

# MGate 5192 Series User Manual

---

Version 1.0, June 2024

[www.moxa.com/products](http://www.moxa.com/products)

**MOXA**®

© 2024 Moxa Inc. All rights reserved.

# MGate 5192 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](http://www.moxa.com/support)

# Table of Contents

<b>1. Introduction</b>	<b>4</b>
<b>2. Getting Started</b>	<b>5</b>
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
<b>3. Web Console Configuration and Troubleshooting</b>	<b>8</b>
System Dashboard	8
System Settings	9
System Settings—General Settings	9
System Settings—Network Settings	11
System Settings—Serial Settings	12
System Settings—SNMP Settings	13
Protocol Settings	18
Protocol Settings—Protocol Conversion	18
Protocol Settings—Modbus RTU/ASCII Server Settings	19
Protocol Settings—Modbus TCP Server Settings	20
Protocol Settings—DNP3 Serial Outstation Settings	22
Protocol Settings—DNP3 TCP/UDP Outstation Settings	23
Protocol Settings—IEC 60870-5-101 Server/Slave Settings	24
Protocol Settings—IEC 60870-5-104 Server Settings	25
Protocol Settings—IEC 61850 Client Settings	26
Diagnostics	33
Diagnostics—Protocol Diagnostics	33
Diagnostics—Protocol Traffic	37
Diagnostics—Event Log	39
Diagnostics—Tag View	43
Diagnostics—Network Connections	43
Diagnostics—Ping	44
Diagnostics—LLDP	44
Security	45
Security—Account Management	45
Security—Service	48
Security—Allow List	49
Security—DoS Defense	49
Security—Login Policy	50
Security—Certificate Management	51
Maintenance	52
Maintenance—Configuration Import/Export	52
Maintenance—Firmware Upgrade	53
Maintenance—Load Factory Default	53
Restart	54
Status Monitoring	54
<b>4. Network Management Tool (MXstudio)</b>	<b>56</b>
<b>A. SNMP Agents with MIB II and RS-232-Like Groups</b>	<b>57</b>
RFC1213 MIB-II Supported SNMP Variables	57
RFC1317 RS-232-Like Groups	58

# 1. Introduction

---

The MGate 5192 is an industrial Ethernet gateway for converting IEC 61850 MMS to Modbus TCP/RTU/ASCII, DNP3 serial/TCP/UDP, IEC 60870-5-101, or IEC 60870-5-104 network communications. To integrate existing IEC 61850 MMS devices into a Modbus TCP/RTU/ASCII, DNP3 serial/TCP/UDP, IEC 60870-5-101, or IEC 60870-5-104 network, use the MGate 5192 as a Modbus client to collect data and exchange data with Modbus TCP/RTU/ASCII, DNP3 serial/TCP/UDP, IEC 60870-5-101, or IEC 60870-5-104 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. 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, DNP3, or IEC 60870-5-101 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.

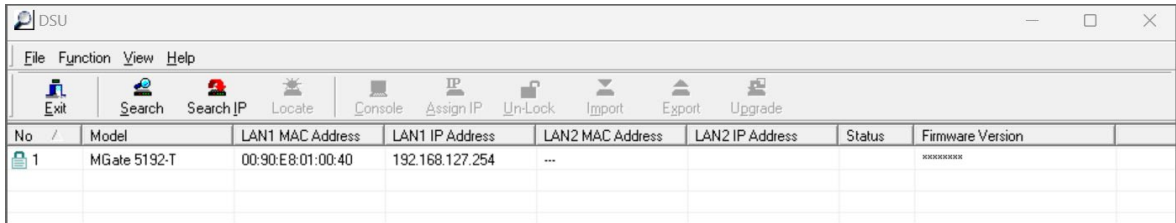
### Installing DSU Software

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 Device Search Utility (DSU) from Moxa's website: [www.moxa.com](http://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.



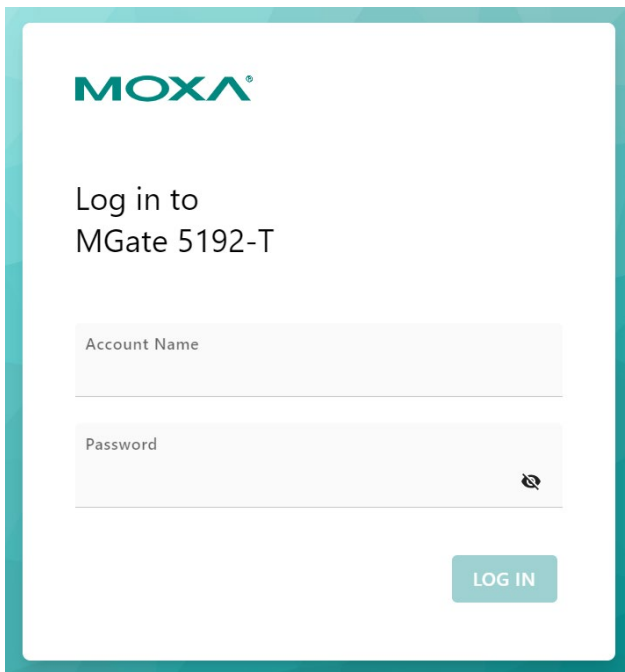
No	Model	LAN1 MAC Address	LAN1 IP Address	LAN2 MAC Address	LAN2 IP Address	Status	Firmware Version
1	MGate 5192-T	00:90:E8:01:00:40	192.168.127.254	...			*****

## 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 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 5192-T

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 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 be copied to the MGate device.

# 3. Web Console Configuration and Troubleshooting

This chapter provides a quick overview of how to configure the MGate 5192 by web console.

## System Dashboard

This page gives a system dashboard of the MGate 5192 gateway.

The screenshot shows the MGate 5192 System Dashboard. The top navigation bar includes the MOXA logo, the device ID 'MGate 5192-T\_00000040', and the user 'Administrator daga'. The left sidebar lists various settings and diagnostic tools. The main content area is divided into several sections:

- System Information:** Displays a photo of the MGate 5192-T device and its specifications: Model Name (MGate 5192-T), Serial no. (MOXA00000040), Firmware version (1.0.0 Build 23091214), Uptime (0 day 00h:07m:19s), IPv4 (192.168.127.254), MAC address (00:90:E8:01:00:40), and MicroSD (Not detected).
- Panel Status:** Shows the status of System LEDs (PWR1, PWR2, READY) and Port LEDs (ETH1, ETH2, 61850, DNP3, MB, 101, 104).
- Event Summary:** A summary table showing 20 Alerts, 16 Warnings, and 14 Info events. Below it is a detailed table of events.
- Relay State:** A table listing relay events and their states, with 'ACKNOWLEDGE' buttons for each.

ID	Severity	Message	Timestamp
1	Alert	Power input 2 failure	2024-03-03T16:22:48.895+00:00
2	Alert	Ethernet port 2 link down	2024-03-03T16:22:48.899+00:00
3	Alert	Power input 2 failure	2024-03-03T15:21:13.396+00:00
4	Alert	Ethernet port 2 link down	2024-03-03T15:21:13.388+00:00
5	Alert	Ethernet port 2 link down	2024-03-03T15:06:33.116+00:00

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

This image shows a close-up of the user profile dropdown menu. The user is identified as 'Administrator admin'. The menu contains two options: '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 5000

Description - Optional

SAVE

### System Settings

Parameter	Value	Description
Host Name	Alphanumeric string	Enter a name that can help you identify the device with precision. 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 Settings

System      **Time**

Current date and time: 2024-05-16 23:21:49

Time Zone  
 (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbo... ▾

Daylight Saving Time  
 Enable     Disable

Mode  
 Manual     Auto

☞ Sync with browser

Date  
 05/16/2024 📅

Hour : Minute : Second  
 23 : 20 : 58

**SAVE**

Parameter	Value	Description
<b>Time zone</b>	User-selectable time zone	Shows the current time zone selected and allows change to a different time zone.
<b>Daylight saving time</b>	Enable Disable	Enable and set up the daylight saving time; or disable daylight saving time
<b>Mode</b>	Manual	Use this setting to manually adjust the time (1900/1/1-2037/12/31) or sync with the browser time
	<b>Auto</b>	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.



### 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 Settings

LAN Mode  
 Switch ▼

#### LAN

IP Configuration  
 Static ▼

IP Address  
 192.168.127.254

Netmask  
 255.255.255.0

Gateway - optional  
 192.168.127.1

#### DNS Server

Preferred DNS Server - optional  
 192.168.127.16

Alternative DNS Server - optional  
 192.168.127.17

SAVE

Parameter	Value	Description
<b>LAN Mode</b>	<b>Switch, Dual IP, Redundant LAN</b>	The <b>Switch</b> mode allows users to install the device with daisy-chain topology. The <b>Dual IP</b> 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 <b>Redundant LAN</b> 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 cannot respond, the device will automatically switch to the backup LAN ETH2.
<b>IP Configuration</b>	<b>DHCP, Static IP</b>	Select <b>Static IP</b> if you are using a fixed IP address. Select the DHCP option if you want the IP address to be dynamically assigned.
<b>IP Address</b>	192.168.127.254 (or other 32-bit number)	The <b>IP Address</b> identifies the server on the TCP/IP network.
<b>Netmask</b>	255.255.255.0 (or other 32-bit number)	Identifies the server as belonging to a Class A, B, or C network.
<b>Gateway</b>	0.0.0.0 (or other 32-bit number)	The IP address of the router that provides network access outside the server's LAN.
<b>Preferred DNS Server</b>	0.0.0.0 (or other 32-bit number)	The IP address of the primary domain name server.
<b>Alternative DNS Server</b>	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, DNP3 serial, or IEC 60870-5-101 protocol. Incorrect settings will cause communication failures.

Port	Interface	Baudrate	Parity, Data Bits, Stop Bits	Flow Control
#1 (Circuit_Breaker)	RS-485 2-wire	38400	None, 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 (Circuit\_Breaker)

Alias - Optional  
Circuit\_Breaker

---

Interface  
RS-485 2-wire

Terminator  
 120 Ω  None

Pull-up and Pull-down Resistor  
 1 kΩ  150 kΩ

Baudrate  
38400

Parity  
None

Data Bits  
 7  8

Stop Bits  
 1  2

FIFO  
 Enable  Disable

**SAVE**

Parameter	Value	Description
<b>Alias</b>	Alphanumeric string	Allows you to define an alias to a port for easier identification. Max. 16 characters.
<b>Interface</b>	<b>RS-232, RS-422, RS-485 2-wire, RS-485 4-wire</b>	

Parameter	Value	Description
<b>Terminator</b>	<b>120 Ω, None</b>	The default is none, which means the terminator is disabled. Try to enable the 120 Ω when the communication has issue, especially for long distance communication.
<b>Pull-up and Pull-down Resistor</b>	<b>1 kΩ, 150 kΩ</b>	The default value is 150 kΩ. Set the value depending on the system requirements.
<b>Baudrate</b>	300 bps to 921600 bps	The baudrate value can be also self-defined as long as it is between 300 bps to 921600 bps.
<b>Parity</b>	<b>None, Odd, Even, Mark, Space</b>	
<b>Data Bits</b>	<b>7,8</b>	
<b>Stop Bits</b>	<b>1, 2</b>	
<b>FIFO</b>	<b>Enable, Disable</b>	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
<b>Flow Control</b> (only for RS-232 mode)	<b>None, RTS/CTS, RTS Toggle</b>	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.
<b>RTS on delay</b>	0 to 100 ms	Only available for the RS-232 mode to implement the RTS Toggle function.
<b>RTS off delay</b>	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

You can set up SNMP Agent for the MGate's management.

## SNMP Agent

General    SNMPv3 Account    SNMPv3 Account Protection

Status:  Disable

**NOTE:**  
Enable/disable this service

Version  
v3 only

Contact

Location

Minimum Authentication/Privacy Password Length  
8

**SAVE**

Parameters	Description
<b>Version</b>	The SNMP version; the MGate supports SNMP V1, V2c, and V3.
<b>Contact</b>	The optional contact information usually includes an emergency contact name and telephone number.
<b>Location</b>	The location information. This string is usually set to the street address where the MGate is physically located.
<b>Read Only Community</b>	A text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
<b>Read/Write Community</b>	A text password mechanism that is used to weakly authenticate changes to agents of managed network devices.
<b>Minimum Authentication/Privacy Password Length</b>	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

General    **SNMPv3 Account**    SNMPv3 Account Protection

**+ CREATE**

Account Name	Status	Authority	Authentication Type	Privacy Type	
Tiffany	<span style="color: green;">●</span> Active	Read/Write	SHA-512	AES-128	⋮

If you need to use SNMPv3, Click on "CREATE" to create a SNMPv3 Account and use the drop-down menu to configure the Authority and Authentication Type.

### Create SNMPv3 Account

Account Name

Authority  
Read/Write

Authentication Type  
Disable

CANCEL SAVE

Parameters	Value	Description
<b>Account Name</b>		The username for which the access level is being defined.
<b>Authority</b>	<b>Read Only</b> <b>Read/Write</b>	The level of access allowed
<b>Authentication Type</b>	<b>Disable (Default)</b> <b>MD5</b> <b>SHA1</b> <b>SHA-224</b> <b>SHA-256</b> <b>SHA-384</b> <b>SHA-512</b>	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication. If you enable an authentication type, please also configure the authentication password.
<b>Privacy Type</b>	<b>Disable (Default)</b> <b>DES-CBC</b> <b>AES-128</b>	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 the right of the configured SNMP item to change settings, such as Authentication Type, or Privacy Type.

### Edit SNMPv3 Account

Account Name  
Tiffany

Authority  
Read/Write

Authentication Type  
SHA-512

Authentication Password  
.....

Privacy Type  
AES-128

Privacy Password  
.....

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

## System Settings—SNMP Settings—SNMP Trap

### SNMP Trap

General    **SNMP Trap Server**

Trap Service

Enable

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

**SAVE**

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



SNMP Trap						
General		SNMP Trap Server				
+ CREATE						
Server IP or Domain Name	Port	Trap Version	Community String	Account Name	Authentication Type	Privacy Type
10.123.5.112	678	SNMPv1	moxa	-	-	-

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

### Create Trap Server

**General Settings**

Server IP or Domain Name

Port

**Trap Method**

Trap Version  
Disable

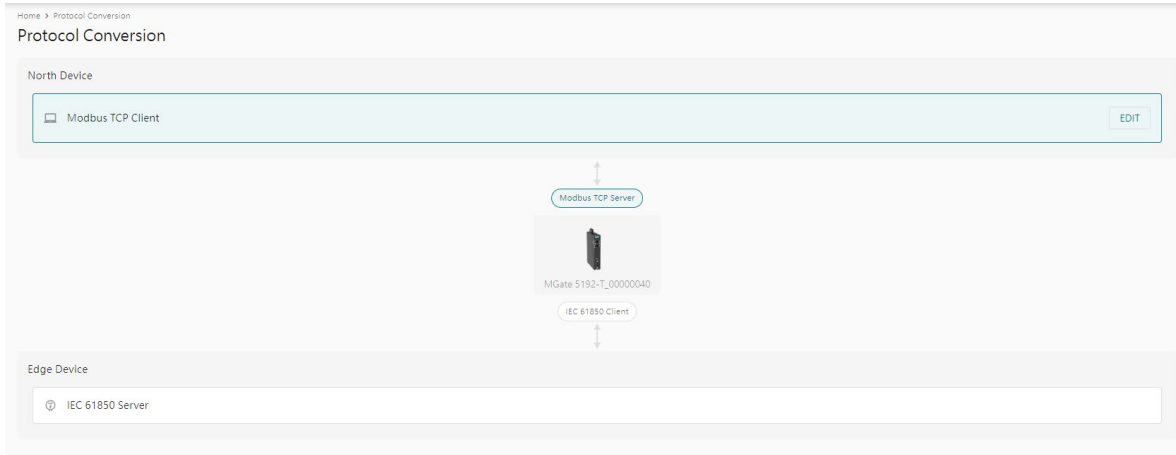
CANCEL SAVE

Parameters	Description
<b>Server IP</b>	SNMP server IP address or domain name.
<b>Port</b>	SNMP server IP Port.
<b>Trap Version</b>	<b>Disable</b> <b>SNMPv1</b> <b>SNMPv2c</b> <b>SNMPv3</b>

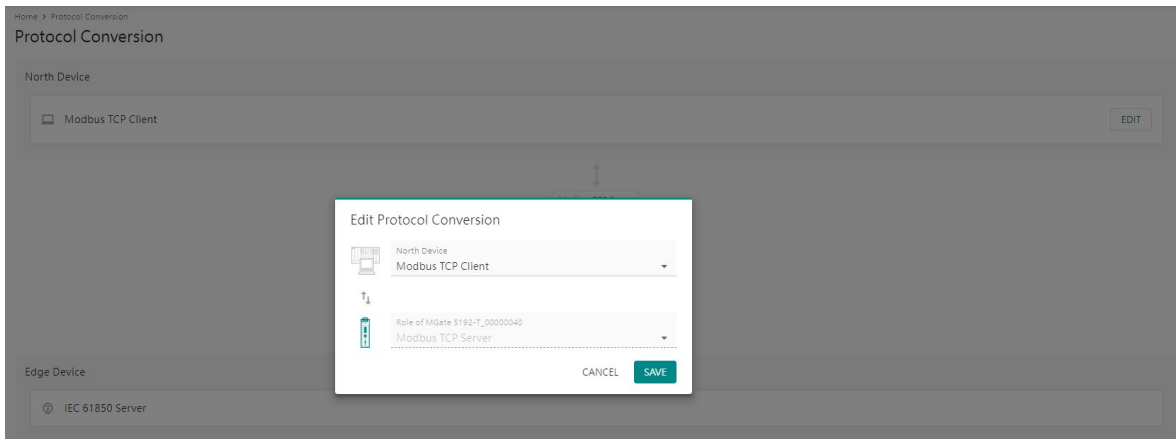
# Protocol Settings

## Protocol Settings—Protocol Conversion

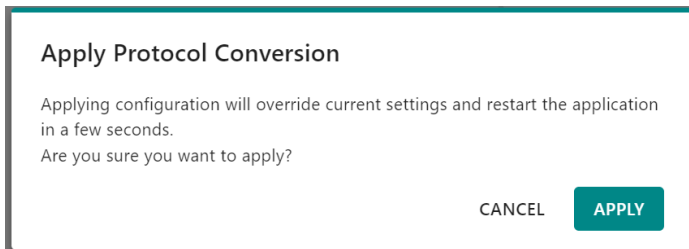
You can click **Edit** and select Modbus TCP/RTU/ASCII, DNP3 serial/TCP/UDP, IEC 60870-5-101, or IEC 60870-5-104 for the north device protocol. IEC 61850 is the edge device protocol. Please note that the MGate 5192 provides a 1-to-1 protocol conversion, which means you can select one protocol for the north device and one protocol for the edge device.



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



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



# Protocol Settings—Modbus RTU/ASCII Server Settings

You can configure the Modbus RTU/ASCII server settings on this page. Click on the COM1 button to edit the settings.

Home > Modbus RTU/ASCII Server

## Modbus RTU/ASCII Server

Modbus RTU/ASCII Server

### Server Settings

Click the card below for more server settings and information.

COM1  
Not configured

After clicking the COM1 button, you can set up the Modbus server ID (slave ID) and add the tags you want to read from the Modbus RTU/or Modbus ASCII client.

Home > Modbus RTU/ASCII Server > Server Settings > COM1

## ← COM1

COM1  
Server ID: 1  
Mode: RTU

EDIT

### Data Mapping - 0 tags

+ ADD TAGS

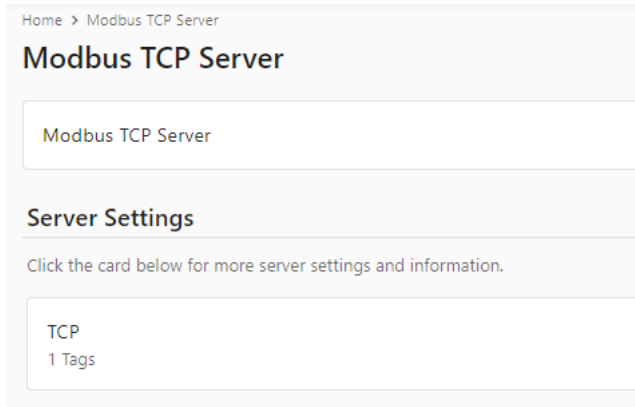
All (View only) - 0    Coil (R/W) - 0    Input Discrete (R) - 0    Holding Register (R/W) - 0    Input Register(R) - 0

🔍

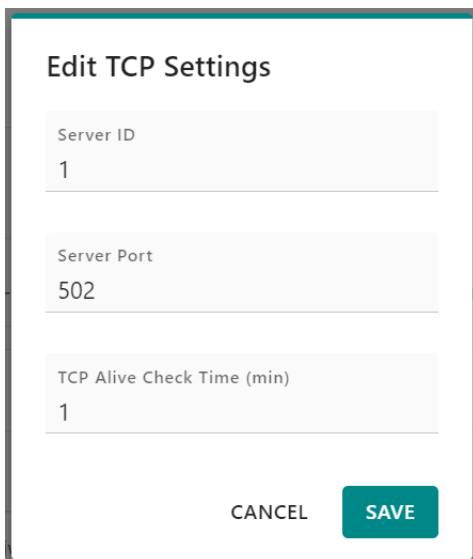
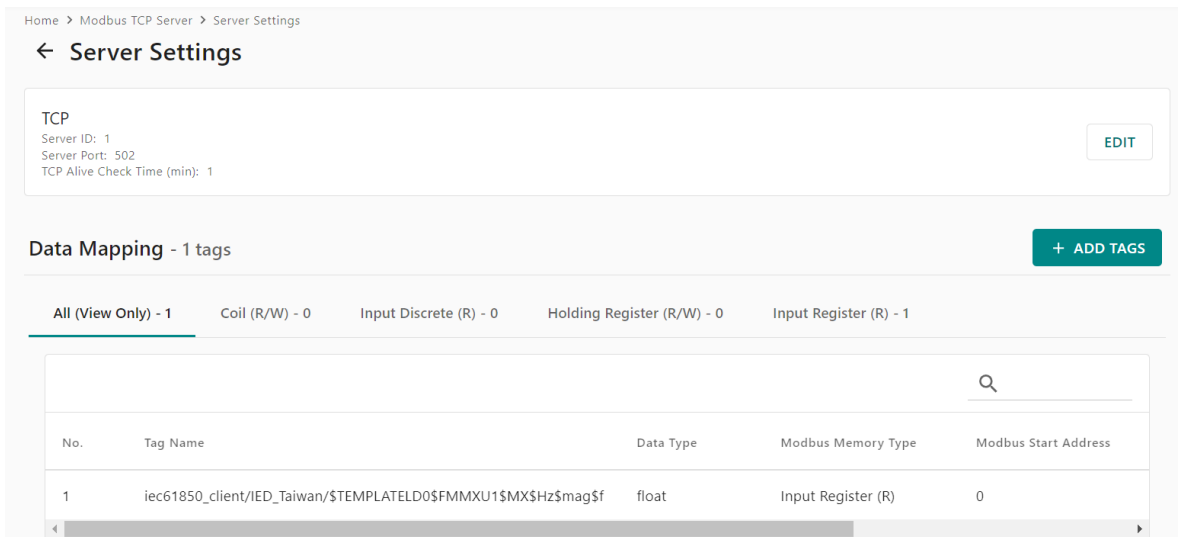
No.	Tag Name	Data Type	Modbus Memory Type	Modbus Start Address
-----	----------	-----------	--------------------	----------------------

# Protocol Settings—Modbus TCP Server Settings

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



After clicking the TCP button, you can set up the Modbus server ID (slave ID), the Modbus TCP server listening port, and the TCP alive check time.



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

Click on ADD TAGS to add data tags from IEC61850 to the Modbus TCP. Notice that the tags must be created in IEC 61850 client. Click DONE after selection.

### Add Tags

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

Providers  
iec61850\_client ▼  
6 Tags

Selected Tags  
status ▼

CANCEL DONE

The selected tags will display in the data mapping column by default with register/coil address. You can view all the data, or view by Modbus functions—Read/Write Coil, Read Discrete Input, Read/Write Holding Register, Read Input Register. You may adjust it manually. After making changes, click APPLY to take effect.

### Data Mapping - 2 tags + ADD TAGS

All (View Only) - 2  
 Coil (R/W) - 0  
 Input Discrete (R) - 0  
 Holding Register (R/W) - 0  
 Input Register (R) - 2

No.	Tag Name	Data Type	Modbus Memory Type	Modbus Start Address
1	iec61850_client/IED_Taiwan/\$TEMPLATELD0\$FMMXU1\$MX\$Hz\$mag\$f	float	Input Register (R)	0
2	iec61850_client/IED_Taiwan/status	int32	Input Register (R)	2

Edit DISCARD APPLY

# Protocol Settings—DNP3 Serial Outstation Settings

You can configure the DNP3 serial outstation settings on this page. Click on the COM1 button to edit the settings.

Home > DNP3 Serial Outstation

## DNP3 Serial Outstation

DNP3 Serial Outstation  
Timestamp Reference: UTC EDIT

### Outstation Settings

Click the card below for more outstation settings and information.

COM1  
Not configured

After clicking the COM1 button, you can set up the DNP3 serial outstation settings and add the tags you want to read from the DNP3 serial client (master).

Home > DNP3 Serial Outstation > Outstation Settings > COM1

## ← COM1

DNP3 Serial Outstation EDIT

- ^ Basic Settings
  - DNP3 Data Link Source Address: 4
  - DNP3 Data Link Destination Address: 3
  - Support Unsolicited Message: Enable
- ∨ Advanced Settings

Data Mapping - 0 tag  FILTER DELETE QUICK SETTINGS + ADD TAGS

<input type="checkbox"/>	No.	Tag Name	Tag Type	Direction	Object Type	Point Index
--------------------------	-----	----------	----------	-----------	-------------	-------------

# Protocol Settings—DNP3 TCP/UDP Outstation Settings

You can configure the DNP3 TCP or UDP outstation settings on this page. Click on the TCP/UDP button to edit the settings.

Home > DNP3 TCP/UDP Outstation

## DNP3 TCP/UDP Outstation

DNP3 TCP/UDP Outstation  
Timestamp Reference: UTC EDIT

### Outstation Settings

Click the card below for more outstation settings and information.

TCP/UDP  
Not configured

After clicking the TCP/UDP button, you can set up the DNP3 TCP or UDP outstation be copied add the tags you want to read from the DNP3 TCP/UDP client.

Home > DNP3 TCP/UDP Outstation > Outstation Settings

## ← Outstation Settings

DNP3 TCP/UDP Outstation EDIT

- ^ Basic Settings
  - DNP3 Data Link Source Address: 4
  - DNP3 Data Link Destination Address: 3
  - Server Port: 20000
  - Network Type: TCP
  - Support Unsolicited Messages: Enable
- ∨ Advanced Settings

Data Mapping - 0 tag SEARCH tag name FILTER DELETE QUICK SETTINGS + ADD TAGS

<input type="checkbox"/>	No.	Tag Name	Tag Type	Direction	Object Type	Point Index
--------------------------	-----	----------	----------	-----------	-------------	-------------

# Protocol Settings—IEC 60870-5-101 Server/Slave Settings

You can configure the IEC 101 server (slave) settings on this page. Click on the COM1 button to edit the settings.

Home > IEC 60870-5-101 Slave

## IEC 60870-5-101 Slave

IEC 60870-5-101 Slave

### Slave Settings

Click the card below for more outstation settings and information.

COM1  
Not configured

After clicking the COM1 button, you can set up the IEC 101 server (slave) settings and add the tags you want to read from the IEC 101 client (master).

Home > IEC 60870-5-101 Slave > Slave Settings > COM1

## ← COM1

IEC 60870-5-101 Slave EDIT

- Basic Settings
  - Link Layer
    - Link Mode: Unbalanced Transmission
    - Link Address Size: 2 bytes
  - Application Layer
    - ASDU Size: 2 bytes
    - COF Size: 1 octet
    - IOA Size: 2 octet
  - Server Address
    - Link Address: 3
    - ASDU Address: 3
- Advanced Settings
  - IEC 60870-5-101 Parameters
    - Frame Timeout: 15000 ms
    - Link Confirm Timeout: 2000 ms
    - Link Layer Retry: 3
    - Single Char Ack: Disable
    - Single Char Response: Disable
  - Time
    - Enable Time Synchronization: Disable
    - Timestamp reference: UTC
    - General Interrogation Timestamp Format: 24 bits
    - Event Timestamp Format: 35 bits
    - Measured Value Cycle Timestamp Format: None
  - Active Termination
    - Enable Cse Activation Termination: Enable
    - Enable Cmd Activation Termination: Enable
  - Measured Value
    - Enable Measured Value Spontaneous: Enable
    - Enable Measured Value(Normalized) Cyclic Report Interval: Disable
    - Enable Measured Value(Scaled) Cyclic Report Interval: Disable
    - Enable Measured Value(Floating) Cyclic Report Interval: Disable
  - Select-operate
    - Supported Control Function: Select-operate
    - Select Timeout: 5000 ms



# Protocol Settings—IEC 60870-5-104 Server Settings

You can configure the IEC 104 server settings on this page. Click on the IEC 60870-5-104 button to edit the settings.

Home > IEC 60870-5-104 Server

## IEC 60870-5-104 Server

IEC 60870-5-104 Server

### Server Settings

Click the card below for more outstation settings and information.

IEC 60870-5-104  
Not configured

After clicking the IEC 60870-5-104 button, you can set up the IEC 104 server settings, and add the tags you want to read from the IEC 104 client.

Home > IEC 60870-5-104 Server > Server Settings

## ← Server Settings

IEC 60870-5-104 Server EDIT

- Basic Settings
  - Server Port: 2404
  - ASDU Address: 3
  - COT Size: 2
- Advanced Settings
  - IEC 60870-5-104 Parameters
    - ki: 12
    - w: 8
    - 11 Timeout: 15000 ms.
    - 12 Timeout: 10000 ms.
    - 13 Timeout: 20000 ms.
  - Time
    - Enable Time Synchronization: Disable
    - Timestamp Reference: UTC
    - General Interrogation Timestamp Format: 24 bits
    - Event Timestamp Format: 56 bits
    - Measured Value Cycle Timestamp Format: None
  - Active Termination
    - Enable Cse Activation Termination: Enable
    - Enable Cmd Activation Termination: Enable
  - Measured Value
    - Enable Measured Value Spontaneous: Enable
    - Enable Measured Value (Normalized) Cyclic Report Interval: Disable
    - Enable Measured Value (Scaled) Cyclic Report Interval: Disable
    - Enable Measured Value (Floating) Cyclic Report Interval: Disable
  - Select-operate
    - Supported Control Function: Select-Operate
    - Select Timeout: 5000 ms.

# Protocol Settings—IEC 61850 Client Settings

Add, edit or manage the IEC 61850 server devices and the data objects on this page. Note that the MGate acts as an IEC 61850 client. The maximum number of connections to IEC 61850 servers is 32, and the maximum data objects that can be converted are 5,000 objects.

Home > IEC 61850 Client

## IEC 61850 Client

IEC 61850 Client MANAGE

- > Client Certificate
- > Trusted CA

### IEC 61850 Server Settings

Click the card below for more server settings and information.

Server Settings  
Not configured

If you need to use secure IEC 61850 communication, click **Manage** to import your certificate.

Click **Server Settings** to set up the IEC 61850 server device.

Note that the MGate 5192 supports RSA certificates.

To add an IEC 61850 server device to the MGate, click the **ADD SERVER** button.

← Server Settings

Common Settings EDIT

Connection Retry Interval (sec): 10  
Response Timeout (sec): 3  
TCP Alive Check Time (min): 0

**ADD SERVER**

IED\_Taiwan  
● Enable  
Server IP: 192.168.127.4  
Server Port: 102  
Number of Tags: 1

Overview Report Read Data Operate Data

Logical Device	FCDA	Data Type	Report	Read	Operate	Scaling
TEMPLATELDD	FMMXU15MXSHz5mag5f	float		●		Disable

Items per page: 100 1 - 1 of 1 < > / 1 >

## Step 1: Add IEC 61850 server device to the MGate

When adding an IEC 61850 server device, click "Choose File" to select the Substation Configuration Language (SCL), or Configured IED Description (CID) file of your device. This file contains the device description and settings of the IEC 61850 server device. After selecting the file, click **UPLOAD** to import the SCL/CID file to the MGate. Note that this file is generated by another SCL/CID generator software or exported from a IED's configuration software.

← Add New Server

1 Basic Settings — 2 Report Settings Optional — 3 Request Settings Optional — 4 Scaling Optional — 5 Confirm

SCL File  
 No file chosen

Parameter	Value	Default	Description
<b>Server Name</b>	Alphanumeric string		Max. 128 characters.
<b>IP Address</b>	0.0.0.0 to 255.255.255.255	0.0.0.0	The IP address of a remote IEC 61850 server device.
<b>Port</b>	1 to 65535	102	The TCP port number of a remote IEC 61850 server device.

After importing the SCL/CID file, check the basic settings of your IEC 61850 server device and add a "Server Name" to identify this server, for example, an IED device on the MGate.

← Add New Server

1 Basic Settings — 2 Report Settings Optional

Server Communication Security

Enable server

SCL File Name  
IED\_124.cid

IED  
TPCS0129

Access Point  
S1

Server Name

IP Address  
192.29.9.71

Port  
102

In the following steps, there are two parts for the data: Report and Request settings. The difference lies in the direction for transmitting data. The Report data are the data actively sent from the IED, and the request data are the ones that will be read or written from the MGate.

## Step 2: Configure the IEC 61850 Report Settings (Optional)

Under Report settings, click on **ADD REPORT** to configure a report and the trigger conditions for data sending actively from the IEC 61850 server. For example, an IED might need to periodically report the current and voltage values and its quality status. In this case, you can configure the data objects to be sent and the send interval.

In the **ADD REPORT** dialog, select the Logical Device, and the data reports you want the IEC 61850 server to report/actively send to the MGate. The report trigger method and the integrity interval, which means the report send interval, can also be configured. Click **DONE** to finish adding the report from the IEC 61850 server.

Parameter	Value	Default	Description
<b>Trigger Option</b>	<b>Data Update</b> <b>Data Change</b> <b>Quality Change</b> <b>General Interrogation</b> <b>Integrity</b>		<p><b>None of the Trigger Options are selected:</b> A report is never sent to the IEC 61850 client.</p> <p><b>Data Update:</b> A report is sent to the IEC 61850 client when the data is refreshed, no matter if there is a change or not.</p> <p><b>Data change:</b> A report is sent to the IEC 61850 client when a change in data is detected.</p> <p><b>Quality Change:</b> A report is sent to the IEC 61850 client when the quality (q value) is changed. For example, if the quality of a data object is changed from good to questionable.</p> <p><b>General Interrogation:</b> A report is sent to the IEC 61850 client when a general interrogation(GI) is received from the client.</p> <p><b>Integrity:</b> A report is sent to the IEC 61850 client periodically at the Integrity Interval specified in the Report settings.</p>
<b>Integrity Interval</b>	100 to 600000 ms	60000 ms	A periodic interval for sending integrity reports. This option is only available when Integrity in report trigger options is enabled.

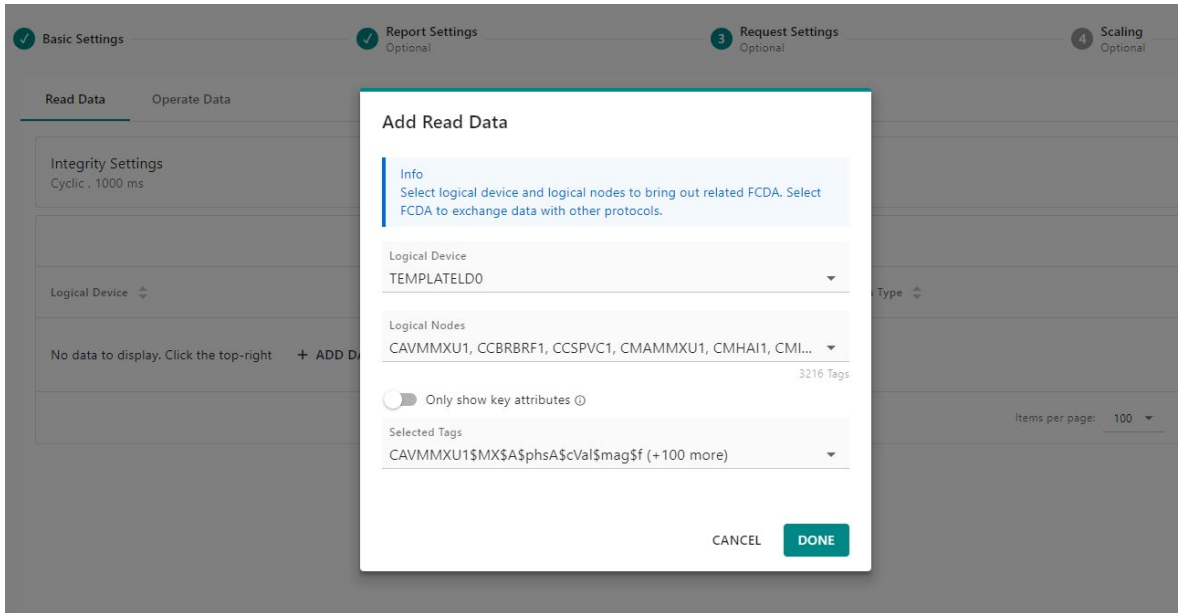
click **NEXT** to go on to the next step.

### Step 3: Configure Read/Operate Request Settings (Optional)

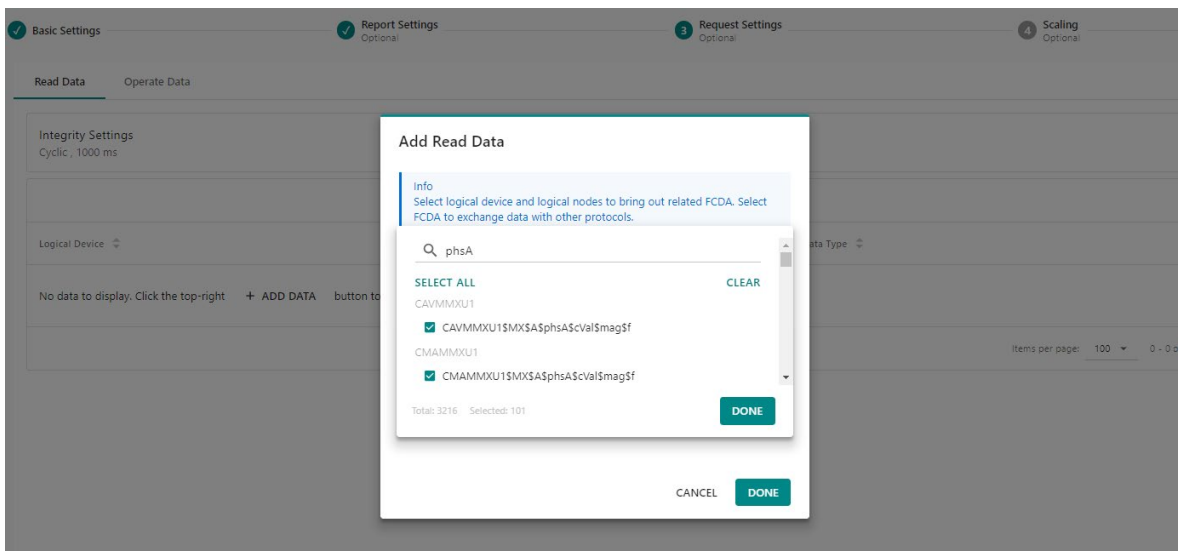
Under Request Settings, click **ADD DATA** to configure the data that you want to read or operate from the MGate. Under the Read Data tab, select the data tags you want to read. Under the Operate Data tab, select the data tags you want to operate, or write.

Click **ADD DATA** to select the Logical Device, Logical Node, and the data tags.

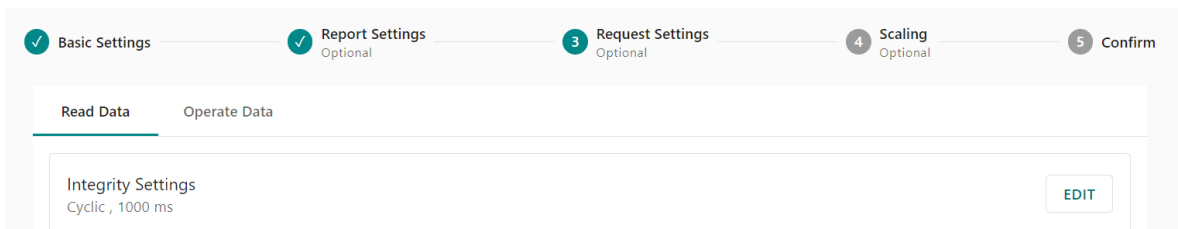
Select the Logical Device, Logic Node, and the data tags that you want to be read from the MGate.



To speed up the data tag selection, use the Search function or the **SELECT ALL** function under the drop-down menus to quickly select multiple items.



The Read data can be triggered by the end of initialization or cyclically. Click on EDIT to change the trigger settings.



Parameters	Value	Description
<b>Integrity settings</b>	None Cyclic (default) End of init	<b>None:</b> MGate will not read IEC61850 data from the server device. <b>Cyclic:</b> The default is 1000; can be configured between 100 to 600000 ms. <b>End of init:</b> Only read when the IEC61850 initialization is finished.

The Operate data will be triggered when the mapping data changed.

Click **NEXT** to go on to the next step.

SNMP Agent

General SNMPv3 Account SNMPv3 Account Protection

+ CREATE

Account Name	Status	Authority	Authentication Type	Privacy Type	
Tiffany	Active	Read/Write	SHA-512	AES-128	

#### Step 4: Configure Scaling of the Data (Optional)

On the scaling page, we can view all the configured reports, read and operate data objects, and perform data scaling or calculations by clicking on the object's pen icon.

← Add New Server

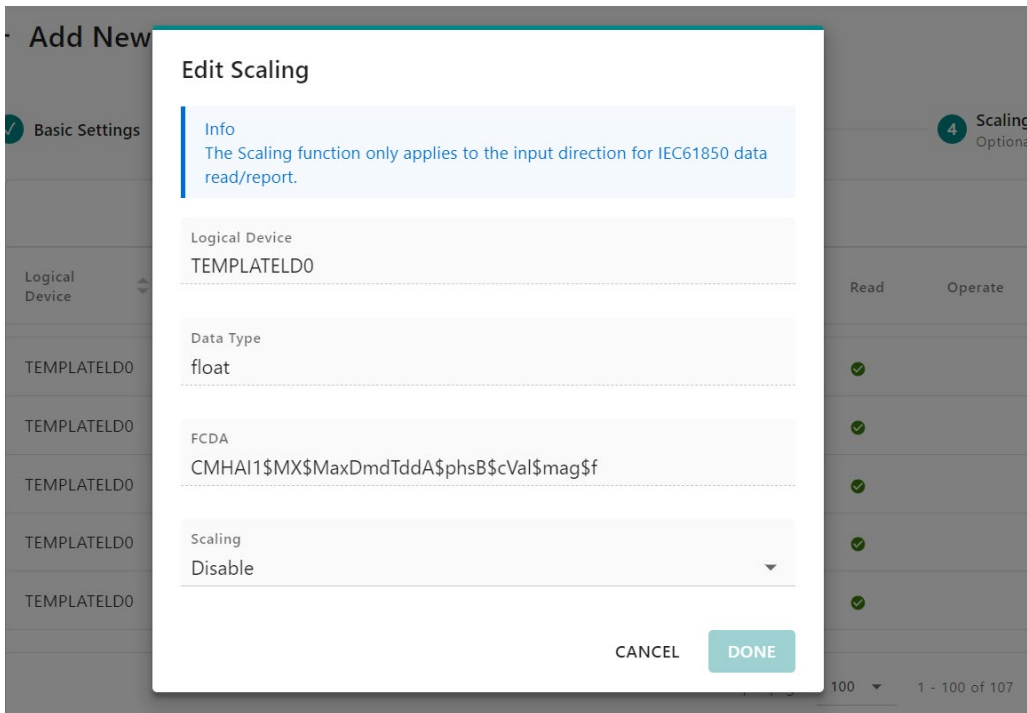
✓ Basic Settings — ✓ Report Settings Optional — ✓ Request Settings Optional — 4 Scaling Optional — 5 Confirm

Logical Device	FCDA	Data Type	Report	Read	Operate	Scaling	
TPCS0129cm9Z001	gen1XCBR1\$ST\$Pos\$stVal	uint8	✓			Disable	✎
TPCS0129cm9Z001	gen2XCBR1\$ST\$Pos\$stVal	uint8	✓			Disable	✎
TPCS0129cm9Z001	gen3XCBR1\$ST\$Pos\$stVal	uint8	✓			Disable	✎
TPCS0129cm9Z001	psFSCC1\$CO\$Mod\$SBOw\$ctIVal	int32		✓	✓	Disable	✎
TPCS0129cm9Z001	psFSCC1\$CO\$Mod\$Cancel\$ctIVal	uint8		✓		Disable	✎
TPCS0129cm9Z001	psFSCC1\$CO\$Mod\$Cancel\$ctIVal	int32		✓		Disable	✎

Items per page: 10 1 - 10 of 18 < < 1 / 2 > >

< BACK CANCEL **NEXT** >

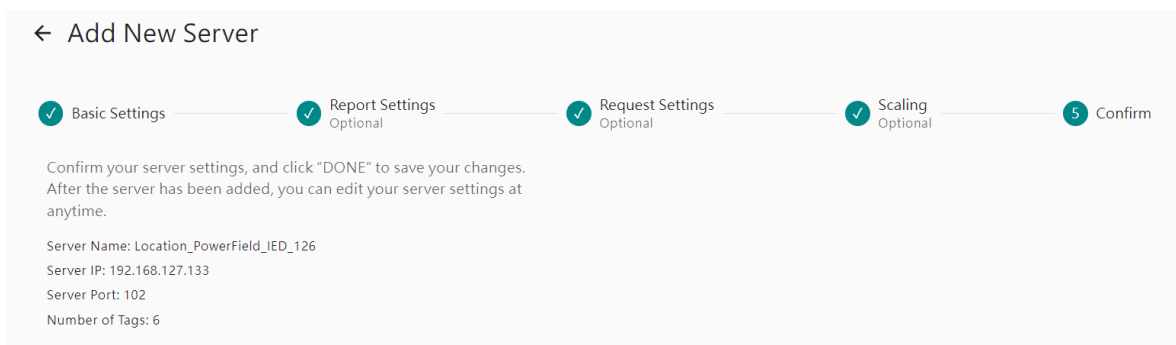
In the Edit Scaling dialog, you can enable two scaling or calculation methods: slope-intercept or point-slope.



Parameters	Value	Description
<b>Data Type</b>	boolean, int8, int16, int32, int64, uint8, uint16, uint32, uint64, float, double	<p>Specifying the tag data type. The default is raw for fast multiple data mapping.</p> <p>For other data types, you could also scale the resource data. There are two types:</p> <ul style="list-style-type: none"> <li> <b>Slope-intercept:</b>  <math>\text{tag value} = (\text{source value} * \text{slope}) + \text{offset}</math>                      Note that Slope intercept is used to compensate for slight adjustments needed during the measurement process.                 </li> <li> <b>Point-slope:</b>  <math>\text{tag value} = \text{source value} * \left( \frac{\text{target max.} - \text{target min.}}{\text{source max.} - \text{source min.}} \right)</math>                      Note that Point-slope is used to convert data values into different units, or user-defined ranges.                 </li> </ul>

### Step 5: Confirm All Your Settings

Click **NEXT** to go on to the last step. In the last step, which is the CONFIRM page, check the overview of the IEC 61850 settings. Click DONE to finish the settings. You can also edit the server settings at any time.



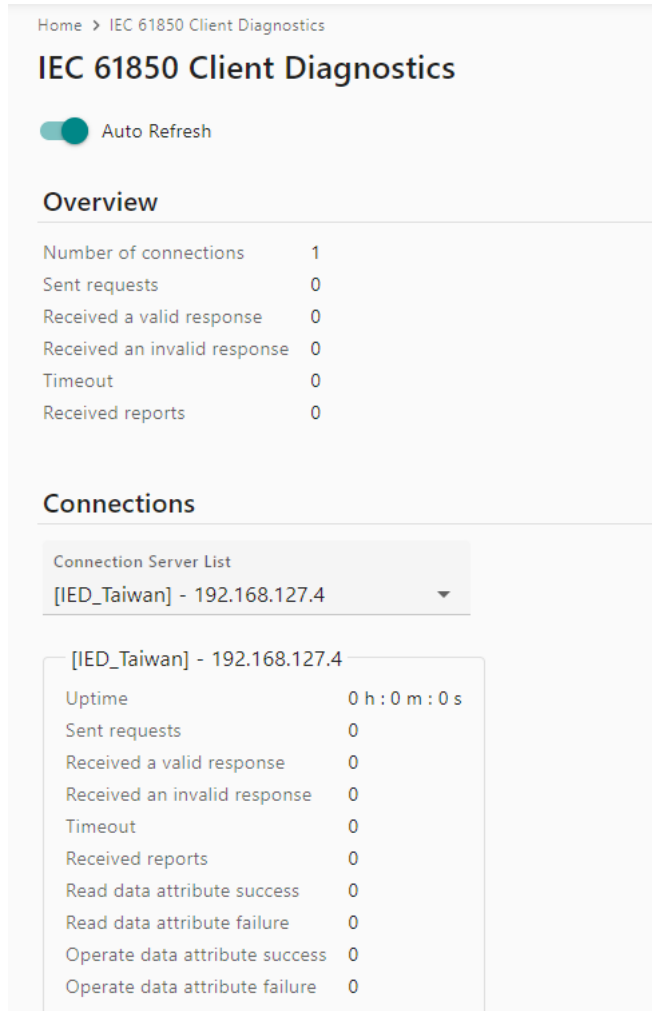


# Diagnostics

## Diagnostics—Protocol Diagnostics

### Dignostics—Protocol Diagnostics—IEC 61850 Client Diagnostic

The MGate provides diagnostics information for all protocols. If communication error occurs, check the protocol diagnostic page for trouble shooting.



Home > IEC 61850 Client Diagnostics

## IEC 61850 Client Diagnostics

Auto Refresh

### Overview

Number of connections	1
Sent requests	0
Received a valid response	0
Received an invalid response	0
Timeout	0
Received reports	0

### Connections

Connection Server List

[IED\_Taiwan] - 192.168.127.4

[IED\_Taiwan] - 192.168.127.4

Uptime	0 h : 0 m : 0 s
Sent requests	0
Received a valid response	0
Received an invalid response	0
Timeout	0
Received reports	0
Read data attribute success	0
Read data attribute failure	0
Operate data attribute success	0
Operate data attribute failure	0

# Diagnostics—Protocol Diagnostics—Modbus RTU/ASCII Diagnostic

Home > Modbus RTU/ASCII Server Diagnostics

## Modbus RTU/ASCII Server Diagnostics

Auto Refresh

### Modbus

Mode	Server
Valid requests received	0
Invalid requests received	0
CRC error requests received	0
Sent responses	0
Sent exceptions	0

### Serial Port

#0

Port number	0
Break	0
Frame error	0
Parity error	0
Overrun error	0
Mode	RTU
Slave ID	1
Valid requests received	0
Invalid requests received	0
CRC error requests received	0
Sent responses	0
Sent exceptions	0

## Diagnostics—Protocol Diagnostics-Modbus TCP Diagnostics

Home > Modbus TCP Server Diagnostics

### Modbus TCP Server Diagnostics

Auto Refresh

#### Modbus

Mode	Server
Number of connections	1
Valid requests received	4
Invalid requests received	0
Sent responses	0
Sent exceptions	4

#### Connections

Connection 1

Status	Exception_response
Remote IP: Port	10.123.5.100:32067
Valid requests received	4
Invalid requests received	0
Sent responses	0
Sent exceptions	4

## Diagnostics—Protocol Diagnostics-DNP3 Serial Outstation Diagnostics

Home > DNP3 Serial Outstation Diagnostics

### DNP3 Serial Outstation Diagnostics

Auto Refresh

COM 1

#### Overview

Connection Status	: Not Connected
Total Transmit Packets	: 0
Total Receive Packets	: 0
Last Transmit Packets Time	: N/A
Last Receive Packets Time	: N/A
Class 1 Pending Event	: 0
Class 2 Pending Event	: 0
Class 3 Pending Event	: 0
Internal Indications	: IIN1.7 Device Restart

#### Connected Client Info

No data

## Diagnostics—Protocol Diagnostics-DNP3 TCP/UCP Outstation Diagnostics

Home > DNP3 TCP/UDP Outstation Diagnostics

### DNP3 TCP/UDP Outstation Diagnostics

Auto Refresh

#### Overview

Connection Status	: Not Connected
Total Transmit Packets	: 0
Total Receive Packets	: 0
Last Transmit Packets Time	: N/A
Last Receive Packets Time	: N/A
Class 1 Pending Event	: 0
Class 2 Pending Event	: 0
Class 3 Pending Event	: 0
Internal Indications	: IIN1.7 Device Restart

#### Connected Client Info

No data

## Diagnostics—Protocol Diagnostics-IEC 60870-5-101 Server/Slave Diagnostics

Home > IEC 60870-5-101 Slave Diagnostics

### IEC 60870-5-101 Slave Diagnostics

COM 1

#### Overview

Total Transmit Non-spontaneous Responses	: 1
Total Transmit Spontaneous Responses	: 0
Total Receive Requests	: 0
Last Transmit Non-spontaneous Response Time	: 2024-03-04T09:03:16.570+00:00
Last Transmit Spontaneous Response Time	: N/A
Last Received Request Time	: N/A
Internal Indications	:



## Diagnostics—Protocol Traffic-Modbus TCP Server 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—Protocol Traffic-DNP3 Serial Outstation Traffic

DNP3 Serial Outstation Traffic Log  
Home > DNP3 Serial Outstation Traffic Log

COM1

**START** Ready to capture

Auto Scroll

No.	Time	Message Layer	Direction	Data
No data to display.				

## Diagnostics—Protocol Traffic-DNP3 TCP/UDP Outstation Traffic

DNP3 TCP/UDP Outstation Traffic Log  
Home > DNP3 TCP/UDP Outstation Traffic Log

**START** Ready to capture

Auto Scroll

No.	Time	Message Layer	Direction	Data
No data to display.				

## Diagnostics—Protocol Traffic-IEC 60870-5-101 Server Traffic

IEC 60870-5-101 Slave Traffic  
Home > IEC 60870-5-101 Slave Traffic

COM1

**START** Ready to capture

Auto Scroll

No.	Time	Message Layer	Direction	Data
No data to display.				

## Diagnostics—Protocol Traffic-IEC 60870-5-104 Server Traffic

IEC 60870-5-104 Server Traffic  
Home > IEC 60870-5-104 Server Traffic

**START** Ready to capture

Auto Scroll

No.	Time	Message Layer	Direction	Connected Client IP: Port	Data
No data to display.					

# Diagnostics—Event Log

## Diagnostics—Event Log-Log View

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

Home > Log View

### Log View

EXPORT CLEAR REFRESH

ID	Severity	Category	Event Name	Source	Message	Timestamp
1	Alert	Network	Ethernet link down	Host 10.123.5.110	Ethernet port 1 link down	2024-05-17T23:07:22.911+00:00
2	Information	System	System start	Host 10.123.5.110	System start	2024-05-17T23:07:22.815+00:00
3	Alert	Network	Ethernet link down	Host 10.123.5.110	Ethernet port 1 link down	2024-05-17T21:44:43.958+00:00
4	Warning	Maintenance	Configuration changed	admin 10.123.5.100	SNMP configuration changed	2024-05-17T17:58:02.465+00:00
5	Warning	Maintenance	Configuration changed	admin 10.123.5.100	SNMP configuration changed	2024-05-17T17:56:32.658+00:00
6	Warning	Maintenance	Configuration changed	admin 10.123.5.100	SNMP configuration changed	2024-05-17T17:53:19.061+00:00
7	Warning	Maintenance	Configuration changed	admin 10.123.5.100	SNMP configuration changed	2024-05-17T17:31:19.061+00:00
8	Warning	Maintenance	Configuration changed	admin 10.123.5.100	SNMP configuration changed	2024-05-17T17:17:33.077+00:00
9	Information	Security	Login success	admin 10.123.5.100	Account 'admin' login successfully	2024-05-17T17:07:11.840+00:00
10	Alert	Network	Ethernet link down	Host 10.123.5.110	Ethernet port 1 link down	2024-05-17T16:00:40.023+00:00

Items per page: 10 11 - 20 of 142 2 / 15

## 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.

Home > Policy Settings

### Policy Settings

#### Channels

Click the edit icon to edit the notification setting and click the SAVE button to apply changes.

Local Log  Configured

Remote Log  Configured

SNMP Trap  Configured

Email  Configured

DISCARD SAVE

#### Events

Select the events and customized notification channels

Severity Channels

- System
- Network
- Security
- Maintenance
- Modbus
- IEC 60870-5-104
- DNP3
- IEC 61850

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's name. After changing the settings, please remember to SAVE it.

Home > Policy Settings

## Policy Settings

### Channels

Click the edit icon to edit the notification setting and click the SAVE button to apply changes.

Local Log  
✔ Configured

Remote Log  
✔ Configured

SNMP Trap  
✔ Configured

Email  
✔ Configured

### Events

DISCARD SAVE

Select the events and customized notification channels

Severity ▾ Channels ▾

System

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

Event Group	Description
<b>System</b>	Start system, User trigger reboot, Power input failure, NTP update failure
<b>Network</b>	IP conflict, DHCP get IP/renew, IP changed, Ethernet link down
<b>Security</b>	Clear event log, Login success, Login failure, Account/group changed, Password reached lifetime, SSL certificate import, Syslog certificate import
<b>Maintenance</b>	Firmware upgrade success, Firmware upgrade failure, Configuration import success, Configuration import failure, Configuration export, Configuration changed, Load factory default
<b>Modbus</b>	Client connected, Client disconnected, Exception function
<b>IEC 60870-5-104</b>	Client connected, Client disconnected
<b>DNP3</b>	TCP Client connected, TCP Client disconnected
<b>IEC 61850</b>	Server connected, Server disconnected, Certificate imported, Certificate expired

## Local Log Settings

### Local Log Settings

Event Log Overwrite Policy

Overwrite the oldest Event Log

Stop Recording Event Log

Log Capacity Warning

Capacity Threshold (%)

80

Warning notice

SNMP Trap  Email

CANCEL SAVE

Local Log Settings	Description
<b>Event Log Overwrite Policy</b>	Overwrites the oldest event log Stops recording event log
<b>Capacity Threshold (%)</b>	When the log amount exceeds the warning
<b>Warning By</b>	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

Remote log settings

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

CANCEL SAVE

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

## SNMP Trap Settings

### SNMP Trap Server

Trap Service

Enable

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

CANCEL SAVE

## Email Settings

### Email Settings

SMTP Service  
Disable ▼

---

Primary Server

Mail Server (SMTP) Port  
0

Security Connection  
None ▼

Requires authentication

From (Email address)

To (Email addresses, separated by semicolon)

CANCEL SAVE

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

Home > Tag View

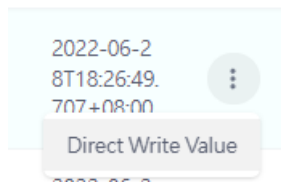
### Tag View

Search: Type to search... REFRESH

Provider	Source	Name	Type	Value	Timestamp
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCBRBF1\$ST5Str\$dirGeneral	int8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCBRBF1\$ST5Str\$General	boolean	false	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCBRBF1\$ST5Str\$OutCmd\$stVal	int8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$COSMod\$Oper\$ctlNum	uint8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$COSMod\$Oper\$ctlVal	int8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$ST5Beh\$stVal	int8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$ST5Blk\$stVal	boolean	false	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$ST5FailCirc\$General	boolean	false	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	STEMPLATELD0\$CCSPVC1\$ST5Mod\$stVal	int8	0x00	2024-05-19T15:22:26.244+00:00
iec61850_client	IED_FieldSite2	status	int32	valid (0x00000000)	2024-05-19T15:17:20.128+00:00

Items per page: 10 1 - 10 of 12

You can write a value to the IEC 61850 server via Direct Write Value function to test the communication with IEC 61850 server device.



## Diagnostics—Network Connections

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

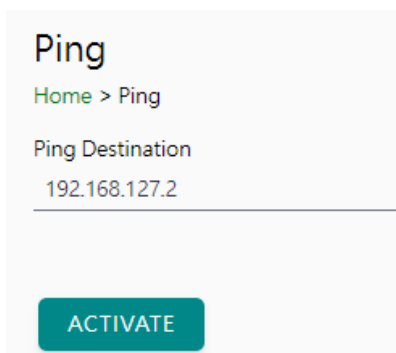
Home > Network Connections

Auto refresh

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

## Diagnostics—Ping

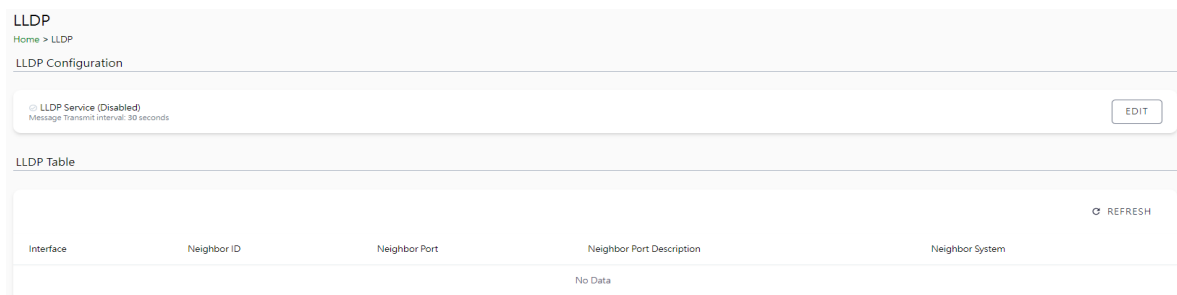
This network testing function is available only on the web console. The MGate gateway will send an ICMP packet through the network to a specified host, and the result can be viewed on the web console immediately.



The screenshot shows the 'Ping' configuration page. At the top, it says 'Ping' in a large font, followed by a breadcrumb 'Home > Ping'. Below that, the 'Ping Destination' is set to '192.168.127.2'. At the bottom of the page, there is a prominent teal 'ACTIVATE' button.

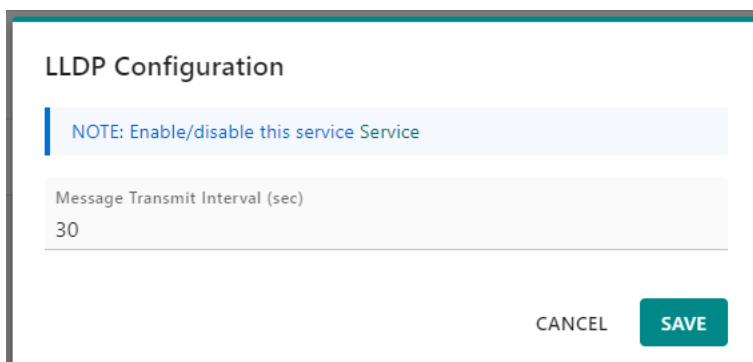
## Diagnostics—LLDP

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. It includes a breadcrumb 'Home > LLDP' and the title 'LLDP Configuration'. The main content area shows 'LLDP Service (Disabled)' with a subtext 'Message Transmit Interval: 30 seconds' and an 'EDIT' button. Below this is an 'LLDP Table' with a 'REFRESH' button. The table has columns for 'Interface', 'Neighbor ID', 'Neighbor Port', 'Neighbor Port Description', and 'Neighbor System', but it currently displays '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.

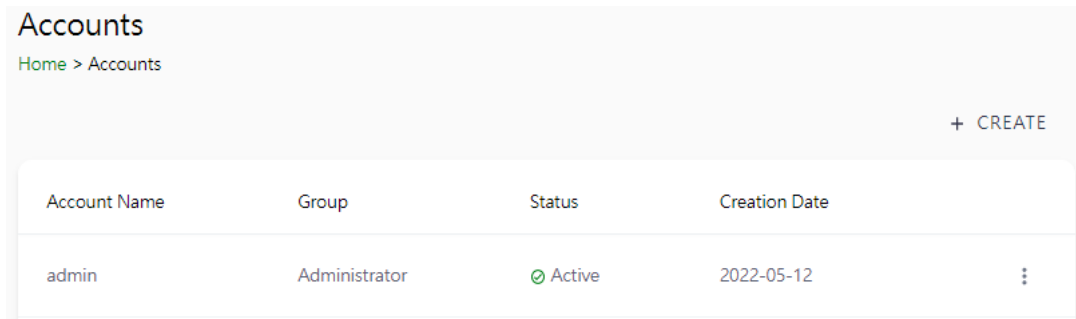


The screenshot shows a modal dialog box titled 'LLDP Configuration'. It features a blue note: 'NOTE: Enable/disable this service Service'. Below the note is a text input field for 'Message Transmit Interval (sec)' with the value '30'. At the bottom right, there are two buttons: 'CANCEL' and 'SAVE'.

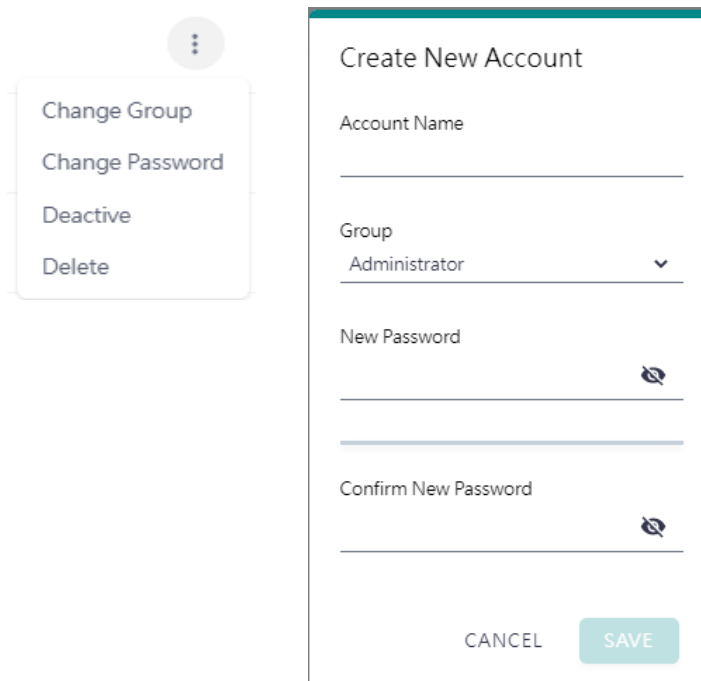
# Security

## Security—Account Management

### Security—Account Management—Accounts



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.



Parameters	Value	Description
<b>Group</b>	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		
<b>Administrator (built-in)</b> 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	⋮
<b>Operator (built-in)</b> 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	⋮
<b>Guest (built-in)</b> 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 title "Create New Group" and a section "Basic Information" with a "Name" field. Below that is a "Description - optional" field. The "Access Permissions" section includes several dropdown menus for different categories:

- System Configuration: Read write
- Protocol Setting: Read write
- Diagnostic: Read write
- Security: No display
- Maintenance: Read write
- Restart: Read write

At the bottom of the form are "CANCEL" and "SAVE" buttons.

Parameters	Value	Description
<b>Basic Information</b>		The name and description (optional) for the new group. The maximum characters for Name are 32, maximum characters for Description is 300 characters.
<b>Access Permissions</b>	No display Read only Read write	Corresponding to the configuration menu on the left-hand side of the web console, including System Configuration, Protocol Settings, Diagnostic, Security, Maintenance, Restart, you can configure different permissions for different groups. When setting "No displays" on a group, the users in that group will not see the page on the left-hand-side menu.

## Security—Account Management—Password Policy

### Password Policy

[Home](#) > Password Policy

#### Password Strength Setting

Password Minimum Length  
8

Password Complexity Strength Check

Select all password strength requirements

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

#### 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
<b>Password Minimum Length</b>	8 to 128	The minimum password length
<b>Password Complexity Strength Check</b>		Select how the MGate checks the password's strength
<b>Password Lifetime Setting</b>	90 to 180 days	Set the password's lifetime period.

# Security—Service



Parameter	Value	Description
<b>HTTP Service</b>	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.
<b>HTTPS Service</b>	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.
<b>Ping Service</b>	Enable/Disable	Disabling this service will block ping requests from other devices.
<b>SD Card</b>	Enable/Disable	Disabling this service will deactivate the SD card function for backup and restore configuration files.
<b>Utility Search Service</b>	Enable/Disable	Disabling this service will block the MGate from being searched by Moxa utilities such as DSU (Device Search Utility) and MXconfig series.
<b>SNMP Agent Service</b>	Enable/Disable	Enable or disable SNMP agent function.
<b>LLDP Service</b>	Enable/Disable	Enable or disable LLDP function.
<b>Reset button disable after 60 sec</b>	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. To set up the allowlist, first you need to enable at least one IP address. Click on the pen icon on the right-hand side and input an IP address and the netmask. Note that it is important to input the KIP of your computer/laptop in case you will be blocked by the Allowlist. After editing the allowlist, click the APPLY button for the settings to take effect. The "Enable the allowlist" switch is the main switch for this function. Switch off and all the allowlist will be disabled.

Home > Allowlist

### Allowlist

NOTICE: Communications are only allowed for the IPs on the list after enabling this allowlist.

Enable the allowlist

DISCARD APPLY

No.	IP Address	Netmask	Status
1	192.168.127.87	255.0.0.0	Enabled
2	192.168.127.22	255.255.255.0	Enabled
3	-	-	Disabled

## 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.

Home > DoS Defense

### DoS Defense

#### Configuration

- Null Scan
- NMAP-Xmas Scan
- SYN/FIN Scan
- FIN Scan
- NMAP-ID Scan

#### SYN Flood

Enable

Limit: 4000 pkts/s

#### ICMP-Death

Enable

Limit: 4000 pkts/s

SAVE

# 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 configuration options: an unchecked checkbox for 'Enable Login Failure Lockout', a 'Max Failure Retry Times' input field with the value '5', another 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)' input field with the value '10', and a 'Lockout Time (min)' input field with the value '10'. A 'SAVE' button is located at the bottom left.

Parameter	Value	Description
<b>Max Failure Retry Times</b>	1 to 10 (default 5)	You can specify the maximum number of failure retries. If you exceed the retry times, the MGate will lock out for that account login
<b>Reset Period (min)</b>	1 to 1440 (default 10)	You can specify the reset period time when enabling the "reset the login failure counter" function
<b>Lockout Time (min)</b>	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
<b>Maximum login users for HTTP+HTTPS</b>	1 to 10 (default 5)	The number of users that can access the MGate at the same time.
<b>Auto logout setting (min)</b>	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 reasons, you can export configuration files 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.

Home > Config. Import/Export

### Config. Import/Export

Configuration | File Authentication

Export configuration

Import configuration  Update network settings

No file chosen

### Configuration Import/Export

Home > Configuration Import/Export

Configuration | File Authentication

File authentication

Enable  Disabled

File authentication key

## Maintenance—Firmware Upgrade

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



### ATTENTION

DO NOT turn off the MGate power before 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 cannot boot. If this happens, contact Moxa RMA services.

The screenshot shows a web console page titled "Firmware Upgrade". At the top, there is a breadcrumb "Home > Firmware Upgrade". Below the title, a warning message states: "Upgrading firmware may cause device to reset to factory default. Back up the configuration of device." There is a file selection area with a "Choose File" button and the text "No file chosen". Below this is a teal "UPLOAD" 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 a web console page titled "Load Factory Default". At the top, there is a breadcrumb "Home > Load Factory Default". Below the title, a warning message states: "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. Below this is a blue information box that says: "Info: To leave the IP address, netmask, and gateway settings unchanged, make sure that Keep IP settings is enabled." At the bottom 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.

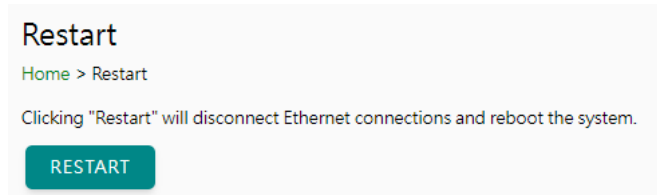
# Restart

You can reboot the MGate by clicking the RESTART button.



## ATTENTION

Unsaved configuration files will be discarded during a reboot.

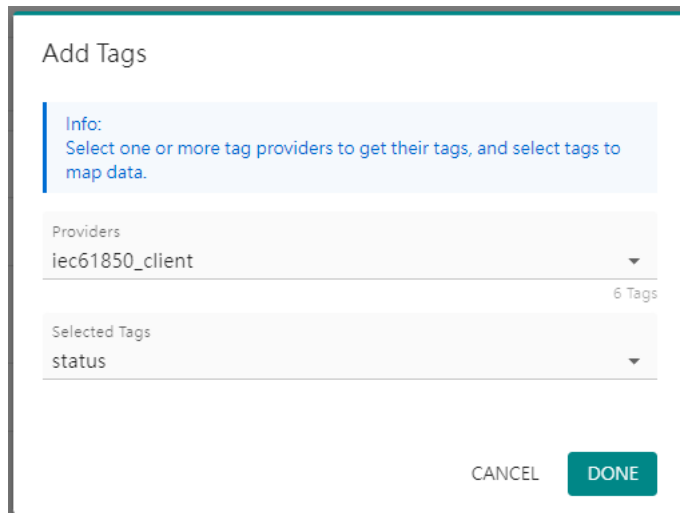


# Status Monitoring

The Status Monitoring function provides status information of IEC 61850 server/IED devices when the MGate is being used as an IEC61850 client. If an IEC 61850 server device fails or a cable comes loose, the gateway won't be able to receive up-to-date data from the IEC 61850 server device. The out-of-date connection fails data will be stored in the gateway's memory and will be retrieved by the client (e.g., SCADA), 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 an IEC 61850 server device is created. This tag is used to show the connection status (valid or invalid) of the IEC 61850 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 the MGate's web, the Tag View page.

To perform the status tag monitoring from your northbound protocol, go to the northbound protocol's page (for example, the Modbus TCP Server page), click **ADD TAGS**, select IEC 61850 client as the tag provider, and select the "status" tag. The MGate will automatically add a mapping from this IEC 61850 tag to the other protocol.



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

Home > Tag View

### Tag View

Search: status REFRESH

Provider	Source	Name	Type	Value	Timestamp	
iec61850_client	IED_FieldSite2	status	int32	valid (0x00000000)	2024-05-19T15:17:20.128+00:00	⋮
iec61850_client	IED_Taiwan	status	int32	valid (0x00000000)	2024-05-19T15:17:20.126+00:00	⋮

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

Home > Tag View

### Tag View

Search: status REFRESH

Provider	Source	Name	Type	Value	Timestamp	
iec61850_client	IED_FieldSite2	status	int32	invalid (0x80000000)	2024-05-19T16:31:14.356+00:00	⋮
iec61850_client	IED_Taiwan	status	int32	invalid (0x80000000)	2024-05-19T16:31:14.352+00:00	⋮

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

## 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.

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		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