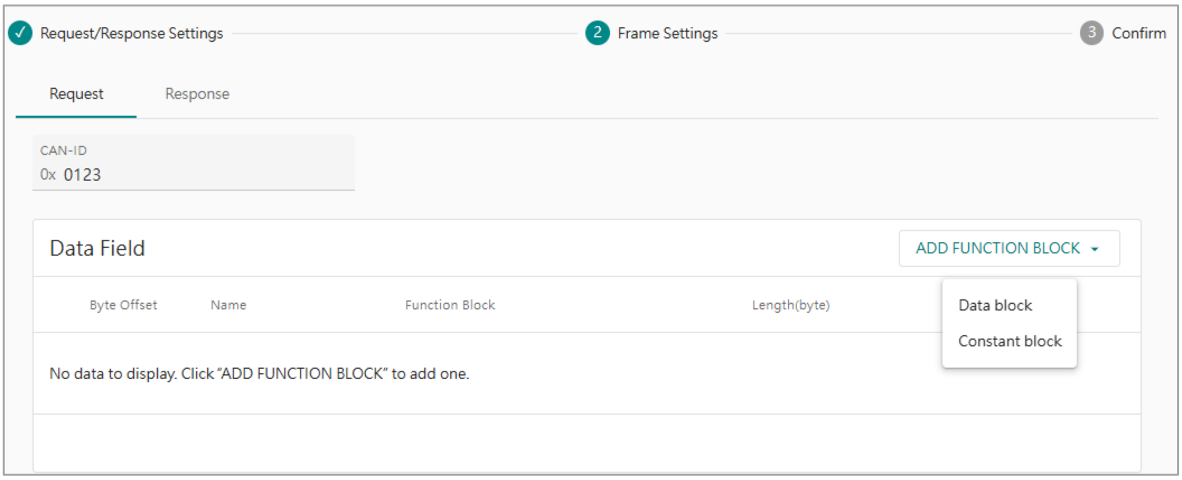
☑ Enable transaction

Transaction Name: ReadData

Response Timeout(ms): 1000

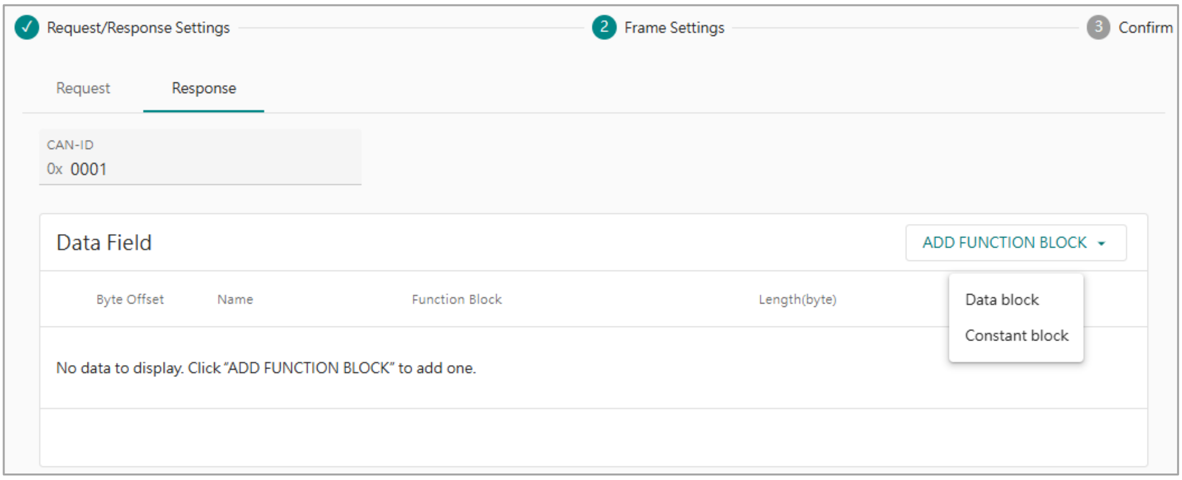
Parameter	Value	Default	Description
Response Timeout (ms)	100 to 65535	1000	The desired response timeout value.

Here, set the request and response frame settings according to the CAN device user manual, including the CAN-ID, Data blocks, or Constant blocks. The block setting is the same as the producer. Refer to Produce Frame Settings’ description.



CAN-ID: 0x 0123

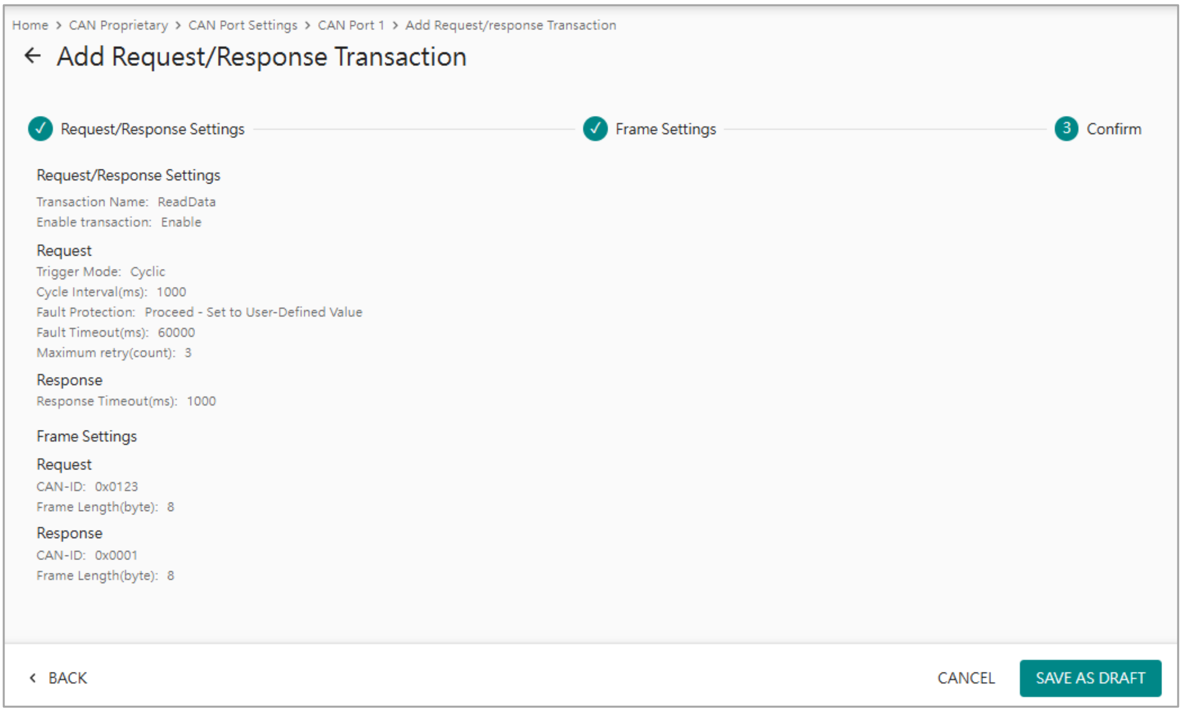
No data to display. Click “ADD FUNCTION BLOCK” to add one.



CAN-ID: 0x 0001

No data to display. Click “ADD FUNCTION BLOCK” to add one.

Confirm the transaction settings. Then click SAVE AS DRAFT.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1 > Add Request/response Transaction

Add Request/Response Transaction

✓ Request/Response Settings ✓ Frame Settings 3 Confirm

Request/Response Settings

Transaction Name: ReadData
Enable transaction: Enable

Request

Trigger Mode: Cyclic
Cycle Interval(ms): 1000
Fault Protection: Proceed - Set to User-Defined Value
Fault Timeout(ms): 60000
Maximum retry(count): 3

Response

Response Timeout(ms): 1000

Frame Settings

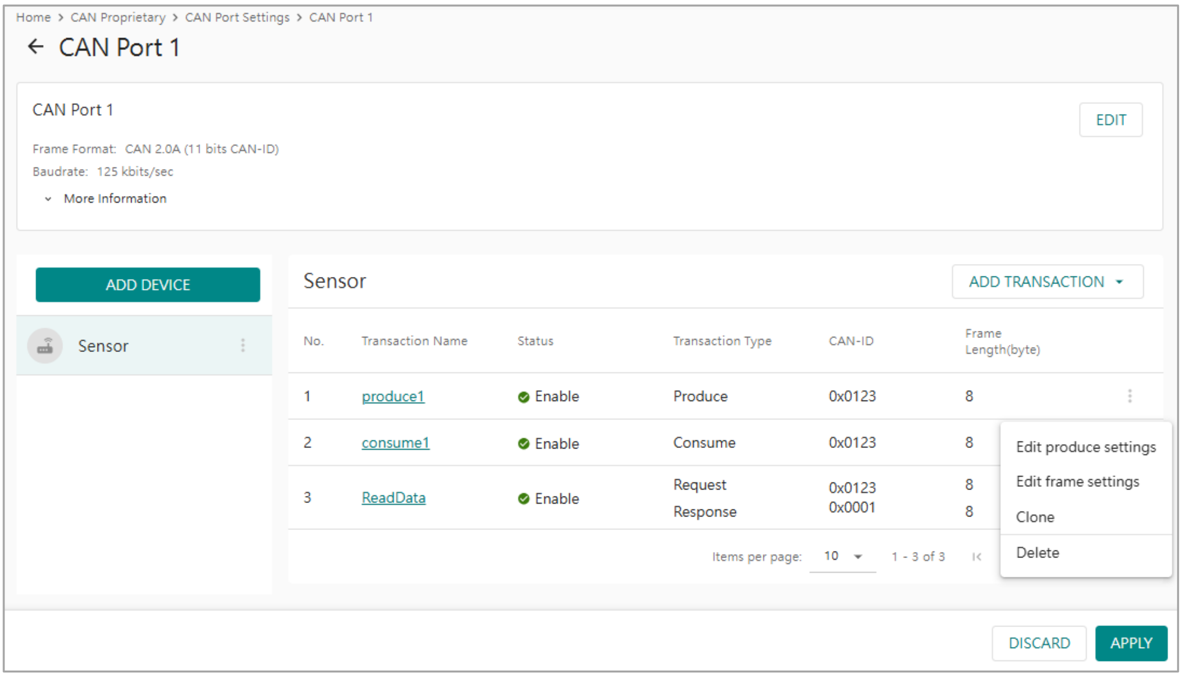
Request

CAN-ID: 0x0123
Frame Length(byte): 8

Response

CAN-ID: 0x0001
Frame Length(byte): 8

After all settings have been created, click the icon on the right-hand side of each transaction to edit, delete or clone it. Finally, click APPLY to activate all settings.


Home > CAN Proprietary > CAN Port Settings > CAN Port 1

CAN Port 1

CAN Port 1

Frame Format: CAN 2.0A (11 bits CAN-ID)
Baudrate: 125 kbits/sec

More Information

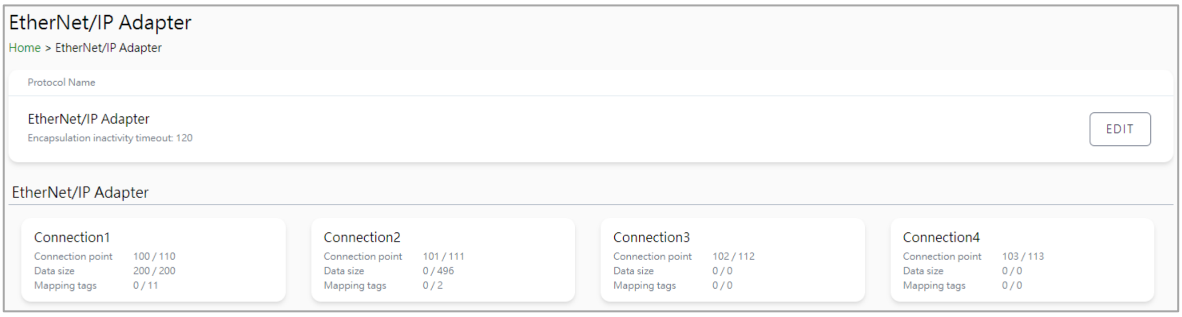
Sensor

No.	Transaction Name	Status	Transaction Type	CAN-ID	Frame Length(byte)
1	produce1	Enable	Produce	0x0123	8
2	consume1	Enable	Consume	0x0123	8
3	ReadData	Enable	Request Response	0x0123 0x0001	8 8

Items per page: 10 1 - 3 of 3

Protocol Settings—EtherNet/IP Adapter Settings

Configure the EtherNet/IP adapter setting on this page.



EtherNet/IP Adapter

Home > EtherNet/IP Adapter

Protocol Name

EtherNet/IP Adapter

Encapsulation inactivity timeout: 120

EtherNet/IP Adapter

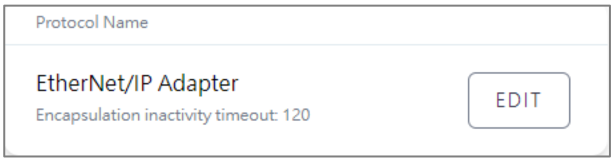
Connection1
Connection point 100 / 110
Data size 200 / 200
Mapping tags 0 / 11

Connection2
Connection point 101 / 111
Data size 0 / 496
Mapping tags 0 / 2

Connection3
Connection point 102 / 112
Data size 0 / 0
Mapping tags 0 / 0

Connection4
Connection point 103 / 113
Data size 0 / 0
Mapping tags 0 / 0

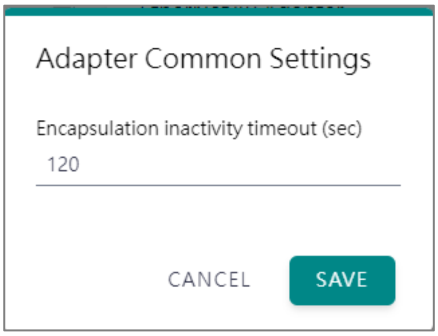
Click **EDIT** to adjust the EtherNet/IP basic settings.



Protocol Name

EtherNet/IP Adapter

Encapsulation inactivity timeout: 120

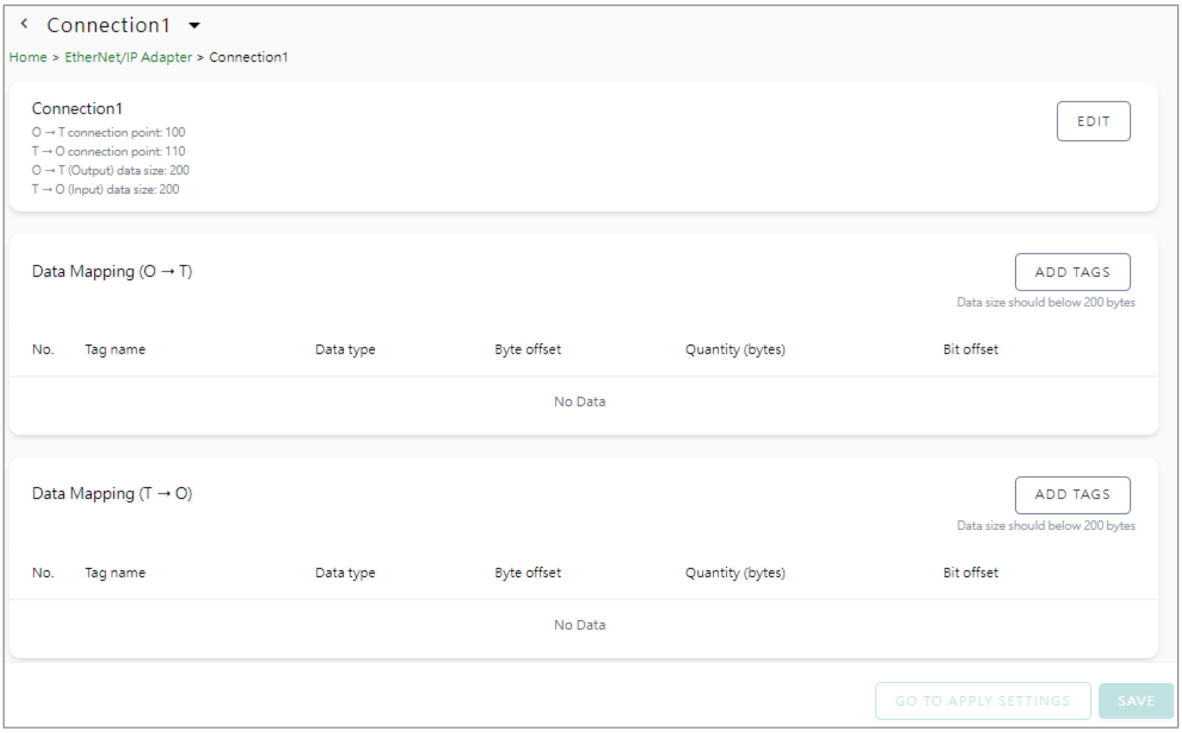


Adapter Common Settings

Encapsulation inactivity timeout (sec)
120

Parameter	Value	Default	Description
Encapsulation inactivity timeout (sec)	0 to 3600, (0 for disable)	120	Unit: second If there is no data exchange in for a while, the Ethernet/IP connection will be disconnected.

Click on the Connection button to add O -T and T-O data.



Connection1

Home > EtherNet/IP Adapter > Connection1

Connection1

O → T connection point: 100
T → O connection point: 110
O → T (Output) data size: 200
T → O (Input) data size: 200

Data Mapping (O → T)

Data size should below 200 bytes

No.	Tag name	Data type	Byte offset	Quantity (bytes)	Bit offset

No Data

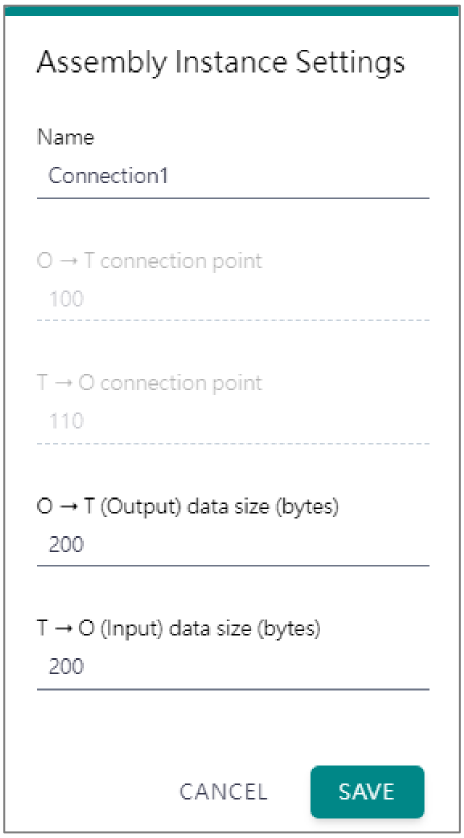
Data Mapping (T → O)

Data size should below 200 bytes

No.	Tag name	Data type	Byte offset	Quantity (bytes)	Bit offset

No Data

Click **EDIT** in the connection column to adjust the connection parameters.



Assembly Instance Settings

Name: Connection1

O → T connection point: 100

T → O connection point: 110

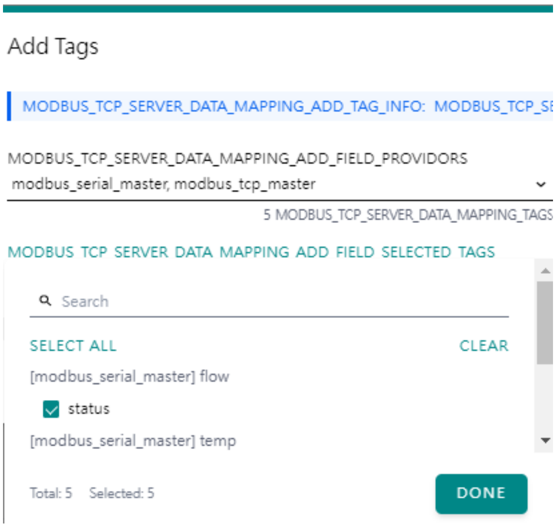
O → T (Output) data size (bytes): 200

T → O (Input) data size (bytes): 200

Parameter	Value	Default	Description
Name		Connection[x]	Name for connection. For example, Connection1
O->T connection point	1 to 2147483647	100	EtherNet/IP connection instance
T->O connection point	1 to 2147483647	110	EtherNet/IP connection instance

Parameter	Value	Default	Description
O->T (Output) data size (bytes)	0 to 496	0	Unit: byte O->T: Originator to Target
T->O (Input) data size (bytes)	0 to 496	0	Unit: byte T->O: Target to Originator

Add Tags for O->T and T-O. Note that the tags must be created in the Modbus client. Click **DONE** after the selection. The selection sequence will also decide the sequence in the EtherNet/IP data frame.



Add Tags

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_TAG_INFO: MODBUS_TCP_SE

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_FIELD_PROVIDORS
modbus_serial_master, modbus_tcp_master

5 MODBUS_TCP_SERVER_DATA_MAPPING_TAGS

MODBUS TCP SERVER DATA MAPPING ADD FIELD SELECTED TAGS

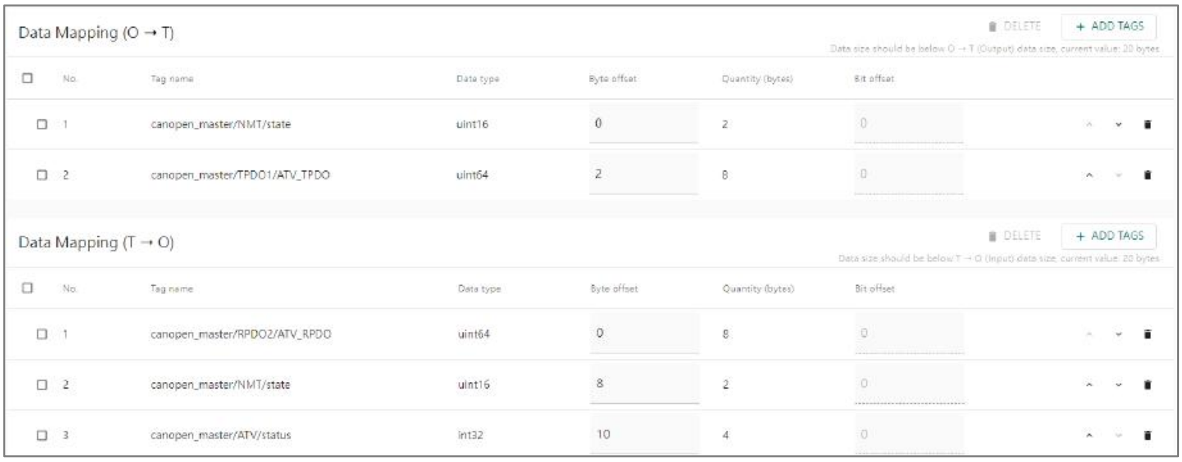
[modbus_serial_master] flow

☑ status

[modbus_serial_master] temp

Total: 5 Selected: 5

The selected tags will display in the data mapping column by default with byte offset. Adjust the offset in the EtherNet/IP IO data frame manually.



Data Mapping (O → T)

Data size should be below O → T (Output) data size, current value: 20 bytes

□	No.	Tag name	Data type	Byte offset	Quantity (bytes)	Bit offset
□	1	canopen_master/NMT/state	uint16	0	2	0
□	2	canopen_master/TPDO1/ATV_TPDO	uint64	2	8	0

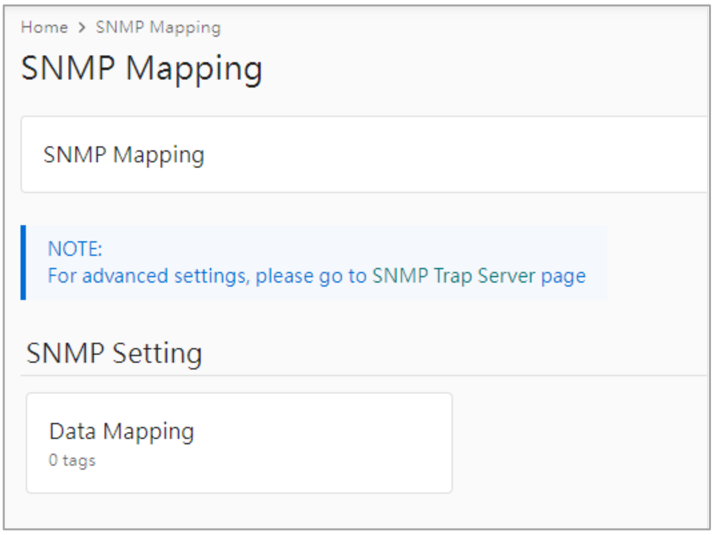
Data Mapping (T → O)

Data size should be below T → O (Input) data size, current value: 20 bytes

□	No.	Tag name	Data type	Byte offset	Quantity (bytes)	Bit offset
□	1	canopen_master/RPDO2/ATV_RPDO	uint64	0	8	0
□	2	canopen_master/NMT/state	uint16	8	2	0
□	3	canopen_master/ATV/status	int32	10	4	0

Protocol Settings—SNMP Mapping Settings

Manage CAN to SNMP mapping data on this page. For detailed SNMP protocol settings, go to the SNMP Trap Server page.



Home > SNMP Mapping

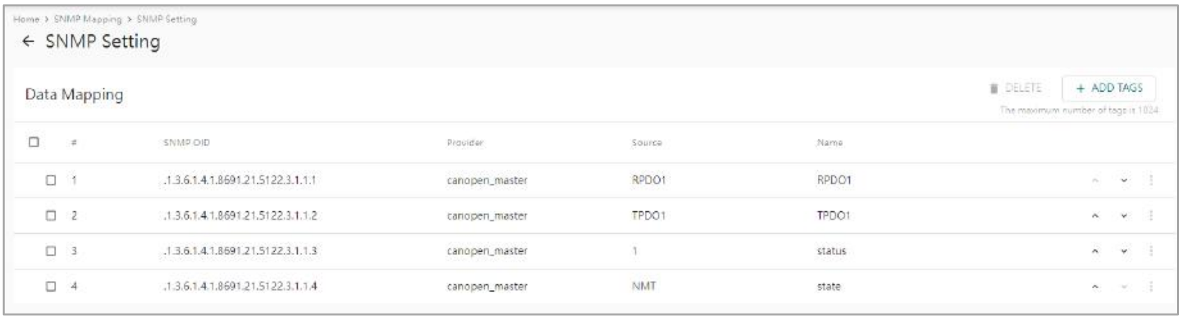
SNMP Mapping

SNMP Mapping

NOTE:
For advanced settings, please go to SNMP Trap Server page

SNMP Setting

Data Mapping
0 tags



Home > SNMP Mapping > SNMP Setting

← SNMP Setting

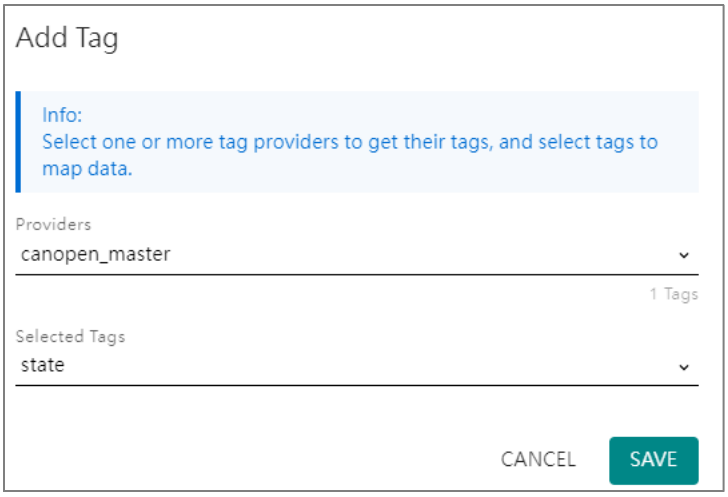
Data Mapping

DELETE | + ADD TAGS

The maximum number of tags is 1024

□	#	SNMP OID	Provider	Source	Name
□	1	.1.3.6.1.4.1.8691.21.5122.3.1.1.1	canopen_master	RPDO1	RPDO1
□	2	.1.3.6.1.4.1.8691.21.5122.3.1.1.2	canopen_master	TPDO1	TPDO1
□	3	.1.3.6.1.4.1.8691.21.5122.3.1.1.3	canopen_master	1	status
□	4	.1.3.6.1.4.1.8691.21.5122.3.1.1.4	canopen_master	NMT	state

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



Add Tag

Info:
Select one or more tag providers to get their tags, and select tags to map data.

Providers: canopen_master

1 Tags

Selected Tags: state

CANCEL | SAVE

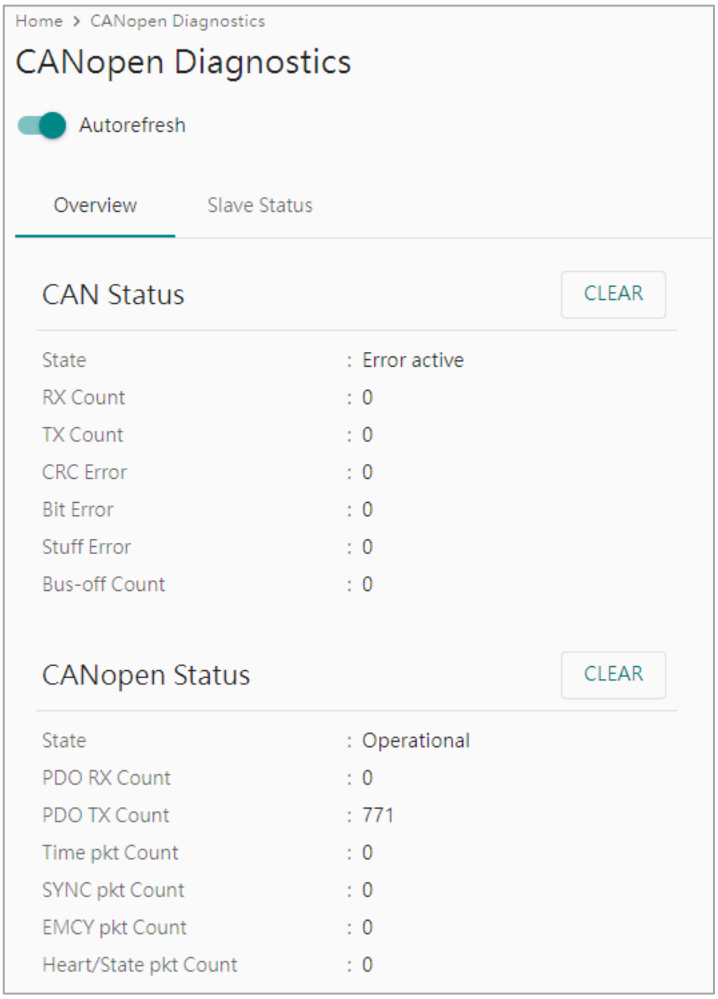
The OID is defined as below:

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
1.3.6.1.4.1.8691.21.5122	mgate5122	{mgate}.5122	Model name
1.3.6.1.4.1.8691.21.5122.1	swMgmt	{mgate5122}.1	SNMP management Information
1.3.6.1.4.1.8691.21.5122.2	trap	{mgate5122}.2	SNMP trap
1.3.6.1.4.1.8691.21.5122.3	mapping	{mgate5122}.3	SNMP mapping
1.3.6.1.4.1.8691.21.5122.3.1	tags	{mapping}.1	Tag mapping
1.3.6.1.4.1.8691.21.5122.3.1.1	array of values	{tags}.1	Tag value
1.3.6.1.4.1.8691.21.5122.3.1.2	array of names	{tags}.2	Tag name
1.3.6.1.4.1.8691.21.5122.3.1.1.x	value of array[x]	{array of values}.x	Index of tag value
1.3.6.1.4.1.8691.21.5122.3.1.2.x	name of array[x]	{array of names}.x	Index of tag name

Diagnostics

Diagnostics—Protocol Diagnostics

Diagnostics—Protocol Diagnostics—CANopen Diagnostics



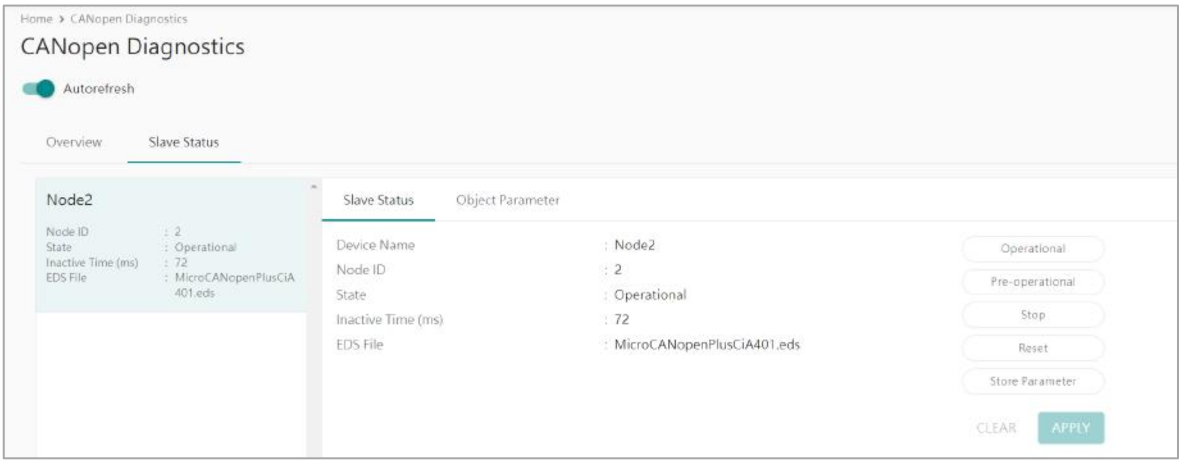
CAN Status

State	: Error active
RX Count	: 0
TX Count	: 0
CRC Error	: 0
Bit Error	: 0
Stuff Error	: 0
Bus-off Count	: 0

CANopen Status

State	: Operational
PDO RX Count	: 0
PDO TX Count	: 771
Time pkt Count	: 0
SYNC pkt Count	: 0
EMCY pkt Count	: 0
Heart/State pkt Count	: 0

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

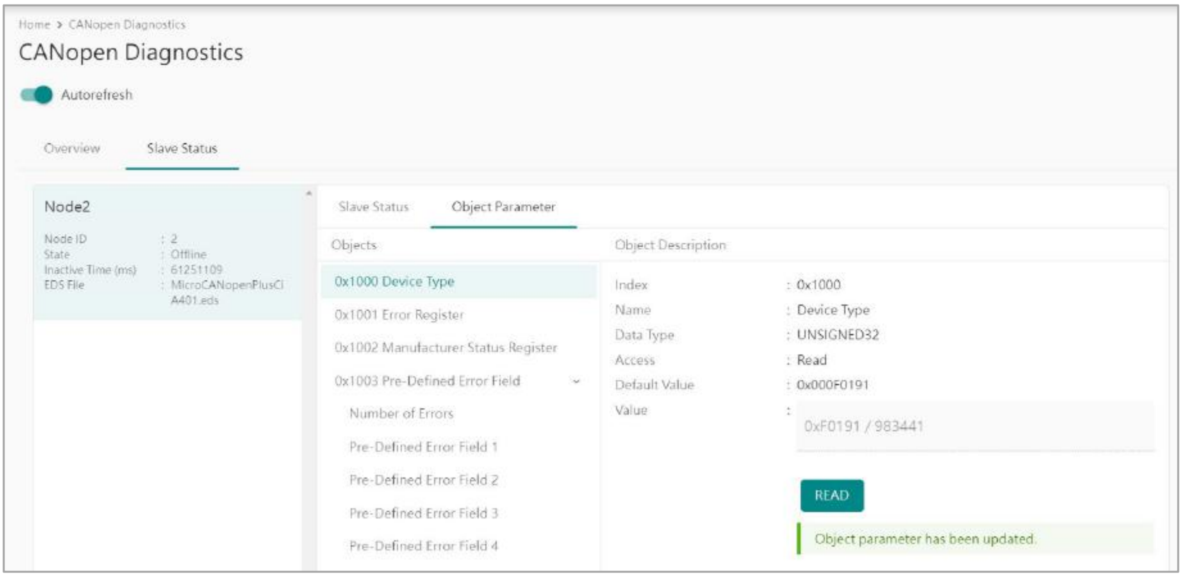


Node2

Node ID : 2
State : Operational
Inactive Time (ms) : 72
EDS File : MicroCANopenPlusCiA401.eds

Device Name : Node2
Node ID : 2
State : Operational
Inactive Time (ms) : 72
EDS File : MicroCANopenPlusCiA401.eds

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


Home > CANopen Diagnostics
CANopen Diagnostics
Autorefresh
Overview
Slave Status
Slave Status
Object Parameter
Objects
0x1000 Device Type
0x1001 Error Register
0x1002 Manufacturer Status Register
0x1003 Pre-Defined Error Field
Number of Errors
Pre-Defined Error Field 1
Pre-Defined Error Field 2
Pre-Defined Error Field 3
Pre-Defined Error Field 4
Object Description
READ

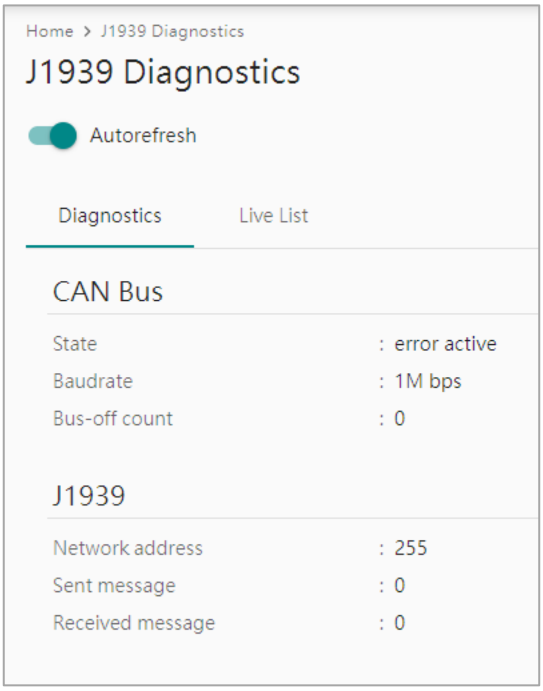
Node2

Node ID : 2
State : Offline
Inactive Time (ms) : 61251109
EDS File : MicroCANopenPlusCiA401.eds

Index : 0x1000
Name : Device Type
Data Type : UNSIGNED32
Access : Read
Default Value : 0x000F0191
Value : 0xF0191 / 983441

Object parameter has been updated.

Diagnostics—Protocol Diagnostics—J1939 Diagnostics



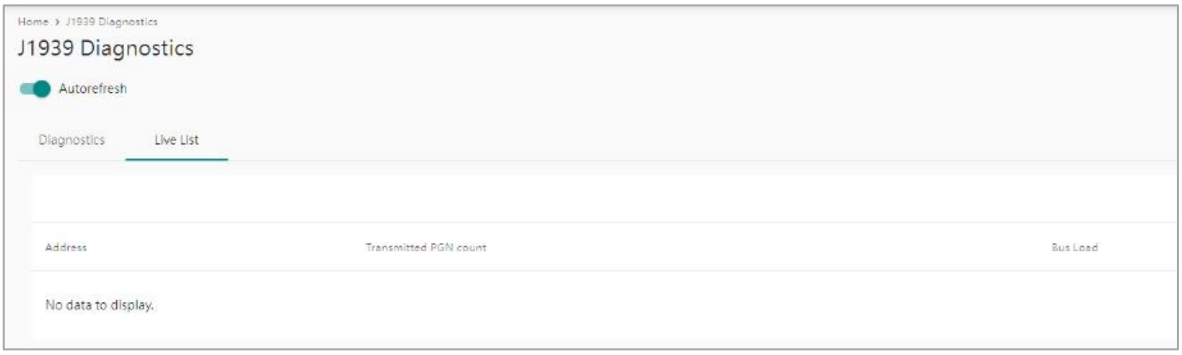
CAN Bus

State : error active
Baudrate : 1M bps
Bus-off count : 0

J1939

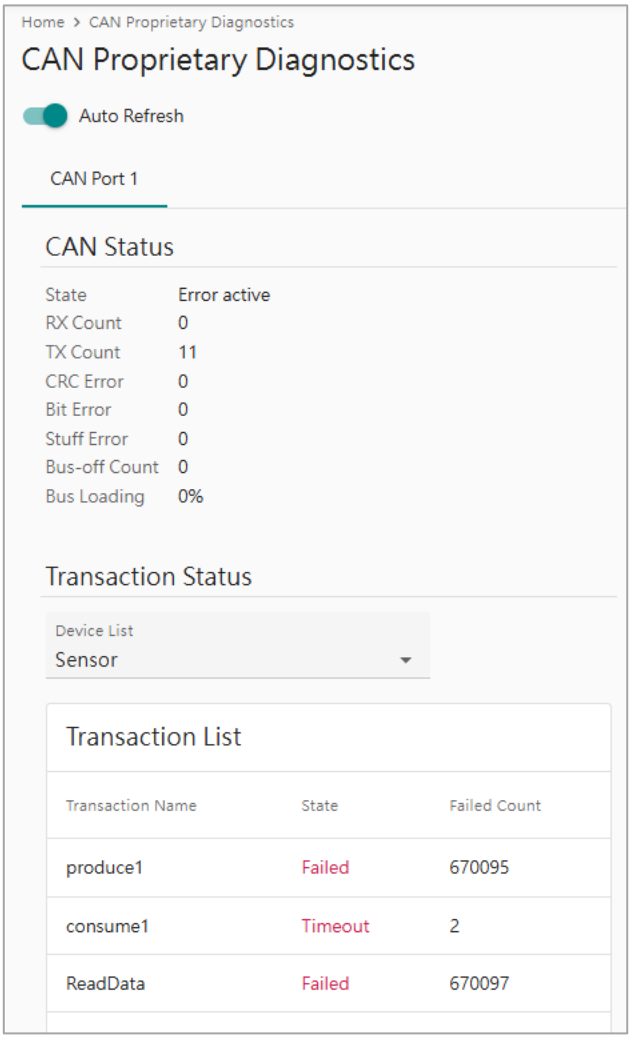
Network address : 255
Sent message : 0
Received message : 0

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



Address	Transmitted PGN count	Bus Load
No data to display.		

Diagnostics—Protocol Diagnostics—CAN Proprietary Diagnostics



Home > CAN Proprietary Diagnostics

CAN Proprietary Diagnostics

Auto Refresh

CAN Port 1

CAN Status

State	Error active
RX Count	0
TX Count	11
CRC Error	0
Bit Error	0
Stuff Error	0
Bus-off Count	0
Bus Loading	0%

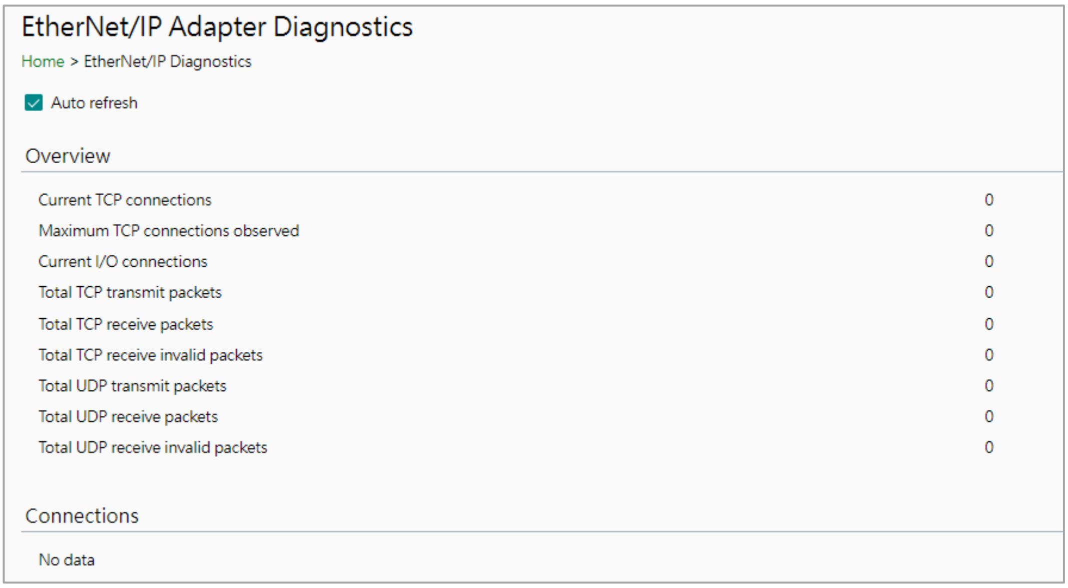
Transaction Status

Device List: Sensor

Transaction List

Transaction Name	State	Failed Count
produce1	Failed	670095
consume1	Timeout	2
ReadData	Failed	670097

Diagnostics—Protocol Diagnostics—EtherNet/IP Diagnostics



EtherNet/IP Adapter Diagnostics

Home > EtherNet/IP Diagnostics

☑ Auto refresh

Overview

Current TCP connections	0
Maximum TCP connections observed	0
Current I/O connections	0
Total TCP transmit packets	0
Total TCP receive packets	0
Total TCP receive invalid packets	0
Total UDP transmit packets	0
Total UDP receive packets	0
Total UDP receive invalid packets	0

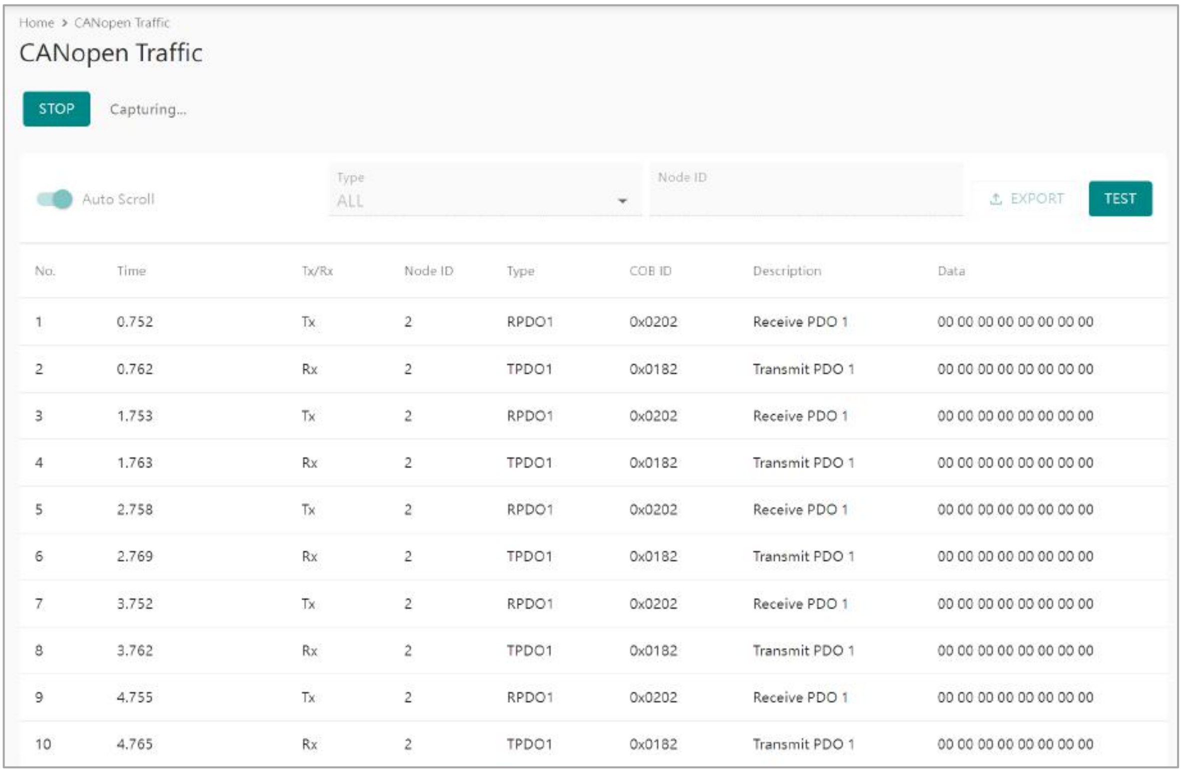
Connections

No data

Diagnostics—Protocol Traffic

Diagnostics—Protocol Traffic—CANopen Traffic

Click **START** to start traffic log.



Home > CANopen Traffic

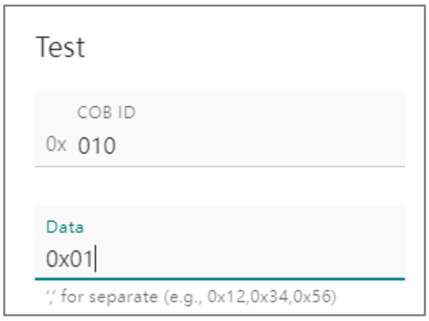
CANopen Traffic

Type: ALL

Node ID:

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.



Test

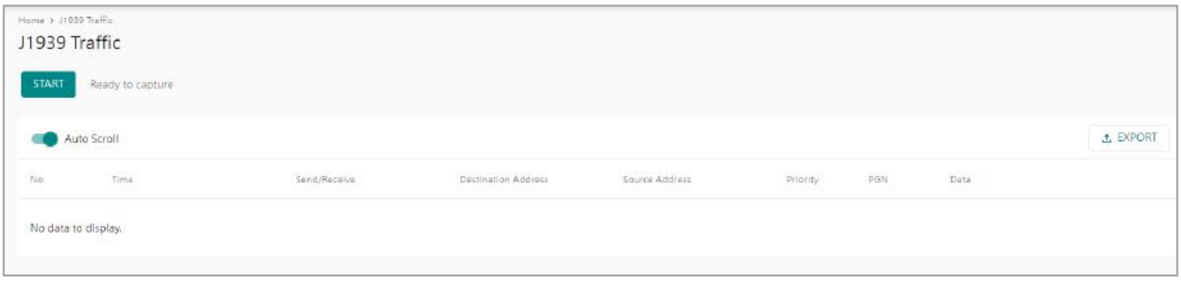
COB ID: 0x 010

Data: 0x01

',' for separate (e.g., 0x12,0x34,0x56)

Diagnostics—Protocol Traffic—J1939 Traffic

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



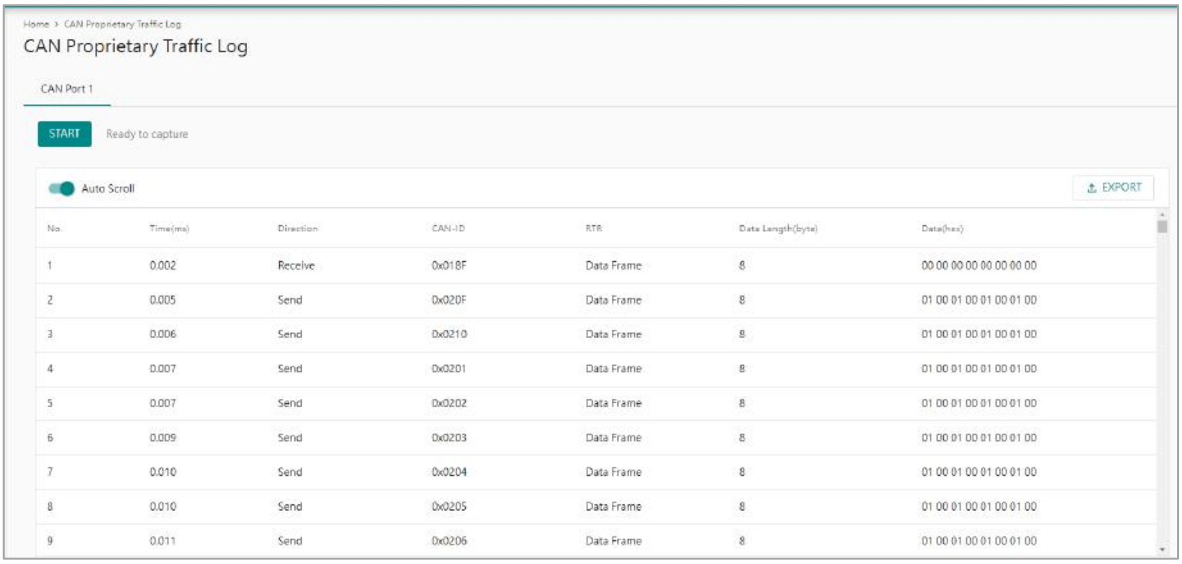
Home > J1939 Traffic

J1939 Traffic

No.	Time	Send/Receive	Destination Address	Source Address	Priority	PGN	Data

No data to display.

Diagnostics—Protocol Traffic—CAN Proprietary Traffic

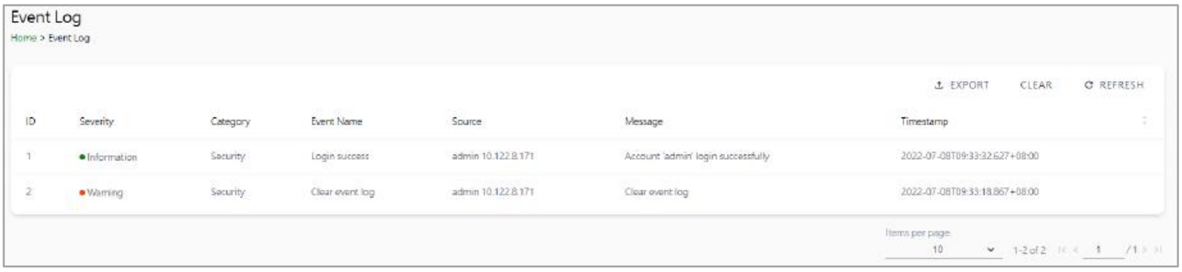

Home > CAN Proprietary Traffic Log
CAN Proprietary Traffic Log
CAN Port 1
START
Ready to capture
Auto Scroll
EXPORT

No.	Time(ms)	Direction	CAN-ID	RTR	Data Length(byte)	Data(hex)
1	0.002	Receive	0x018F	Data Frame	8	00 00 00 00 00 00 00 00
2	0.005	Send	0x020F	Data Frame	8	01 00 01 00 01 00 01 00
3	0.006	Send	0x0210	Data Frame	8	01 00 01 00 01 00 01 00
4	0.007	Send	0x0201	Data Frame	8	01 00 01 00 01 00 01 00
5	0.007	Send	0x0202	Data Frame	8	01 00 01 00 01 00 01 00
6	0.009	Send	0x0203	Data Frame	8	01 00 01 00 01 00 01 00
7	0.010	Send	0x0204	Data Frame	8	01 00 01 00 01 00 01 00
8	0.010	Send	0x0205	Data Frame	8	01 00 01 00 01 00 01 00
9	0.011	Send	0x0206	Data Frame	8	01 00 01 00 01 00 01 00

Diagnostics—Event Log

Diagnostics—Event Log—Log View

Review and export all event information in the event log.



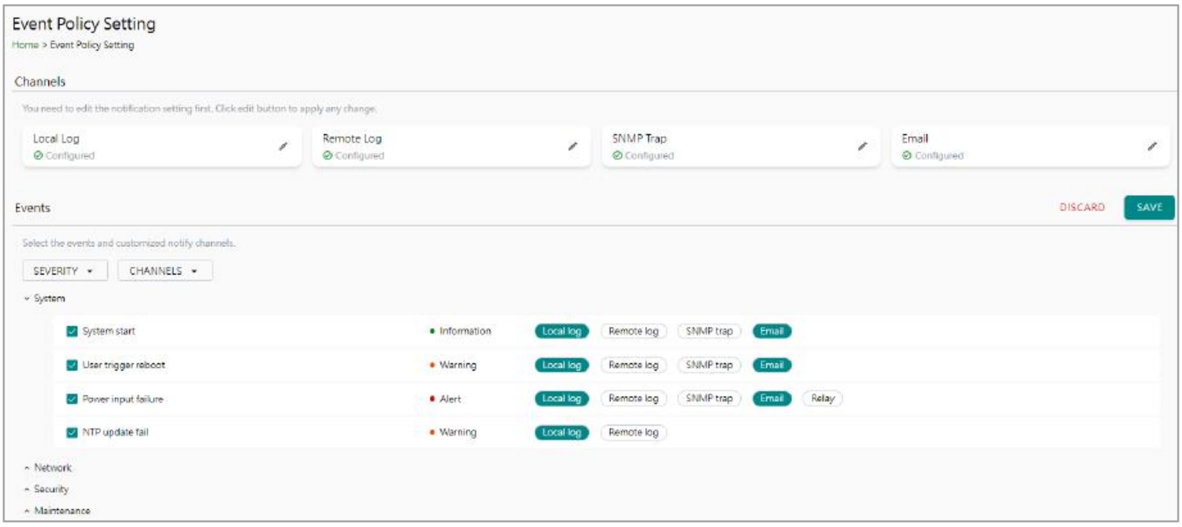
ID	Severity	Category	Event Name	Source	Message	Timestamp
1	● Information	Security	Login success	admin 10.122.8.171	Account 'admin' login successfully	2022-07-08T09:33:32.627+08:00
2	● Warning	Security	Clear event log	admin 10.122.8.171	Clear event log	2022-07-08T09:33:18.867+08:00

Diagnostics—Event Log—Policy Settings

The event policy settings allow the MGate to record important events in the Remote Log to Syslog server and Local Log, storing up to 10,000 events.

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.

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. Select the channels you want to use by clicking the channel name. After changing the settings, remember to SAVE it.



Event Policy Setting

Home > Event Policy Setting

Channels

You need to edit the notification setting first. Click edit button to apply any change.

Local Log	Configured
Remote Log	Configured
SNMP Trap	Configured
Email	Configured

Events

Select the events and customized notify channels.

System

☑ System start	● Information	Local log	Remote log	SNMP trap	Email	
☑ User trigger reboot	● Warning	Local log	Remote log	SNMP trap	Email	
☑ Power input failure	● Alert	Local log	Remote log	SNMP trap	Email	Relay
☑ NTP update fail	● Warning	Local log	Remote log			

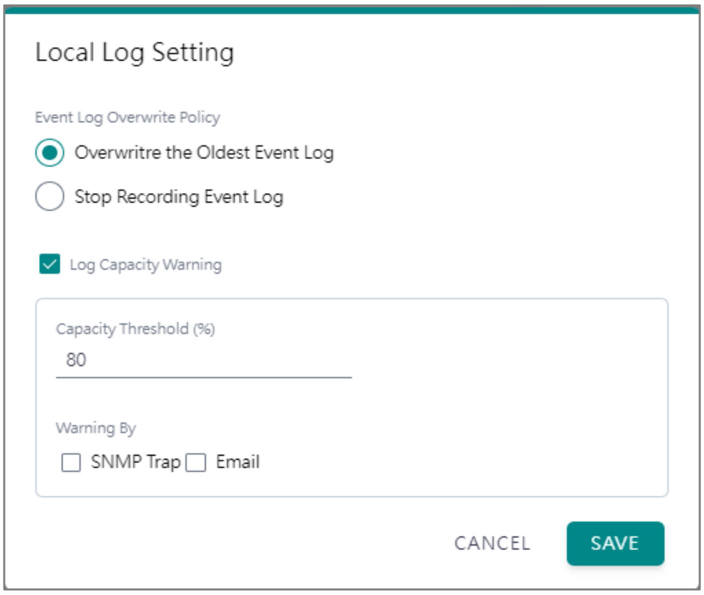
Network

Security

Maintenance

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 state changed; CAN bus-off; slave initialization failed
J1939	CAN bus-off
CAN proprietary	CAN Error Passive, CAN bus-off, Transaction Success, Transaction Failed, Transaction Timeout

Local Log Settings



Local Log Setting

Event Log Overwrite Policy

● Overwritre the Oldest Event Log

○ Stop Recording Event Log

☑ Log Capacity Warning

Capacity Threshold (%)

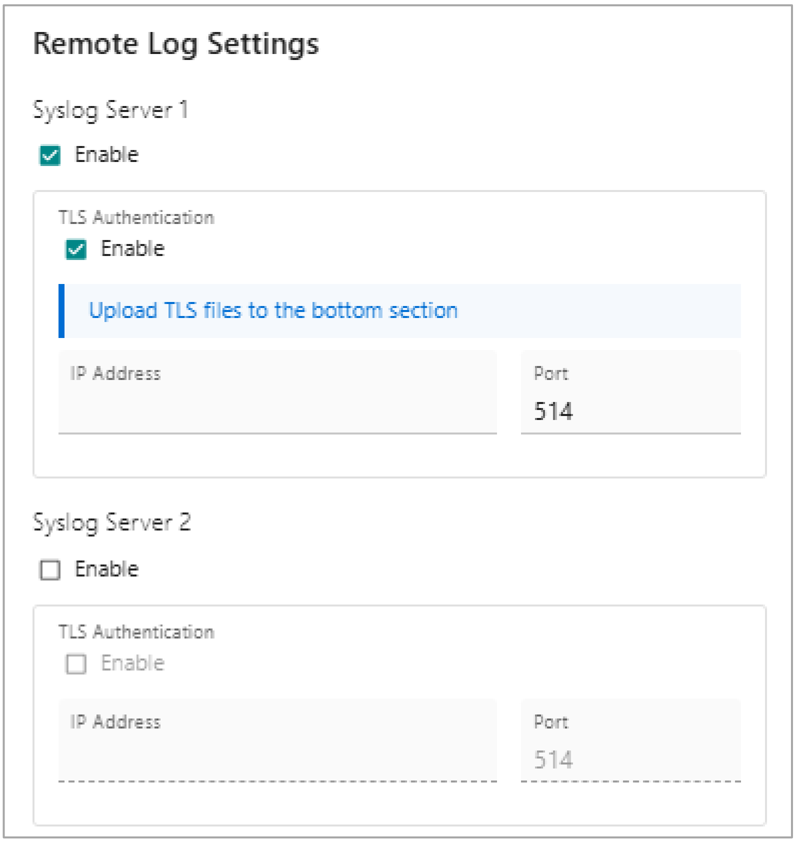
80

Warning By

□ SNMP Trap □ Email

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

Remote Log Settings



Remote Log Settings

Syslog Server 1

☑ Enable

TLS Authentication

☑ Enable

Upload TLS files to the bottom section

IP Address

Port

514

Syslog Server 2

□ Enable

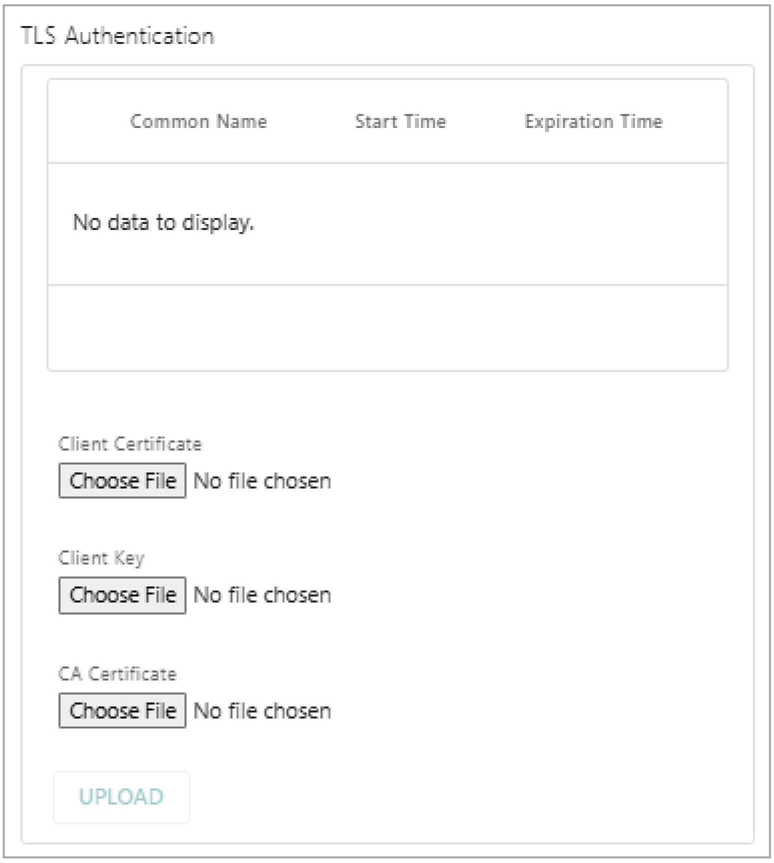
TLS Authentication

□ Enable

IP Address

Port

514


TLS Authentication

Common Name	Start Time	Expiration Time
No data to display.		

Client Certificate

No file chosen

Client Key

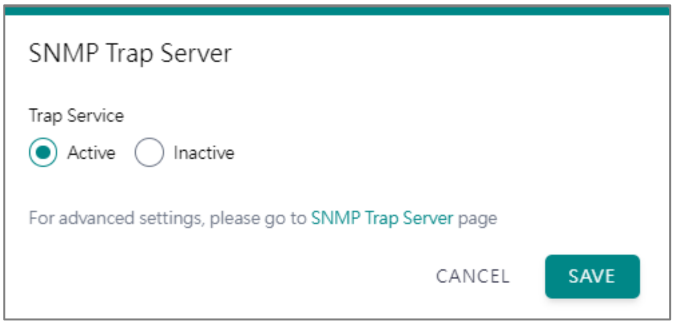
No file chosen

CA Certificate

No file chosen

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. Note that TLS files must be uploaded for a successful connection.

SNMP Trap Settings

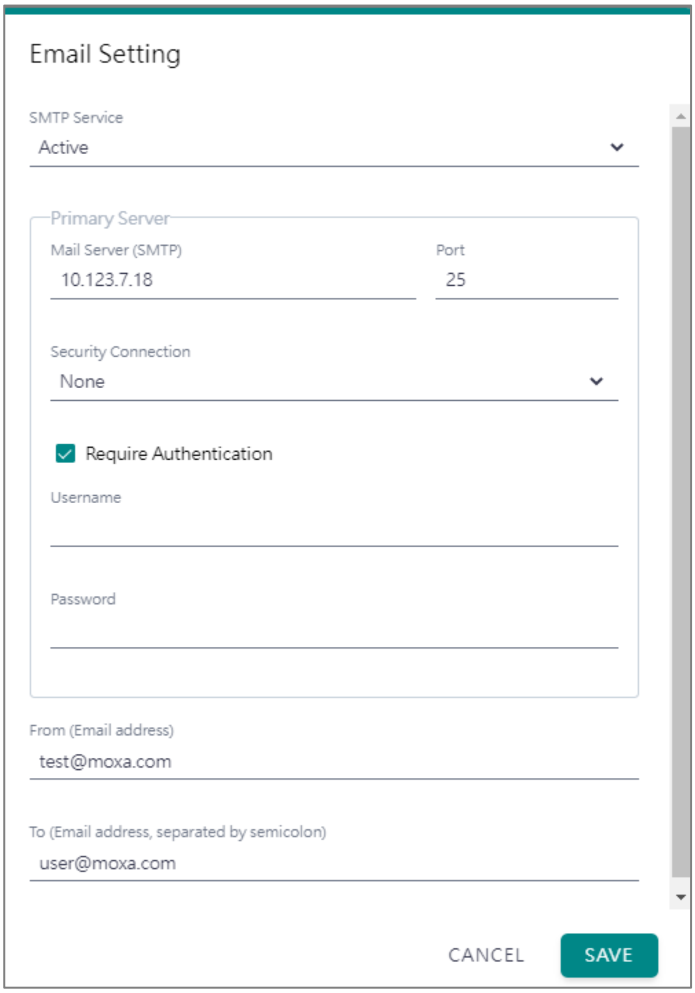

SNMP Trap Server

Trap Service

● Active ○ Inactive

For advanced settings, please go to SNMP Trap Server page

Email Settings


Email Setting

SMTP Service: Active

Primary Server

Mail Server (SMTP): 10.123.7.18

Port: 25

Security Connection: None

☑ Require Authentication

Username:

Password:

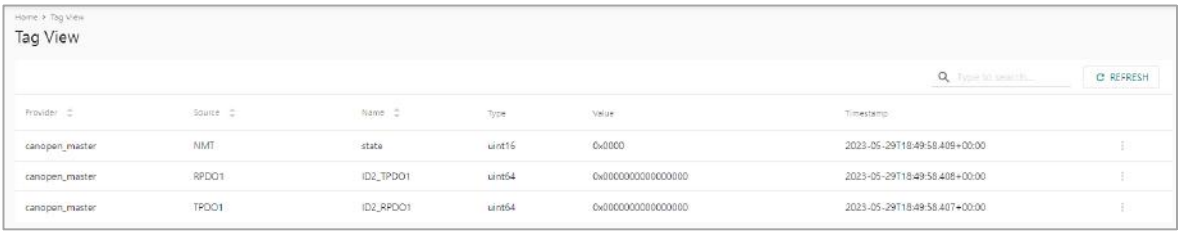
From (Email address): test@moxa.com

To (Email address, separated by semicolon): user@moxa.com

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

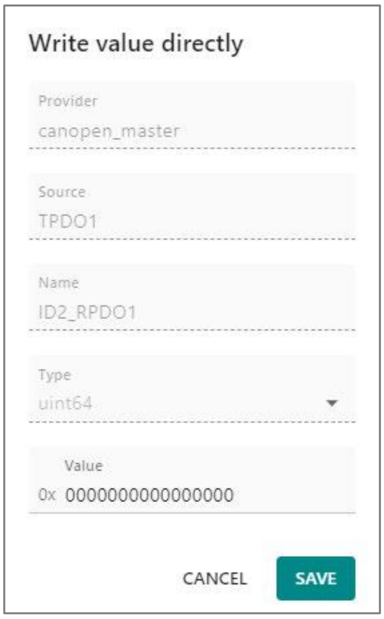
Diagnostics—Tag View

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. For example, when the CANopen_master NMT state showing the master current state, 0 means the master is in operational mode, 1 it is in preoperational mode, and 2 it is stop mode.



Provider	Source	Name	Type	Value	Timestamp
canopen_master	NMT	state	uint16	0x0000	2023-05-29T18:49:58.409+00:00
canopen_master	RPDO1	ID2_TPDO1	uint64	0x0000000000000000	2023-05-29T18:49:58.408+00:00
canopen_master	TPDO1	ID2_RPDO1	uint64	0x0000000000000000	2023-05-29T18:49:58.407+00:00

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



Write value directly

Provider: canopen_master

Source: TPDO1

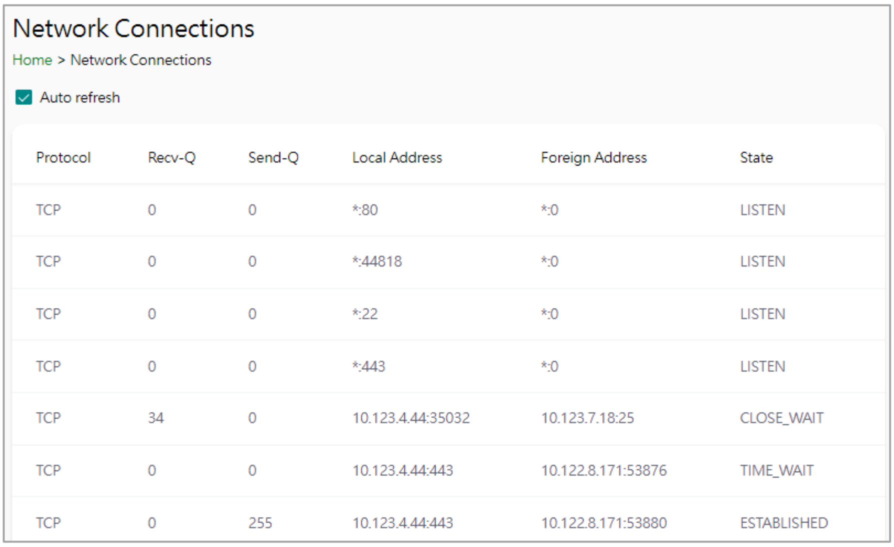
Name: ID2_RPDO1

Type: uint64

Value: 0x 0000000000000000

Diagnostics—Network Connections

See network-related information, including protocol, address, and state.



Network Connections

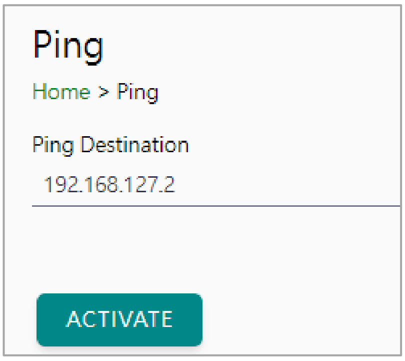
Home > Network Connections

☑ Auto refresh

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	*:80	*:0	LISTEN
TCP	0	0	*:44818	*:0	LISTEN
TCP	0	0	*:22	*:0	LISTEN
TCP	0	0	*:443	*:0	LISTEN
TCP	34	0	10.123.4.44:35032	10.123.7.18:25	CLOSE_WAIT
TCP	0	0	10.123.4.44:443	10.122.8.171:53876	TIME_WAIT
TCP	0	255	10.123.4.44:443	10.122.8.171:53880	ESTABLISHED

Diagnostics—Ping

This network testing function is available only on the web console. The MGate gateway will send an ICMP packet through the network to a specified host; the web console will immediately display the result.



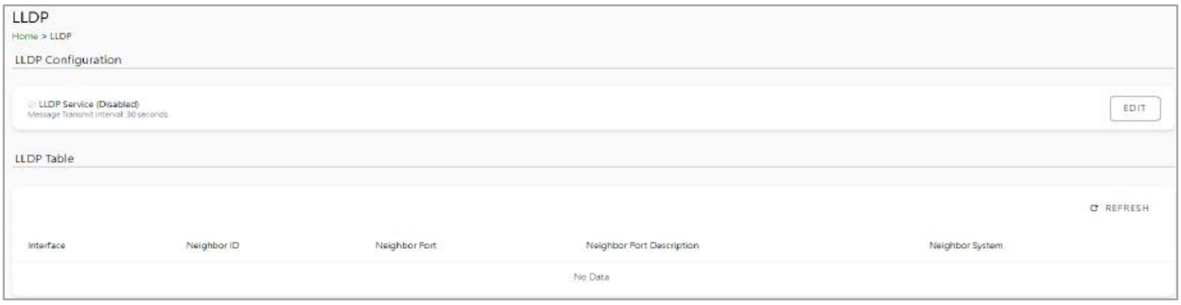
Ping

Home > Ping

Ping Destination: 192.168.127.2

Diagnostics—LLDP

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.



LLDP

Home > LLDP

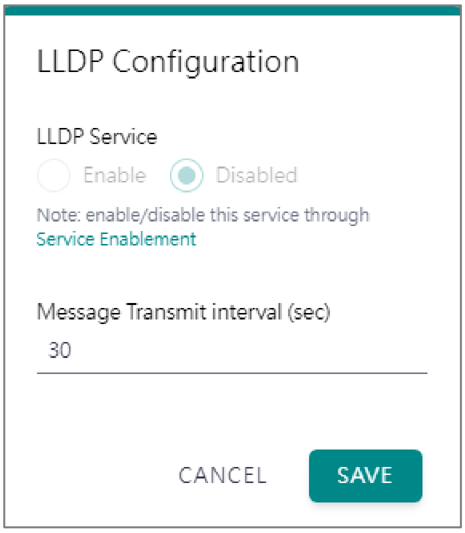
LLDP Configuration

○ LLDP Service (Disabled)
Message Transmit interval: 30 seconds

LLDP Table

Interface	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System
No Data				

After clicking EDIT, to enable or disable the LLDP service, click the Service hyperlink, or go to Security > Service page to change its status.



LLDP Configuration

LLDP Service

○ Enable ● Disabled

Note: enable/disable this service through Service Enablement

Message Transmit interval (sec)

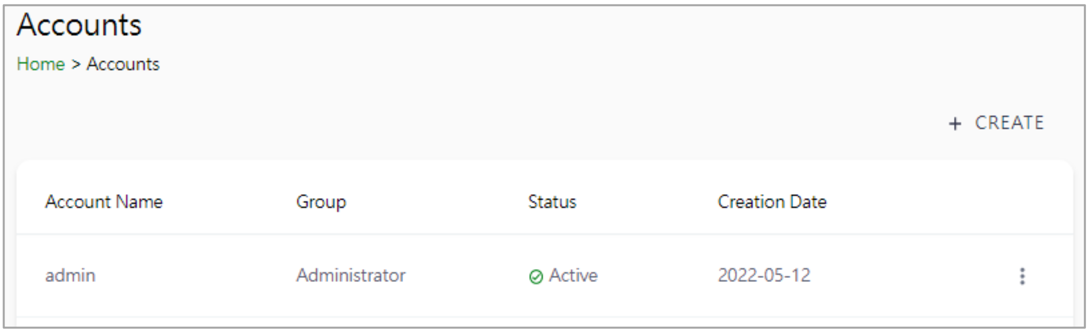
30

Security

To secure your MGate, refer to the following security functions and configure it according to your requirements. We also provide a guideline of recommended steps as best practices for secure configurations in most applications. For this, refer to the Security Hardening Guide for the MGate 5000 Series.

Security—Account Management

Security—Account Management—Accounts

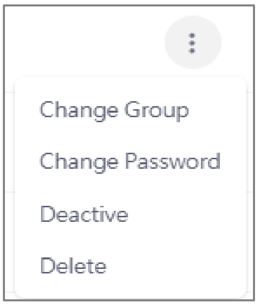


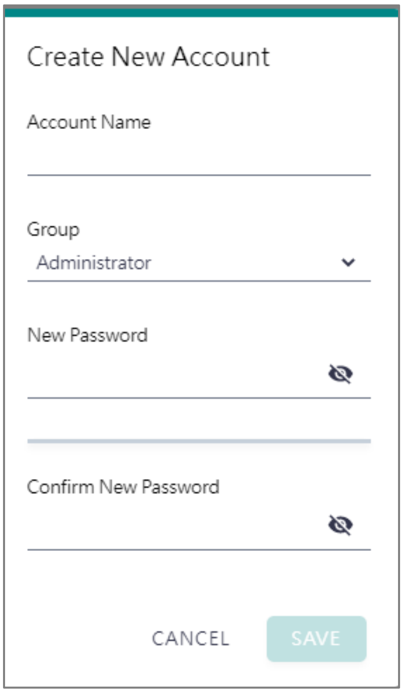
Accounts

Home > Accounts

Account Name	Group	Status	Creation Date
admin	Administrator	✓ Active	2022-05-12

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




Create New Account

Account Name

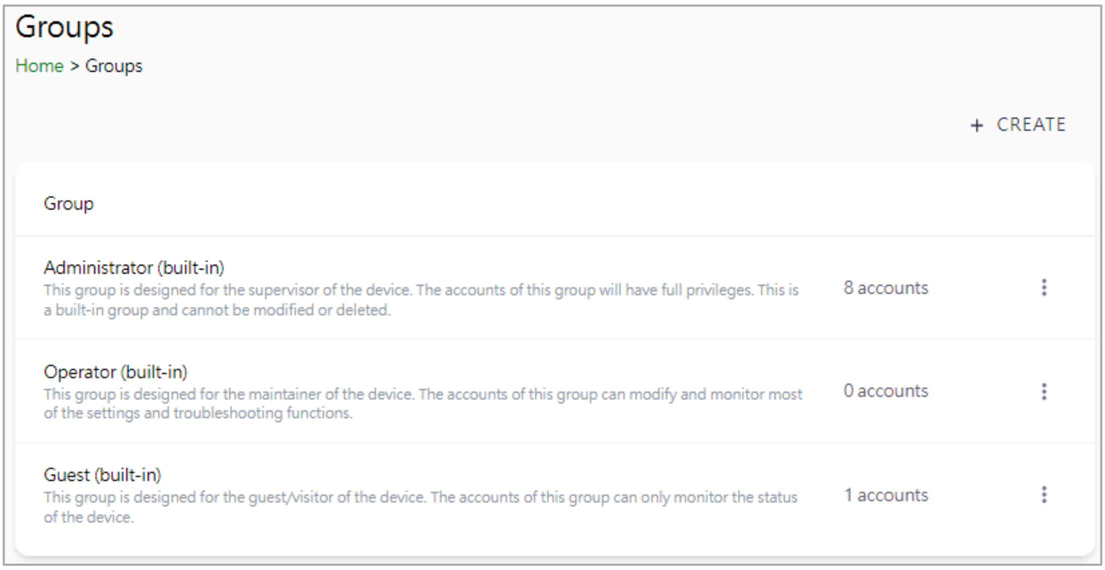
Group
Administrator

New Password

Confirm New Password

Parameters	Value	Description
Group	Administrator, Operator, Guest	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. Create your own group for account management.

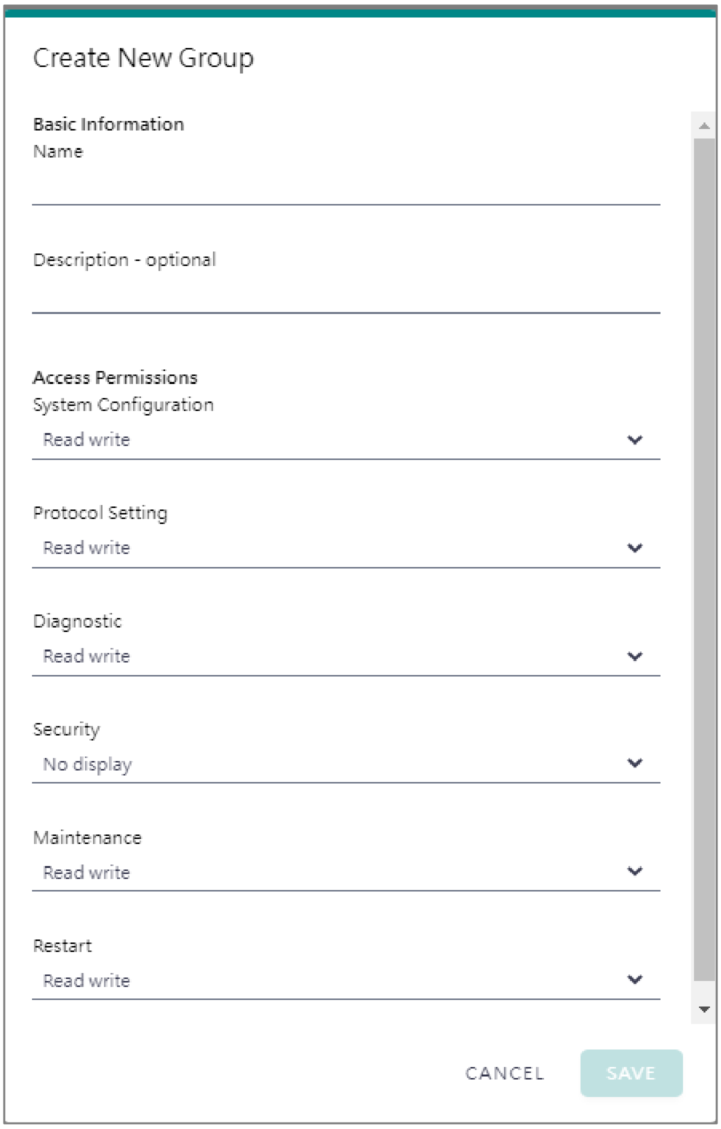
Security—Account Management—Groups


Groups

Home > Groups

Group		
Administrator (built-in) This group is designed for the supervisor of the device. The accounts of this group will have full privileges. This is a built-in group and cannot be modified or deleted.	8 accounts	⋮
Operator (built-in) This group is designed for the maintainer of the device. The accounts of this group can modify and monitor most of the settings and troubleshooting functions.	0 accounts	⋮
Guest (built-in) This group is designed for the guest/visitor of the device. The accounts of this group can only monitor the status of the device.	1 accounts	⋮

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



Create New Group

Basic Information

Name

Description - optional

Access Permissions

System Configuration: Read write

Protocol Setting: Read write

Diagnostic: Read write

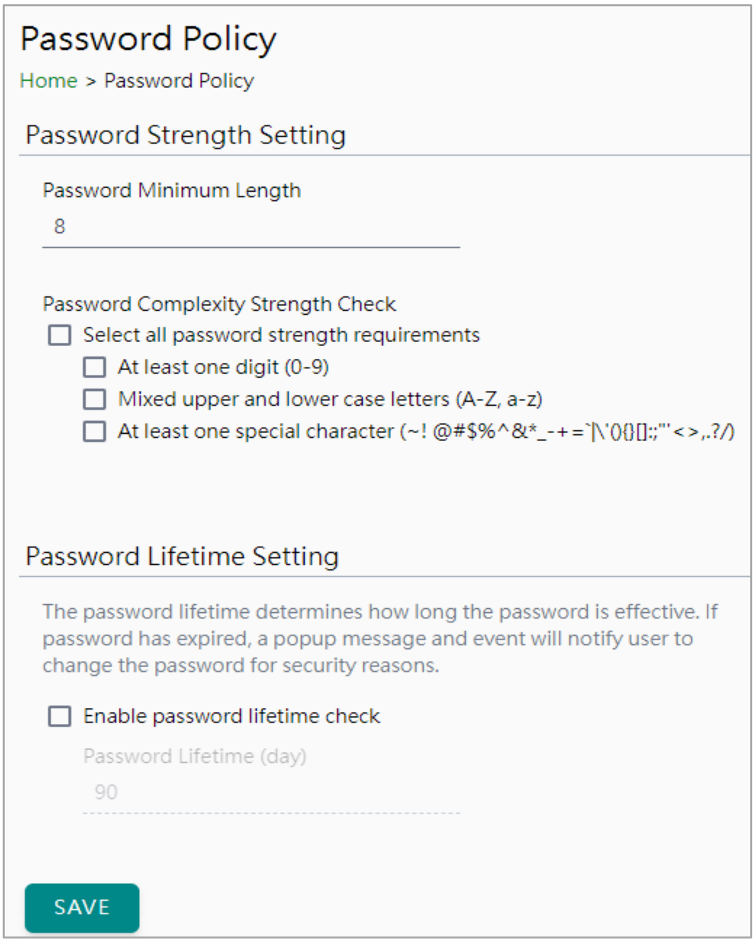
Security: No display

Maintenance: Read write

Restart: Read write

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



Password Policy

Home > Password Policy

Password Strength Setting

Password Minimum Length

8

Password Complexity Strength Check

□ Select all password strength requirements

□ At least one digit (0-9)

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

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

Password Lifetime Setting

The password lifetime determines how long the password is effective. If password has expired, a popup message and event will notify user to change the password for security reasons.

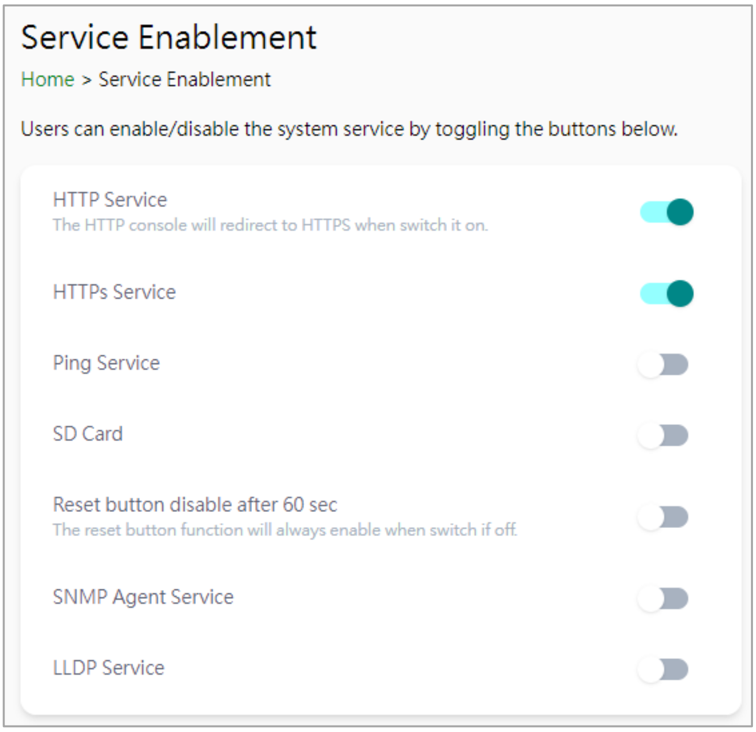
□ Enable password lifetime check

Password Lifetime (day)

90

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



Service Enablement

Home > Service Enablement

Users can enable/disable the system service by toggling the buttons below.

HTTP Service
The HTTP console will redirect to HTTPS when switch it on.

HTTPs Service

Ping Service

SD Card

Reset button disable after 60 sec
The reset button function will always enable when switch if off.

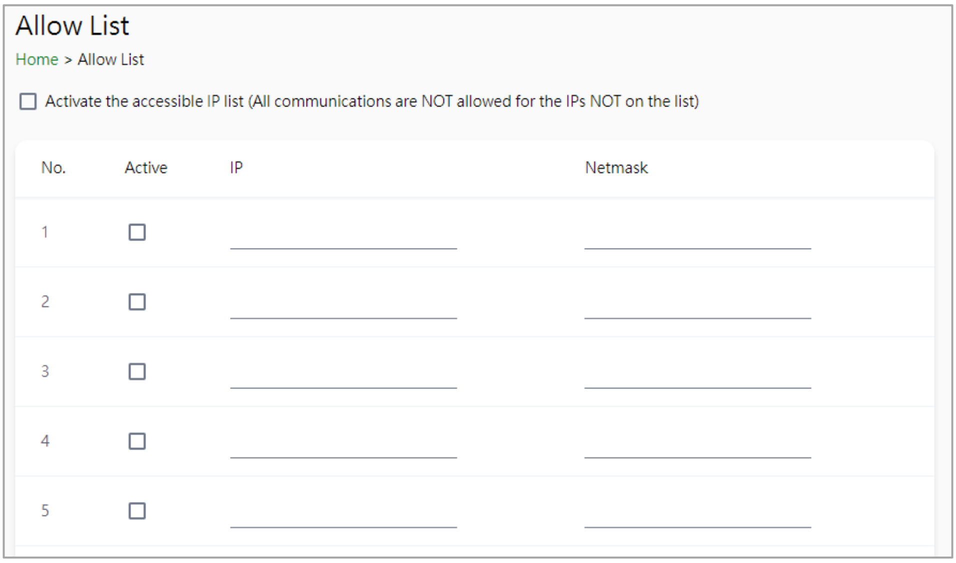
SNMP Agent Service

LLDP 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, you 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.



Allow List

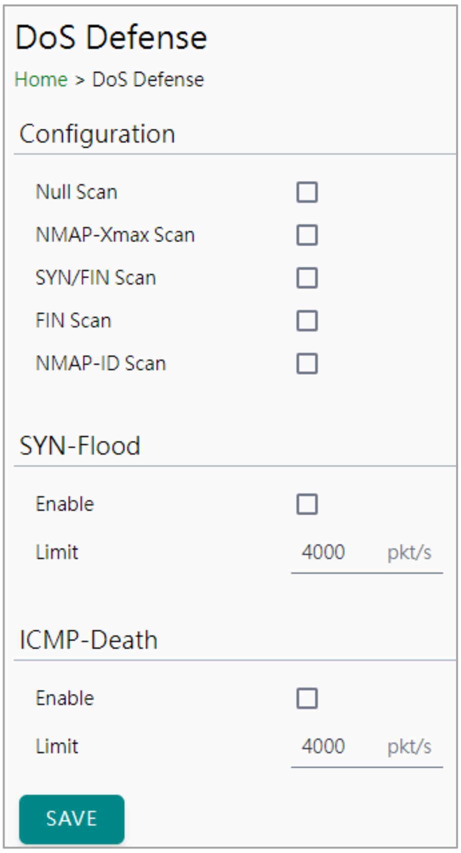
Home > Allow List

☐ Activate the accessible IP list (All communications are NOT allowed for the IPs NOT on the list)

No.	Active	IP	Netmask
1	☐		
2	☐		
3	☐		
4	☐		
5	☐		

Security—DoS Defense

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. Select from the following options to counter DoS attacks.



DoS Defense

Home > DoS Defense

Configuration

Null Scan ☐

NMAP-Xmax Scan ☐

SYN/FIN Scan ☐

FIN Scan ☐

NMAP-ID Scan ☐

SYN-Flood

Enable ☐

Limit 4000 pkt/s

ICMP-Death

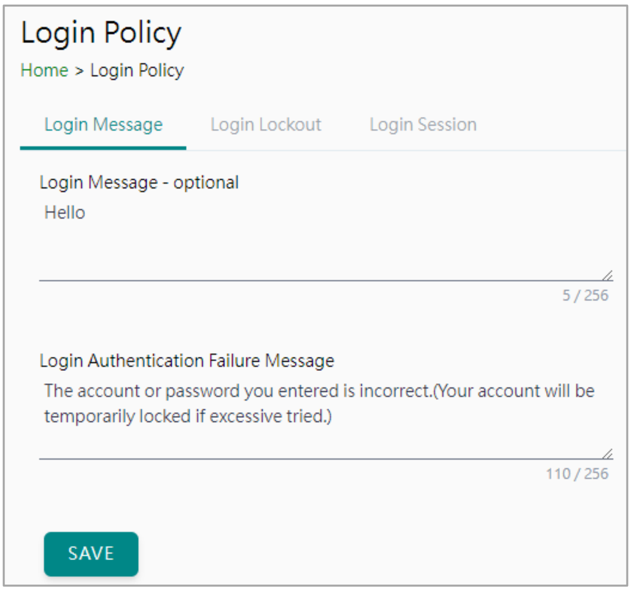
Enable ☐

Limit 4000 pkt/s

Security—Login Policy

Login Message

Input a message for Login or for Login authentication failure messages.



Login Policy

Home > Login Policy

Login Message - optional

Hello

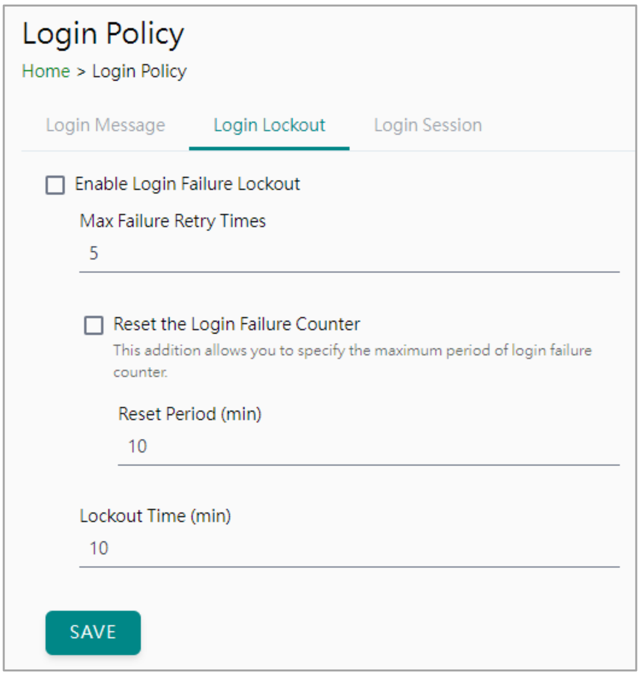
5 / 256

Login Authentication Failure Message

The account or password you entered is incorrect.(Your account will be temporarily locked if excessive tried.)

110 / 256

Login Lockout



Login Policy

Home > Login Policy

☐ Enable Login Failure Lockout

Max Failure Retry Times

5

☐ Reset the Login Failure Counter

This addition allows you to specify the maximum period of login failure counter.

Reset Period (min)

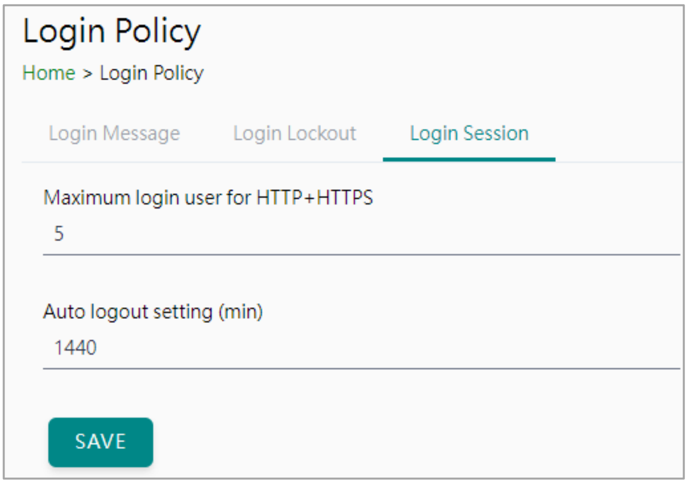
10

Lockout Time (min)

10

Parameter	Value	Description
Max Failure Retry Times	1 to 10 (default 5)	Specify the maximum number of failures reties. If the retry times are exceeded, the MGate will lock out for that account login.
Reset Period (min)	1 to 1440 (default 10)	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



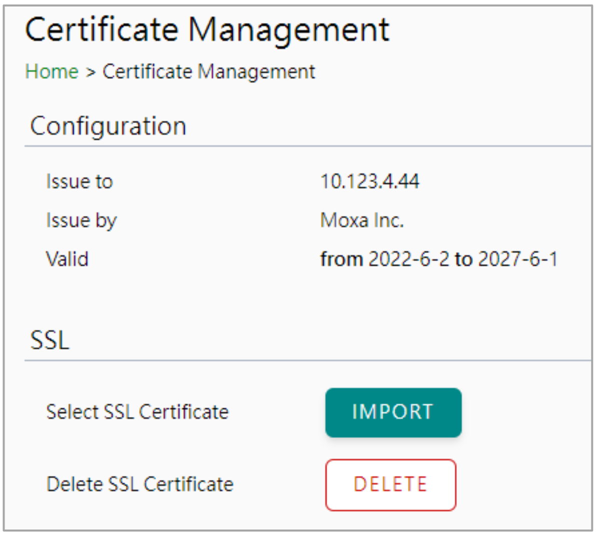
Maximum login user for HTTP+HTTPS: 5

Auto logout setting (min): 1440

Parameter	Value	Description
Maximum login users for HTTP+HTTPS	1 to 10 (default 5)	The number of users that can access the MGate simultaneously.
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. Import or delete SSL certificate/key files. This function is only available for the web console.



Issue to: 10.123.4.44

Issue by: Moxa Inc.

Valid: from 2022-6-2 to 2027-6-1

Maintenance

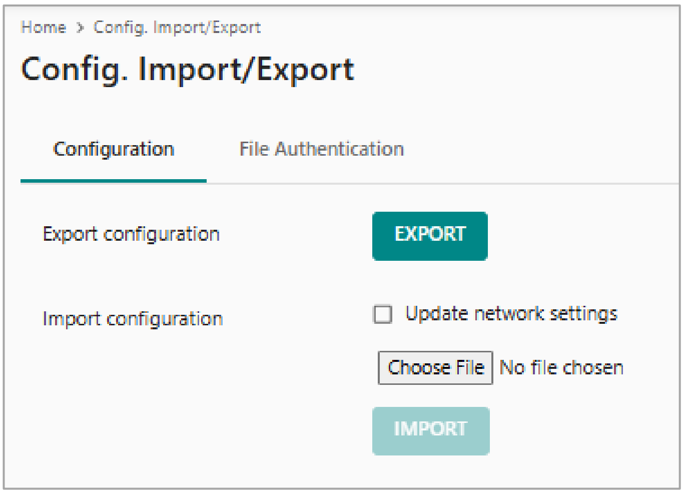
Maintenance—Configuration Import/Export

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. 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.

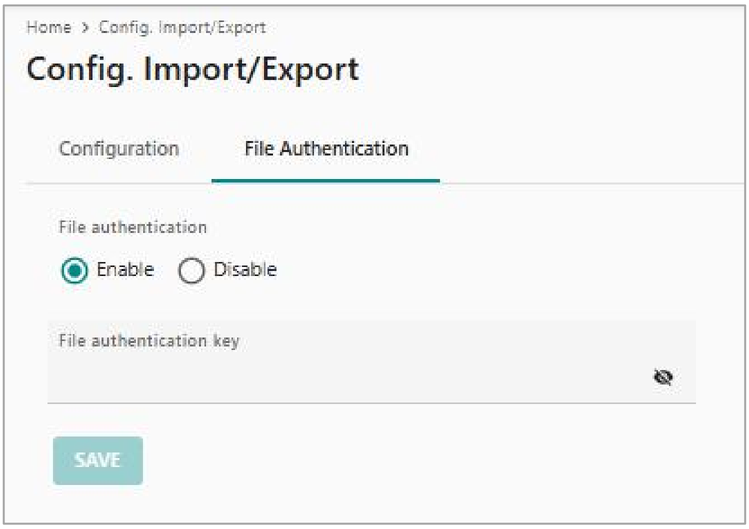
For cybersecurity reasons, you can export the configuration file with an authentication key, length from 8 to 16 characters. Importing will fail if the configuration file's key doesn't match the exported file's key.



Export configuration

Import configuration ☐ Update network settings

No file chosen



File authentication

● Enable ○ Disable

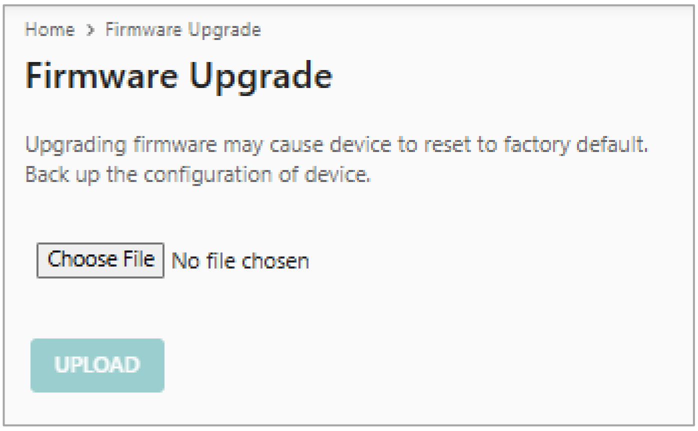
File authentication key

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 you complete the firmware upgrade process. 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 cannot boot. If this happens, contact Moxa RMA services.



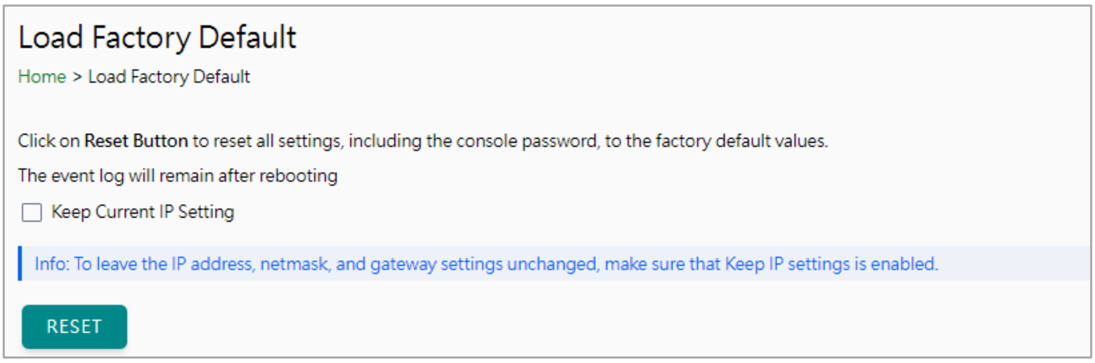
Home > Firmware Upgrade

Firmware Upgrade

Upgrading firmware may cause device to reset to factory default.
Back up the configuration of device.

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.



Load Factory Default

Home > Load Factory Default

Click on **Reset Button** to reset all settings, including the console password, to the factory default values.

The event log will remain after rebooting

□ Keep Current IP Setting

Info: To leave the IP address, netmask, and gateway settings unchanged, make sure that Keep IP settings is enabled.

ATTENTION

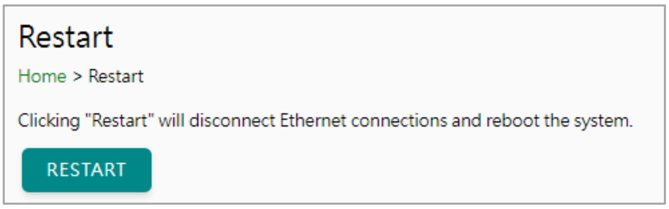
Load Default will completely reset the configuration of the unit, and all the parameters you have saved will be discarded. Do not use this function unless you are sure you want to completely reset your unit.

Restart

Reboot the MGate by clicking the RESTART button.

ATTENTION

A reboot will discard unsaved configuration files.



Restart

Home > Restart

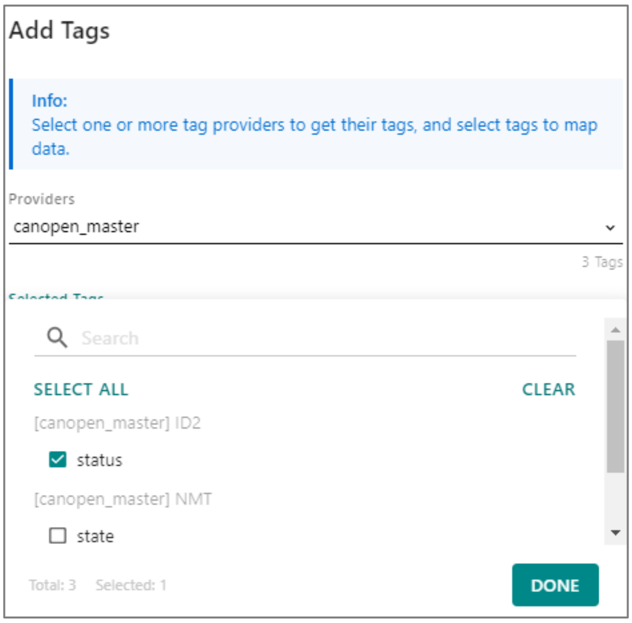
Clicking "Restart" will disconnect Ethernet connections and reboot the system.

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 cannot receive up-to-date data from the CAN device. The gateway stores the out-of-date data in its memory, and the client (e.g., PLC)) retrieves it. The lattter 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 automatically creates a status tag upon the creation of a CAN-based server device. This tag is used to show the connection status (valid or invalid) of the CAN-based server device. To monitor the status of the status tag, convert this tag to the northbound protocol and read for the northbound SCADA/device. Or, you can check the tag status on the MGate's web, the Tag View page.

To perform the status tag monitoring from your northbound protocol, go to the northbound protocol's page (for example, the EtherNet/IP adapter page). Cick ADD TAGS and select canopen_master as the tag provider and select the "status" tag. The MGate will automatically add a mapping from this CAN-based tag to the EtherNet/IP.



Add Tags

Info:
Select one or more tag providers to get their tags, and select tags to map data.

Providers: canopen_master

3 Tags

[canopen_master] ID2

☑ status

[canopen_master] NMT

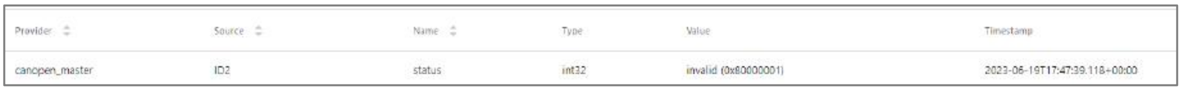
☐ state

Total: 3 Selected: 1

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

Further details on the status codes:

1. Valid (0x00000000) - Indicates the status is connected.
2. Invalid (0x80000000) - Indicates the status is unknown.
3. Invalid (0x80000001) - Indicates the status is offline.



Provider	Source	Name	Type	Value	Timestamp
canopen_master	ID2	status	int32	invalid (0x80000001)	2023-06-19T17:47:39.118+00:00

4. Network Management Tool (MXstudio)

Moxa's MXstudio industrial network management suite includes tools such as MXconfig and MXview. MXconfig is for industrial network mass configuration; MXview is for industrial management software. For the software and related detailed information regarding MXview and MXconfig, as well as the supported product firmware versions, refer to the Moxa website at https://www.moxa.com/en/products/industrial-network-infrastructure/network-management-software.

When you discover a Moxa product that has not been integrated into the MXview or MXconfig, you may not be able to retrieve the product information from MXview or MXconfig. To solve this, you can download the plugin file from the Moxa MGate product website and then import/install the plugin into MXview or MXconfig.

After importing/installing the plugin files, the MGate products can be supported by MXview/MXconfig. Refer to the Moxa MGate product website to download plugin files: http://www.moxa.com. For more detailed functions, such as supported functions on MXview/MXconfig, refer to the Tech Note: Configuring and Monitoring with MXview One/MXview and MXconfig.

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

B. CIP Objects of EtherNet/IP

Several communication objects are defined in CIP (Common Industrial Protocol). Moxa's MGate supports the following for PLCs and SCADA systems to monitor:

- Identity Object
- TCP/IP Interface Object
- Ethernet Link Object
- Assembly Object
- Message Router Object
- Connection Manager Object
- Port Object

The supported attributes and services of the above objects are introduced in the table below, including the access rules for each attribute. To understand the details of each attribute of the standard objects, refer to the official documents of CIP introduction (Vol. 1) and the EtherNet/IP Adaptation of CIP (Vol. 2).

Identity Object

The Class code of Identity object is **0x01** (Defined in CIP Vol1, 5-2).

There is **one** instance of this object in our product. It stores the information of the production and the device. The following tables summarize the class attributes and the instance attributes.

Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object
2	Get	Max Instance	UINT (16)	Maximum instance number of an object created in this class level of the device
3	Get	Number of Instances	UINT (16)	Number of object instances created in this class level of the device.
6	Get	Maximum ID Number Class Attributes	UINT (16)	The attribute ID number of the last class attribute of the class definition implemented in the device
7	Get	Maximum ID Number Instance Attributes	UINT (16)	The attribute ID number of the last instance attribute of the class definition implemented in the device

Instance Attribute List

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Vendor ID		UINT (16)	991, the vendor ID of Moxa
2	Get	Device Type		UINT (16)	0 x 0C, "Communications Adapter"
3	Get	Product Code		UINT (16)	Refer to Product Code Table
4	Get	Revision		(Struct.)	The version of the Identity object
			Major	USINT (8)	The structure member, major
			Minor	USINT (8)	The structure member, minor
5	Get	Status		WORD (16)	Not used
6	Get	Serial Number		UDINT (32)	The serial number of each device
7	Get	Product Name		SHORT_STRING	The product name in human-readable format
15	Get/Set	Assigned Name		STRINGI	The assigned MGate name For example: Same as the server name set in the basic settings. By default, it is "MGate xxxx_xx" (xxxx_xx represents the product series number and serial number)
17	Get/Set	Geographic Location		STRINGI	The assigned MGate location Same as the server location set in the basic settings. By default, it is blank.

The Identity Object Instance supports the following CIP Common services:

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x01	✓	✓	Get_Attribute_All	Returns the contents of all attributes of the class
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x10		✓	Set_Attribute_Single	Used to write an object instance attribute
0x05		✓	Reset	Invokes the reset service for the device

Product Code	Model Name
0x1040	MGate 5122

TCP/IP Interface Object

The Class code of TCP/IP Interface object is **0xf5** (Defined in CIP Vol2, 5-3). There is **one** instance of this object.

The following tables summarize the attributes of this object.

Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object.
2	Get	Max Instance	UINT (16)	Maximum instance number of an object currently created in this class level of the device
3	Get	Number of Instances	UINT (16)	Number of object instances currently created at this class level of the device
6	Get	Maximum ID Number Class Attributes	UINT (16)	The attribute ID number of the last class attribute of the class definition implemented in the device
7	Get	Maximum ID Number Instance Attributes	UINT (16)	The attribute ID number of the last instance attribute of the class definition implemented in the device

Instance Attribute List

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Status		DWORD (32)	Interface status 0 = The Interface Configuration attribute has not been configured 1 = The Interface Configuration attribute contains valid configuration obtained from BOOTP, DHCP or non-volatile storage
2	Get	Configuration Capability		DWORD (32)	Interface capability flags Bit map of capability flags: Bit 0: BOOTP Client Bit 1: DNS Client Bit 2: DHCP Client Bit 3: DHCP-DNS Update Bit 4: Configuration Settable
3	Get/Set	Configuration Control		DWORD (32)	Interface control flags Bit map of control flags: Bit 0 to 3: Startup Configuration • 0 = The device shall use the interface configuration values previously stored (for example, in non-volatile memory or via hardware witches) • 1 = The device shall obtain its interface configuration values via BOOTP • 2 = The device shall obtain its interface configuration values via DHCP upon start-up • 3 to15 = Reserved
4	Get	Physical Link Object		(Struct.)	Path to physical link object
			Path Size	UINT (16)	Size of Path
			Path	Padded EPATH	Logical segments identifying the physical link object
5	Get/Set	Interface Configuration		(Struct.)	TCP/IP network interface configuration
			IP Address	UDINT (32)	The device's IP address
			Network Mask	UDINT (32)	The device's network mask
			Gateway Address	UDINT (32)	Default gateway address
			Name Server	UDINT (32)	Primary name server
			Name Server2	UDINT (32)	Secondary name server
			Domain Name	STRING	Default domain name
6	Get/Set	Host Name		STRING	Host name

The TCP/IP Object Instance supports the following CIP Common services:

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x01	✓	✓	Get_Attribute_All	Returns the contents of all attributes of the class
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x10		✓	Set_Attribute_Single	Used to change an object instance attribute

Ethernet Link Object

The Class code of Ethernet Link object is **0xf6** (Defined in CIP Vol2, 5-4). For each MGate Ethernet port, there is an instance of this class. The following table shows the mapping of instance number and the MGate Ethernet port number.

Instance Number	Mapping to
0	Ethernet Link class
1	First MGate Ethernet port
2	Second MGate Ethernet port

The following tables summarize the attributes of the Ethernet Link object.

There are some vendor specific attributes in the table (Starting from attribute Id 100).

Class Attribute List

Attr. ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object
2	Get	Max Instance	UINT (16)	Maximum instance number of an object created in this class level of the device
3	Get	Number of Instances	UINT (16)	Number of object instances currently created in this class level of the device
6	Get	Maximum ID Number Class Attributes	UINT (16)	The attribute ID number of the last class attribute of the class definition implemented in the device
7	Get	Maximum ID Number Instance Attributes	UINT (16)	The attribute ID number of the last instance attribute of the class definition implemented in the device

Instance attribute list

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Interface Speed		UDINT (32)	Interface speed in use (Speed in Mbps, e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags		DWORD (32)	Refer to the Interface Flags table
3	Get	Physical Address		ARRAY of 6 USINT(8)	MAC layer address (The System MAC address)
4	Get	Interface Counters		(Struct.)	Counters relevant to the receipt of packets
			In Octets	UDINT (32)	Octets received on the interface
			In Ucast Packets	UDINT (32)	Unicast packets received on the interface
			In NUcast Packets	UDINT (32)	Non-unicast packets received on the interface
			In Discards	UDINT (32)	Inbound packets received on the interface but are discarded
			In Errors	UDINT (32)	Inbound packets that contain errors (does not include In Discards)
			Out Octets	UDINT (32)	Octets sent on the interface
			Out Ucast Packets	UDINT (32)	Unicast packets sent on the interface
			Out NUcast Packets	UDINT (32)	Non-unicast packets sent on the interface
			Out Discards	UDINT (32)	Discarded outbound packets
			Out Errors	UDINT (32)	Outbound packets that contain errors
5	Get	Media Counters		(Struct.)	
			Alignment Errors	UDINT (32)	Received frames that are not an integral number of octets in length
			FCS Errors	UDINT (32)	Received frames that do not pass the FCS check

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
			Single Collisions	UDINT (32)	Successfully transmitted frames which experienced exactly one collision
			Multiple Collisions	UDINT (32)	Successfully transmitted frames which experienced more than one collision
			SQE Test Errors	UDINT (32)	The number of times the SQE test error message is generated
			Deferred Transmissions	UDINT (32)	Frames for which first transmission attempt is delayed because the medium is busy
			Late Collisions	UDINT (32)	The number of times a collision is detected later than 512 bit times into the transmission of a packet
			Excessive Collisions	UDINT (32)	Frames for which transmission fails because of excessive collisions
			MAC Transmit Errors	UDINT (32)	Frames for which transmission fails because of an internal MAC sublayer transmit error
			Carrier Sense Errors	UDINT (32)	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
			Frame Too Long	UDINT (32)	Received frames that exceed the maximum permitted frame size
			MAC Receive Errors	UDINT (32)	Frames for which reception on an interface fails because of an internal MAC sublayer receive error
6	Get/Set	Interface Control		(Struct.)	Configuration for physical interface
			Control Bits	WORD (16)	Bit 0: Auto-Negotiate • Value 0: Force • Value 1: Auto-Nego Bit 1: Half/Full Duplex • Value 0: half duplex • Value 1: full duplex Bit 2 to 15: Reserved, all zero
			Forced Interface Speed	UINT (16)	Speed at which the interface is forced to operate
10	Get	Interface Label		SHORT_STRING	Human readable identification
11	Get	Interface Capability		(Struct.)	Indicates the capabilities of the interface
			Capability Bits	DWORD (32)	Interface capabilities, other than speed/duplex
			Speed/Duplex Options	(Struct.)	Indicates speed/duplex pairs supported in the Interface Control attribute
				USINT (8)	Speed/Duplex Array Count
				(Array Struct.)	Speed/Duplex Array
				UINT (16)	Interface Speed
				USINT (8)	Interface Duplex Mode

Interface Flags

Bit(s)	Called	Definition
0	Link Status	0 indicates an inactive link; 1 indicates an active link.
1	Half/Full Duplex	0 indicates half duplex; 1 indicates full duplex.
2-4	Negotiation Status	Indicates the status of link auto-negotiation 0 = Auto-negotiation in progress. 1 = Auto-negotiation and speed detection failed. Using default values for speed and duplex. Default values are product-dependent; recommended defaults are 10Mbps and half duplex. 2 = Auto negotiation failed but detected speed. Duplex defaulted. Default value is product-dependent; recommended default is half duplex. 3 = Successfully negotiated speed and duplex. 4 = Auto-negotiation is not attempted. Forced speed and duplex.
5	Manual Setting Requires Reset	0 indicates the interface can activate changes to link parameters (auto-negotiate, duplex mode, interface speed) automatically. 1 indicates the device requires a reset service to be issued to its Identity Object in order for the changes to take effect.
6	Local Hardware Fault	0 indicates the interface detects no local hardware fault; 1 indicates a local hardware fault is detected. The meaning of this is product- specific. For example, an AUI/MII interface might detect no transceiver attached, or a radio modem might detect no antenna attached. In contrast to the soft, possibly self-correcting nature of the Link Status being inactive, this is assumed a hard-fault requiring user intervention.
7~31	Reserved.	Shall be set to zero

The Ethernet Link Object Instance supports the following CIP common services:

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute

Assembly Object

The MGate supports **static** assembly object for CIP I/O messaging. The Class code is **0x04** (Defined in CIP Vol 1, 5-5).

There are three instances of this object as the following.

	Instance Number	Size (bytes)
Input	4	1984
Output	4	1984
Configuration	1	0

The **Input** means the MGate produces the data, which includes the information and status report to the originator for monitoring. The **Output** means the data is generated by the originator (remote host) and is consumed by MGate.

Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object

Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
3	Get	Data		Array of BYTE	The implicit messaging content
4	Get	Size		UINT (16)	Number of bytes in Attr. 3

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute

Message Router Object

The object within a node that distributes messaging requests to the appropriate application objects. The supported messaging connections are:

- Explicit Messaging
- Unconnected Messaging
- Implicit messaging

When using the UCMM to establish an explicit messaging connection, the target application object is the Message Router object (Class Code **2**).

Class Attribute List

Attr. ID	Access Rule	Name	Data Type	Descriptions
1	Get	Revision	UINT (16)	Revision of this object

Instance Attribute List

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Object_list		(Struct.)	A list of supported objects
			Number	UINT (16)	The number of supported classes in the classes array
			Classes	Array of UINT (16)	List of supported class codes
2	Get	Number Available		UINT (16)	The maximum number of connections supported
3	Get	Number Active		UINT (16)	The number of connections used by system components
4	Get	Active Connections		Array of UINT (16)	A list of the connection IDs of the currently active connections

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute

Connection Manager Object

The Connection Manager Class allocates and manages the internal resources associated with both I/O and Explicit Messaging connections.

The class code is **0x06**. There is one instance of this object.

The supported connection trigger type is ***cyclic*** and ***change of state***. The following introduces the instance attribute list.

Class Attribute List

Attr. ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x0e	✓		Get_Attribute_Single	Returns the contents of the specified attribute
0x4E		✓	Forward_Close	Closes a connection
0x54		✓	Forward_Open	Opens a connection

Port Object

The port object represents the underlying interface of CIP, which is EtherNet/IP. The class code is **0xf4**. There is one instance of this object.

The instance attribute "**Port Type**" identifies the CIP adaptation.

Class Attribute List

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Revision		UINT (16)	Revision of this object
2	Get	Max Instance		UINT (16)	Maximum instance number of an object currently created in this class level of the device
3	Get	Number of Instances		UINT (16)	Number of object instances currently created at this class level of the device.
8	Get	Entry Port		UINT (16)	The attribute ID number of the last class attribute of the class definition implemented in the device
9	Get	Port Instance Info		(Array of Struct.)	
			Port Type	UINT (16)	Enumerates the type of port
			Port Number	UINT (16)	CIP port number associated with this port

Instance Attribute List

Attr. ID	Access Rule	Name	(Struct.)	Data Type	Description
2	Get	Port Number		UINT (16)	CIP port number associated with this port. (Value 1 is reserved for internal product use)
3	Get	Link Object		(Struct.)	
			Path Length	UINT (16)	The number of 16-bit words in the following path
			Link Path	Padded EPATH	Logical path segments that identify the object for this port
4	Get	Port Name		SHORT_STRI NG	String, which names the physical network port. The maximum number of characters in the string is 64.
7	Get	Node Address		Padded EPATH	Node number of this device on port. The range within this data type is restricted to a Port Segment.
10	Get	Port Routing Capabilities		DWORD (32)	Bit string that defines the routing capabilities of this port

Common Service List

Service Code	Implementation		Service Name	Description
	Class	Instance		
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x01	✓	✓	Get_Attributes_All	Returns the contents of all attributes of the class/instance