

MGate 5134 Series User Manual

Version 1.0, September 2022

www.moxa.com/products

MOXA[®]

© 2022 Moxa Inc. All rights reserved.

MGate 5134 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

© 2022 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

| | |
|--|-----------|
| 1. Introduction | 4 |
| 2. Getting Started | 5 |
| Connecting the Power | 5 |
| Connecting Serial Devices | 5 |
| Connecting to a Network | 5 |
| Installing DSU Software | 5 |
| Log In to the Web Console | 6 |
| microSD | 7 |
| 3. Web Console Configuration and Troubleshooting | 8 |
| System Overview Dashboard | 8 |
| System Settings | 9 |
| System Settings—General Settings | 9 |
| System Settings—Network Settings | 11 |
| System Settings—Serial Settings | 13 |
| System Settings—SNMP Settings | 14 |
| Protocol Settings | 18 |
| Protocol Settings—Modbus Client Settings | 18 |
| Protocol Settings—PROFINET IO Device Settings | 24 |
| Diagnostics | 28 |
| Diagnostics—Protocol Diagnostics | 28 |
| Diagnostics—Protocol Traffic | 30 |
| Diagnostics—Event Log | 30 |
| Diagnostics—Tag View | 34 |
| Diagnostics—Network Connections | 35 |
| Diagnostics—Ping | 35 |
| Diagnostics—LLDP | 36 |
| Security | 37 |
| Security—Account Management | 37 |
| Security—Service | 40 |
| Security—Allow List | 41 |
| Security—DoS Defense | 42 |
| Security—Login Policy | 43 |
| Security—Certificate Management | 44 |
| Maintenance | 45 |
| Maintenance—Configuration Import/Export | 45 |
| Maintenance—Firmware Upgrade | 46 |
| Maintenance—Load Factory Default | 46 |
| Restart | 47 |
| Status Monitoring | 47 |
| 4. Network Management Tool (MXstudio) | 48 |
| A. SNMP Agents with MIB II and RS-232-Like Groups | 49 |
| RFC1213 MIB-II Supported SNMP Variables | 49 |
| RFC1317 RS-232-Like Groups | 50 |

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

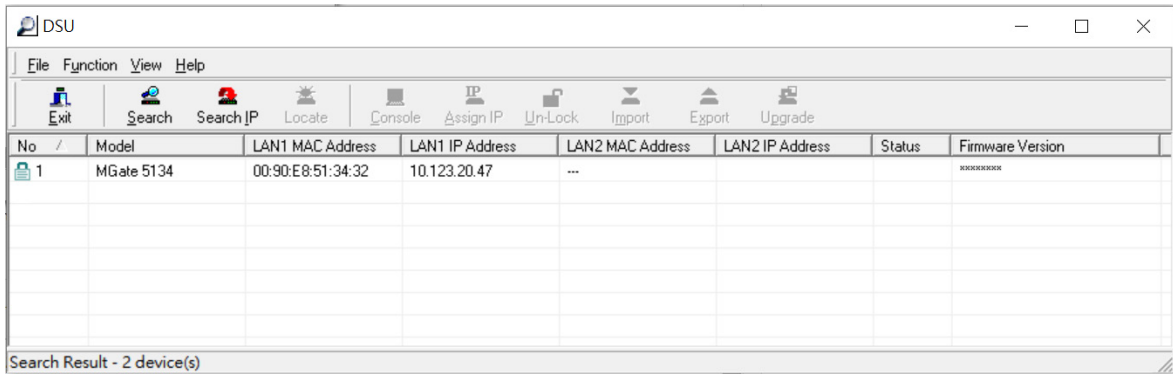
If you do not know the MGate gateway's IP address when setting it up for the first time (default IP is *192.168.127.254*); use an Ethernet cable to connect the host PC and MGate gateway directly. If you connect the gateway and host PC through the same Ethernet switch, make sure there is no router between 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_xxxxxxx.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.



Log in to
MGate 5134_1234567

Account Name

Password

LOG IN

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.

The screenshot shows the 'System Dashboard' page for an MGate 5134 gateway. The interface includes a left-hand navigation menu with categories like 'DASHBOARD', 'SYSTEM SETTINGS', 'PROTOCOL SETTING', 'DIAGNOSTIC', and 'SECURITY'. The main content area is divided into several sections:

- System Information:** Displays a small image of the MGate 5134 device and its specifications: Model Name (MGate 5134), Serial No. (TEFD09876543), Firmware version (1.0.0 Build 22090811), Uptime (4 days 08h 48m 24s), IPv4 (10.123.4.46), MAC address (00:90:E8:83:2A:2), and MicroSD (Not detected).
- Panel Status:** Shows the status of various LEDs: System LED (PWR1, PWR2, READY), Port LED (ETH1, ETH2, PN, MB), and Relay State.
- Event Summary:** A summary table showing 47 Alerts, 122 Warnings, and 94 Info events. Below this is a detailed table of recent events.
- Relay State:** A table listing events such as 'Power input 1 failure', 'Power input 2 failure', 'Ethernet 1 link down', and 'Ethernet 2 link down', each with a state and an 'ACKNOWLEDGE' button.

| ID | Severity | Message | Timestamp |
|----|----------|---------------------------|-------------------------------|
| 1 | Alert | Power input 1 failure | 2022-09-08T03:56:05.110+08:00 |
| 2 | Alert | Ethernet port 1 link down | 2022-09-08T03:56:05.098+08:00 |
| 3 | Alert | Power input 1 failure | 2022-09-08T03:54:00.526+08:00 |
| 4 | Alert | Ethernet port 1 link down | 2022-09-08T03:54:00.520+08:00 |
| 5 | Alert | Power input 1 failure | 2022-09-07T07:17:06.923+08:00 |
| 6 | Alert | Ethernet port 1 link down | 2022-09-07T07:17:06.900+08:00 |

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

The image shows a user profile dropdown menu. At the top, it displays 'Administrator' and 'admin' with a downward arrow. Below this, there are two buttons: 'Change Password' and 'Log Out'.

System Settings

System Settings—General Settings

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

Home > General Settings

General Settings

System Time

Host Name
MGate 5134_1234567

Description - Optional

SAVE

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.

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

SAVE

| 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.

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

[SAVE](#)

| Parameter | Value | Description |
|-------------------------------|---|--|
| LAN Mode | Switch, Dual IP, Redundant LAN | <p>The Switch mode allows users to install the device with daisy-chain topology.</p> <p>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.</p> <p>NOTE: In the Dual IP mode, the PROFINET protocol can only be used on the LAN1 port (ETH1).</p> <p>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.</p> |
| 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.

| Port | Interface | Baud Rate | Parity, Data Bits, Stop Bits | Flow Control |
|----------|-----------|-----------|------------------------------|--------------|
| #1 AAAAA | RS-232 | 115200 | Even, 8, 1 | None |

< # 1

Home > Serial Setting > # 1

Alias

Interface

RS-485 2-wire

Terminator

120Ω None

Pull-up & Pull-down Resistor

1kΩ 150kΩ

Baud Rate

38400

Parity

None

Data Bits

5 6 7 8

Stop Bits

1 2

FIFO

Enable Disabled

| 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. |

Flow Control
RTS toggle RTS on delay: 0 RTS off delay: 0

| 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

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

SAVE

| 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:

SNMP Agent

Home > SNMP Agent

General **SNMPv3 Account** SNMPv3 Account Protection

+ CREATE
maximum number of account is 2

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

Create SNMPv3 Account

Account Name

Authority

Read Only ▼

Authentication Type

Disable ▼

CANCEL SAVE

| 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. |

SNMP Agent

General

SNMPv3 Account

SNMPv3 Account Protection

 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

SAVE

| 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

SNMP Trap

Home > SNMP Trap

General SNMP Trap Server

Trap Service

Active Inactive

SAVE

SNMP Trap

Home > SNMP Trap

General SNMP Trap Server

+ CREATE
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

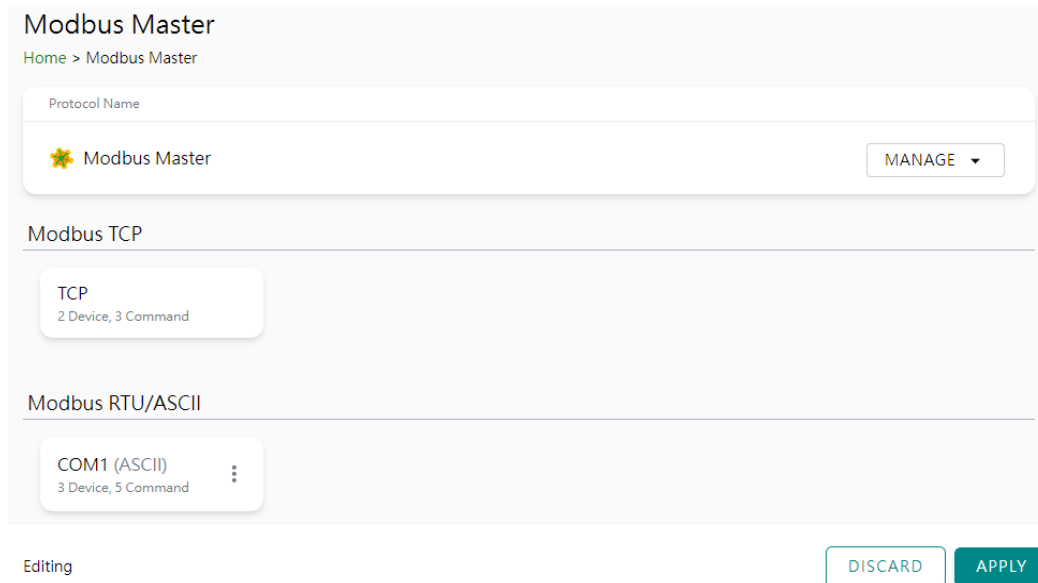
CANCEL **SAVE**

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

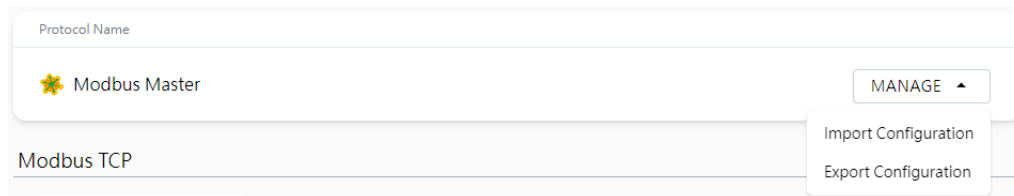
Protocol Settings

Protocol Settings—Modbus Client Settings

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

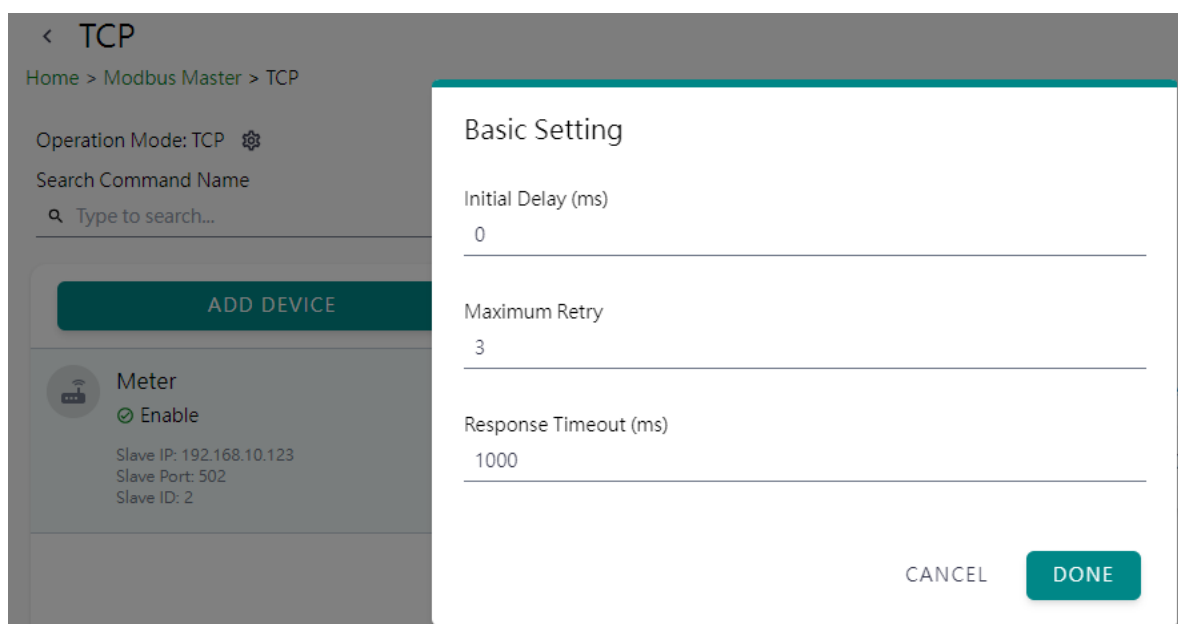


The MGate supports csv file import/export for Modbus settings; it is easy to use when you back up the settings or during installation stage.



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

The screenshot shows the 'TCP' configuration page for the Modbus Master. The breadcrumb is 'Home > Modbus Master > TCP'. The operation mode is set to 'TCP'. There is a search bar for command names. A green 'ADD DEVICE' button is visible. Below it, a device card for 'Meter' is shown, which is enabled and has the following details: Slave IP: 192.168.10.123, Slave Port: 502, and Slave ID: 2. To the right, a table titled 'Meter' lists the configured commands. The table has columns for No., Command Name, Function, Address, Quantity, Trigger, Poll Interval (ms), and Enable. One command is listed: No. 1, Command Name 'Voltage', Function '3', Address 'Read 0, 10', Trigger 'Cyclic', Poll Interval '1000', and Enable 'Enable'. At the bottom, there is an 'Editing' status and a 'GO TO APPLY SETTINGS' button.

Step 1: Add Modbus device information

< Create New Device

1 Basic Setting ————— 2 Command ————— 3 Confirm

Enable this device

Device Name
Meter

Slave IP
192.168.10.123

Slave Port
502

Slave ID
2

CANCEL NEXT

| 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

Edit Command

Enable this command

Basic

Command Name
Voltage

Function
23 - Read/Write Multiple Registers

Read/Write Multiple Registers

| | |
|------------------------|----------------|
| Read Starting Address | Read Quantity |
| 0 | 10 |
| Write Starting Address | Write Quantity |
| 0 | 1 |

Trigger
Data Change

Endian Swap
None

Fault Protection
Keep latest data

Tag
Tag Type
raw

CANCEL
DONE

| 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: <ul style="list-style-type: none"> Slope-intercept: tag value = (source value * slope) + offset Point-slope: tag value = source value * $\left(\frac{\text{target max.} - \text{target min.}}{\text{source max.} - \text{source min.}}\right)$ |

Step 3: Quick review result, click DONE to finish

< Create New Device

✓ Basic Setting ————— ✓ Command ————— 3 Confirm

Confirm your device settings, and click "DONE" to save your changes. After the device was created, you can edit your device settings any time.

Device Name: Meter

Slave ID: 2

Slave IP: 192.168.10.123

Slave Port: 502

Status: Enable

Number of Commands: 1

< BACK CANCEL **DONE**

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

< TCP

Home > Modbus Master > TCP

Operation Mode: TCP ⚙

Search Command Name

Type to search...

ADD DEVICE

Meter

+ ADD COMMAND ↓ IMPORT ↓ EXPORT

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

Editing GO TO APPLY SETTINGS

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

COM1
Home > Modbus Master > COM1
Operation Mode: ASCII
Search Command Name
Type to search...

ADD DEVICE

| No. | Command Name | Function | Address, Quantity | Trigger | Poll Interval (ms) | Enable |
|-----|--------------|----------|-------------------|-------------|--------------------|--------|
| 1 | power | 3 | Read 100, 10 | Cyclic | 1000 | Enable |
| 2 | voltage | 3 | Read 100, 10 | Cyclic | 1000 | Enable |
| 3 | reset | 16 | Write 0, 2 | Data Change | 1000 | Enable |

Editing GO TO APPLY SETTINGS

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.

Modbus Master
Home > Modbus Master

Protocol Name
Modbus Master MANAGE

Modbus TCP
TCP
1 Device, 1 Command

Modbus RTU/ASCII
COM1 (ASCII)
3 Device, 5 Command

Editing DISCARD **APPLY**

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.

Home > PROFINET IO Device
PROFINET IO

PROFINET IO
Device Name: MANAGE

PROFINET IO Device

| Application Relation 1 | | Application Relation 2 | |
|------------------------|---|------------------------|---|
| Input data size | 0 | Input data size | 0 |
| Output data size | 0 | Output data size | 0 |
| Input slot | - | Input slot | - |
| Output slot | - | Output slot | - |

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

Edit PROFINET IO Device Name

CANCEL

SAVE

| 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.

Home > PROFINET IO Device > Application Relation 1

< Application Relation 1 >

Application Relation 1
 Input data size 24
 Output data size 0

I/O Mapping + ADD SLOT

| Slot Number | Slot Name | Type | Data Size(bytes) | | | | | | | | | | | | | | | | |
|---|-----------|------------|------------------|-----|----------|-----------|------------|------------------|--|-------------------------|-----|--------|----|-----|-----------------------------|-------|---------|---|-----|
| 1 | voltage | Input | 24 | | | | | | | | | | | | | | | | |
| <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Tag name</th> <th>Data type</th> <th>Byte index</th> <th>Quantity (bytes)</th> <th></th> </tr> </thead> <tbody> <tr> <td>modbus_tcp_client/d1/c1</td> <td>raw</td> <td>0 - 19</td> <td>20</td> <td style="text-align: right;">^ v</td> </tr> <tr> <td>modbus_tcp_client/d1/status</td> <td>int32</td> <td>20 - 23</td> <td>4</td> <td style="text-align: right;">^ v</td> </tr> </tbody> </table> | | | | | Tag name | Data type | Byte index | Quantity (bytes) | | modbus_tcp_client/d1/c1 | raw | 0 - 19 | 20 | ^ v | modbus_tcp_client/d1/status | int32 | 20 - 23 | 4 | ^ v |
| Tag name | Data type | Byte index | Quantity (bytes) | | | | | | | | | | | | | | | | |
| modbus_tcp_client/d1/c1 | raw | 0 - 19 | 20 | ^ v | | | | | | | | | | | | | | | |
| modbus_tcp_client/d1/status | int32 | 20 - 23 | 4 | ^ v | | | | | | | | | | | | | | | |

Edit GO TO APPLY SETTINGS SAVE

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

Add Slot

Slot Number
1

Type
Input

Slot Name
voltage

Select Tags

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

Providers
modbus_tcp_client

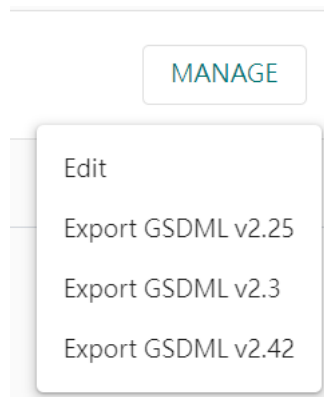
2 Tags

Selected Tags
c1 (+1 more)

CANCEL SAVE

| 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.

Modbus RTU/ASCII Diagnostics

[Home](#) > [Modbus RTU/ASCII Diagnostics](#)

Auto refresh

Modbus

| | |
|----------------------------|--------|
| Role | Master |
| Sent requests | 519613 |
| Received valid responses | 0 |
| Received invalid responses | 0 |
| Received CRC/LRC errors | 0 |
| Received exceptions | 0 |
| Timeout | 519612 |

Serial port

| | | |
|-----|----------------------------|--------|
| # 0 | Port number | 0 |
| | Break | 0 |
| | Frame error | 0 |
| | Parity Error | 0 |
| | Overrun Error | 0 |
| | Mode | ASCII |
| | Sent requests | 519613 |
| | Received valid responses | 0 |
| | Received invalid responses | 0 |
| | Received CRC/LRC errors | 0 |
| | Received exceptions | 0 |
| | Timeout | 519612 |

Diagnostics—Protocol Diagnostics-Modbus TCP Diagnostics

Modbus TCP Diagnostic

[Home](#) > Modbus TCP Diagnostics

Auto refresh

Modbus

| | |
|---------------------------|--------|
| Mode | Master |
| Number of connections | 0 |
| Sent requests | 0 |
| Received valid response | 0 |
| Received invalid response | 0 |
| Received exceptions | 0 |
| Timeout | 0 |

Connections

No data

Diagnostics—Protocol Diagnostics- PROFINET Diagnostics

[Home](#) > PROFINET Diagnostics

PROFINET Diagnostics

Auto refresh

Application Relation 1 Application Relation 2

IO Controller Status

| | |
|---------------|---|
| MAC Address | - |
| Operator Mode | - |

Parameters

| | |
|------------------|---|
| Update Time (ms) | - |
| Device Name | - |

I/O Slots

| Slot Number | Slot Name | Type | Data Size (bytes) | Data (hex byte) | Status |
|-------------|-----------|------|-------------------|-----------------|--------|
| No Data | | | | | |

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.

Modbus RTU/ASCII Traffic

Home > Modbus RTU/ASCII Traffic

Auto Scroll

START **STOP** **EXPORT** Ready to capture

| No. | Time | Role | Send/Receive | Port | Data Type | Slave ID | Function Code | Data |
|-----|-------------------------------|--------|--------------|------|-----------|----------|---------------|---|
| 1 | 2022-07-04T18:54:23.263+08:00 | Master | Resend | 1 | ASCII | 23 | 3 | 3A 31 37 30 33 30 30 33 37 30 30 41 41 35 0D 0A |
| 2 | 2022-07-04T18:54:24.268+08:00 | Master | Request | 1 | ASCII | 23 | 3 | 3A 31 37 30 33 30 30 33 37 30 30 41 41 35 0D 0A |

Diagnostics—Protocol Traffic-Modbus TCP Traffic

Modbus TCP Traffic Log

Home > Modbus TCP Traffic

Auto Scroll

START **STOP** **EXPORT** Ready to capture.

| No. | Time | Role | Send/Receive | Remote IP:Port | Slave ID | Function Code | Data |
|---------|------|------|--------------|----------------|----------|---------------|------|
| No Data | | | | | | | |

Diagnostics—Event Log

Diagnostics—Event Log-Log View

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

Event Log

Home > Event Log

EXPORT **CLEAR** **REFRESH**

| 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 |

Items per page: 10 1-2 of 2 < 1 /1 >

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.

The screenshot shows the 'Event Policy Setting' page. Under 'Channels', there are four buttons: 'Local Log' (Configured), 'Remote Log' (Configured), 'SNMP Trap' (Configured), and 'Email' (Configured). Under 'Events', there are four categories: System, Network, Security, and Maintenance. The 'System' category is expanded, showing four events: 'System start' (Information), 'User trigger reboot' (Warning), 'Power input failure' (Alert), and 'NTP update fail' (Warning). Each event has checkboxes for 'Local log', 'Remote log', 'SNMP trap', 'Email', and 'Relay'.

| 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

The screenshot shows the 'Local Log Setting' page. Under 'Event Log Overwrite Policy', there are two radio buttons: 'Overwrite the Oldest Event Log' (selected) and 'Stop Recording Event Log'. Under 'Log Capacity Warning', there is a checked checkbox. Below that, there is a 'Capacity Threshold (%)' field with the value '80'. Under 'Warning By', there are two checkboxes: 'SNMP Trap' and 'Email'. At the bottom, there are 'CANCEL' and 'SAVE' buttons.

| 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 Setting

Syslog Server 1

Enable

TLS Authentication
 Enable

IP Address Port

_____ 514

Syslog Server 2

Enable

TLS Authentication
 Enable

IP Address Port

----- 514

CANCEL

SAVE

TLS Authentication

UPLOAD

| Common Name | Start Time | Expire Time |
|-------------|------------|-------------|
| No Data | | |

Client Certificate
 未選擇任何檔案

Client KEY
 未選擇任何檔案

CA Certificate
 未選擇任何檔案

| 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

SNMP Trap Server

Trap Service

Active Inactive

For advanced settings, please go to [SNMP Trap Server](#) page

CANCEL **SAVE**

Email Settings

Email Setting

SMTP Service

Active

Primary Server

| Mail Server (SMTP) | Port |
|--------------------|------|
| 10.123.7.18 | 25 |

Security Connection

None

Require Authentication

Username

Password

From (Email address)

test@moxa.com

To (Email address, separated by semicolon)

user@moxa.com

CANCEL **SAVE**

| 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. |

Diagnostics—Network Connections

You can 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 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.

Ping

Home > Ping

Ping Destination

192.168.127.2

ACTIVATE

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.

LLDP
Home > LLDP

LLDP Configuration

LLDP Service (Disabled)
Message Transmit Interval: 30 seconds EDIT

LLDP Table

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

REFRESH

LLDP Configuration

LLDP Service

Enable Disabled

Note: enable/disable this service through [Service Enablement](#)

Message Transmit interval (sec)

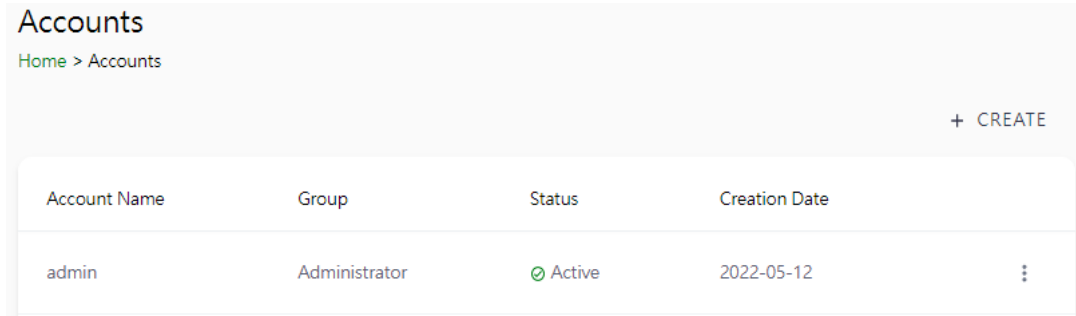
30

CANCEL SAVE

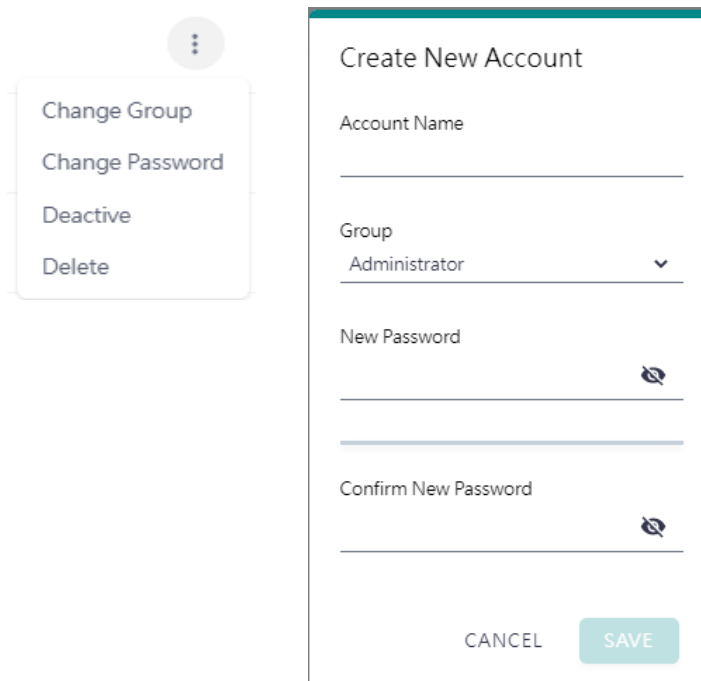
Security

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

The screenshot shows a web interface for managing groups. At the top, it says "Groups" and "Home > Groups". There is a "+ CREATE" button in the top right corner. Below this is a table listing three built-in 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 built-in types of groups are shown; you can also create your own group by clicking **CREATE**.

The screenshot shows a "Create New Group" form. It has a vertical scrollbar on the right side. The form is divided into several sections:

- Basic Information**
 - Name:
 - Description - optional:
- Access Permissions**
 - System Configuration: Read write (dropdown)
- Protocol Setting**
 - Read write (dropdown)
- Diagnostic**
 - Read write (dropdown)
- Security**
 - No display (dropdown)
- Maintenance**
 - Read write (dropdown)
- Restart**
 - Read write (dropdown)

At the bottom of the form, there are two buttons: "CANCEL" and "SAVE".

| Parameters | Value | Description |
|---------------------------|------------|--|
| Basic Information | | Includes Name and Description for the new Group. |
| Access Permissions | No display | 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. |
| | Read only | |
| | Read write | |

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 (~! @\$%^&* _-+=`\'0000;'"<>.,/?)

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

SAVE

| 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, 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.

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 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 2 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 3 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 4 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 5 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |

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.

DoS Defense

[Home](#) > DoS Defense

Configuration

| | |
|----------------|--------------------------|
| Null Scan | <input type="checkbox"/> |
| NMAP-Xmax Scan | <input type="checkbox"/> |
| SYN/FIN Scan | <input type="checkbox"/> |
| FIN Scan | <input type="checkbox"/> |
| NMAP-ID Scan | <input type="checkbox"/> |

SYN-Flood

| | |
|--------|---|
| Enable | <input type="checkbox"/> |
| Limit | <input type="text" value="4000"/> pkt/s |

ICMP-Death

| | |
|--------|---|
| Enable | <input type="checkbox"/> |
| Limit | <input type="text" value="4000"/> pkt/s |

Security—Login Policy

Login Message

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

The screenshot shows the 'Login Policy' configuration page with the 'Login Message' tab selected. It contains two text input fields. The first is labeled 'Login Message - optional' and contains the text 'Hello'. The second is labeled 'Login Authentication Failure Message' and contains the text 'The account or password you entered is incorrect.(Your account will be temporarily locked if excessive tried.)'. Both fields have a character count indicator at the bottom right (5 / 256 and 110 / 256 respectively). A 'SAVE' button is located at the bottom left.

Login Lockout

The screenshot shows the 'Login Policy' configuration page with the 'Login Lockout' tab selected. It features several settings: an unchecked checkbox for 'Enable Login Failure Lockout', a 'Max Failure Retry Times' field set to 5, an unchecked checkbox for 'Reset the Login Failure Counter' with a sub-note 'This addition allows you to specify the maximum period of login failure counter.', a 'Reset Period (min)' field set to 10, and a 'Lockout Time (min)' field set to 10. A 'SAVE' button is located at the bottom left.

| Parameter | Value | Description |
|--------------------------------|------------------------|---|
| Max Failure Retry Times | 1 to 10 (default 5) | You can specify the maximum number of failures retries, 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

Login Policy

Home > Login Policy

Login Message Login Lockout **Login Session**

Maximum login user for HTTP+HTTPS
5

Auto logout setting (min)
1440

SAVE

| 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.

Certificate Management

Home > Certificate Management

Configuration

Issue to 10.123.4.44
Issue by Moxa Inc.
Valid from 2022-6-2 to 2027-6-1

SSL

Select SSL Certificate **IMPORT**

Delete SSL Certificate **DELETE**

Maintenance

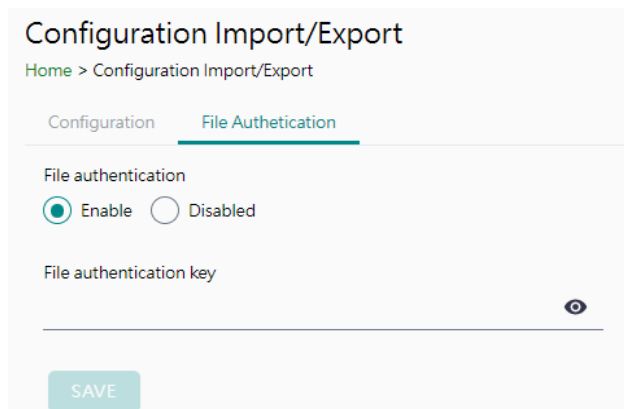
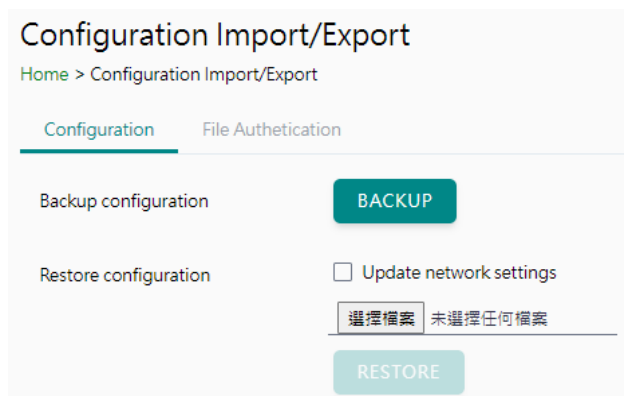
Maintenance—Configuration Import/Export

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.

The screenshot shows the 'Firmware Upgrade' page in a web console. At the top, it says 'Firmware Upgrade' with a breadcrumb 'Home > Firmware Upgrade'. Below that, a warning message states: 'Upgrading firmware may cause devices to reset to factory default. We suggest you back up the configuration of all devices.' There is a selection area with a dropdown menu currently showing '選擇檔案' and the text '未選擇任何檔案'. At the bottom of the form is a teal 'SUBMIT' button.

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.

The screenshot shows the 'Load Factory Default' page in a web console. At the top, it says 'Load Factory Default' with a breadcrumb 'Home > Load Factory Default'. Below that, instructions state: 'Click on Reset Button to reset all settings, including the console password, to the factory default values. The event log will remain after rebooting.' There is a checkbox labeled 'Keep Current IP Setting' which is currently unchecked. A blue information box contains the text: 'Info: To leave the IP address, netmask, and gateway settings unchanged, make sure that Keep IP settings is enabled.' At the bottom of the form is a teal 'RESET' button.



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.

Restart

[Home](#) > [Restart](#)

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

RESTART

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.

ADD TAGS

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

Providers
modbus_serial_master ▼

2 Tags

Selected Tags

🔍 Search

SELECT ALL CLEAR

[modbus_serial_master] d1

c1
 status

Total: 2 Selected: 1 **DONE**

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 | <ol style="list-style-type: none">1. System name and login password modification2. Network settings3. Configuration import/export4. Firmware upgrade |
| MXview | <ol style="list-style-type: none">1. Configuration import/export2. LLDP for topology analysis3. 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 |