MGate 5134 Series User Manual

Version 1.0, September 2022

www.moxa.com/products

MGate 5134 Series User Manual

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 5134 is an industrial Ethernet gateway for converting Modbus RTU/ASCII/TCP to PROFINET network communications. To integrate existing Modbus devices into a PROFINET network, use the MGate 5134 as a Modbus client to collect data and exchange data with PROFINET host. All models are protected by a rugged and compact metal housing, are DIN-rail mountable, and offer built-in serial isolation. The rugged design is suitable for industrial applications such as factory automation, power, oil & gas, water and wastewater, and other process automation industries.

2. Getting Started

Connecting the Power

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

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

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

Connecting Serial Devices

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

Connecting to a Network

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

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

Installing DSU Software

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

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

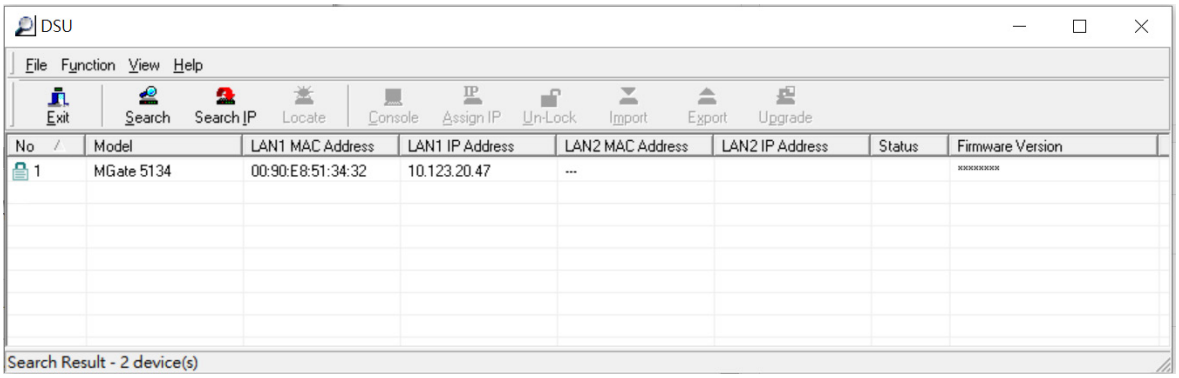
1. Locate and run the following setup program to begin the installation process:

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

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

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

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

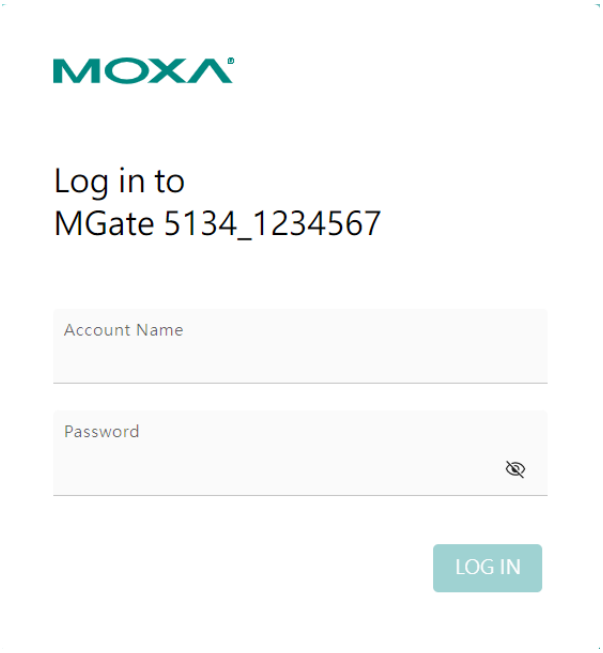


Log In to the Web Console

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

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

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



microSD

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

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

1. Format the microSD card as FAT file system through a PC.
2. Power off the MGate and insert the microSD card (ensure that the microSD card is empty).
3. Power on the MGate. The default settings will be copied to the microSD card.
4. Manually configure the MGate via the 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 to 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 20 Mbytes of free space remaining.
2. The microSD card is write-protected.
3. The file system is corrupted.
4. The microSD card is damaged.

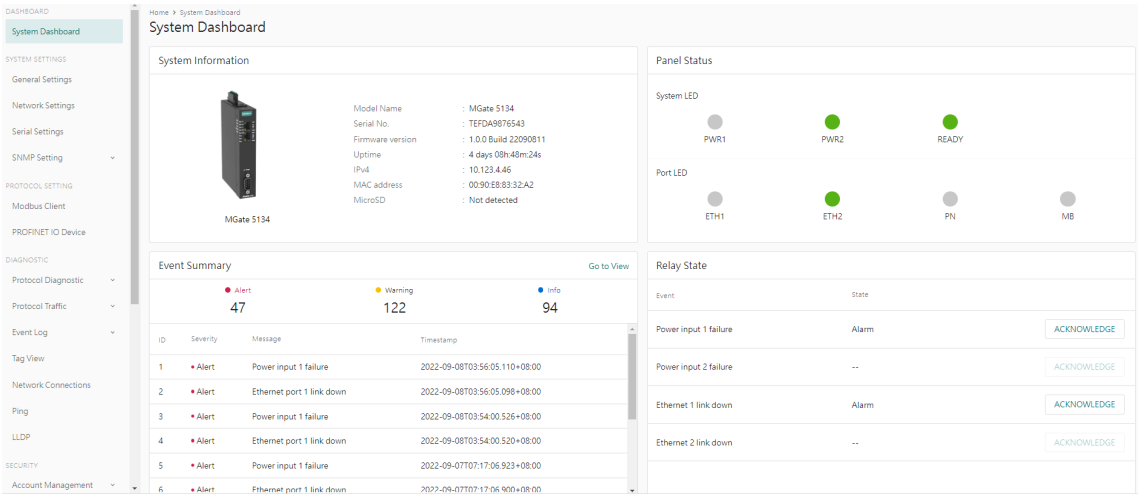
The MGate will stop working in case of the above events, accompanied by a flashing Ready LED and beeping alarm. When you replace the MGate gateway’s microSD card, the microSD card will synchronize the configurations stored on the MGate gateway. Note that the replacement microSD card should not contain any configuration files on it; otherwise, the out-of-date configuration will copy to the MGate device.

3. Web Console Configuration and Troubleshooting

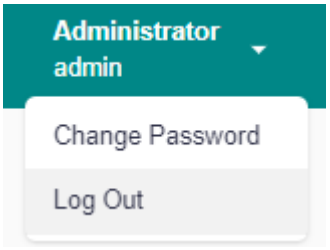
This chapter provides a quick overview of how to configure the MGate 5134 by web console.

System Dashboard

This page gives a system dashboard of the MGate 5134 gateway.



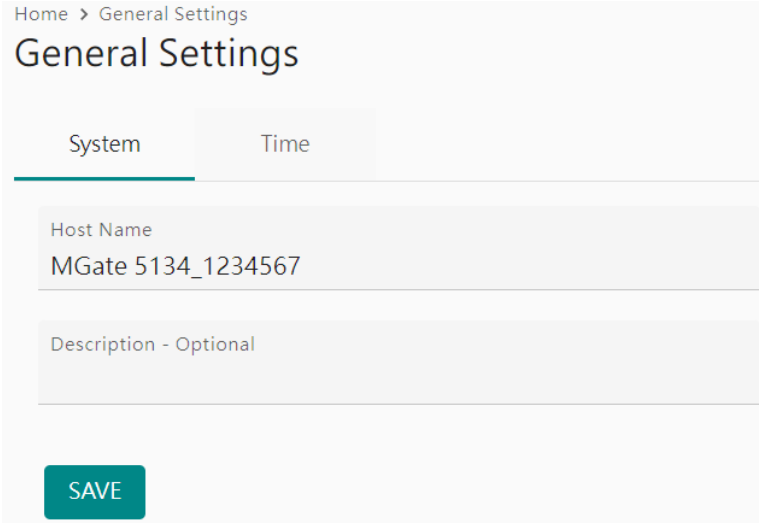
You can change your password or log out using the options on the top-right corner of the page.



System Settings

System Settings—General Settings

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



System Settings

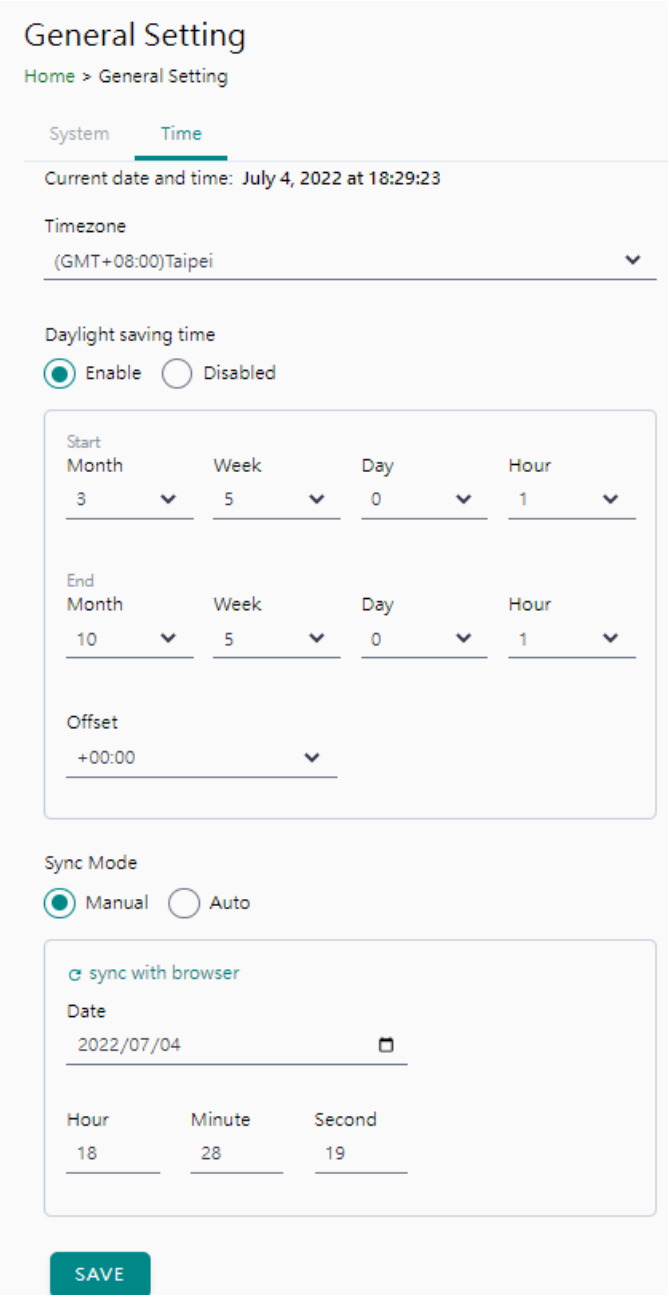
Parameter	Value	Description
Host Name	Alphanumeric string	Enter a name that can help you uniquely identify the device. For example, you can include the name and function of the device.
Description	Alphanumeric string	(optional) You can include additional description about the device such as function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

Time Settings

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

ATTENTION

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



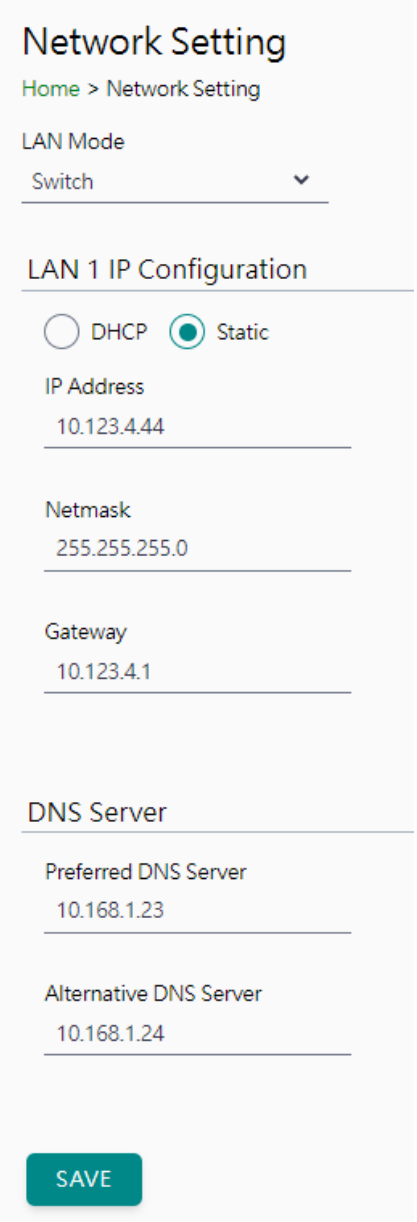
Parameter	Value	Description
Time zone	User-selectable time zone	Shows the current time zone selected and allows change to a different time zone.
Daylight saving time	Enable Disable	Set the daylight saving time.
Sync Mode	Manual	Use this setting to manually adjust the time (1900/1/1-2037/12/31) or sync 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 configured time period.

ATTENTION

If the dispersion of the time server is higher than the client (MGate), the client will not accept NTP messages from the time server. The MGate's dispersion is 1 second. You must configure your time server with a dispersion value lower than 1 sec for the NTP process to complete.

System Settings—Network Settings

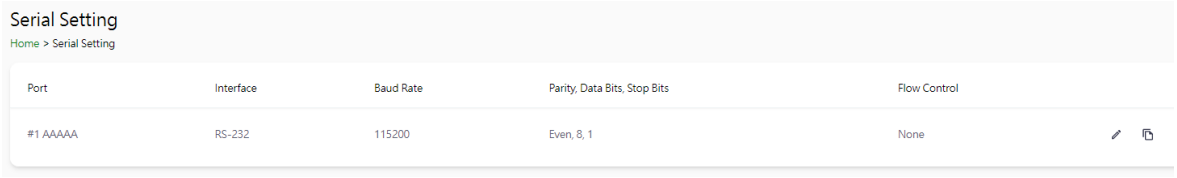
You can change the IP Configuration, IP Address, Netmask, Default Gateway, and DNS settings on the **Network Settings** page.

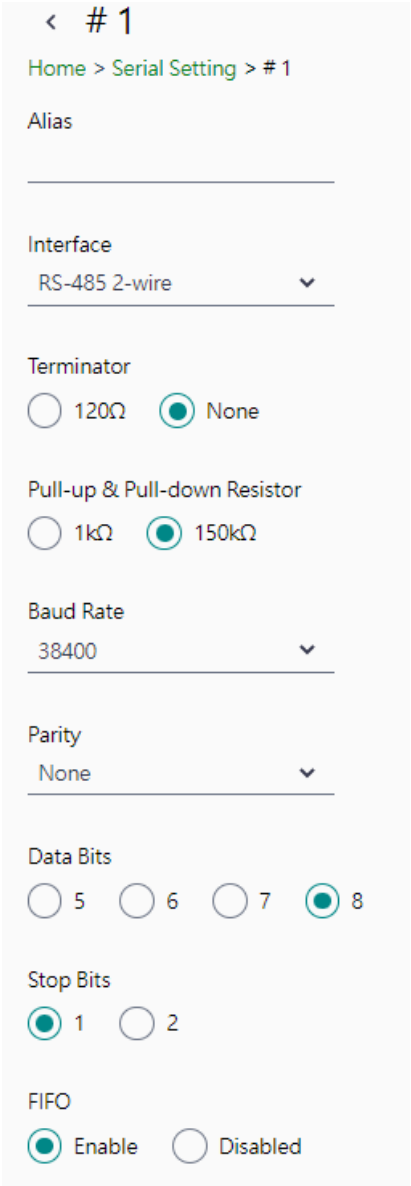


Parameter	Value	Description
LAN Mode	**Switch, Dual IP, Redundant LAN**	The **Switch** mode allows users to install the device with daisy-chain topology. The **Dual IP** mode allows the gateway to have two different IP addresses, each with distinct netmask and gateway settings. The IP addresses can have the same MAC address. **NOTE:** In the **Dual IP** mode, the PROFINET protocol can only be used on the LAN1 port (ETH1). The **Redundant LAN** mode allows users to use the same IP address on both Ethernet ports. The default active LAN port is ETH1 after bootup. If the active LAN fails to respond, 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.
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—Serial Settings

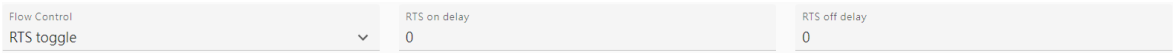
The serial interface supports RS-232, RS-422, and RS-485 interfaces. You must configure the baudrate, parity, data bits, and stop bits before using the serial interface for the Modbus RTU/ASCII protocol. Incorrect settings will cause communication failures.





Parameter	Value	Description
Interface	**RS-232, RS-422, RS-485 2-wire, RS-485 4-wire**	
Baudrate	300 bps to 921600 bps	
Parity	**None, Odd, Even, Mark, Space**	
Data Bits	**7,8**	
Stop Bits	**1, 2**	

Parameter	Value	Description
FIFO	**Enable, Disable**	The internal buffer of UART. Disabling FIFO can reduce the latency time when receiving data from serial communications, but this will also slow down the throughput.



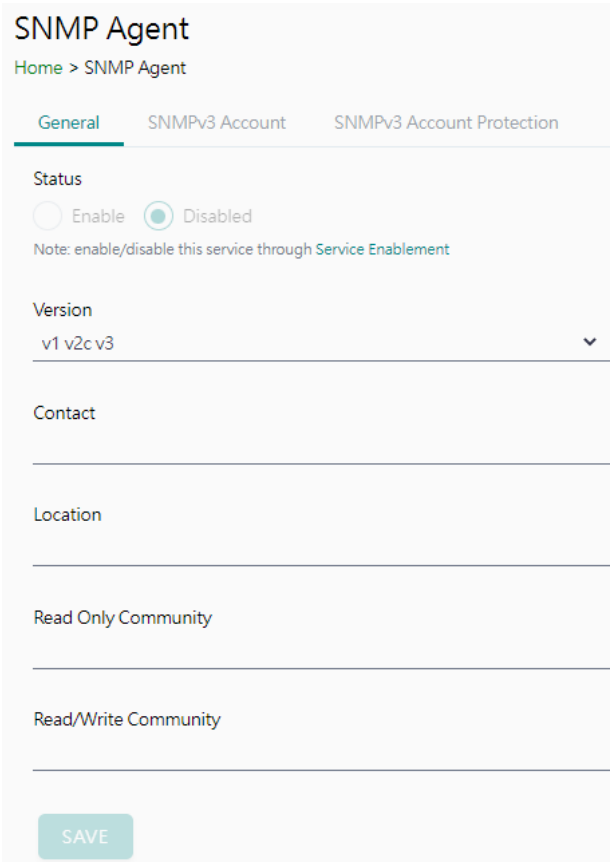
Parameter	Value	Description
Flow Control (only for RS-232 mode)	**None, RTS/CTS, RTS Toggle**	The RTS Toggle will turn off the RTS signal when there is no data to be sent. If there is data to be sent, the RTS toggle will turn on the RTS signal before a data transmission and off on completion of the transmission.
RTS on delay	0 to 100 ms	Only available for the RS-232 mode to implement the RTS Toggle function.
RTS off delay	0 to 100 ms	Only available for the RS-232 mode to implement the RTS Toggle function.

RTS Toggle

The RTS Toggle function is available only in the **RS-232** mode. This flow-control mechanism is achieved by toggling the RTS pin in the transmission direction through a software setting. Data is transmitted after the RTS pin is toggled ON for the specified time interval. After the data transmission is finished, the RTS pin will toggle OFF for the specified time interval automatically.

System Settings—SNMP Settings

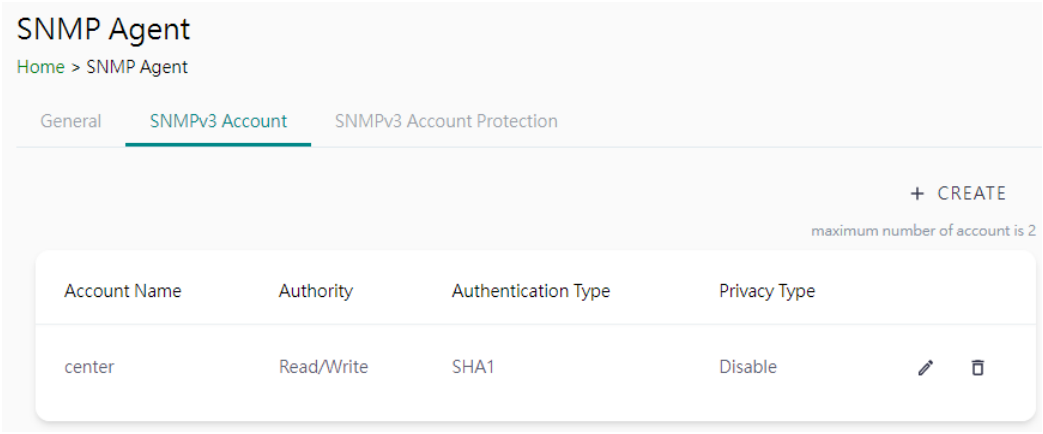
System Settings—SNMP Settings—SNMP Agent

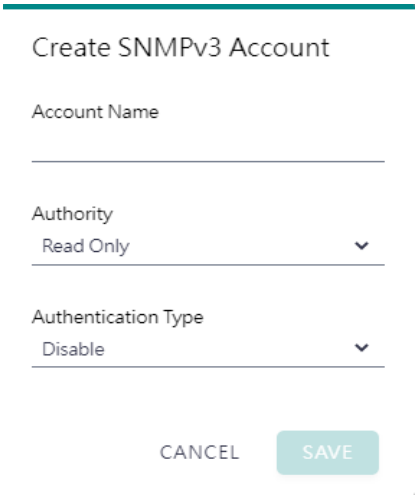


Parameters	Description
Version	The SNMP version; MGate supports SNMP V1, V2c, and V3.
Contact	The optional contact information; usually includes an emergency contact name and telephone number.
Read Only Community	A text password mechanism that is used to weakly authenticate queries to agents of managed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

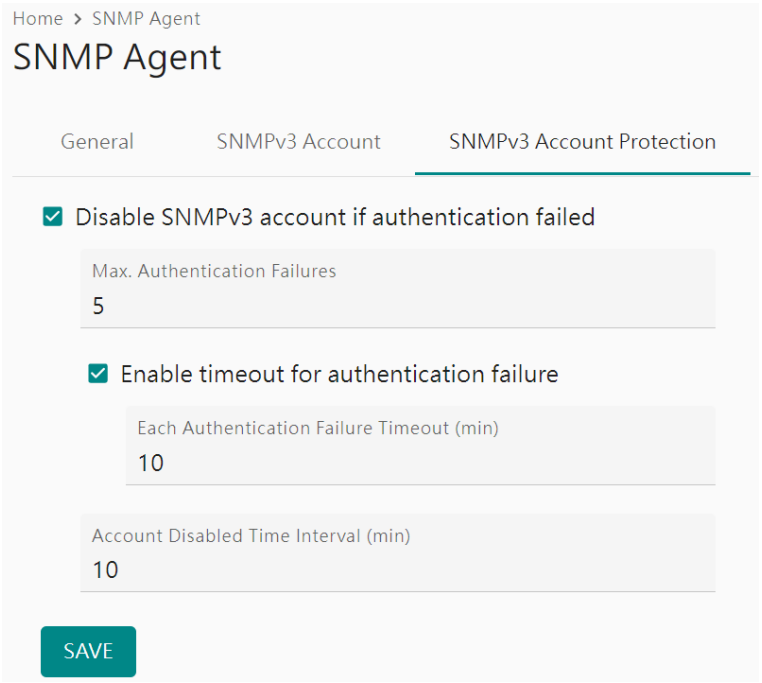
Read-only and Read/write Access Control

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



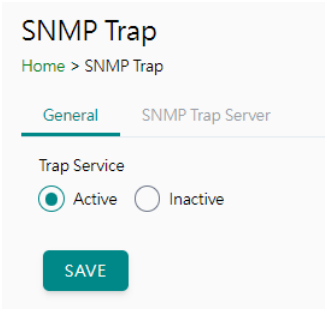


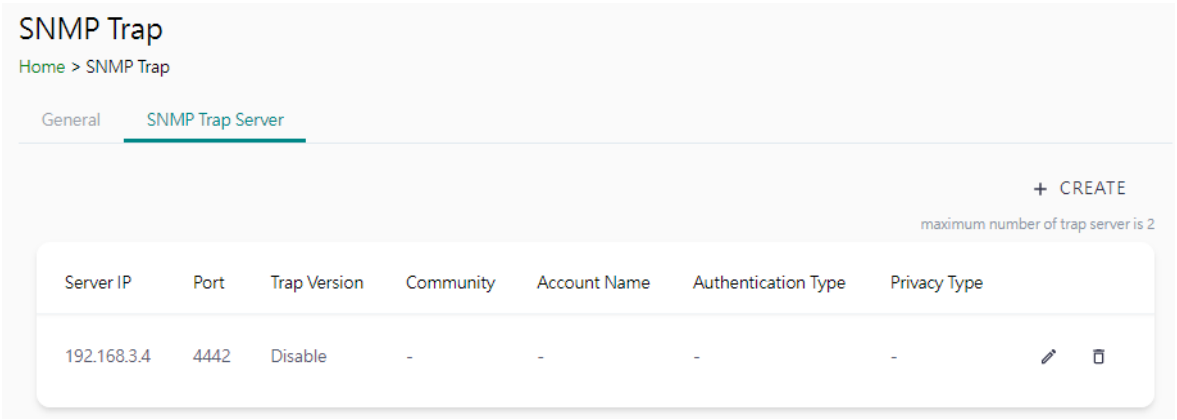
Parameters	Value	Description
Account Name		The username for which the access level is being defined.
Authority	**Read Only** **Read/Write**	The level of access allowed
Authentication Type	**Disable** **MD5** **SHA1** **SHA-224** **SHA-256** **SHA-384** **SHA-512**	Use this field to select MD5 or SHA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

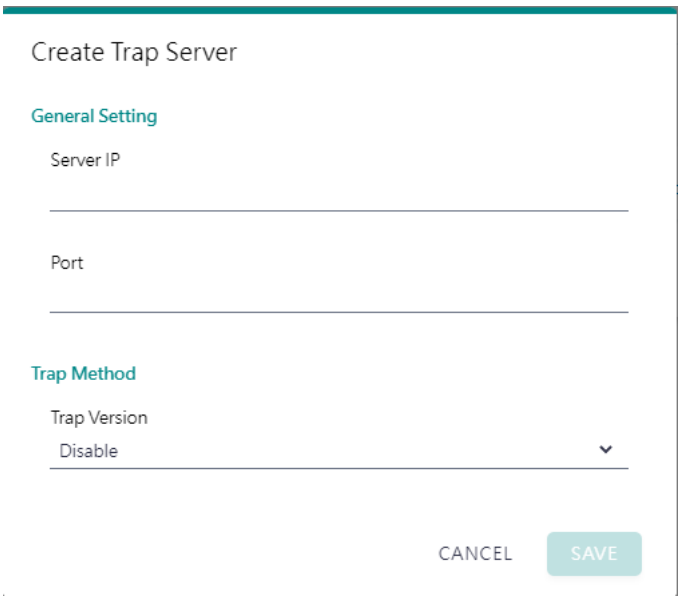


Parameters	Value	Description
Max Authentication Failures	1 to 10 (default 5)	Specifies the maximum number for authentication failures. If this number is exceeded, the MGate will disable SNMPv3.
Each Authentication Failure Timeout (min)	1 to 1440 (default 10)	Specifies a timeout period when enabling the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

System Settings—SNMP Settings—SNMP Trap





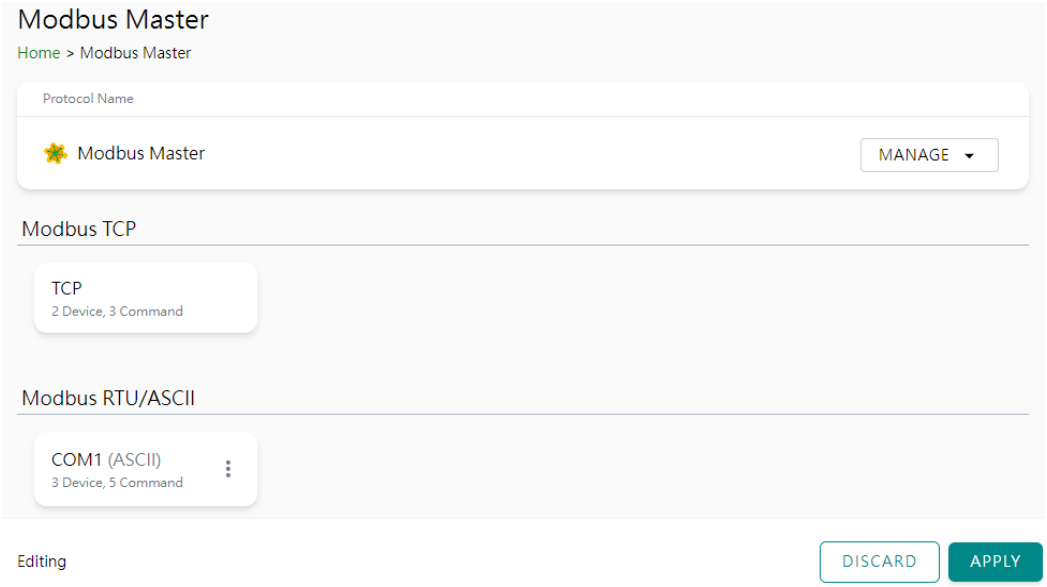


Parameters	Description
Server IP	SNMP server IP address or domain name.
Port	SNMP server IP Port.
Trap Version	**Disable** **SNMPv1** **SNMPv2** **SNMPv3**

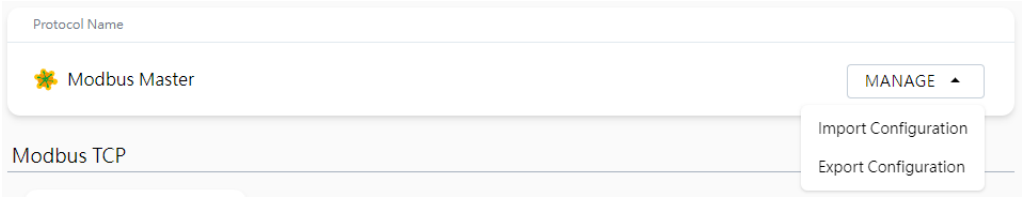
Protocol Settings

Protocol Settings—Modbus Client Settings

You can manage Modbus devices and their Modbus command tables on this page.

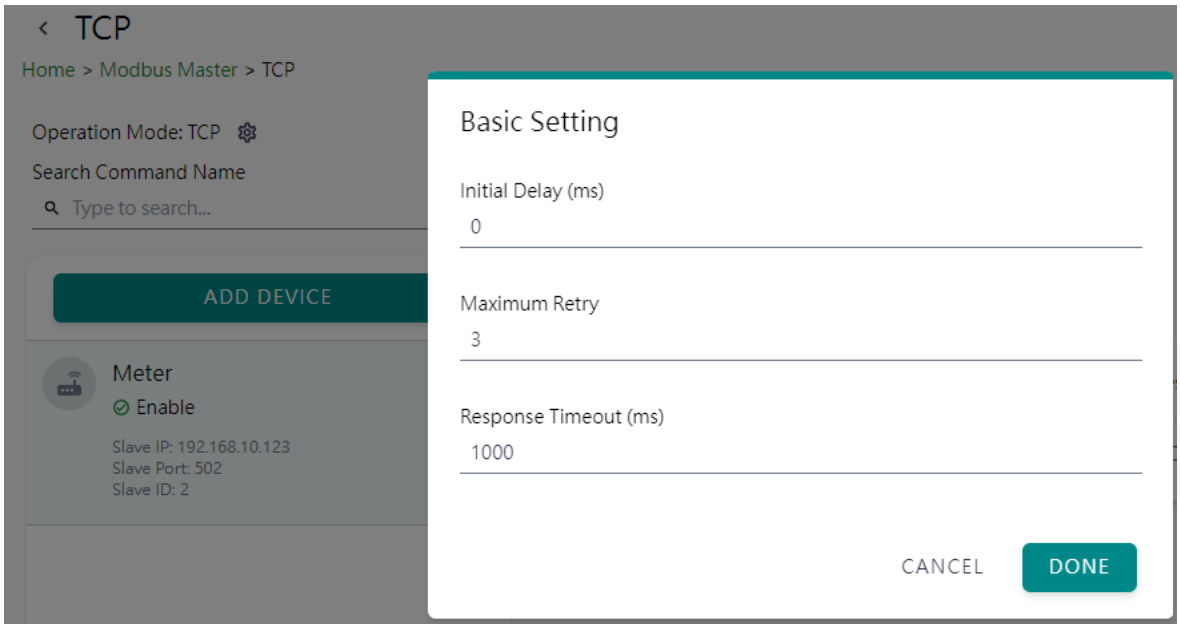


The MGate supports csv file import/export for Modbus settings; it is easy to use when you back up the settings or during installation stage.



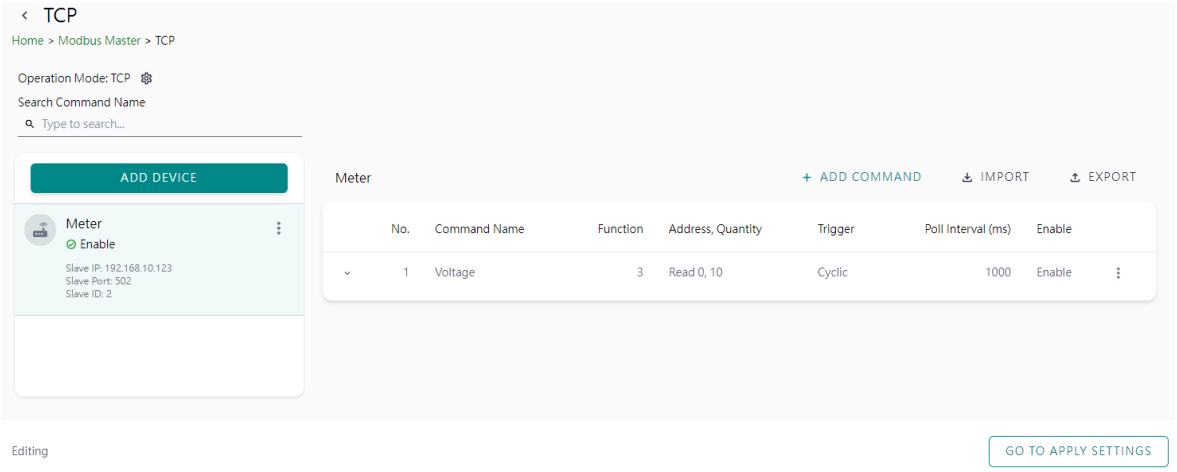
Click TCP or the serial port column to set up the Modbus device.

Configure the basic setting for Modbus TCP by clicking the icon next to the Operation Mode: TCP.

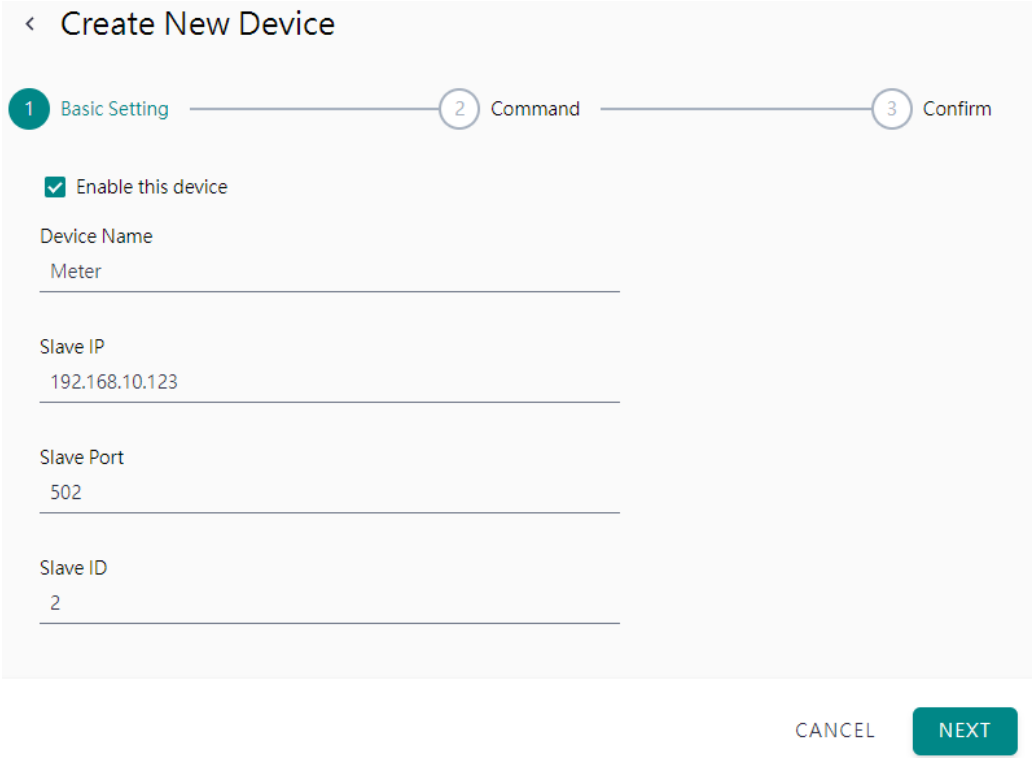


Parameter	Value	Default	Description
Initial delay	0 to 30000 ms	0	Some Modbus slaves may take more time to boot up than other devices. In some environments, this may cause the entire system to experience repeated exceptions during the initial boot-up. After booting up, you can force the MGate to wait before sending the first request with the Initial Delay setting.
Maximum Retry	0 to 5	3	This is used to configure how many times the MGate will try to communicate with the Modbus slave when the Modbus command times out.
Response Timeout	10 to 120000 ms	1000	Based on the Modbus standard, the device manufacturer defines the time a slave device takes to respond to a request. A Modbus master can be configured to wait a certain amount of time for a slave's response. If no response is received within the specified time, the master will disregard the request and continue operation. This allows the Modbus system to continue the operation even if a slave device is disconnected or faulty. On the MGate , the Response timeout field is used to configure how long the gateway will wait for a response from a Modbus slave. Refer to your device manufacturer's documentation to manually set the response timeout.

Add the Modbus device by clicking the **ADD DEVICE** button

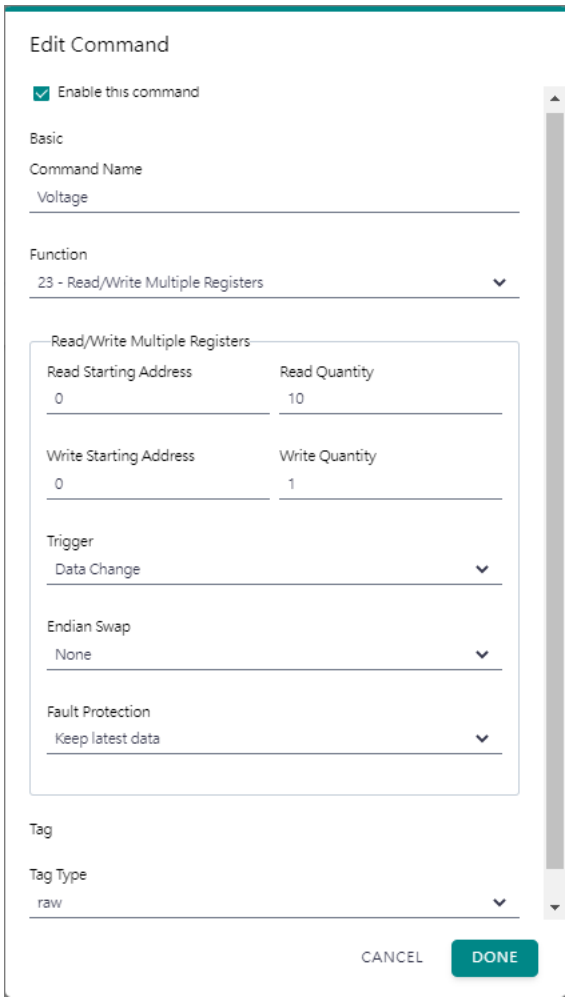


Step 1: Add Modbus device information



Parameter	Value	Default	Description
Device Name	Alphanumeric string		Max. 32 characters.
Slave IP	0.0.0.0 to 255.255.255.255	0.0.0.0	The IP address of a remote slave device.
Slave Port	1 to 65535	502	The TCP port number of a remote slave device.
Slave ID	1 to 255	1	The Modbus slave ID.

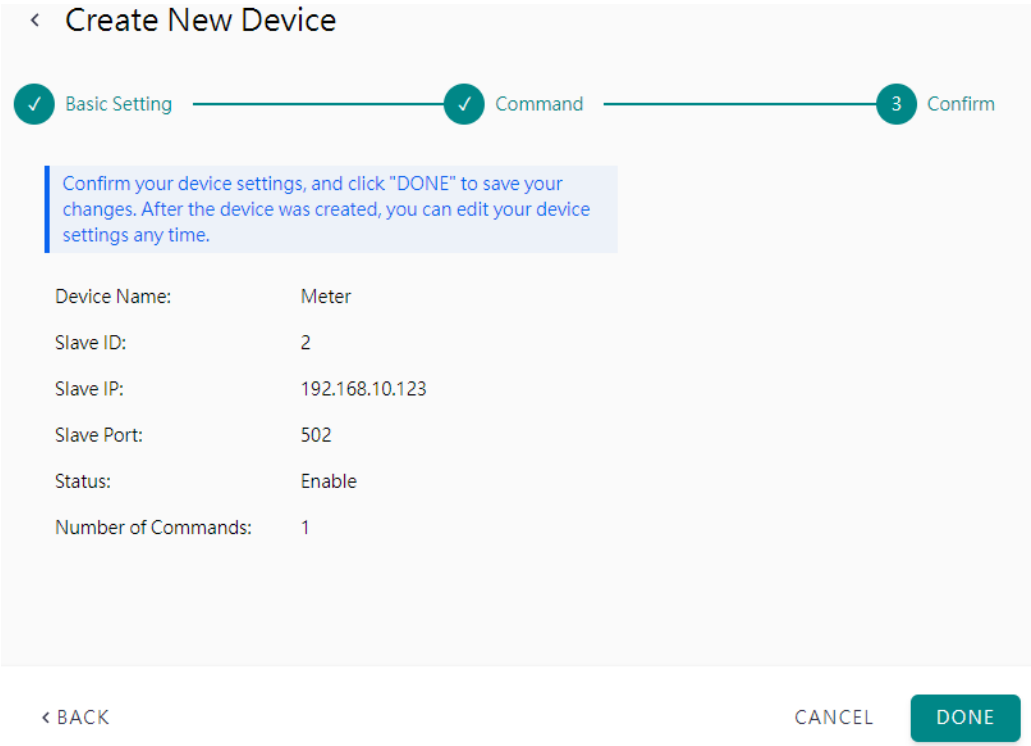
Step 2: Add Modbus commands



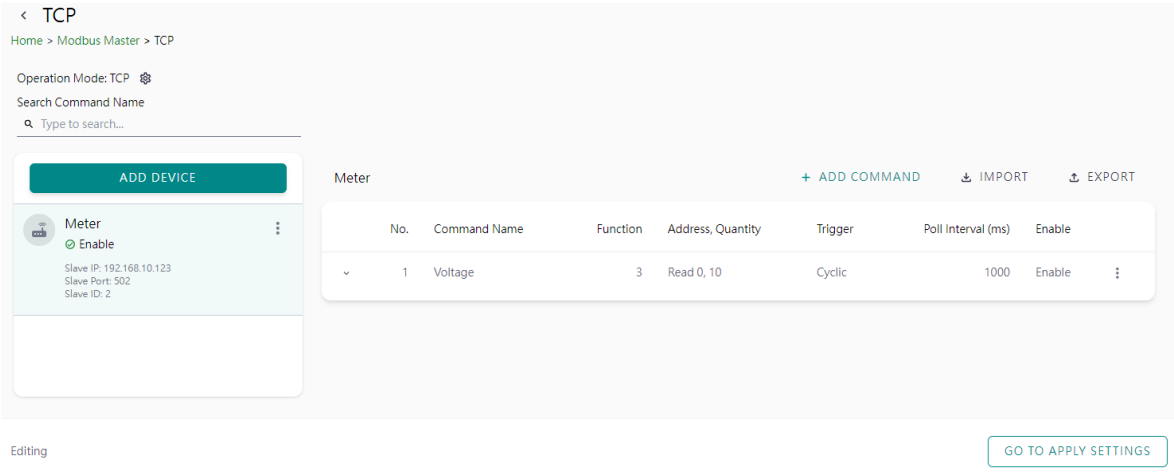
Parameter	Value	Default	Description
Command Name	Alphanumeric string		Max. 32 characters.
Function	**1 - Read Coils** **2 - Read Discrete Inputs** **3 - Read Holding Registers** **4 - Read Inputs Registers** **5 - Write Single Coil** **6 - Write Single Register** **15 - Write Multiple Coils** **16 - Write Multiple Registers** **23 - Read/Write Multiple Registers**		When a message is sent from a Client to a Server device, the function code field tells the server what kind of action to perform.
Trigger	**Cyclic** **Data Change** **Disable**		Disable: The command was never 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.
Poll Interval (This will show up when you select trigger mode 'cyclic'.)	100 to 1200000 ms	1000	Polling intervals are in milliseconds. Since the module sends all requests in turns, the actual polling interval also depends on the number of requests in the queue and their parameters. The range is from 100 to 1,200,000 ms.

Parameter	Value	Default	Description
Endian Swap	**None** **Byte** **Word** **Byte and Word**	None	Data Byte Swapping None: Don't need to swap Byte: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0B, 0x0A, 0x0D, 0x0C Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0C, 0x0D, 0x0A, 0x0B. Byte and Word: 0x0A, 0x0B, 0x0C, 0x0D becomes 0x0D, 0x0C, 0x0B, 0x0A.
Read Starting Address	0 to 65535	0	Modbus register address.
Read Quantity	Read Coils: 1 to 2000 Read Discrete Inputs: 1 to 2000 Read Inputs Registers: 1 to 125 Read Holding Registers: 1 to 125 Read/Write Multiple Registers: 1 to 125	10	Specifying how many items to read.
Write Starting Address	0 to 65535	0	Modbus register address.
Write Quantity	Write Multiple Coils: 1 to 1968 Write Multiple Registers: 1 to 123 Read/Write Multiple Registers: 1 to 123	1	Specifying how many items to write into.
Fault Protection	Keep latest data Clear all data bits to 0 Set to user defined value		If the MGate's connection to the other side (server/slave) fails, the gateway cannot receive data, but the gateway will continuously send output data to the Modbus TCP server device. To avoid problems in this case, the MGate can be configured to react in one of the following three ways: Keep the latest data, clear data to zero, set the data bits to user-defined values.
User-defined Value (This will show up when you select Fault Protection mode as 'Set to user defined value'.)	00 to FF (Hex)	00 00	The user-defined values to write into the data bits when the Set to user defined value option is selected.
Fault Timeout (This will show up when you select Fault Protection mode as 'Set to user defined value'.)	1 to 86400 ms	3600	Defines the communication timeout for the opposite side.
Tag Type	**raw, boolean, int16, int32, int64, uint16, uint32, uint64, float, double, string**	raw	Specifying the tag data type. The default is raw for fast multiple data mapping. For other data types, you could also scale the resource data. There are two types: • Slope-intercept: tag value = (source value * slope) +offset • Point-slope: tag value = source value * $(\frac{\text{target max. - target min.}}{\text{source max. - source min.}})$

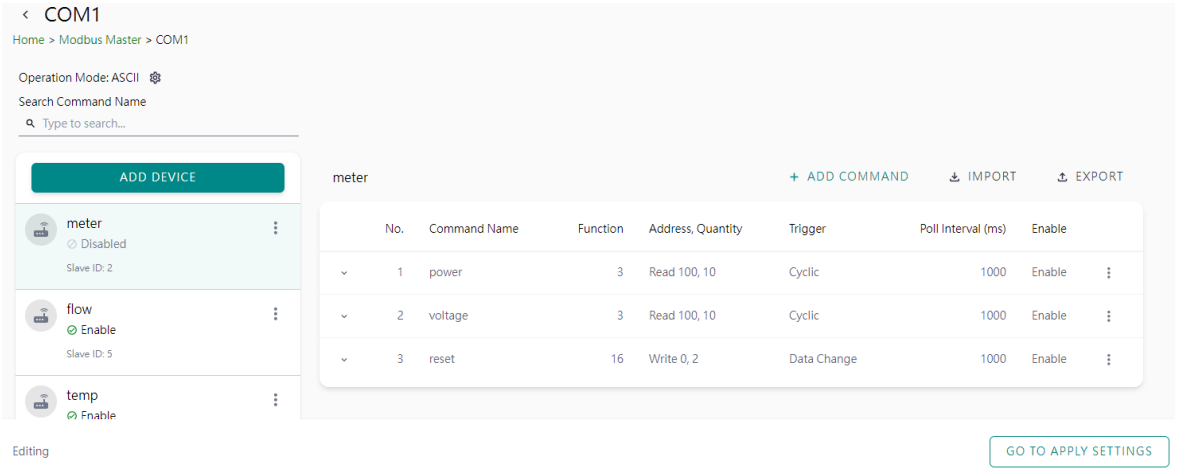
Step 3: Quick review result, click DONE to finish



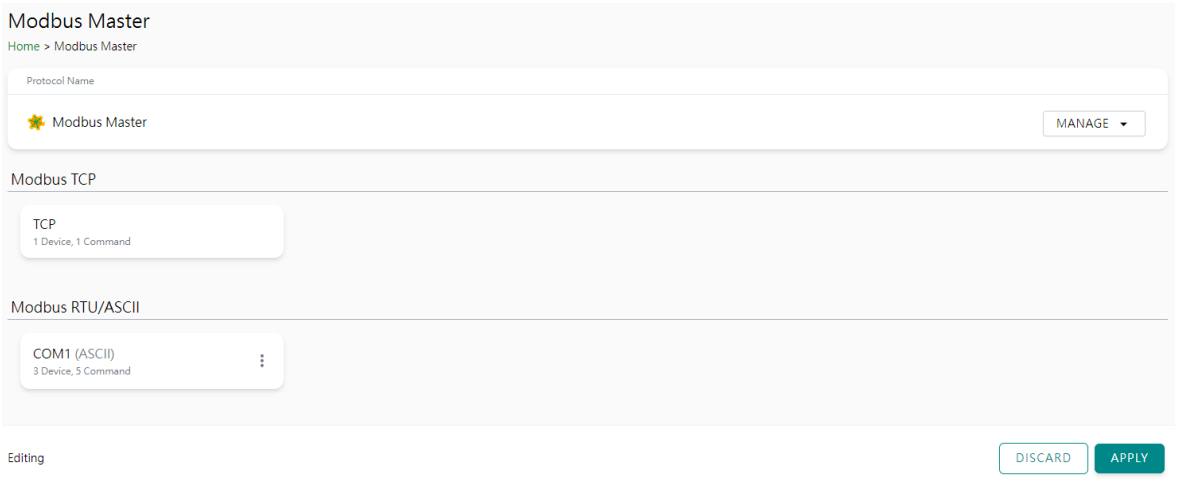
It is convenient if you already backed up a frequently used meter profile, just import or export one Modbus device CSV file.



Follow the same steps for Modbus RTU/ASCII devices in serial port.

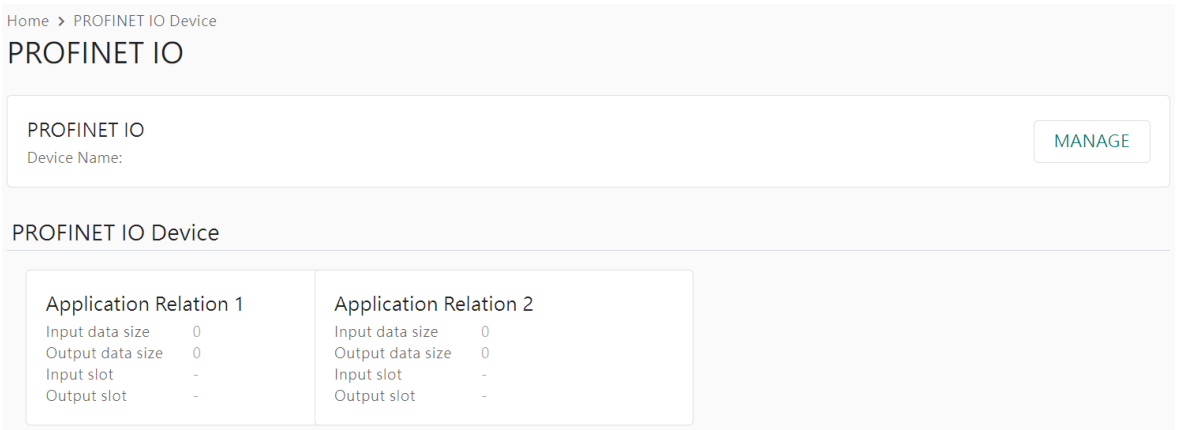


After configuring all Modbus TCP or Modbus RTU/ASCII settings, please remember to click **GO TO APPLY SETTING** and press the **APPLY** button at the bottom right-hand side corner.

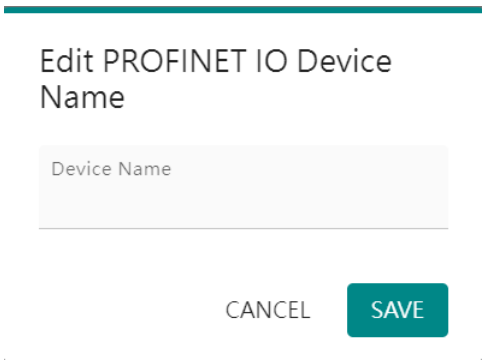


Protocol Settings—PROFINET IO Device Settings

You can configure the PROFINET IO Device setting on this page. The MGate 5134 supports two Application Relations (Ars) for two PLCs to access the same data via a shared device feature.

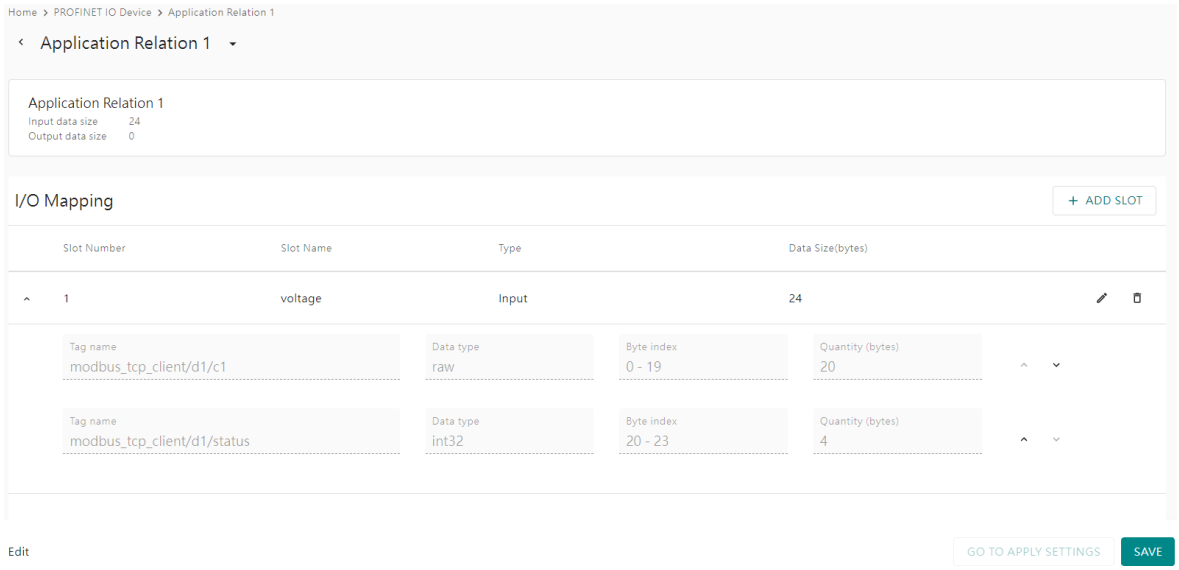


Click **MANAGE** to edit PROFINET Device Name.

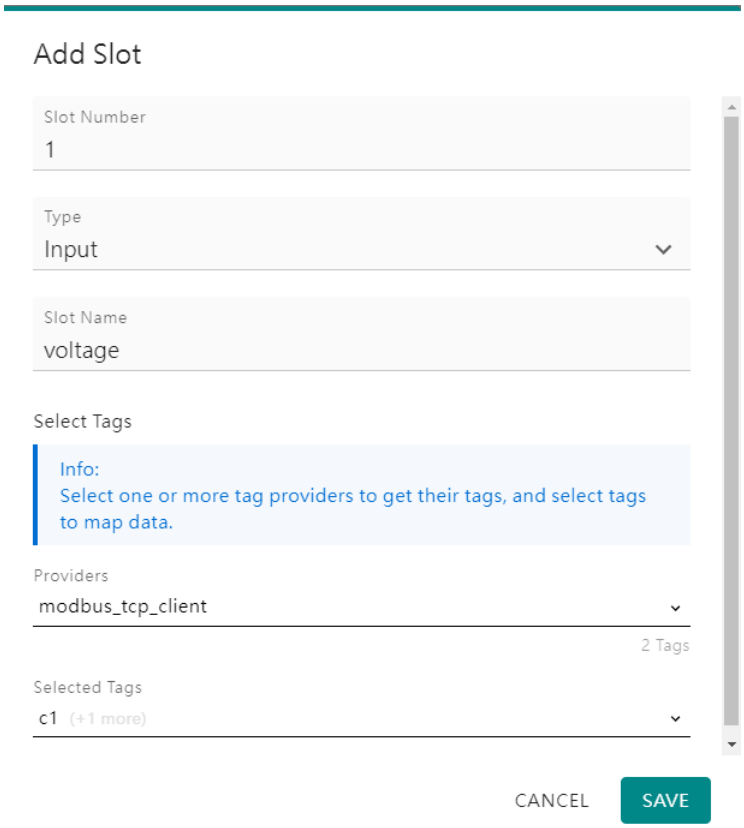


Parameter	Value	Description
Device Name	<alphanumeric string>	Enter the PROFINET server name (if you type the name incorrectly, the connection will fail).

Click on the **Application Relation** button to add tag data.

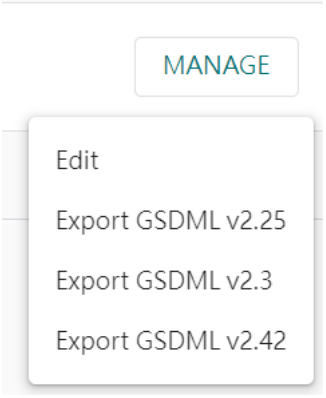


Click **ADD SLOT** in the I/O Mapping to add tag data to PROFINET slots.



Parameter	Value	Description
Slot number	1 to 128	Slot number in PROFINET IO Controller program develops environment setting
Type	Input Output	Input or output type to PROFINET IO Controller
Slot Name	<alphanumeric string>	Set the name for slot
Providers		Select what tag data you would like to map to PROFINET

On completing the PROFINET mappings, click MANAGER to export the GSDML files. A GSDML file is used for easy configuration when setting the PROFINET IO controller system. Typically, users waste a lot of time on importing the MGate 5134 general GSDML files and setting the IO modules, respectively. If we import the specified GSDML, which is based on Modbus settings, we just need to pull the module to the PROFINET system. Then, the IO modules will be set, and you can run the communication.

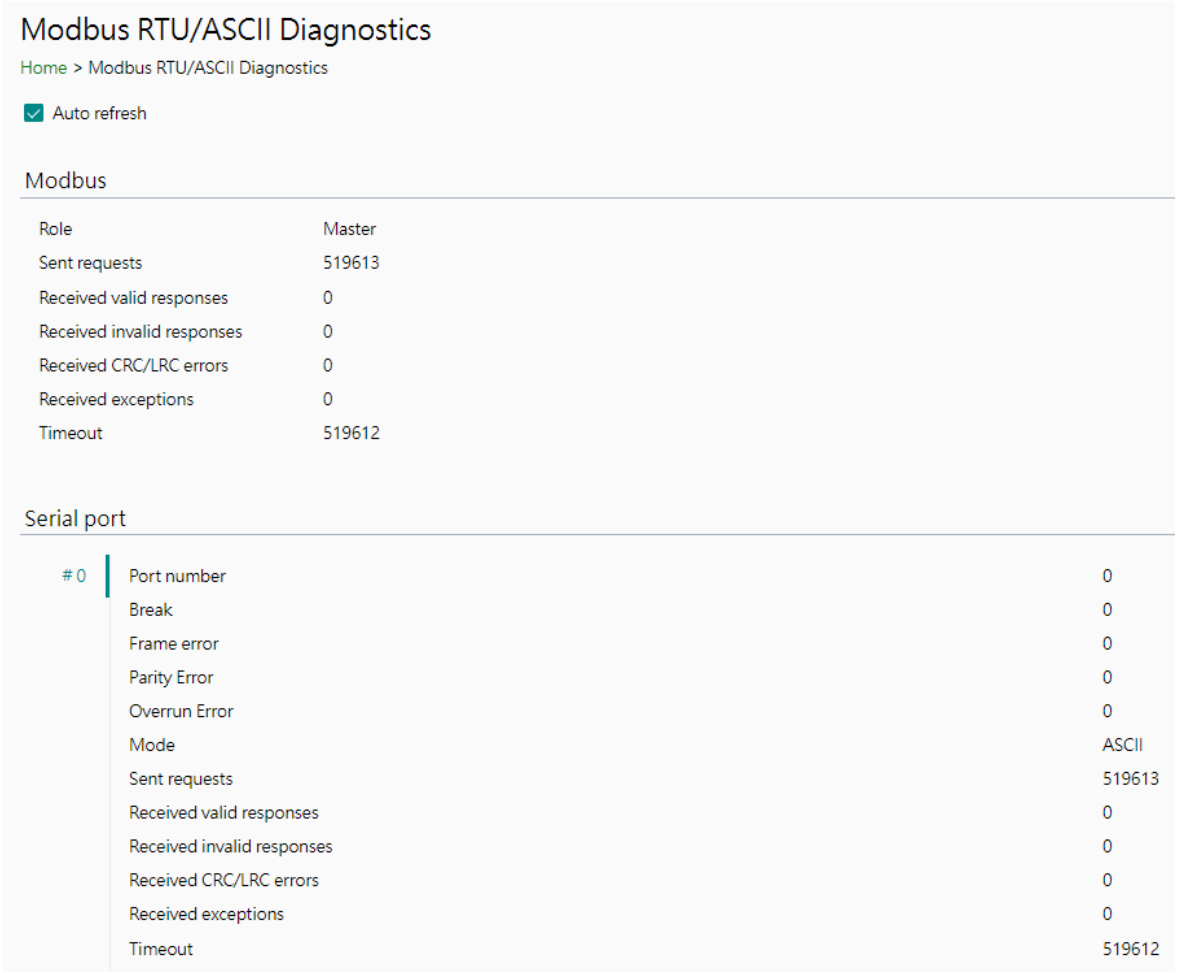


Diagnostics

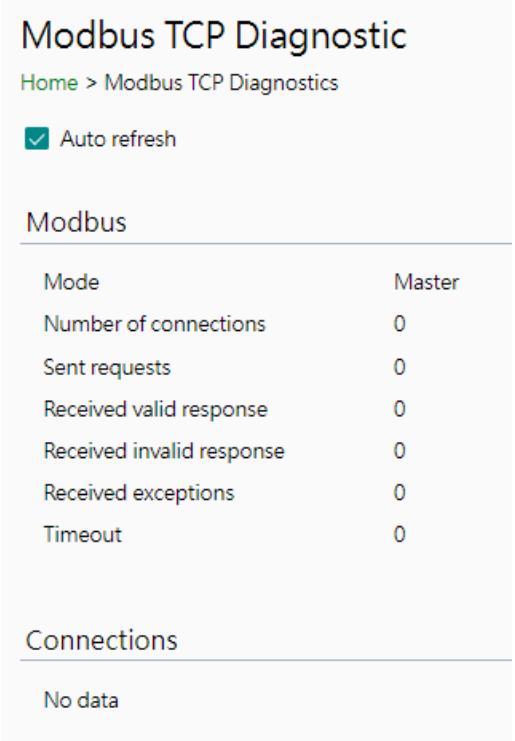
Diagnostics—Protocol Diagnostics

Diagnostics—Protocol Diagnostics—Modbus RTU/ASCII Diagnostic

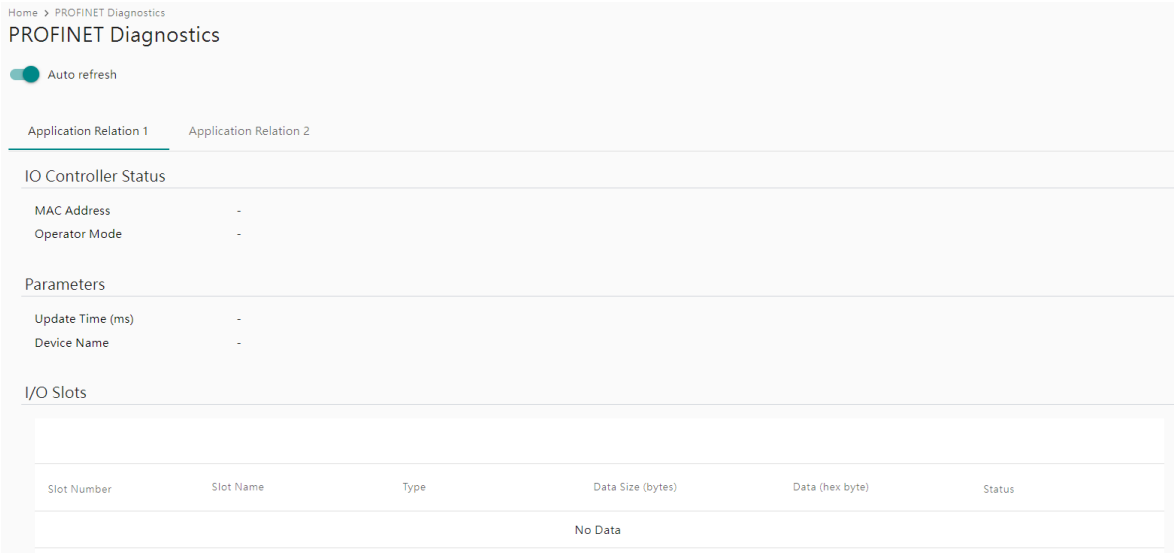
The MGate provides status information for Modbus RTU/ASCII/TCP, EtherNet/IP troubleshooting. Verify data or packet counters to make sure the communications are running smoothly.



Diagnostics—Protocol Diagnostics-Modbus TCP Diagnostics



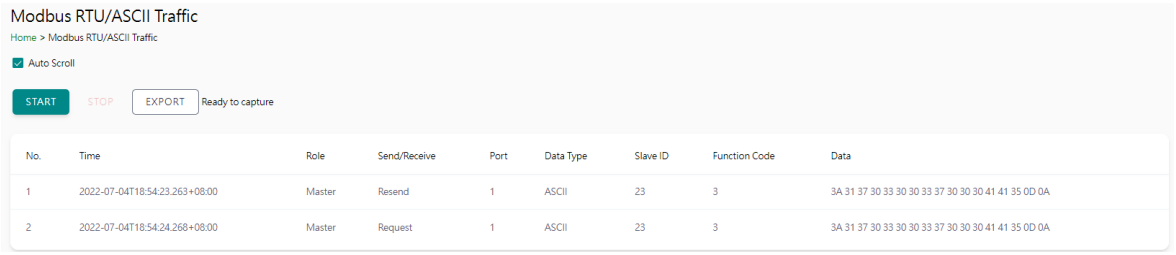
Diagnostics—Protocol Diagnostics- PROFINET Diagnostics



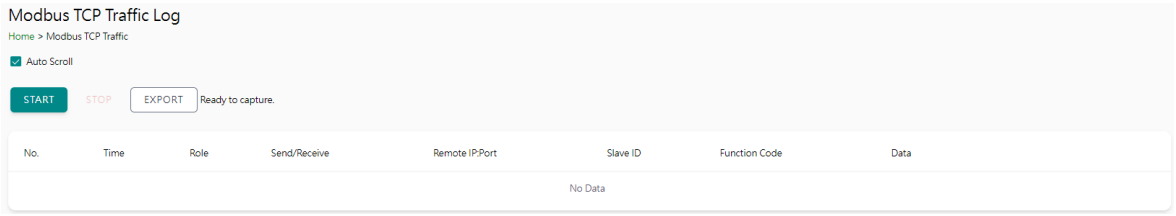
Diagnostics—Protocol Traffic

Diagnostics—Protocol Traffic-Modbus RTU/ASCII Traffic

To troubleshoot efficiently, the MGate provides a traffic monitoring function that can capture communication traffic for all protocols. These logs present the data in an intelligent, easy-to-understand format with clearly designated fields, including source, destination, function code, and data. Save the complete log in a file by clicking EXPORT csv file.



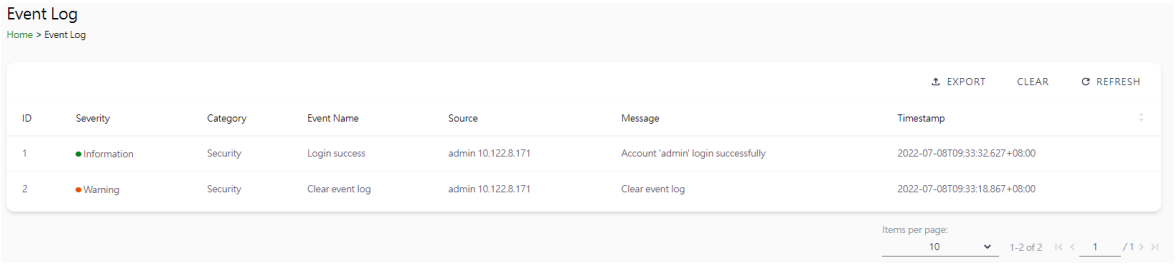
Diagnostics—Protocol Traffic-Modbus TCP Traffic



Diagnostics—Event Log

Diagnostics—Event Log-Log View

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

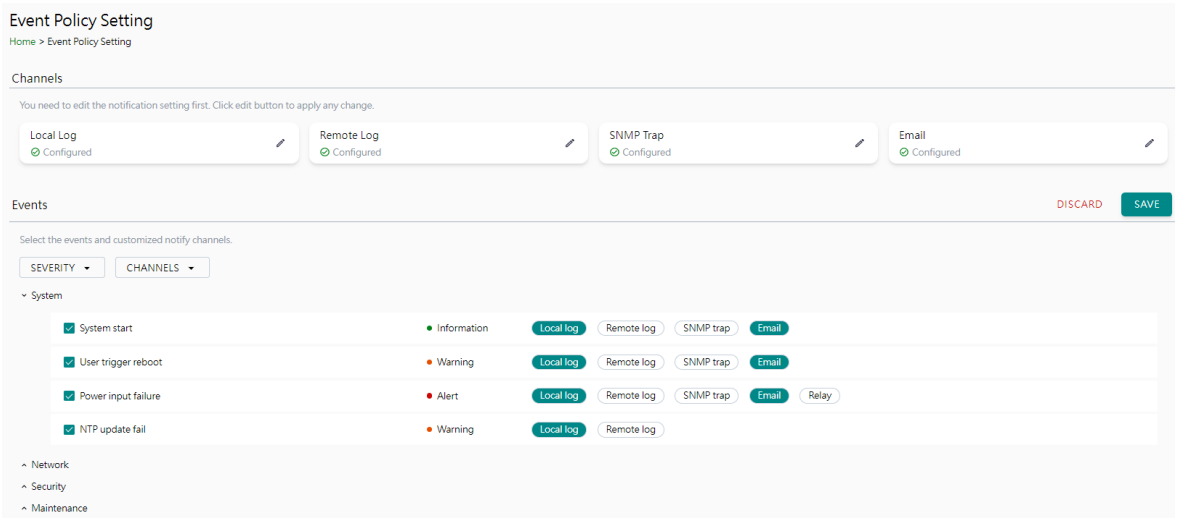


Diagnostics—Event Log-Policy Settings

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

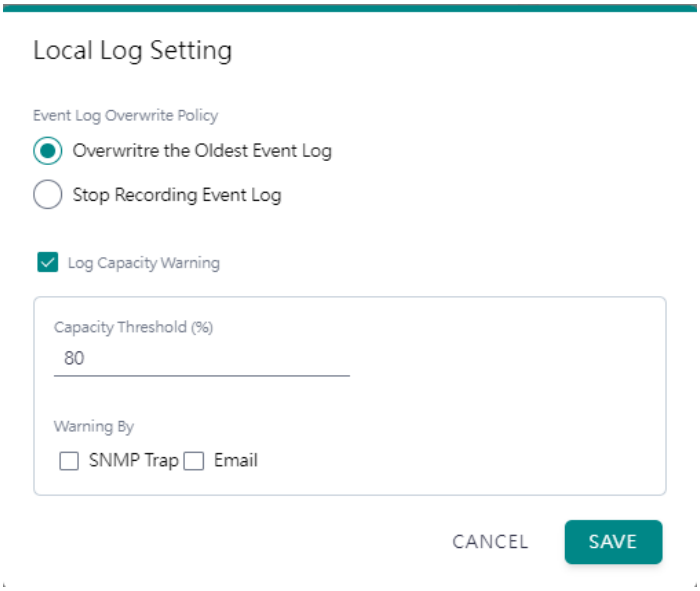
The MGate can also send email alerts, SNMP Trap messages, or open/close the circuit of the relay output when a selected event was triggered.

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



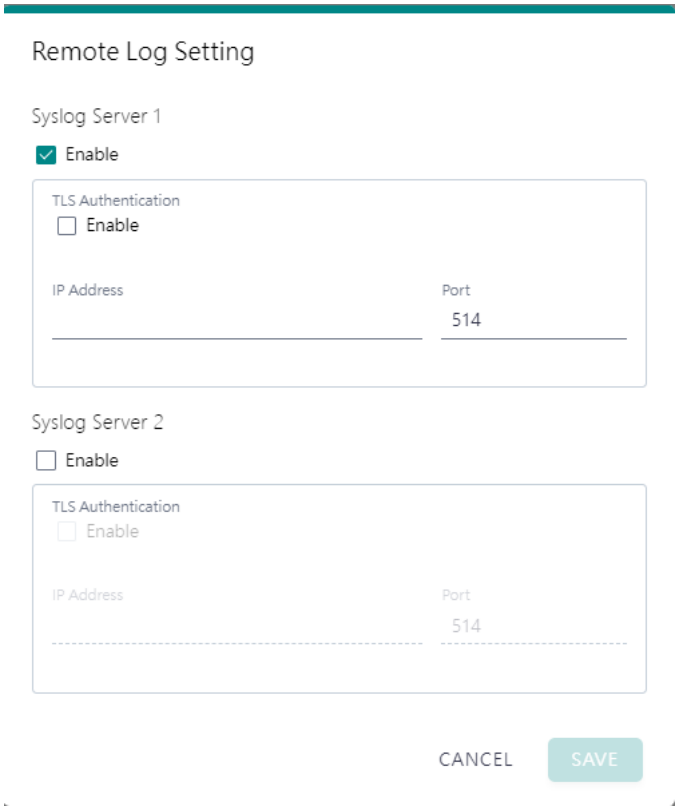
Event Group	Description
System	Start system, User trigger reboot, Power input failure, NTP update failure
Network	IP conflict, DHCP get IP/renew, IP changed, Ethernet link down
Security	Clear event log, Login success, Login failure, Account/group changed, Password reached lifetime, SSL certificate import,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

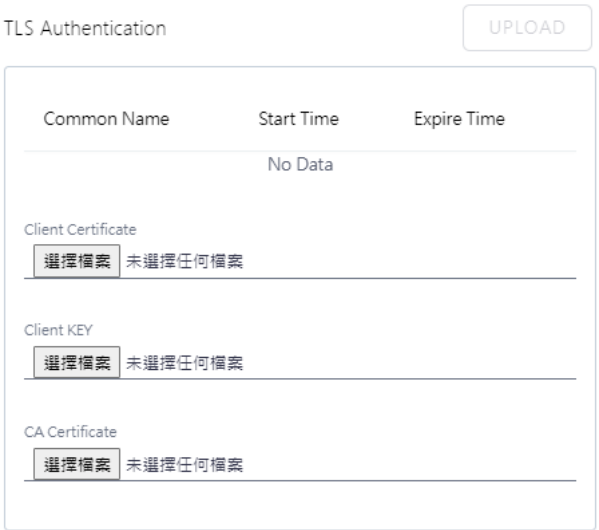
Local Log Settings



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

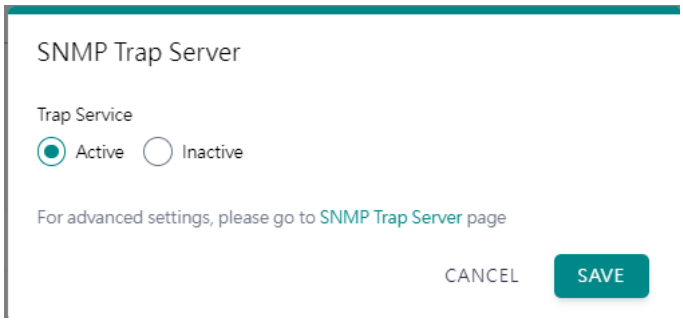
Remote Log Settings



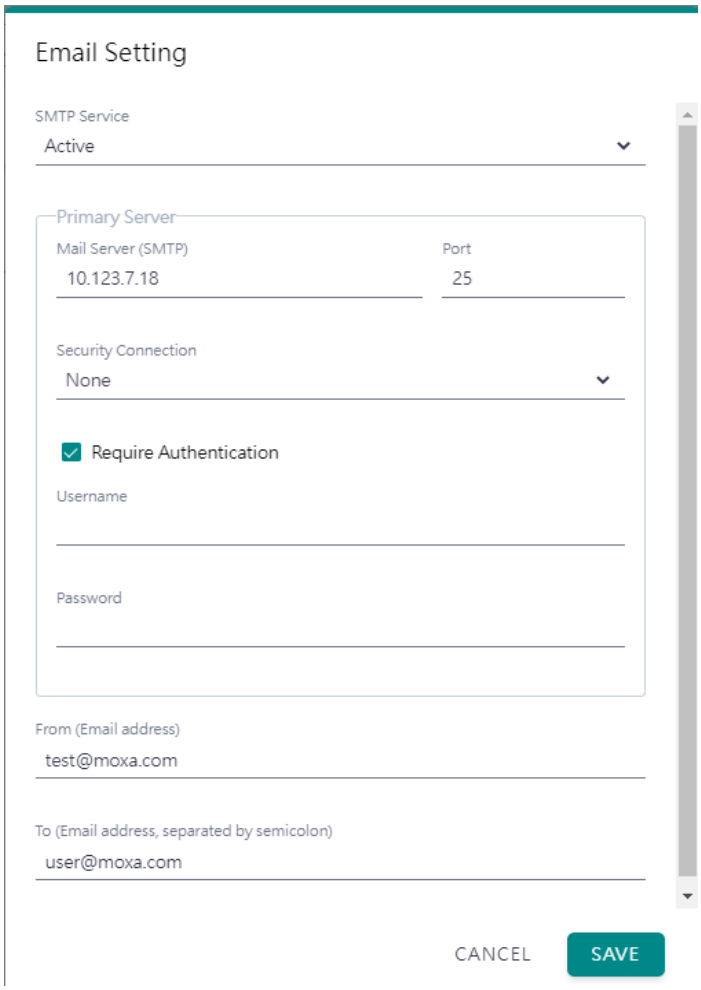


Remote Log Settings	Description
Syslog Server IP	IP address of a server that will record the log data
Syslog Server port	514
TLS Authentication	Enable TLS authentication. Notice TLS files must be uploaded for a successful connection.

SNMP Trap Settings



Email Settings

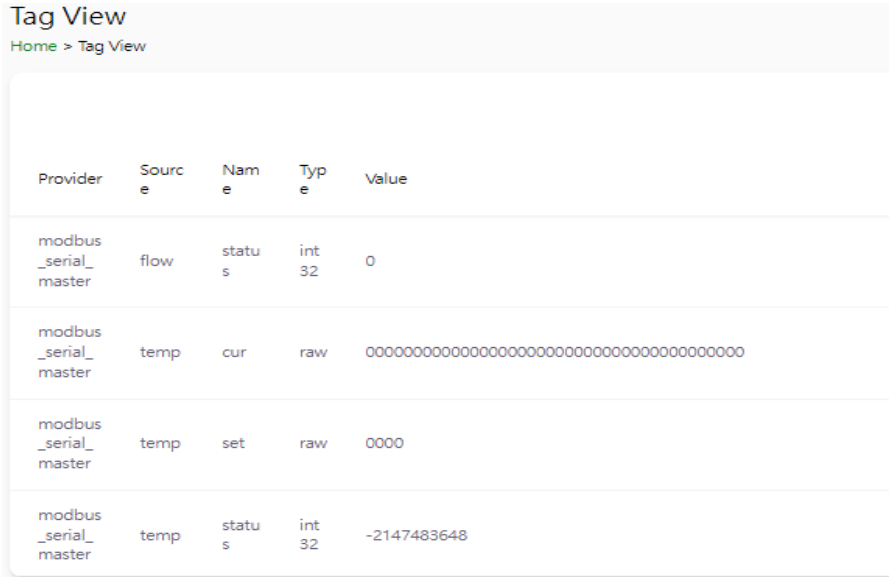


Parameters	Description
Mail Server (SMTP)	The mail server's domain name or IP address.
Port	The mail server's IP port.
Security Connection	TLS STARTTLS STARTTLS-None None
Username	This field is for your mail server's username, if required.
Password	This field is for your mail server's password, if required.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

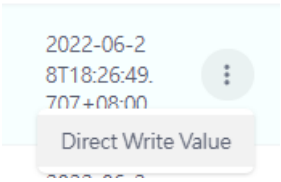
Parameters	Description
To (Email address, separated by semicolon)	Email addresses to which automatic email warnings will be sent.

Diagnostics—Tag View

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

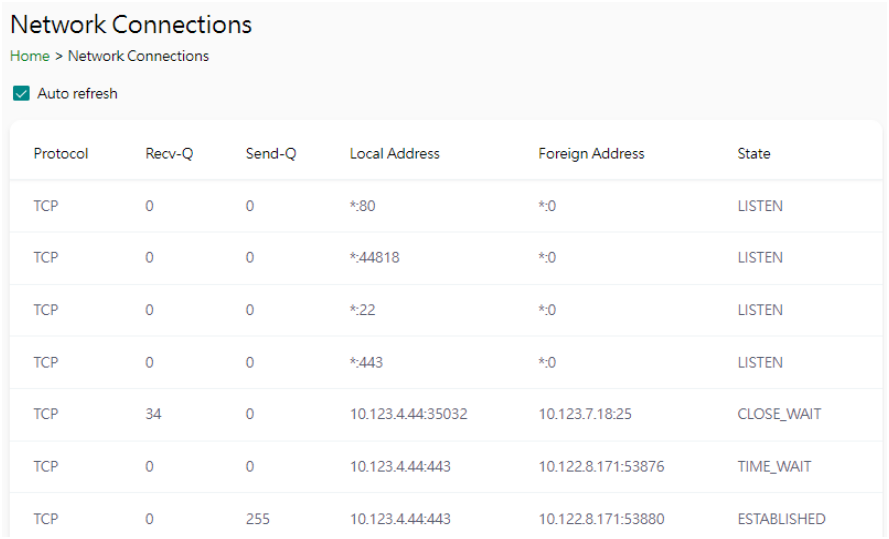


You can write a value to the Modbus via Direct Write Value to test the communication with Modbus device.



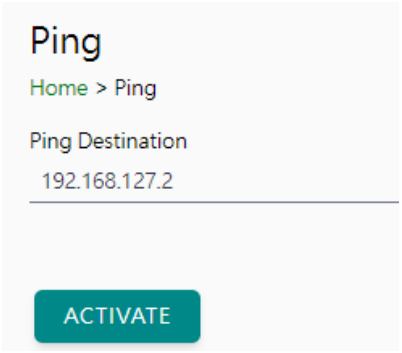
Diagnostics—Network Connections

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



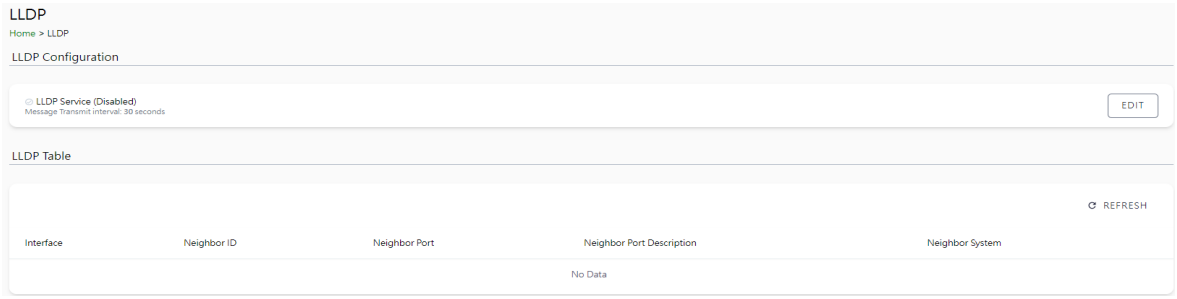
Diagnostics—Ping

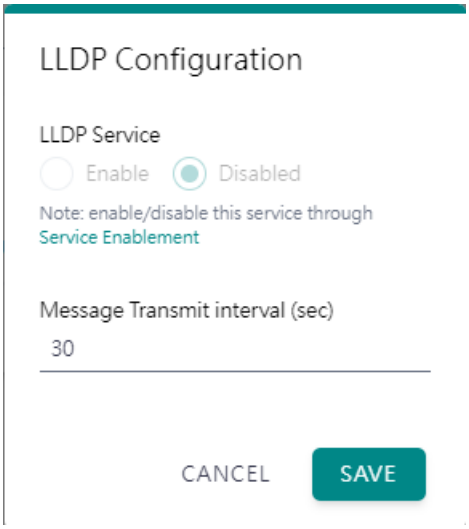
This network testing function is available only in the web console. The MGate gateway will send an ICMP packet through the network to a specified host, and the result can be viewed on the web console immediately.



Diagnostics—LLDP

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

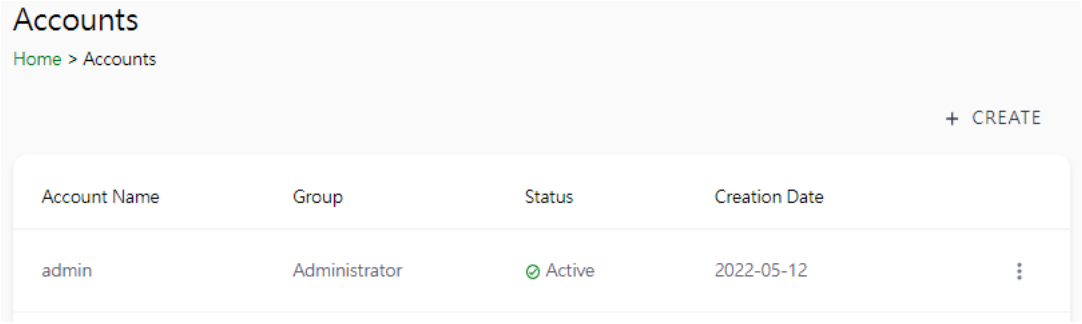




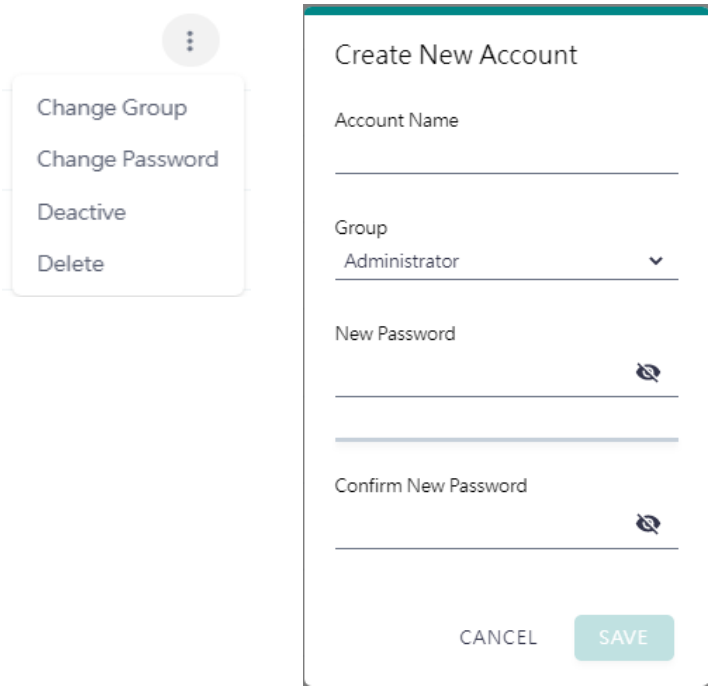
Security

Security—Account Management

Security—Account Management—Accounts

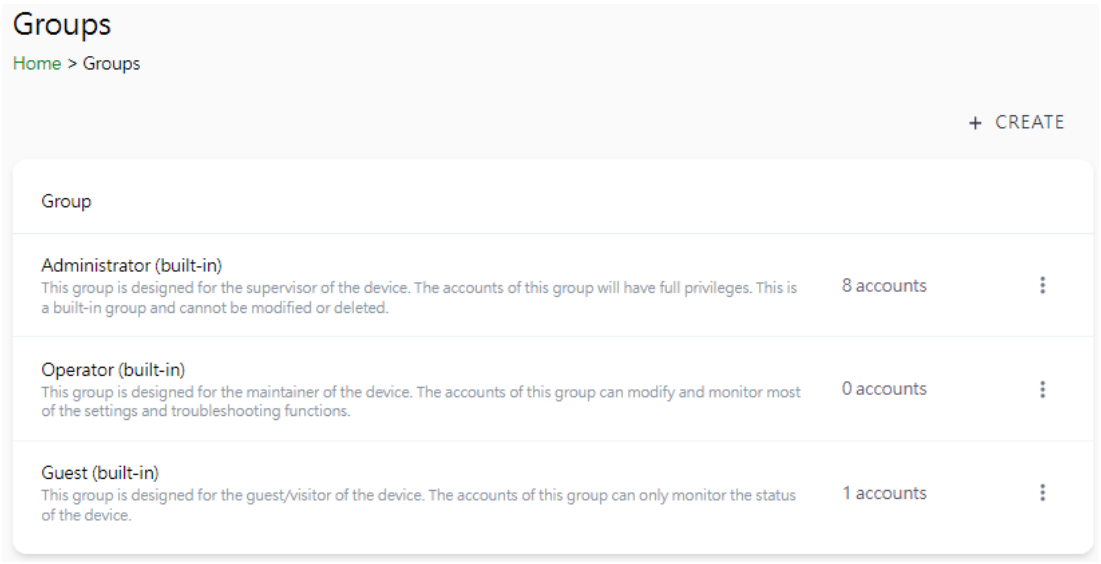


Only Administrator group can create or edit accounts for user management. Click **CREATE** to add new accounts. Click the dot icon to edit the account.

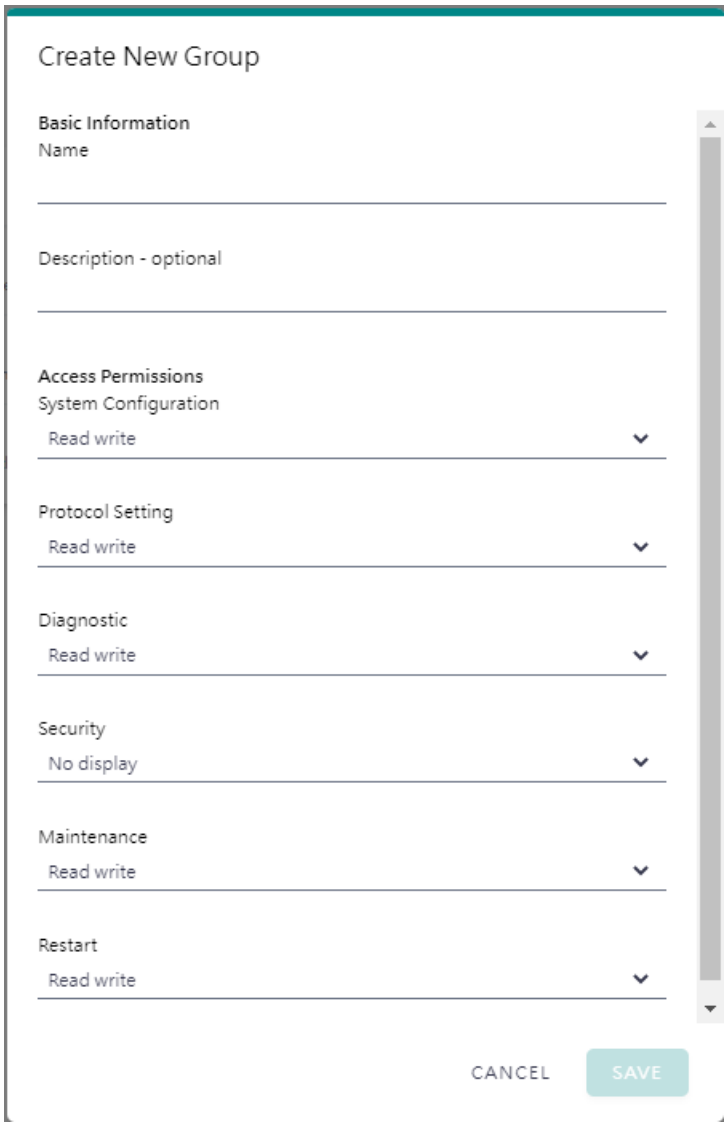


Parameters	Value	Description
Group	Administrator, Operator, Guest	Users can change the password for different accounts. The MGate provides three build-in account groups, administrator, operator and guest. Administrator account can access all settings. Operator accounts can access most settings, except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

Security—Account Management—Groups

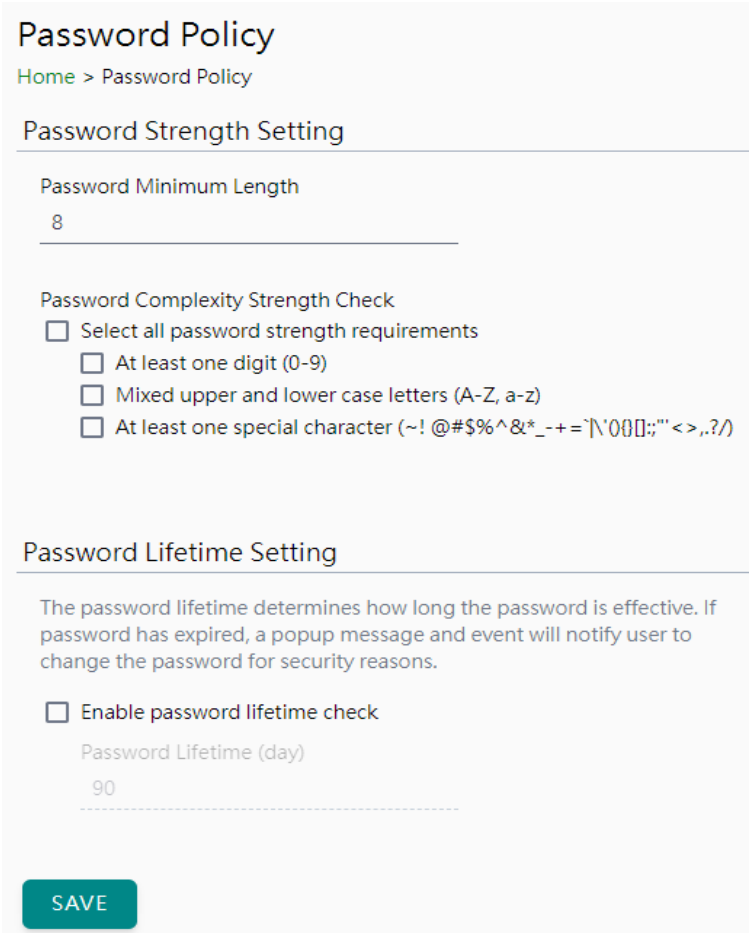


Three MGate build-in types of groups are shown; you can also create your own group by clicking **CREATE.**



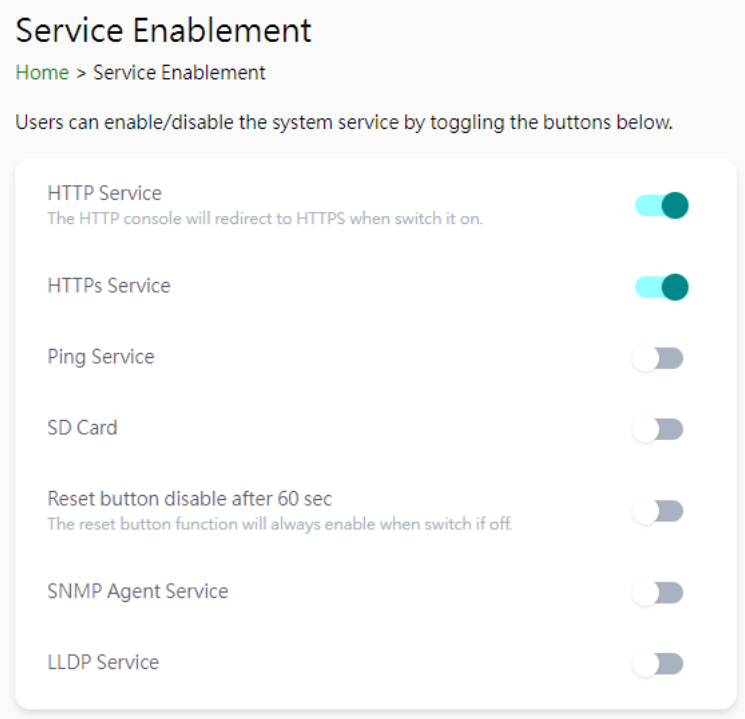
Parameters	Value	Description
Basic Information		Includes Name and Description for the new Group.
Access Permissions	No display Read only Read write	Corresponding to the configuration menu on the left-hand side of the web console, you can select different permissions for a new group. Displays will not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

Security—Account Management—Password Policy



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

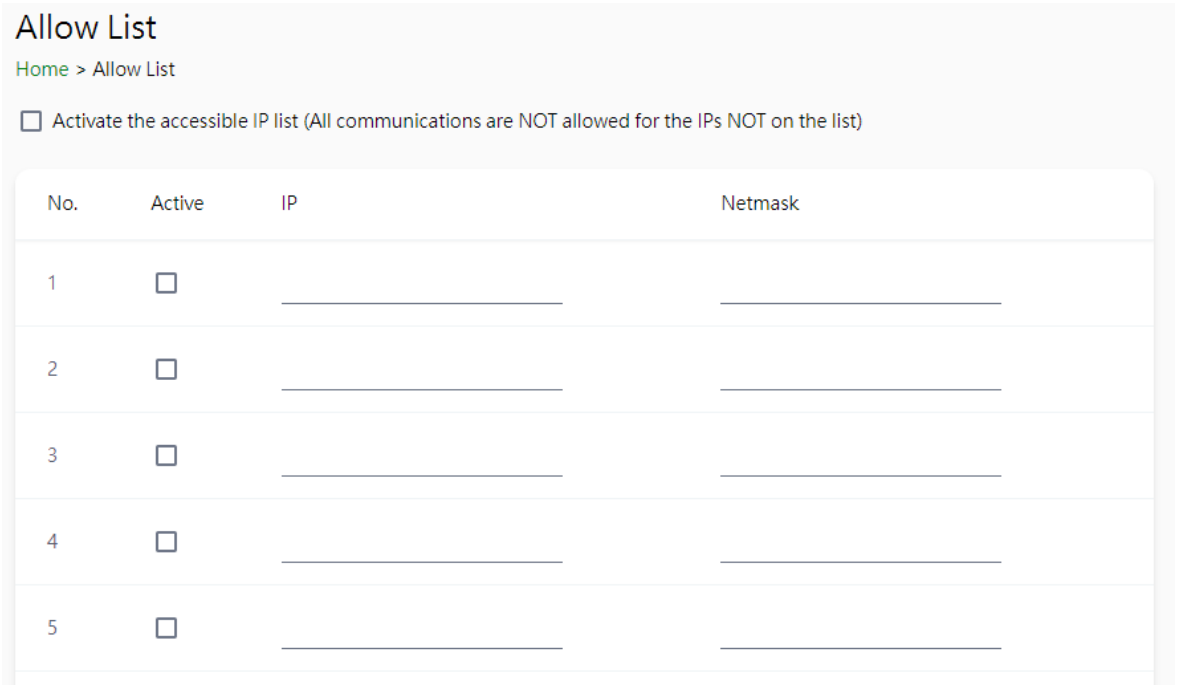
Security—Service



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

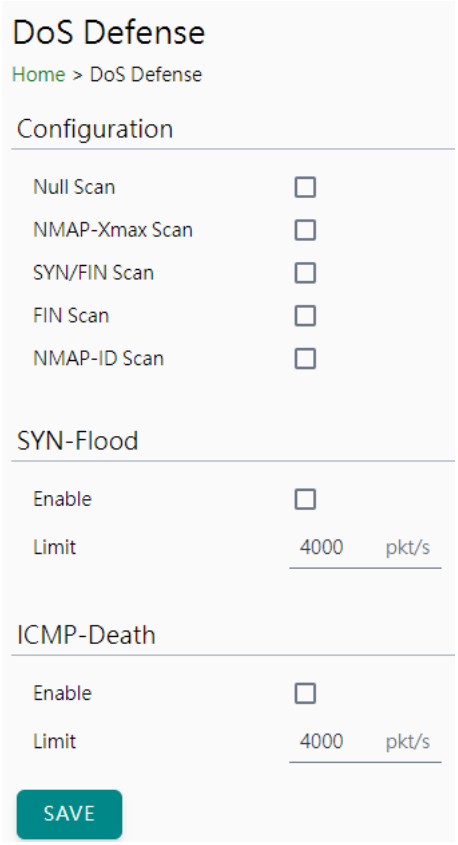
Security—Allow List

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



Security—DoS Defense

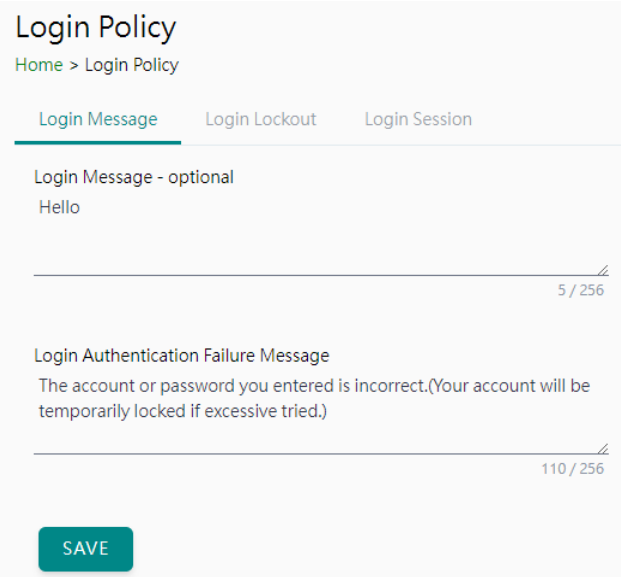
Users can select from several options to enable DoS Defense to fend off cybersecurity attacks. A denial-of-service (DoS) attack is an attempt to make a machine or a network resource unavailable. Users can select from the following options to counter DoS attacks.



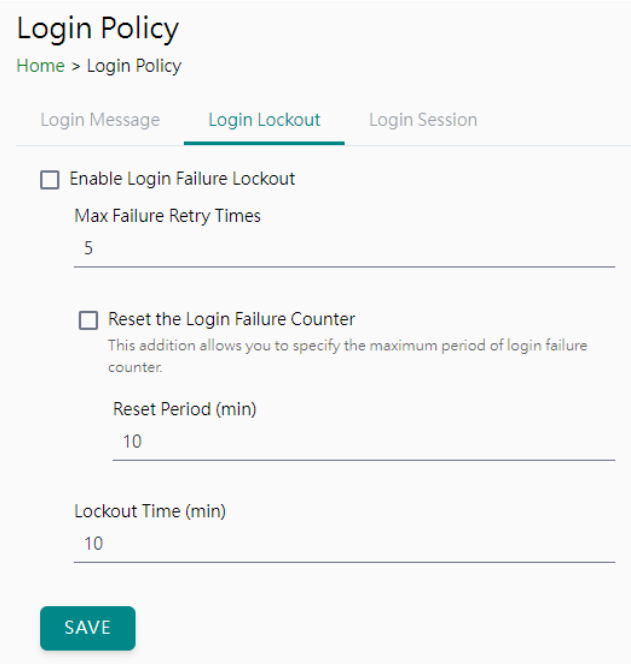
Security—Login Policy

Login Message

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

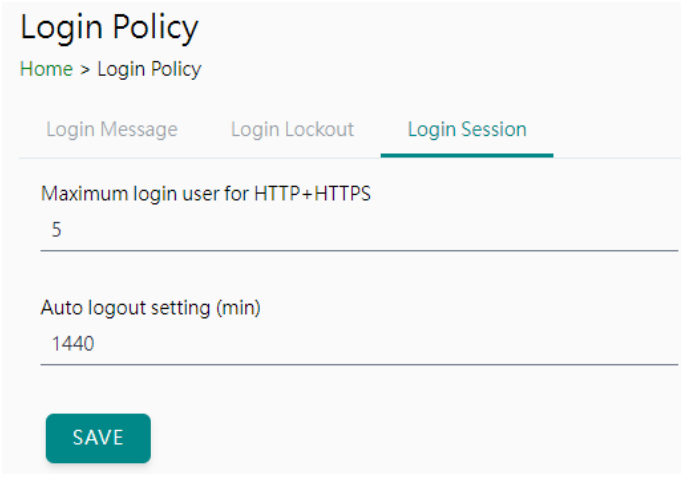


Login Lockout



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

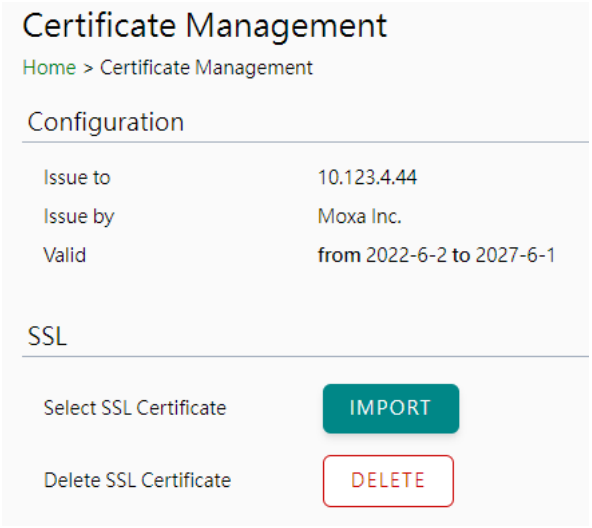
Login Session



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

Security—Certificate Management

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



Maintenance

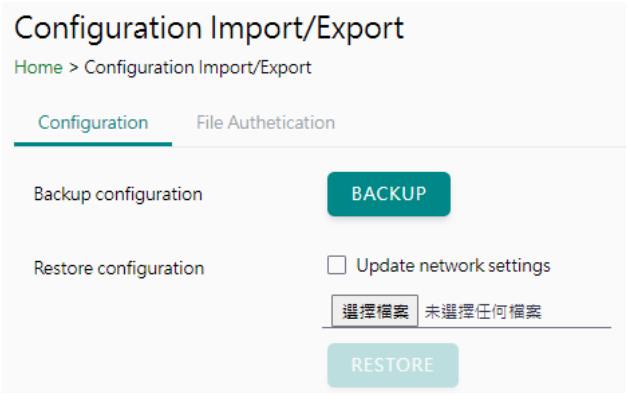
Maintenance—Configuration Import/Export

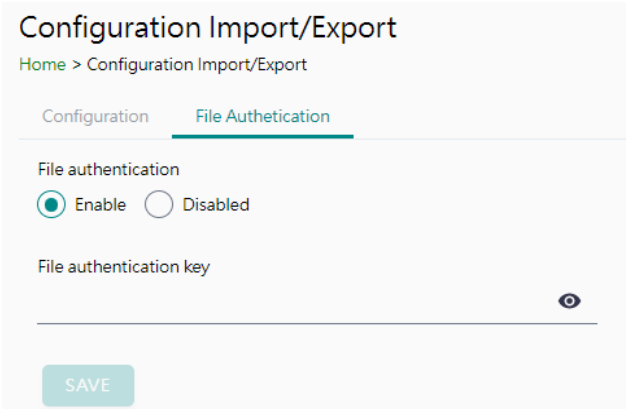
There are three main reasons for using the Import and Export functions:

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

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

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





Maintenance—Firmware Upgrade

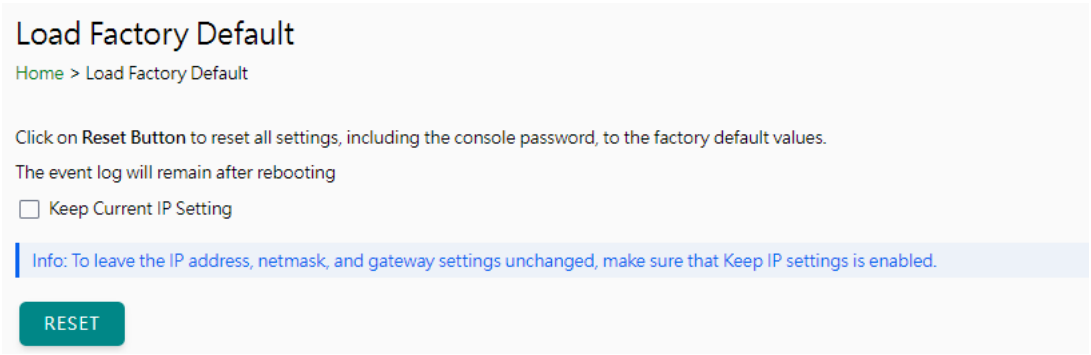
Firmware updates for the MGate are available on the Moxa website. After you have downloaded the new firmware onto your PC, you can use the web console to write it onto your MGate. Select the desired unit from the list in the web console and click **Submit** to begin the process.

ATTENTION

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

Maintenance—Load Factory Default

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



ATTENTION

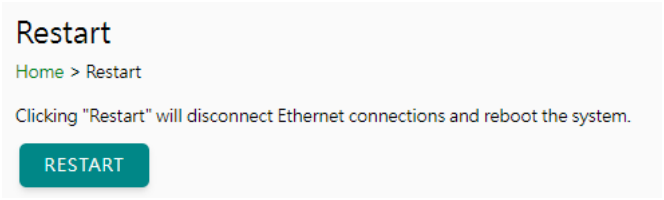
Load Default will completely reset the configuration of the unit, and all the parameters you have saved will be discarded. Do not use this function unless you are sure you want to completely reset your unit.

Restart

You can reboot the MGate by clicking the RESTART button.

ATTENTION

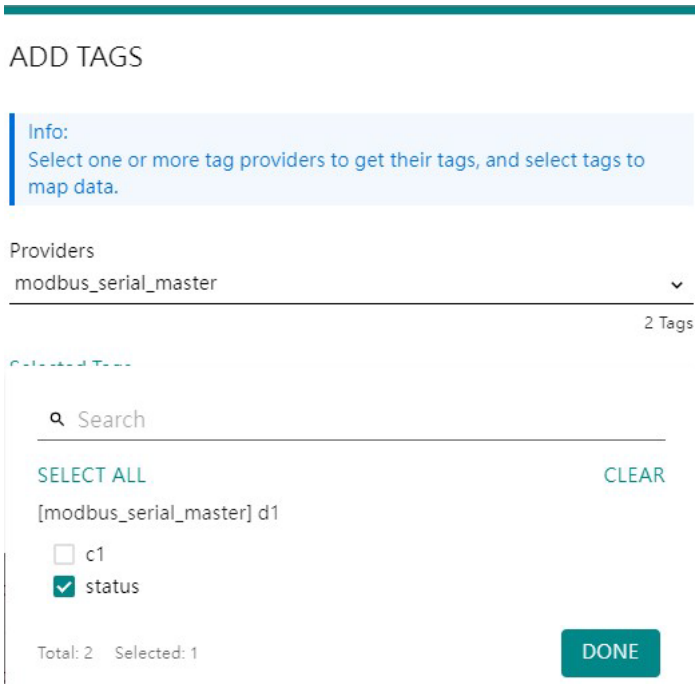
Unsaved configuration files will be discarded during a reboot.



Status Monitoring

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

The MGate will create a status tag when a Modbus device is created. This shows if the Modbus device connection is valid or invalid. However, these tags cannot be added to the EtherNet/IP mapping of a client (e.g., PLC) to get the alive status of the Modbus devices.



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

Provider	Source	Name	Type	Value	Timestamp
modbus_tcp_master	Meter1	status	int32	valid (0x0000)	2022-08-01T10:41:10.542+08:00

Provider	Source	Name	Type	Value	Timestamp
modbus_tcp_master	Meter1	status	int32	invalid (0x80000000)	2022-08-01T10:46:31.403+08:00

4. Network Management Tool (MXstudio)

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

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

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

A. SNMP Agents with MIB II and RS-232-Like Groups

The MGate has built-in Simple Network Management Protocol (SNMP) agent software that supports SNMP Trap, RFC1317 and RS-232-like groups, 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

RFC1317 RS-232-Like Groups

RS-232 MIB	Async Port MIB
rs232Number	rs232AsyncPortIndex
rs232PortIndex	rs232AsyncPortBits
rs232PortType	rs232AsyncPortStopBits
rs232PortInSigNumber	rs232AsyncPortParity
rs232PortOutSigNumber	
rs232PortInSpeed	
rs232PortOutSpeed	

Input Signal MIB	Output Signal MIB
rs232InSigPortIndex	rs232OutSigPortIndex
rs232InSigName	rs232OutSigName
rs232InSigState	rs232OutSigState