

MGate 5135/5435 Series User Manual

Version 1.2, July 2024

www.moxa.com/products



© 2024 Moxa Inc. All rights reserved.

MGate 5135/5435 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

© 2024 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	5
2. Getting Started	6
Connecting the Power	6
Connecting Serial Devices	6
Connecting to a Network	6
Installing DSU Software.....	6
Log In to the Web Console	7
microSD	7
3. Web Console Configuration and Troubleshooting	9
System Dashboard.....	9
System Settings	10
System Settings—General Settings.....	10
System Settings—Network Settings	12
System Settings—Serial Settings.....	13
System Settings—SNMP Settings.....	15
Protocol Settings	19
Protocol Settings—Modbus Client Settings	19
Protocol Settings—EtherNet/IP Adapter Settings	27
Diagnostics	30
Diagnostics—Protocol Diagnostics.....	30
Diagnostics—Protocol Traffic	32
Diagnostics—Event Log	32
Diagnostics—Tag View	36
Diagnostics—Network Connections	37
Diagnostics—Ping	37
Diagnostics—LLDP	38
Security.....	39
Security—Account Management	39
Security—Service	42
Security—Allow List	43
Security—DoS Defense	44
Security—Login Policy	45
Security—Certificate Management	46
Maintenance	47
Maintenance—Configuration Import/Export.....	47
Maintenance—Firmware Upgrade.....	48
Maintenance—Load Factory Default	48
Restart	49
Status Monitoring	49
4. Network Management Tool (MXstudio).....	50
A. SNMP Agents with MIB II and RS-232-Like Groups	51
RFC1213 MIB-II Supported SNMP Variables	51
RFC1317 RS-232-Like Groups	52
B. CIP Objects of EtherNetIP	53
Identity Object	53
Class Attribute List	53
Instance Attribute List.....	53
Common Service List	54
TCP/IP Interface Object.....	54
Class Attribute List	54
Instance Attribute List.....	54
Common Service List	55
Ethernet Link Object	55
Class Attribute List	56
Instance attribute list.....	56
Interface Flags	57
Common Service List	58
Assembly Object.....	58

Class Attribute List	58
Instance Attribute List.....	58
Common Service List	59
Message Router Object.....	59
Class Attribute List	59
Instance Attribute List.....	59
Common Service List	59
Connection Manager Object	59
Class Attribute List	60
Common Service List	60
Port Object	60
Class Attribute List	60
Instance Attribute List.....	60
Common Service List	61

1. Introduction

The MGate 5135/5435 gateways are 1- and 4-port industrial Ethernet gateways, with the former for Modbus RTU/ASCII/TCP and the latter for EtherNet/IP network communications. To integrate existing Modbus devices onto an EtherNet/IP network, use the MGate 5135/5435 gateway as a Modbus client to collect data and exchange data with EtherNet/IP 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 and 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. Connect the 12 to 48 VDC power line or DIN-rail power supply to the MGate's power terminal block.
2. Tighten the screws on both sides of the terminal block.
3. Turn on the power source.

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

Connecting 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.

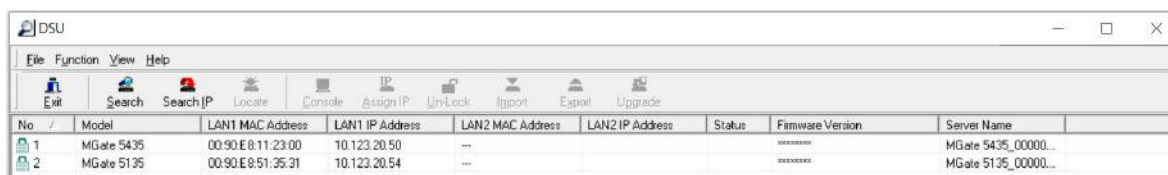
Installing DSU Software

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 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.



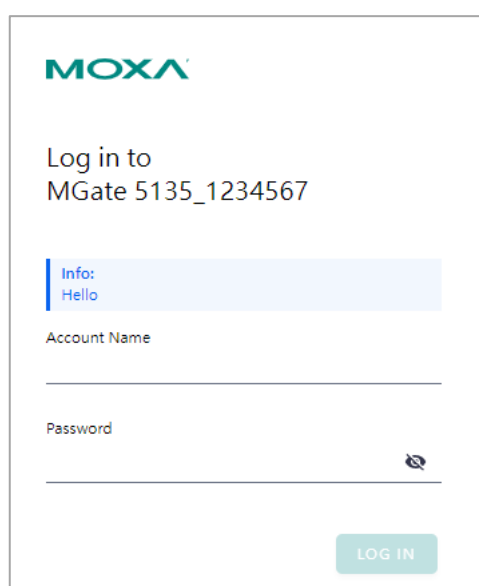
No.	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status	Firmware Version	Server Name
1	MGate 5435	00:90:E8:11:23:00	10.123.20.50	---	---	---	-----	MGate 5435_00000...
2	MGate 5135	00:90:E8:51:35:31	10.123.20.54	---	---	---	-----	MGate 5135_00000...

Log In to the Web Console

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

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

On the login page, create an account name and set a password that is at least 8 characters long when you log in for the first time. Or if you have already an account, log in with your account name and password. If you change the MGate's IP and other related network settings, click SAVE, and the MGate will reboot.




MOXA

Log in to
MGate 5135_1234567

Info:
Hello

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 web console, and all the stored changes will be copied 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 be copied 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 be copied 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 be copied 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.

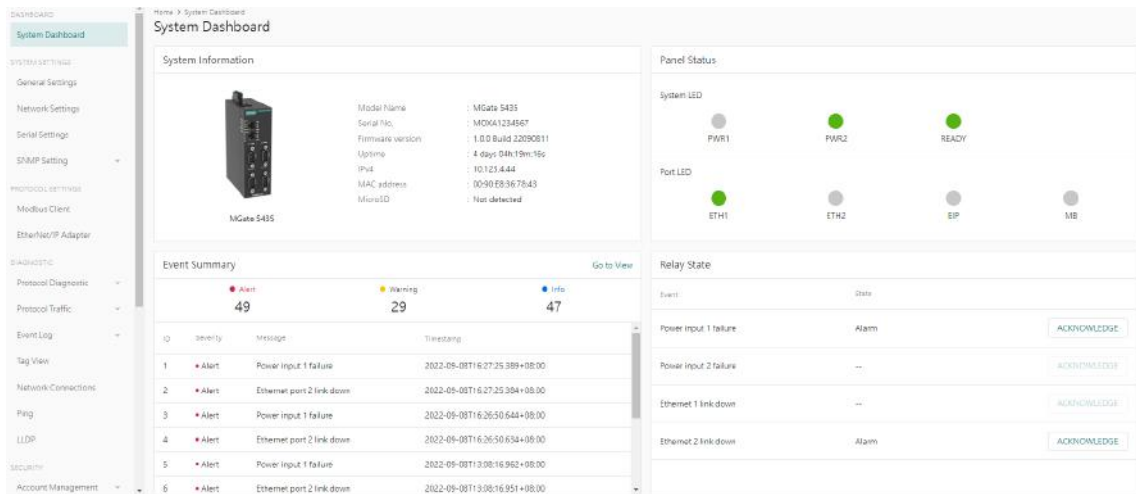
The MGate will stop working in case of the above events, accompanied by a flashing Ready LED and beeping alarm. When you replace the MGate gateway's microSD card, the microSD card will synchronize the configurations stored on the MGate gateway. Note that the replacement microSD card should not contain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

3. Web Console Configuration and Troubleshooting

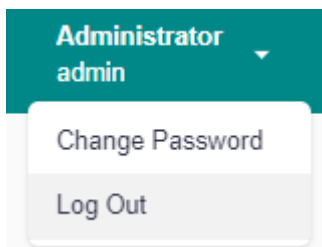
This chapter provides a quick overview of how to configure the MGate 5135/5435 by web console.

System Dashboard

This page gives a system dashboard of the MGate 5135/5435 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.

General Setting

[Home](#) > [General Setting](#)

[System](#) [Time](#)

Host Name

MGate 5135_1234567

Description


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 change the real-time clock, select Local time. MGate’s firmware will change the GMT time according to the Time Zone setting.

General Setting

Home > General Setting

System Time

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

Timezone
(GMT+08:00)Taipei

Daylight saving time
☒ Enable ☐ Disabled

Start

Month Week Day Hour

3 5 0 1

End

Month Week Day Hour

10 5 0 1

Offset

+00:00

Sync Mode
☒ Manual ☐ Auto

sync with browser

Date

2022/07/04

Hour Minute Second

18 28 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	Enable and set up the daylight saving time; or, disable 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 set configured time.

System Settings—Network Settings

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

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

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

System Settings—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.

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

Click the “pen” icon to configure serial port parameters, such as the interface, baudrate, terminator, and pull-up/pull-down resistor.

< # 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
Alias	Alphanumeric string	Allows you to define an alias to a port for easier identification. Max. 16 characters.
Interface	RS-232, RS-422, RS-485 2-wire, RS-485 4-wire	
Terminator	120Ω, None	Default is none, which means the terminator is disabled. Try to enable the 120 Ω when the communication has issues, especially for long distance communication.
Pull-up and Pull-down Resistor	1kΩ, 150kΩ	Default value is 150 kΩ. Set the value depending on the system requirements.
Baudrate	300 bps to 921600 bps	The baudrate value can be also self-defined if it is between 300 bps to 921600 bps.
Parity	None, Odd, Even, Mark, Space	
Data Bits	5, 6, 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.

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.

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 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 after the transmission is completed.
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.

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; the MGate supports SNMP V1, V2c, and V3.
Contact	The optional contact information usually includes an emergency contact name and telephone number.
Location	The location information. This string is usually set to the street address where the MGate is physically located.

Parameters	Description
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.
Minimum Authentication/Privacy Password Length	Minimum Authentication/Privacy Password Length must be between 8 and 64.

Read-only and Read/write Access Control



You can define usernames, passwords, and authentication parameters in SNMP for two levels of access control: read-only and read/write. The 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 (Default) MD5 SHA1 SHA-224 SHA-256 SHA-384 SHA-512	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication.
Privacy Type	Disable (Default) DES-CBC AES-128	Use this field to enable or disable data encryption for the specified level of access. If you enable a privacy type, please also configure the privacy password.

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

Create SNMPv3 Account

Account Name

Authority
Read/Write

Authentication Type
SHA-512

Authentication Password

Privacy Type
AES-128

Privacy Password

CANCEL
SAVE

Home > SNMP Agent

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

MGate 5135/5435 Series User Manual

17

System Settings—SNMP Settings—SNMP Trap

SNMP Trap

Home > SNMP Trap

General
SNMP Trap Server

Trap Service

☒ Active
☐ Inactive

SAVE

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

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	-	-	-	-	

Configure the SNMP trap server by inputting the server's IP or domain name.

Create Trap Server

General Setting

Server IP

Port

Trap Method

Trap Version

Disable

CANCELSAVE

Parameters	Description
Server IP	SNMP server IP address or domain name; the maximum number of trap servers is 2
Port	SNMP server IP Port.
Trap Version	Disable SNMPv1 SNMPv2c SNMPv3

Protocol Settings

Protocol Settings—Modbus Client Settings

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

Modbus Master

Home > Modbus Master

Protocol Name

★ Modbus Master MANAGE ▾

Modbus TCP

TCP
2 Device, 3 Command

Modbus RTU/ASCII

COM1 (ASCII)
3 Device, 5 Command

Editing DISCARD APPLY

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.

Protocol Name

★ Modbus Master MANAGE ▾

Modbus TCP

Import Configuration

Export Configuration

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.

< TCP

Home > Modbus Master > TCP

Operation Mode: TCP ⚙

Search Command Name

🔍 Type to search...

ADD DEVICE

Meter
🟢 Enable
Slave IP: 192.168.10.123
Slave Port: 502
Slave ID: 2

Basic Setting

Initial Delay (ms)
0

Maximum Retry
3

Response Timeout (ms)
1000

CANCEL DONE

Parameter	Value	Default	Description
Initial delay	0 to 30000 ms	0	Some Modbus servers/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 server/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 server/slave device takes to respond to a request. A Modbus client/master can be configured to wait a certain amount of time for a server/slave's response. If no response is received within the specified time, the client/master will disregard the request and continue operation. This allows the Modbus system to continue the operation even if a server/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 server/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 MGate Modbus Master configuration interface. On the left, a sidebar contains a search bar and a list of devices. The 'Meter' device is selected and shown in detail, including its IP address (192.168.10.123), port (502), and ID (2). The main area displays a table of commands for the 'Meter' device. The table has columns for No., Command Name, Function, Address, Quantity, Trigger, Poll Interval (ms), and Enable. A single command is listed: 'Voltage' with function 3, address 0, quantity 10, and a cyclic trigger with a 1000 ms poll interval. Buttons for '+ ADD COMMAND', 'IMPORT', and 'EXPORT' are visible. At the bottom right, there is a 'GO TO APPLY SETTINGS' button.

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

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 server/slave device.
Slave Port	1 to 65535	502	The TCP port number of a remote server/slave device.
Slave ID	1 to 255	1	The Modbus server/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
0

Read Quantity
10

Write Starting Address
0

Write Quantity
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: A command is issued when a change in data is detected.
Poll Interval (this will show up when user 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 in a server mode fails, the gateway cannot receive data, but the gateway will continuously send output data to the Modbus 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 (in a server role).
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, user 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 = target min + (source value - source min) * ($\frac{\text{target max.} - \text{target min.}}{\text{source max.} - \text{source min.}}$)

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

If you already have 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

Enable

Slave IP: 192.168.10.123

Slave Port: 502

Slave ID: 2

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

GO TO APPLY SETTINGS

MGate 5135/5435 Series User Manual

24

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

Serial Basic Settings

Mode

☒ RTU

☐ ASCII

Initial Delay (ms)

0

Max. Retries

3

Response Timeout (ms)

1000

☒ Inter-frame delay automatically determined

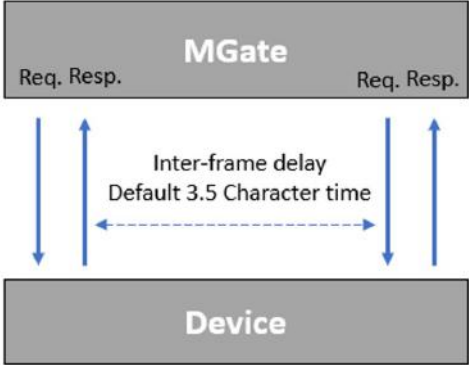
The system will automatically determine the delay time of the data frame transmission from the server device to the upstream. You may choose to set the delay time manually by unchecking this option.

☒ Automatically determines the Intercharacter delay

The system will automatically determine the timeout interval between characters for Modbus devices that cannot receive Rx signals within an expected interval. You may choose to set the timeout interval manually by unchecking this option.

CANCEL

DONE

Parameters	Description
Inter-frame delay (only for Modbus RTU)	<p>Defines the time interval between an RTU response and the next RTU request. The system will automatically determine the delay time of the data frame transmission from the server device to the upstream. When the baudrate is lower than 19200 bps, the default is 3.5 character time. When the baudrate is larger than 19200 bps, the MGate uses a predefined fixed value that is not user-configurable. This function solves the issue when some devices can't handle the RTU requests that quickly, so the MGate opens to user-defined values. You may choose to set the delay time manually by unchecking this option. The value range is 10 to 500 ms.</p> <p>How to calculate Modbus character time? E.g., if the baudrate is 9600 bps, 1 character time is about 1 ms. In a serial frame (11 bits, including start bit, data, parity bit, and stop bit), 9600 bps approximately equals to 960 characters/s, so transmitting one character needs about $1/960 = 1$ ms.</p> 

Parameters	Description
Inter-character timeout (only for Modbus RTU)	<p>The time interval between characters in one frame. When the serial side of the MGate receives one character, and the next one comes after the “inter-character timeout” defined, the frame will be discarded because of timeout.</p> <p>The system will automatically determine the timeout interval between characters for Modbus devices. When the baudrate is lower than 19200 bps, the default is 1.5 character time. When the baudrate is larger than 19200 bps, MGate uses a predefined fixed value that is not user-configurable. You may choose to set the timeout interval manually by unchecking this option. The value range is 10 to 500 ms.</p>

< COM1

Home > Modbus Master > COM1

Operation Mode: ASCII

Search Command Name

Type to search...

ADD DEVICE

meter

meter

ADD COMMAND IMPORT EXPORT

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—EtherNet/IP Adapter Settings

You can configure the EtherNet/IP adapter setting on this page.

EtherNet/IP Adapter

[Home](#) > [EtherNet/IP Adapter](#)

Protocol Name

EtherNet/IP Adapter

Encapsulation inactivity timeout: 120

EDIT

EtherNet/IP Adapter

Connection1

Connection point100 / 110

Data size200 / 200

Mapping tags0 / 11

Connection2

Connection point101 / 111

Data size0 / 496

Mapping tags0 / 2

Connection3

Connection point102 / 112

Data size0 / 0

Mapping tags0 / 0

Connection4

Connection point103 / 113

Data size0 / 0

Mapping tags0 / 0

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

Protocol Name

EtherNet/IP Adapter

Encapsulation inactivity timeout: 120

EDIT

Adapter Common Settings

Encapsulation inactivity timeout (sec)

120

CANCEL

SAVE

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

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

< Connection1 ▾

Home > EtherNet/IP Adapter > Connection1

Connection1

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

EDIT

Data Mapping (O → T)

ADD TAGS

Data size should below 200 bytes

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

Data Mapping (T → O)

ADD TAGS

Data size should below 200 bytes

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

GO TO APPLY SETTINGS

SAVE

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

Assembly Instance Settings

Name

Connection1

O → T connection point

100

T → O connection point

110

O → T (Output) data size (bytes)

200

T → O (Input) data size (bytes)

200

CANCEL

SAVE

Parameter	Value	Default	Description
Name		Connection[x]	Name for connection. For example, Connection1
O->T connection point	1 to 2147483647	100	EtherNet/IP connection instance
T->O connection point	1 to 2147483647	110	EtherNet/IP connection instance
O->T (Output) data size (bytes)	0 to 496	0	Unit: byte O->T: Originator to Target
T->O (Input) data size (bytes)	0 to 496	0	Unit: byte T->O: Target to Originator

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

Add Tags

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_TAG_INFO: MODBUS_TCP_Si

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_FIELD_PROVIDERS
modbus_serial_master, modbus_tcp_master

5 MODBUS_TCP_SERVER_DATA_MAPPING_TAGS

MODBUS TCP SERVER DATA MAPPING ADD FIELD SELECTED TAGS

Search

SELECT ALL CLEAR

[modbus_serial_master] flow

☒ status

[modbus_serial_master] temp

Total: 5 Selected: 5

DONE

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

Data Mapping (T → O)						ADD TAGS
No.	Tag name	Data type	Byte offset	Quantity (bytes)	Bit offset	
1	modbus_serial_master/flow/status	int32	0	4	0	
2	modbus_serial_master/temp/cur	raw	4	20	0	
3	modbus_serial_master/temp/status	int32	24	4	0	

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-EtherNet/IP Diagnostics

EtherNet/IP Adapter Diagnostics

[Home](#) > EtherNet/IP Diagnostics

☒ Auto refresh

Overview

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

Connections

No data

Diagnostics—Protocol Traffic

Diagnostics—Protocol Traffic-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	2022-07-04T16:54:23.263+08:00	Master	Resend	1	ASCII	23	3	3A 31 37 30 33 30 30 33 37 30 30 30 41 41 35 0D 0A
2	2022-07-04T16:54:24.269+08:00	Master	Request	1	ASCII	23	3	3A 31 37 30 33 30 30 33 37 30 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.

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
EtherNet/IP	Adapter connected; Adapter disconnected

Local Log Settings

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

Remote Log Settings

Remote Log 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

Common Name

Start Time

Expiration Time

No data to display.

Client Certificate

Choose File

No file chosen

Client Key

Choose File

No file chosen

CA Certificate

Choose File

No file chosen

UPLOAD

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)
10.123.7.18

Port
25

Security Connection
None

☒ Require Authentication

Username

Password

From (Email address)
test@moxa.com

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

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

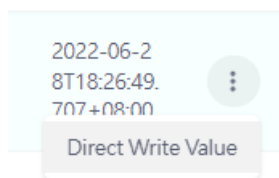
Parameters	Description
Username	This field is for your mail server's username, if required.
Password	This field is for your mail server's password, if required.
From (Email address)	Email address from which automatic email warnings will be sent.
To (Email address, separated by semicolon)	Email addresses to which automatic email warnings will be sent.

Diagnostics—Tag View

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

Tag View				
Home > Tag View				
Provider	Source	Name	Type	Value
modbus_serial_master	flow	status	int32	0
modbus_serial_master	temp	cur	raw	00000000000000000000000000000000
modbus_serial_master	temp	set	raw	0000
modbus_serial_master	temp	status	int32	-2147483648

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.

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.

The screenshot shows the 'LLDP' configuration page. At the top, there's a breadcrumb 'Home > LLDP'. Below it is the 'LLDP Configuration' section. It contains a status bar showing 'LLDP Service (Disabled)' and 'Message Transmit interval: 30 seconds', with an 'EDIT' button on the right. Below this is the 'LLDP Table' section, which has a 'REFRESH' button. The table has five columns: 'Interface', 'Neighbor ID', 'Neighbor Port', 'Neighbor Port Description', and 'Neighbor System'. The table is currently empty, showing 'No Data'.

After clicking EDIT, if you need to enable or disable LLDP service, click on the “Service” hyperlink or navigate to Security > Service page to enable/disable it.

The screenshot shows the 'LLDP Configuration' dialog box. It has a title bar 'LLDP Configuration'. Inside, there's a section 'LLDP Service' with two radio buttons: 'Enable' and 'Disabled'. The 'Disabled' button is selected. Below this is a note: 'Note: enable/disable this service through [Service Enablement](#)'. There's a field for 'Message Transmit interval (sec)' with the value '30'. At the bottom, there are two buttons: 'CANCEL' and 'SAVE'.

Security

Security—Account Management

Security—Account Management—Accounts

Accounts

Home > Accounts

+ CREATE

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

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

Change Group

Change Password

Deactive

Delete

Create New Account

Account Name

Group

Administrator

New Password

Confirm New Password

CANCEL

SAVE

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

Groups

Home > Groups

+ CREATE

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

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

Create New Group

Basic Information

Name

Description - optional

Access Permissions

System Configuration

Read write

▼

Protocol Setting

Read write

▼

Diagnostic

Read write

▼

Security

No display

▼

Maintenance

Read write

▼

Restart

Read write

▼

CANCEL

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

Password Complexity Strength Check
☐ Select all password strength requirements

☐ At least one digit (0-9)
☐ Mixed upper and lower case letters (A-Z, a-z)
☐ At least one special character (~! @\$%^&* _-+ = `\'"{}[];:'''<>.,/?/)

Password Lifetime Setting

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

☐ Enable password lifetime check
 Password Lifetime (day)

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.	<input checked="" type="checkbox"/>
HTTPS Service	<input checked="" type="checkbox"/>
Ping Service	<input type="checkbox"/>
SD Card	<input type="checkbox"/>
Reset button disable after 60 sec The reset button function will always enable when switch if off.	<input type="checkbox"/>
SNMP Agent Service	<input type="checkbox"/>
LLDP Service	<input type="checkbox"/>

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 in order 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

☐

NMAP-Xmax Scan

☐

SYN/FIN Scan

☐

FIN Scan

☐

NMAP-ID Scan

☐

SYN-Flood

Enable

☐

Limit

4000

pkt/s

ICMP-Death

Enable

☐

Limit

4000

pkt/s

SAVE

Security—Login Policy

Login Message

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

Login Policy

Home > Login Policy

[Login Message](#) [Login Lockout](#) [Login Session](#)

Login Message - optional

Hello

5 / 256

Login Authentication Failure Message

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

110 / 256

SAVE

Login Lockout

Login Policy

Home > Login Policy

[Login Message](#) [Login Lockout](#) [Login Session](#)

☐ Enable Login Failure Lockout

Max Failure Retry Times

5

☐ Reset the Login Failure Counter

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

Reset Period (min)

10

Lockout Time (min)

10

SAVE

Parameter	Value	Description
Max Failure Retry Times	1 to 10 (default 5)	You can specify the maximum number of failure retries. If retry times are exceeded, the 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 at 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.

The screenshot shows the 'Config. Import/Export' interface with the 'Configuration' tab selected. It features two main sections: 'Export configuration' with an 'EXPORT' button, and 'Import configuration' with a checkbox for 'Update network settings', a 'Choose File' button, and an 'IMPORT' button. The 'No file chosen' text is visible next to the 'Choose File' button.

The screenshot shows the 'Configuration Import/Export' interface with the 'File Authentication' tab selected. It includes a breadcrumb trail 'Home > Configuration Import/Export'. The 'File authentication' section has radio buttons for 'Enable' (selected) and 'Disabled'. Below this is a 'File authentication key' field with a toggle icon on the right. A 'SAVE' button is located at the bottom left.

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.

Firmware Upgrade

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

No file chosen

Maintenance—Load Factory Default

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

Load Factory Default

[Home](#) > Load Factory Default

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

The event log will remain after rebooting

☐ Keep Current IP Setting

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



ATTENTION

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

Restart

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 will not 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 server/slave device is not providing up-to-date data. To handle this situation, the MGate provides a warning mechanism to report the list of server/slave devices that are still "alive" through the Status Monitoring function.

The MGate automatically creates a status tag when a Modbus device is created. This tag is used to show the connection status (valid or invalid) of the Modbus server device. To monitor the status of the status tag, you can convert this tag to the northbound protocol and read for the northbound SCADA/device. Or, you can check the tag status on MGate's web, the Tag View page.

To perform the status tag monitoring from your northbound protocol, go to the northbound protocol's page (for example, the EtherNet/IP adapter page), click **Add Tags**, select Modbus serial master as the tag provider, and select the "status" tag. MGate will automatically add a mapping from this Modbus tag to the other protocol.

Add Tags

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_TAG_INFO: MODBUS_TCP_S

MODBUS_TCP_SERVER_DATA_MAPPING_ADD_FIELD_PROVIDERS

modbus_serial_master, modbus_tcp_master

5 MODBUS_TCP_SERVER_DATA_MAPPING_TAGS

MODBUS TCP SERVER DATA MAPPING ADD FIELD SELECTED TAGS

Search

SELECT ALL **CLEAR**

[modbus_serial_master] flow

☒ status

[modbus_serial_master] temp

Total: 5 Selected: 5

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 and MXview. MXconfig is for industrial network configuration; MXview is for industrial management software. 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:

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

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

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		snmpInReadOnlyls
	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

B. CIP Objects of EtherNet/IP

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

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

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

Identity Object

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

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

Class Attribute List

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

Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Vendor ID		UINT (16)	991, the vendor ID of Moxa.
2	Get	Device Type		UINT (16)	0 x 0C, "Communications Adapter"
3	Get	Product Code		UINT (16)	Please refer to Product Code Table.
4	Get	Revision		(Struct.)	The version of the Identity object
			Major	USINT (8)	The structure member, major
			Minor	USINT (8)	The structure member, minor.
5	Get	Status		WORD (16)	Not used
6	Get	Serial Number		UDINT (32)	The serial number of each device
7	Get	Product Name		SHORT_STRING	The product name in human-readable format

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
15	Get/Set	Assigned Name		STRINGI	The assigned MGate name, for example: Same as the server name set in the basic settings. By default, it is "MGate xxxx_xx" (xxxx_xx represents the product series number and serial number).
17	Get/Set	Geographic Location		STRINGI	The assigned MGate location Same as the server location set in the basic settings. By default, it is blank.

The Identity Object Instance supports the following CIP Common services:

Common Service List

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

Product Code	Model Name
0x1036	MGate 5135
0x1038	MGate 5435

TCP/IP Interface Object

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

The following tables summarize the attributes of this object.

Class Attribute List

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

Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Status		DWORD (32)	Interface status 0 = The Interface Configuration attribute has not been configured. 1 = The Interface Configuration attribute contains valid configuration got from BOOTP, DHCP or non-volatile storage.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
2	Get	Configurati on Capability		DWORD (32)	Interface capability flags Bit map of capability flags: Bit 0: BOOTP Client Bit 1: DNS Client Bit 2: DHCP Client Bit 3: DHCP-DNS Update Bit 4: Configuration Settable
3	Get/Set	Configurati on Control		DWORD (32)	Interface control flags Bit map of control flags: Bit 0 to 3: Startup Configuration <ul style="list-style-type: none"> 0 = The device shall use the interface configuration values previously stored (for example, in non-volatile memory or via hardware witches). 1 = The device shall obtain its interface configuration values via BOOTP. 2 = The device shall obtain its interface configuration values via DHCP upon start-up. 3 to15 = Reserved.
4	Get	Physical Link Object		(Struct.)	Path to physical link object
			Path Size	UINT (16)	Size of Path
			Path	Padded EPATH	Logical segments identifying the physical link object
5	Get/Set	Interface Configurati on		(Struct.)	TCP/IP network interface configuration
			IP Address	UDINT (32)	The device's IP address
			Network Mask	UDINT (32)	The device's network mask
			Gateway Address	UDINT (32)	Default gateway address
			Name Server	UDINT (32)	Primary name server
			Name Server2	UDINT (32)	Secondary name server
			Domain Name	STRING	Defauult domain name
6	Get/Set	Host Name		STRING	Host name

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

Common Service List

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

Ethernet Link Object

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

Instance Number	Mapping to
0	Ethernet Link class
1	1 st MGate Ethernet port
2	2 nd MGate Ethernet port

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

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

Class Attribute List

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

Instance attribute list

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

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
			Multiple Collisions	UDINT (32)	Successfully transmitted frames which experienced more than one collision.
			SQE Test Errors	UDINT (32)	The number of times the SQE test error message is generated.
			Deferred Transmissions	UDINT (32)	Frames for which first transmission attempt is delayed because the medium is busy.
			Late Collisions	UDINT (32)	The number of times a collision is detected later than 512 bit times into the transmission of a packet.
			Excessive Collisions	UDINT (32)	Frames for which transmission fails due to excessive collisions.
			MAC Transmit Errors	UDINT (32)	Frames for which transmission fails due to an internal MAC sublayer transmit error.
			Carrier Sense Errors	UDINT (32)	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
			Frame Too Long	UDINT (32)	Received frames that exceed the maximum permitted frame size.
			MAC Receive Errors	UDINT (32)	Frames for which reception on an interface fails because of an internal MAC sublayer receive error.
6	Get/Set	Interface Control		(Struct.)	Configuration for physical interface.
			Control Bits	WORD (16)	Bit 0: Auto-Negotiate <ul style="list-style-type: none"> Value 0: Force Value 1: Auto-Nego Bit 1: Half/Full Duplex <ul style="list-style-type: none"> Value 0: half duplex Value 1: full duplex Bit 2 to 15: Reserved, all zero
			Forced Interface Speed	UINT (16)	Speed at which the interface shall be forced to operate.
10	Get	Interface Label		SHORT_STRING	Human readable identification
11	Get	Interface Capability		(Struct.)	Indicates the capabilities of the interface
			Capability Bits	DWORD (32)	Interface capabilities, other than speed/duplex
			Speed/Duplex Options	(Struct.)	Indicates speed/duplex pairs supported in the Interface Control attribute
				USINT (8)	Speed/Duplex Array Count
				(Array Struct.)	Speed/Duplex Array
				UINT (16)	Interface Speed
				USINT (8)	Interface Duplex Mode

Interface Flags

Bit(s)	Called	Definition
0	Link Status	0 indicates an inactive link; 1 indicates an active link.
1	Half/Full Duplex	0 indicates half duplex; 1 indicates full duplex.

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

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

Common Service List

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

Assembly Object

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

There are three instances of this object as the following.

	Instance Number	Size (bytes)
Input	MGate 5135: 4	MGate 5135: 1984
	MGate 5435: 8	MGate 5435: 3968
Output	MGate 5135: 4	MGate 5135: 1984
	MGate 5435: 8	MGate 5435: 3968
Configuration	1	0

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

Class Attribute List

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

Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
3	Get/Set	Data		Array of BYTE	The implicit messaging content

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
4	Get	Size		UINT (16)	Number of bytes in Attr. 3

Common Service List

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

Message Router Object

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

- Explicit Messaging
- Unconnected Messaging
- Implicit messaging

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

Class Attribute List

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

Instance Attribute List

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

Common Service List

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

Connection Manager Object

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

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

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

Class Attribute List

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

Common Service List

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

Port Object

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

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

Class Attribute List

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

Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Port Type		UINT (16)	Enumerates the type of port. 4 = EtherNet/IP.
2	Get	Port Number		UINT (16)	CIP port number associated with this port. (Value 1 is reserved for internal product use)
3	Get	Link Object		(Struct.)	
			Path Length	UINT (16)	Number of 16-bit words in the following path.
			Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name		SHORT_STRING	String which names the physical network port. The maximum number of characters in the string is 64.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
7	Get	Node Address		Padded EPATH	Node number of this device on port. The range within this data type is restricted to a Port Segment.
10	Get	Port Routing Capabilities		DWORD (32)	Bit string that defines the routing capabilities of this port.

Common Service List

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