

NPort IA5000-G2 Series User Manual

Version 1.0, September 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

NPort IA5000-G2 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

© 2025 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	6
Overview	6
Package Checklist	7
NPort IA5000-G2 Models	7
2. Getting Started	8
Panel Layout	8
NPort IA5100-G2 Models	8
NPort IA5200-G2 Models	9
NPort IA5400-G2 Models	9
Connecting the Hardware.....	10
Wiring Requirements	10
Powering the NPort IA5000-G2	10
LED Indicators	11
Pin Assignments of the Serial Ports	12
Mounting Options	12
Connecting to the Network	13
3. First-time Setup.....	14
Find the Device	14
Search Device.....	15
First-time login with Device Search Utility.....	15
Unlock	17
Assign IP.....	17
COM Mapping	19
Console.....	19
Locate.....	19
First Time Login Process	20
4. Mapping COM Ports.....	23
Mapping COM Ports on Windows Platforms	23
Mapping COM Ports With Real COM Mode	23
Mapping COM Ports on Linux Platforms.....	25
Mapping TTY Ports.....	26
Removing Mapped TTY Ports.....	26
Removing Linux Driver Files.....	26
Mapping COM Ports on macOS Platforms	27
Installing macOS TTY Driver Files	27
Mapping macOS TTY Port	30
Uninstalling the macOS Driver	32
Mapping COM Ports on UNIX-Like Platforms	33
Installing the UNIX Fixed TTY Driver	33
Configuring the UNIX Driver	34
5. Cybersecurity Considerations	35
Updating Firmware.....	35
Turn Off Unused Service and Ports.....	35
Turn On Services That Are Necessary.....	36
Limited IP Access.....	37
Account and Password.....	37
System Log.....	37
Deployment of the Device.....	38
Testing the Security Environment	38
6. Management Consoles	40
Configuration Options.....	40
Device Search Utility.....	40
Web Console.....	40
Serial Console.....	40
7. Configuration with the Web Console.....	42
Factory Default IP Address.....	42
Using Your Web Browser.....	42
Opening the Web Console.....	42

Web Console Navigation	44
Dashboard Introduction	45
System Settings	45
General	46
Notification	48
SNMP Agent	52
Network Settings	54
IP Address	55
Port Speed	57
Routing Table	57
Serial Port Settings	58
Operation Modes	58
Serial Parameters	93
Secure Connection	97
Security	99
Services	99
Allowlist	101
Certificate	101
DoS Defense	102
Login Settings	103
Account Management	104
Accounts	104
Groups	106
Password Policy	108
Maintenance	109
Config. Import/Export	109
Firmware Upgrade	110
Reset to Default	111
Restart	112
Diagnostics	112
Support	112
System Log	114
Active Relay Events	117
Operation Mode Statistics	117
Network Monitor	120
Ping	122
Traffic Monitor	122
8. Mass Deployment/Maintenance	124
Mass Configuration With GUI Tool: Device Search Utility v3.0 or Newer	124
Import/Export Configuration	125
Import Certificate	126
Firmware Upgrade	126
Mass Configuration with CLI tool: MCC Tool	127
Import/Export Configuration	127
Firmware Upgrade	128
Change Password	129
9. Advanced Settings of NPort Windows Driver Manager	130
Configure the mapped COM ports	130
Change the number of a mapped COM port	130
COM Splitting	131
Advanced Setting	133
Security	135
Importing/Exporting COM mapping	136
Port Sniffer Wizard	137
10. Frequently Asked Questions	145
Q1. If I disable the Web console, how can I change the settings?	145
Q2. Can different users use the same account to log in to the device server?	145
Q3. Why Device Search Utility v3.0 and later cannot be executed on my Windows 7 or Windows 2008 R2?... ..	145
Q4. How can I check the CRC value of the runtime settings?	146

Q5. Is there an easier way to copy the settings of a NPort IA-5000/IA5000A device server to a NPort IA5000-G2?.....	146
Q6. If there is a power outage during a firmware upgrade, how can I recover the device?	146
Q7. Before calling Moxa customer service, is there anything I can prepare to save both of us time?.....	146
Q8. How to set up a Secure Connection of Real COM mode?.....	147
A. Pinouts and Cable Wiring.....	148
Cable Wiring Diagrams	149
Ethernet Cables.....	149
Serial Cables.....	150
B. Accessory Introduction.....	151
Convert the DB9 Connector to Other Connectors	151
Selecting Suitable Power Adapter Depends on the Environment.....	152
C. Well-known Port Numbers.....	154
D. SNMP MIB List	156
RFC1213 MIB-II Supported SNMP Variables	156
RFC1317 RS-232 Like Groups.....	157
Moxa-NPIA5000-G2-MIB.....	158
E. Event List.....	163
F. Command List of the Serial Console.....	166
G. How to Become a Registered User	168

1. Introduction

By leveraging the IEC 62443-4-1 secure development life-cycle process, Moxa has created a new line of secure terminal servers. The NPort 6000-G2 Series secure terminal servers follow the IEC 62443-4-2 design and guidelines to connect your legacy serial devices to industrial networks securely. Furthermore, Moxa's 35 years of experience in serial-connectivity contributes to an enhanced user experience with flexible installation options and a convenient troubleshooting tool for maintenance.

The NPort IA5000-G2 Series of secure serial device servers has many exceptional features. The NPort IA5000-G2 Series includes a lineup of over 20 models. What distinguishes the models apart are the number of ports and the type of network connection they employ. The NPort IA5000-G2 Series shares the same instructions and information across all its models. We will specify any variations between models. To learn more about the variations between models in the series, please refer to the Product Selection Chart section in this chapter.

Overview

The NPort IA5000-G2 device servers are an ideal choice for establishing network access to RS-232/422/485 serial devices, including PLCs, sensors, meters, motors, drives, barcode readers, and operator displays. All models are housed in a compact, rugged, DIN-rail mountable housing, and come with redundant power inputs, cascading Ethernet ports, and industrial-grade certifications, DNV and Hazardous certificates like C1D2, ATEX and IECEx.

The NPort IA5000-G2 enables connection of serial devices to Ethernet networks and supports multiple operation modes. In particular, the NPort IA5000-G2 has support for Secure Real COM, Secure TCP Server, Secure TCP Client, and Secure Pair Connection modes. This makes it ideal for security-critical applications. With these secure operation modes, you'll have access to supported protocols, authentication control, advanced data encryption, and more.

The NPort IA5000-G2's Any Baudrate feature, which is based on Moxa's UART IC, allows the use of nonstandard baudrates. For example, some special applications may require a baudrate of 500 kbps. Most device servers can only support a baudrate of 460.8 kbps, leading to an error rate of 7.84%. The margin of error allowed for serial communication is just 3%. With the NPort IA5000-G2, you can configure the baudrate more precisely and transmit serial data at a rate of 491.5 kbps. This is only a 1.7% margin of error, which is well within the acceptable margin for serial data.

Package Checklist

Each NPort IA5000-G2 serial device server is packaged individually with various standard accessories. When you receive your shipment, please check the contents of the box carefully and notify your Moxa sales representative if any of the items are missing or appear to be damaged.

NPort IA5000-G2 Models

The supported models of NPort IA5000-G2 Series:

Model Name	No. of Ethernet ports	No. of serial ports	Serial Standards	Serial Isolation	Operating Temp.
NPort IA5150-G2	2 x RJ45	1	RS-232/422/485	–	-10 to 60°C
NPort IA5150-G2-T	2 x RJ45	1	RS-232/422/485	–	-40 to 75°C
NPort IA5150I-G2	2 x RJ45	1	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5150I-G2-T	2 x RJ45	1	RS-232/422/485	2 kV	-40 to 75°C
NPort IA5150-M-SC-G2	1 x Multi-SC, 1 x RJ45	1	RS-232/422/485	–	-10 to 60°C
NPort IA5150-M-SC-G2-T	1 x Multi-SC, 1 x RJ45	1	RS-232/422/485	–	-40 to 75°C
NPort IA5150-S-SC-G2	1 x Single-SC, 1 x RJ45	1	RS-232/422/485	–	-10 to 60°C
NPort IA5150-S-SC-G2-T	1 x Single-SC, 1 x RJ45	1	RS-232/422/485	–	-40 to 75°C
NPort IA5150-SFP-G2	1 x SFP, 1 x RJ45	1	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5150-SFP-G2-T	1 x SFP, 1 x RJ45	1	RS-232/422/485	2 kV	-40 to 75°C
NPort IA5250-G2	2 x RJ45	2	RS-232/422/485	–	-10 to 60°C
NPort IA5250-G2-T	2 x RJ45	2	RS-232/422/485	–	-40 to 75°C
NPort IA5250I-G2	2 x RJ45	2	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5250I-G2-T	2 x RJ45	2	RS-232/422/485	2 kV	-40 to 75°C
NPort IA5250-TB-G2	2 x RJ45	2 x 5-pin TB	RS-232/422/485	–	-10 to 60°C
NPort IA5250-TB-G2-T	2 x RJ45	2 x 5-pin TB	RS-232/422/485	–	-40 to 75°C
NPort IA5250I-TB-G2	2 x RJ45	2 x 5-pin TB	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5250I-TB-G2-T	2 x RJ45	2 x 5-pin TB	RS-232/422/485	2 kV	-40 to 75°C
NPort IA5450-G2	2 x RJ45	4	RS-232/422/485	–	-10 to 60°C
NPort IA5450-G2-T	2 x RJ45	4	RS-232/422/485	–	-40 to 75°C
NPort IA5450I-G2	2 x RJ45	4	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5450I-G2-T	2 x RJ45	4	RS-232/422/485	2 kV	-40 to 75°C
NPort IA5450-TB-G2	2 x RJ45	4 x 5-pin TB	RS-232/422/485	–	-10 to 60°C
NPort IA5450-TB-G2-T	2 x RJ45	4 x 5-pin TB	RS-232/422/485	–	-40 to 75°C
NPort IA5450I-TB-G2	2 x RJ45	4 x 5-pin TB	RS-232/422/485	2 kV	-10 to 60°C
NPort IA5450I-TB-G2-T	2 x RJ45	4 x 5-pin TB	RS-232/422/485	2 kV	-40 to 75°C

Standard Accessories for the NPort IA5000-G2 Models

- NPort IA5000-G2 with DIN-rail mounting kit
- Quick installation guide (printed)

For optional accessories, like power adapters for a wide-temperature environment or connecting cables, refer to the Accessories section in the datasheet or the user manual.

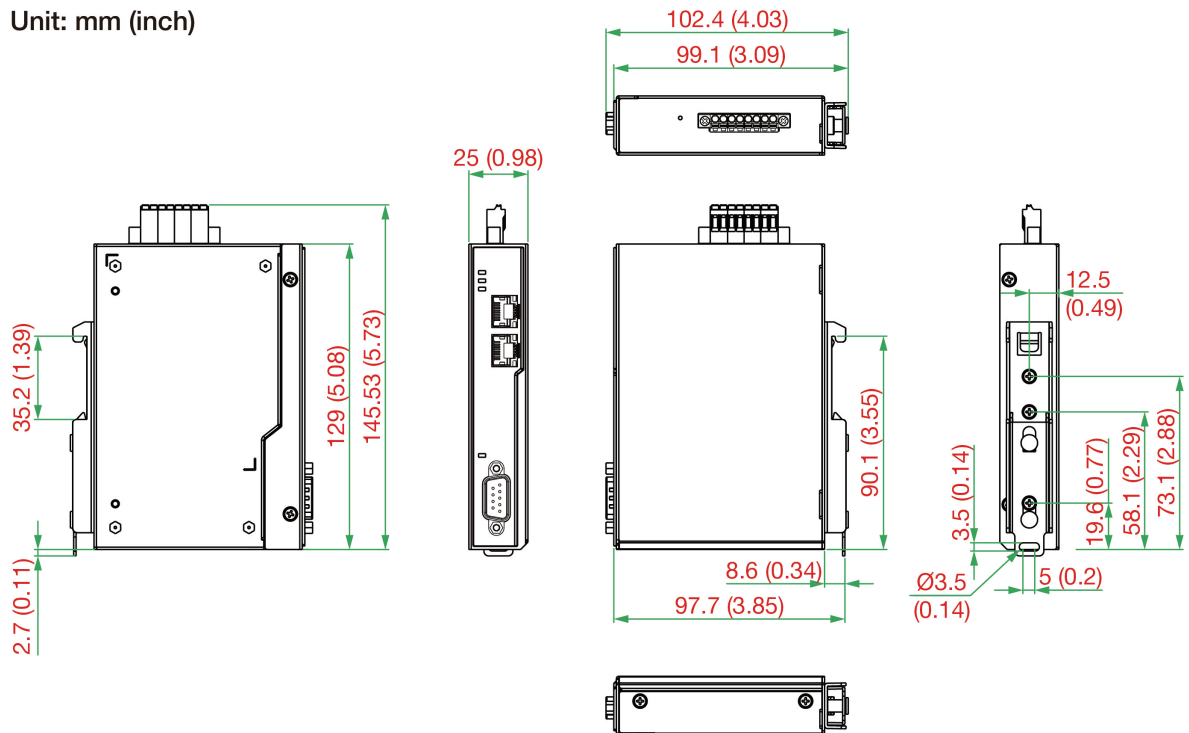
2. Getting Started

This chapter covers the hardware installation of the NPort IA5000-G2. The software installation is covered in the following chapters.

Panel Layout

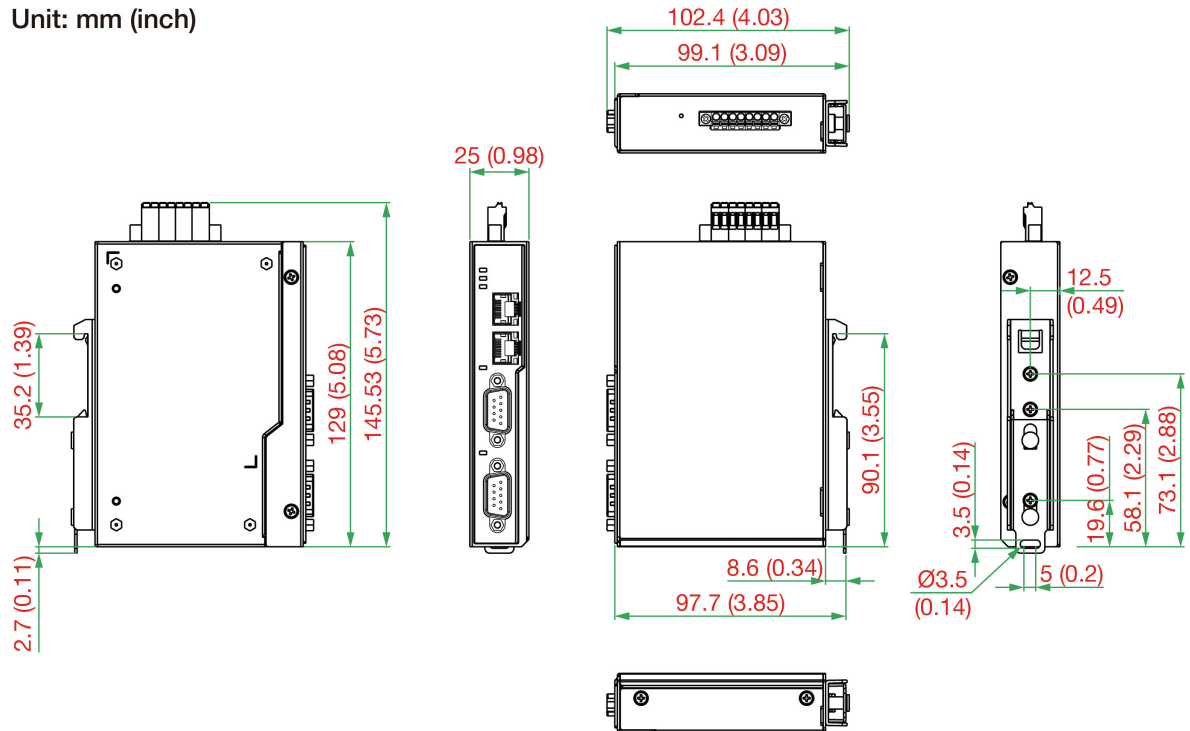
NPort IA5100-G2 Models

Unit: mm (inch)



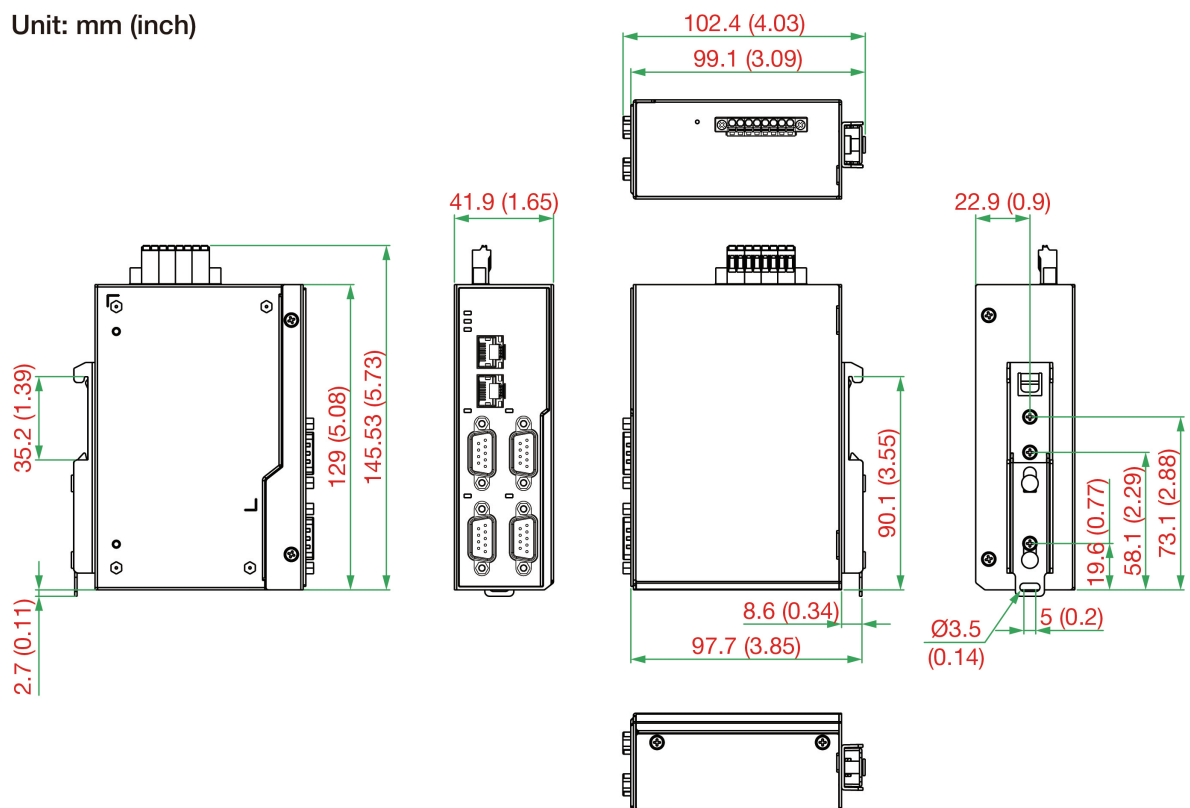
NPort IA5200-G2 Models

Unit: mm (inch)



NPort IA5400-G2 Models

Unit: mm (inch)



Connecting the Hardware

This section describes how to connect the power supply to the NPort IA5000-G2.



ATTENTION

Disconnect the power before installing and wiring

Disconnect the power cord before installing and/or wiring your NPort IA5000-G2.

Do not exceed the maximum current for the wiring

Determine the maximum possible current for each power wire and common wire. Adhere to electrical codes that dictate the maximum current allowed for each wire size.

If the current exceeds the maximum rating, the wiring could overheat, causing serious damage to your equipment.

Server may get hot; use caution when handling

Exercise caution when handling the NPort IA5000-G2 after it has been plugged in. The internal components generate heat, and the casing may get too hot to touch.

Wiring Requirements

You should also heed the following guidelines:

- Use separate paths to route wiring for power and devices. If power-wiring and device-wiring paths must cross, make sure the wires are perpendicular at the intersection point.



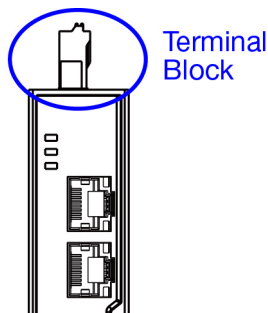
NOTE

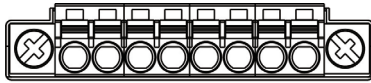
Do not run signal or communication wiring and power wiring in the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.





- The type of signal transmitted through a wire should determine which wires should be kept separate. The rule of thumb is that wires sharing similar electrical characteristics may be bundled together.
- Keep input wiring and output wiring separately.
- It is good practice to label the wiring to all devices in the system.

Powering the NPort IA5000-G2

Unbox the device server and power it up by connecting the proper pin assignment of the terminal block on the top of it. The location and the pin assignment of the terminal block on the device server is indicated in the following figures:



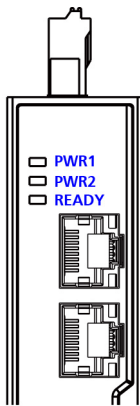


	V2+	V2-				V1+	V1-
Chassis GND	DC Power 2	DC Power 2	N.O.	Common	N.C.	DC Power 1	DC Power 1

When wiring the relay contact (R) and power inputs (P1/P2), we suggest using American Wire Gauge (AWG) 16 to 20 as a cable and the corresponding pin-type cable terminals. The stripping length is recommended to be 8 to 9 mm. The wire temperature rating should be at least 85°C. Use copper conductors only. The shielding ground screw (M4) is near the power connector. When you connect the shielded ground wire (min. 16 AWG), the noise is routed from the metal chassis to the ground.

When you are using a DIN-rail power supply, ensure that the ground pin is properly connected. The ground pin must be connected with the chassis ground of the rack or the system.

After powering up the device, the Ready LED should turn solid Red first. After a couple of seconds, the Ready LED should turn solid Green, and you should hear a beep, which indicates that the device is ready. For detailed behavior of the LED indicators, see the *LED Indicators* section.



LED Indicators

The LED indicators on the front panel of the NPort IA5000-G2 are described in the following table.

LED Name	LED Color	LED Function	
PWR1 PWR2	Green	Steady	Power is on.
		Off	Power is off.
Ready	Red	Steady	Power is on and the NPort is booting up.
		Blinking	Indicates an IP conflict or the DHCP server did not respond properly, or a relay output occurred.
	Green	Steady	Power is on and the NPort is functioning normally.
		Blinking	The device server has been located by the Administrator's location function.
	Red + Green	When pushing the reset button, red and green LEDs blink (looks like amber), indicating the reset to default function will be enabled after 5 seconds.	
		When pushing the reset button for over 5 seconds, the red and green LEDs will turn steady, indicating you can release the button, and the device will start with default settings.	
P1, P2	Off	Power is off, or a power error condition exists.	
	Yellow	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	No data is being transmitted or received through the serial port.	

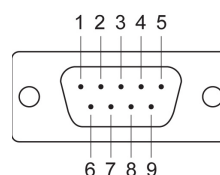
When the device is ready, connect an Ethernet cable to the NPort 6100-G2/6200-G2 directly with computer's Ethernet port or an Ethernet port of a switch.

To connect the serial device to the serial port of the NPort 6100-G2/6200-G2, follow the pin assignment below.

Pin Assignments of the Serial Ports

RS-232/422/485 pin assignment (male DB9):

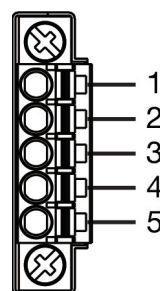
Pin	RS-232	RS-422 4-wire RS-485	2-wire RS-485
1	DCD	TxD-(A)	–
2	RxD	TxD+(B)	–
3	TxD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	–	–	–



The serial cables needed to connect the NPort IA5000-G2 to a serial device can be purchased separately. Please refer to [Appendix A](#).

The 5-pin terminal block pin assignments are as following.

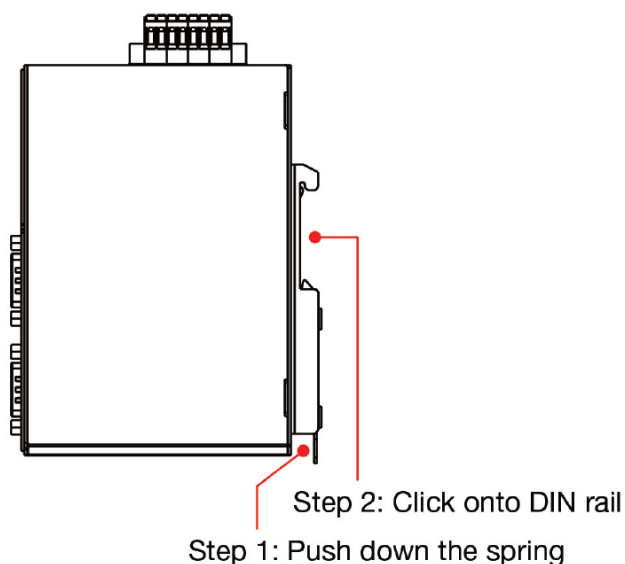
Pin	RS-232	RS-422 4-wire RS-485	2-wire RS-485
1	GND	GND	GND
2	–	RxD-(A)	Data-(A)
3	TxD	RxD+(B)	Data+(B)
4	–	TxD-(A)	–
5	RxD	TxD+(B)	–



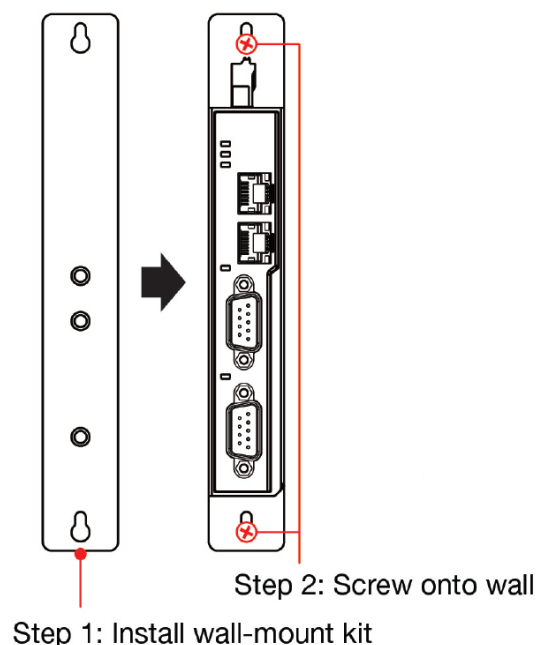
Mounting Options

The NPort IA5000-G2 device servers include a DIN-rail mounting kit in the box, which can be used to mount the NPort to a DIN-rail or the inside of a cabinet. You can order a Wall-mount kit separately for different placement options, as illustrated in the following diagrams:

DIN-rail Mounting (with DK-89-01)



Wall Mounting (with WK-178-01)

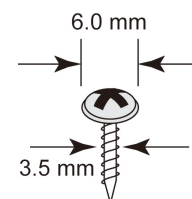


The mounting kit packages include screws. However, if you prefer to buy your own, refer to the dimensions below:

- Wall-mounting kit screws: FMS M3 x 5 mm
- DIN-rail mounting kit screws: FTS M3 x 5 mm

For attaching the device server to a wall or the inside of a cabinet, we recommend using a M3 screw with the following specifications:

- The head of the screw should be between 4 to 6.5 mm in diameter.
- The shaft should be 3.5 mm in diameter.
- The length should be longer than 5 mm.



Connecting to the Network

Connect one end of the Ethernet cable to the NPort IA5000-G2's 10/100M Ethernet port and the other end of the cable to the Ethernet network.

If the cable is properly connected, the NPort IA5000-G2 will show a valid connection to the Ethernet:

- The Ethernet LED glows solid green when connected to a 100 Mbps Ethernet network.
- The Ethernet LED glows solid orange when connected to a 10 Mbps Ethernet network.
- The Ethernet LED flashes when Ethernet packets are being transmitted or received.

LED Name	LED Color	LED Function
High speed of the RJ45 connector	Green	Steady on: The 100 Mbps Ethernet is connected Blinking: The Ethernet packets are being transmitted or received
	Off	The 100 Mbps Ethernet is disconnected
Low speed of the RJ45 connector	Yellow	Steady on: The 10 Mbps Ethernet is connected Blinking: The Ethernet packets are being transmitted or received
	Off	The 10 Mbps Ethernet is disconnected

3. First-time Setup

The NPort IA5000-G2 device server allows IP access to traditional serial devices (RS-232/422/485). The device server is a small computer with a CPU and TCP/IP protocols that can convert data between serial and Ethernet formats in both directions. With your computer, you can remotely control, manage, and configure facilities and equipment from any location in the world using the Internet.

Traditional SCADA and data collection systems rely on serial ports to collect data from various kinds of instruments. With the NPort IA5000-G2, your SCADA and data collection system can access all instruments on a standard TCP/IP network, whether they are used locally or remotely, thanks to its compatibility with RS-232, RS-422, and RS-485 communication ports.

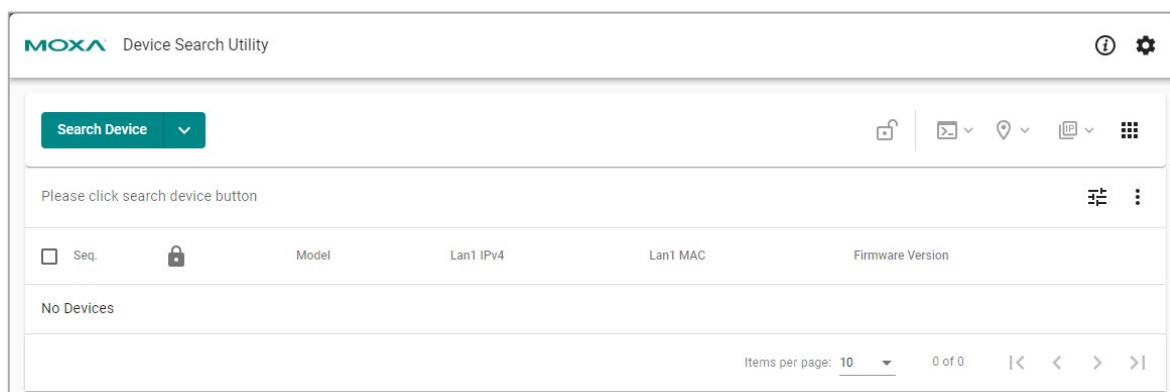
The NPort IA5000-G2 is an external network device that adds more serial ports to a host computer as needed. If your host computer is TCP/IP protocol compatible, you won't be restricted by bus limitations or lack of drivers for a variety of operating systems.

To combat the rising number and complexity of cyberattacks, network device vendors are including protective functions to secure sensitive business and personal information. Thanks to our dedicated efforts, all Moxa products meet the security standard, allowing customers to use them worry-free.

To accomplish this, the services will be disabled until you set up the first username and password for the unit. The unit can only be configured and made functional using a web console (HTTPS) or Moxa service.

Find the Device

The default IP address of each NPort IA5000-G2 Series is <https://192.168.127.254>. Directly input the IP address at the address bar of a browser to open the web console to set up the first username and password. Or download the **Device Search Utility (DSU) v3.0** and search for the device to access its web console.



DSU is a handy tool for easily finding NPort device servers and deploying single or multiple devices. DSU v3.0 functions as a web-based application that works on Chrome, Firefox and (Microsoft) Edge.

To use the web-based application DSU v3.0, your browser version and operating system must meet certain minimum requirements:

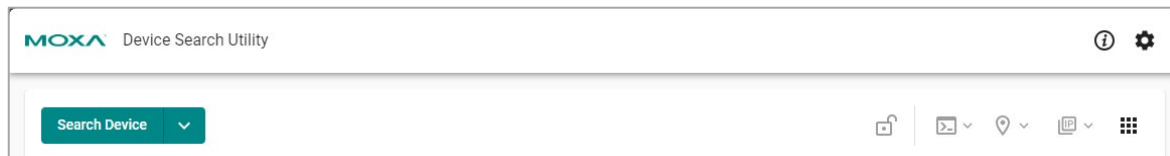
- Chrome:
 - For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
 - For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions
- Edge:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions



NOTE

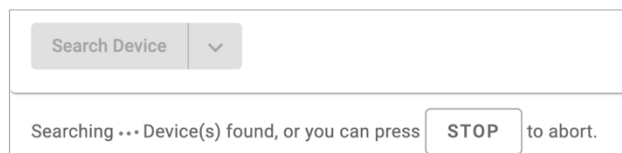
For detailed instruction of how to use **DSU**, please download the user manual from moxa.com.

Search Device



When connecting the NPort device server to the network, the DSU's **Search Device** function for him to find the target NPort device server. Searching can be done in three different ways. To see the options, click on the pull-down menu:

Search	Default button action. It will search the devices by multicasting.
Search by IP	Search the device by a specific IP
Search by IP range	Search the device in a certain IP range; the search results will only display the corresponding IP type. For example, if you search by IPv4, only IPv4 values will be displayed.

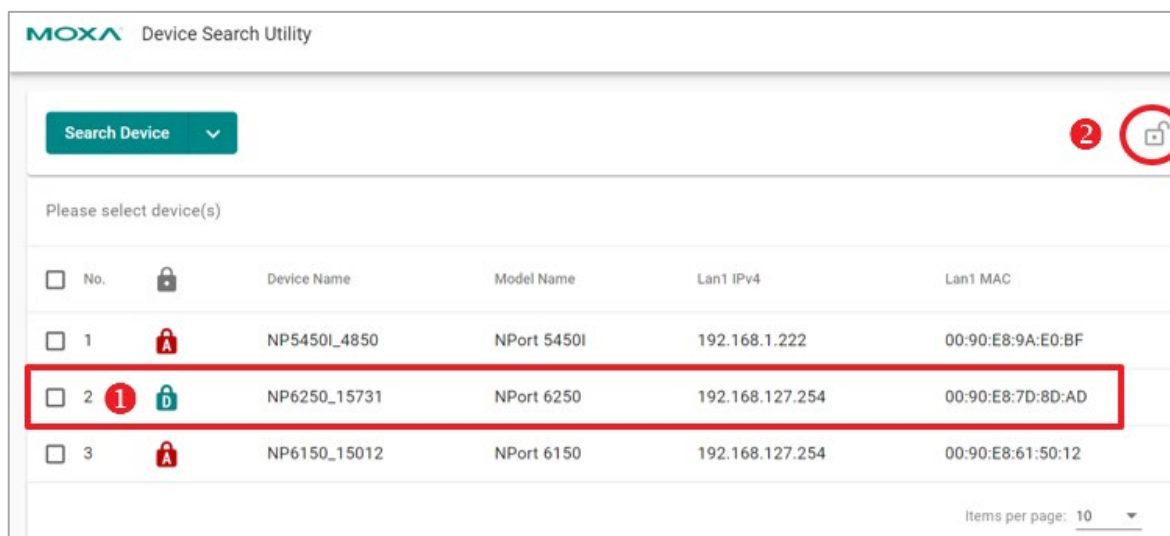




It's possible to stop the search at any stage of the process. A **STOP** button appears on top of the table; click it to halt the search and keep the already searched devices on the list.

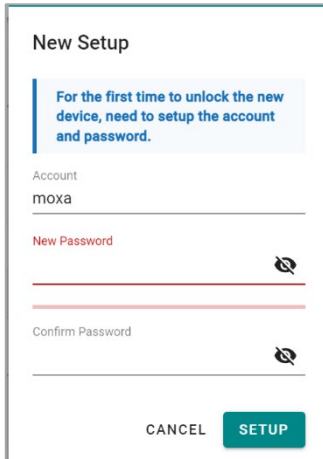
The default search time is 10 seconds. DSU will continue searching until time runs out. If your device(s) does not appear, you may change the search timeout limit in **Preferences > Device Search > Timeout limit for device searching**, to give the network a bit more time to respond.

First-time login with Device Search Utility

To address cybersecurity concerns, the NPort device server found through DSU will prompt for an account name and password during the first login.



Please select the target device  and click the unlock button . The login window will remind you to set up the account name and password, and it will show the password minimum requirements as tips below the password field.



New Setup

For the first time to unlock the new device, need to setup the account and password.





Account
moxa

New Password

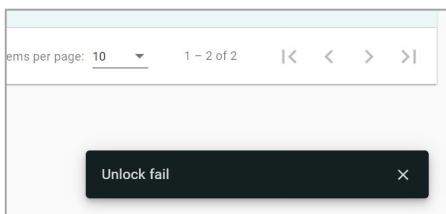
Confirm Password

CANCEL SETUP

Once you configure the first account and password successfully, the device may restart. After completing a new search, the lock icon will change to **Advance** type:

Please select device(s)						
<input type="checkbox"/>	No.		Device Name	Model Name	Lan1 IPv4	Lan1 MAC
<input type="checkbox"/>	1		NP5450L_4850	NPort 5450L	192.168.1.222	00:90:E8:9A:E0:BF
<input type="checkbox"/>	2		NP6150_15012	NPort 6150	192.168.127.254	00:90:E8:61:50:12
<input type="checkbox"/>	3		NP6250_15731	NPort 6250	192.168.127.254	00:90:E8:7D:8D:AD

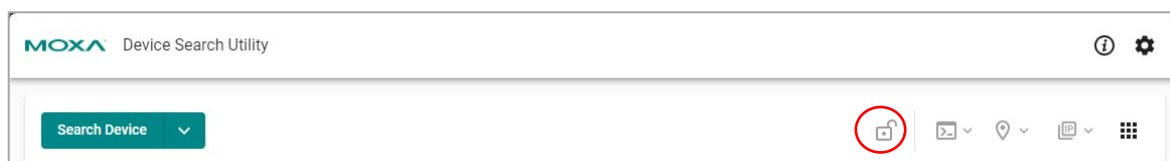
If there is an error during the unlocking process, like entering the wrong password, you will be notified with an error message at the bottom right of the screen.







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

Unlock fail

Unlock



When selecting one or multiple NPort device servers, use can click the **Unlock** button to unlock them. Because of different product series, there are four types of the login permission types:

	Login Permission Type	Definition
	Default	The device has not completed the first-time login process, which requires setting the first account name and password.
	Basic	The device only has password protection; the login requires to input the password only.
	Advance	The device has username and password protection; the login requires inputting both account name and password.
	Legacy/Unlocked	The device is unlocked, or not requiring any protection to log in.

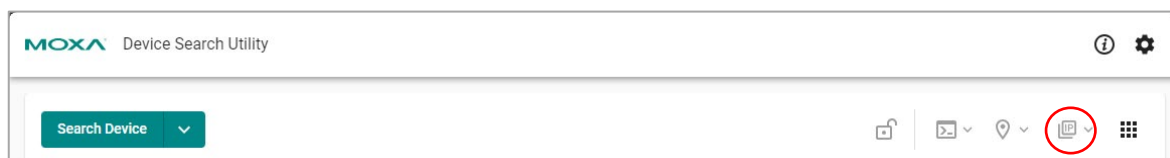
To unlock multiple devices at once, they must be of the same model name.



NOTE

The DSU solely facilitates unlocking the device; for account name or password changes, you must access the web console and find the Account Management function.

Assign IP



The device(s) needs to be unlocked before the **Assign IP** function can be used.

Assign IPv4 or IPv6 (if supported) for the device. Clicking the button will show you all the options under **Assign IP**:

- Assign IPv4
- Assign IPv6
- Assign IPv4 & IPv6

If your device does not support certain options, they will be disabled.

Assign IPv4

Mode: Static or DHCP

Click on the field of **IP Address**, **Subnet Mask**, **Default Gateway – opt**, to manually key in the values.

If you have selected multiple devices and the specific IP is not required for each device, you may consider using **ASSIGN IP SEQUENTIALLY** to quickly set up an IP. The function increments the IP address based on the IP value of the first device in the list.

Assign IP

3 Device(s)

ASSIGN IP SEQUENTIALLY

No.	Model Name & Mac	IP Address	Subnet Mask	Default Gateway - opt.	
1	NPort 5450I 00:90:E8:9A:E0:BF	192.168.1.222	255.255.255.0		⋮
2	NPort 5210A 00:90:E8:AD:45:6A	192.168.1.223	255.255.255.0		⋮
3	NPort 5210A 00:90:E8:AD:45:10	192.168.1.224	255.255.255.0		⋮

CANCEL ASSIGN & RESTART

Clone "Network Mask" / "Default Gateway" to All Devices

This is a quick way to copy and paste Netmask or gateway values to all the selected devices. Edit **Subnet Mask** and **Default Gateway – Opt** of any device first, and find the options in the menu icon at the end of the list and apply:

No.	Model Name & Mac	IP Address	Subnet Mask	Default Gateway - opt.	
1	NPort 5450I 00:90:E8:9A:E0:BF	192.168.1.222	255.255.255.0		⋮
2	NPort 5210A	192.168.127.254	255.255.255.0		⋮

Clone "Network Mask" to all devices

Clone "Default Gateway" to all devices

START

Apply the changes

After you have set everything, click **ASSIGN & RESTART** to restart your device(s) and set a new IP. DSU should display the result, whether it is successful or failed, in the **Status & Message** columns of each device.

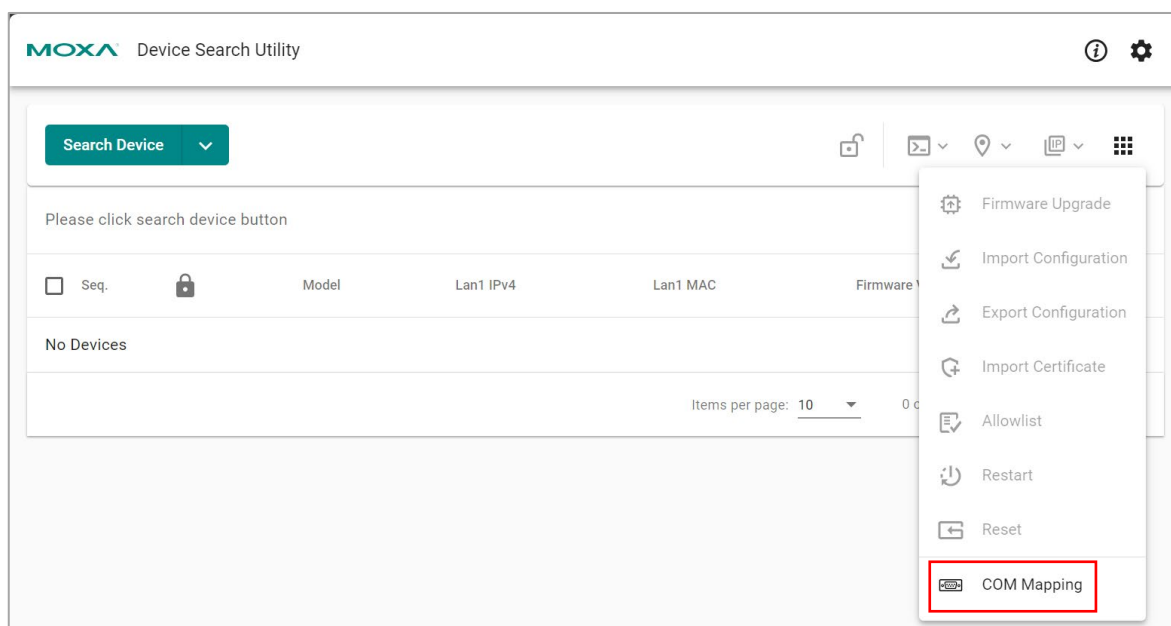
Info: It may take a while to execute this process, please wait for it to end before performing other actions.


Assigning IP and restarting for 3 device(s) ...

Device Name	Model Name	Status	Message	Last Updated Time
NP5450I_4850	NPort 5450I	Progressing	Processing...	Feb 06, 2024 14:41:35
NP5210A_8295	NPort 5210A	Failed	Session timeout. Please retry.	Feb 06, 2024 14:41:35
NP5210A_8205	NPort 5210A	Success	Success.	Feb 06, 2024 14:41:35

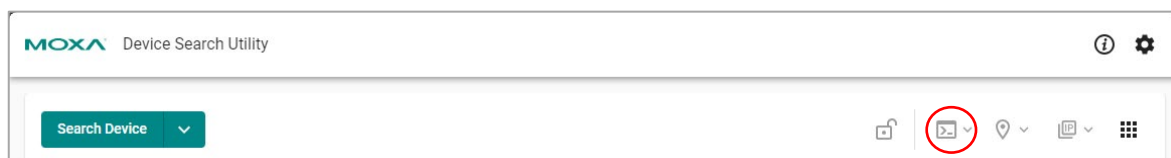
Items per page: 10 1 – 3 of 3


COM Mapping



After setting up the first user account, password and IP address, if the software to communicate with the serial devices by opening a COM port/TTY port, you can click the **More functions**  to find **COM Mapping** function for next step. Please refer to the [Chapter 4 Mapping COM Ports](#) for more information.

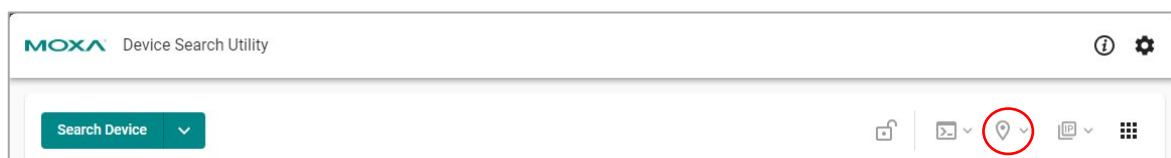
Console



When user wants to configure more detail settings, please click the **Console** button  to connect to the HTTPS console of the NPort IA5000-G2 Series.

For how to use web console for configuration, please refer to [Chapter 7. Configuration with the Web Console](#)

Locate



You need to unlock the device before you can use the **Locate** function.


This is to locate the device by triggering the buzzer to help the user to find the target device server easily. Clicking the button would show all options of **Locate**. If your device does not support certain options, they will be disabled:

- Locate (IPv4)

First Time Login Process

When user clicks the Console button at Device Search Utility or he/she inputs the default IP address, 192.168.127.254 to first time login to the web console of an NPort IA5000-G2 series, there will be a first-time login wizard to guide him/her to initialize the device with setting up the first administrator and the network settings of this device.

When seeing this page, click on the **START** button to start the process.




Getting Started with
NPort-IA5150-SFP-G2_0027

Thank you for choosing Moxa.
This wizard will help you quickly initialize the device.

START

If the user had an existing configuration file of an NPort IA5000 or NPort IA5000-G2, he/she can select the file and import it at the first step. Then the NPort IA5000-G2 will be configured as the old unit he/she has and the wizard will directly jump to step 5 for the user to confirm if the settings are correct?

If the user doesn't have an existing configuration file, please click **SKIP** to skip this step.



Import Configuration

Select the configuration file type to import, or skip this step.

File Type
-- Select One --

1 Import Configuration
Optional

2 IP Settings

3 Create Account

4 Confirmation

SKIP **NEXT >**

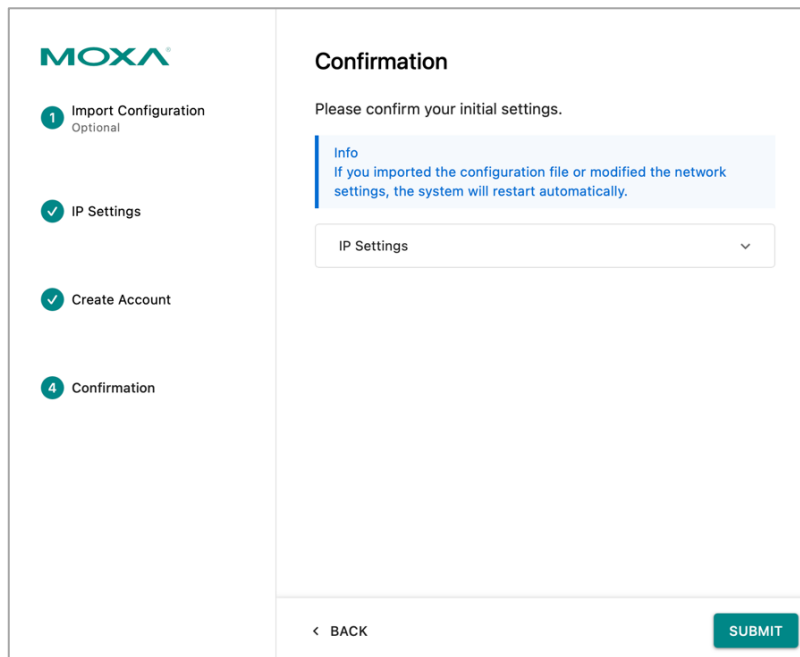
The default IP address of NPort IA5000-G2 series is 192.168.127.254/255.255.255.0. User can base on his network topology to modify it to DHCP or a different IP address. Please click **NEXT** to next step.

The screenshot shows the MOXA configuration interface for the NPort IA5000-G2 series. On the left, a sidebar contains four steps: 1. Import Configuration (Optional), 2. IP Settings (highlighted with a green circle), 3. Create Account, and 4. Confirmation. The main area is titled 'IP Address' and includes the instruction 'Configure the IP settings of the device.' Below this, there is a 'LAN Mode' dropdown menu set to 'Switch mode'. A section titled 'LAN Settings' contains an 'IPv4 Address' dropdown menu set to 'Manual'. Below the dropdown are three input fields: 'IPv4 Address' with the value '192.168.127.254', 'Subnet Mask' with the value '255.255.255.0', and 'IPv4 Gateway - Optional' which is empty. At the bottom of the main area, there are two buttons: '< BACK' and 'NEXT >'.

As there is no default username/password for NPort IA5000-G2 devices, please set up the first account of this unit. The first user of the device will have full privilege through this account. Keep the account name and password protected. A minimum of 8 characters is required for the default password complexity. The Password Policy function in the Account Management category allows you to change it.

The screenshot shows the MOXA configuration interface for the NPort IA5000-G2 series, specifically the 'Create Account' page. The left sidebar shows the same four steps as the previous screenshot, but step 2 'IP Settings' is now marked with a green checkmark, and step 3 'Create Account' is highlighted with a green circle. The main area is titled 'Create Account' and includes the instruction 'Create the first account of the device.' Below this, there are three input fields: 'Account Name' with the value 'admin', 'Password' with a masked value of eight dots, and 'Confirm Password' with a masked value of eight dots. Each password field has a small icon to toggle visibility. At the bottom of the main area, there are two buttons: '< BACK' and 'NEXT >'.

Double-check the network settings at the "Confirmation" step. If everything is OK, click the **SUBMIT** button and the unit will reboot, affecting the above settings.



The image shows a screenshot of the Moxa web console interface during the initial setup. On the left, a sidebar lists four steps: 1. Import Configuration (Optional), 2. IP Settings, 3. Create Account, and 4. Confirmation (highlighted with a green circle). The main area is titled 'Confirmation' and contains the text 'Please confirm your initial settings.' Below this is an 'Info' box with a blue border stating: 'If you imported the configuration file or modified the network settings, the system will restart automatically.' Under the info box is a dropdown menu labeled 'IP Settings' with a downward arrow. At the bottom of the main area, there is a '< BACK' link on the left and a green 'SUBMIT' button on the right.

Once you complete the initial login, you'll have various next steps to choose from:

1. Read [Chapter 5 Cybersecurity Considerations](#) for the recommendations from Moxa to securely using the NPort IA5000-G2 device server.
2. For using Real COM mode users, refer to [Chapter 4 Mapping COM Ports](#) for more information.
3. For other operation mode users, refer to [Chapter 7 Configuration with Web Console](#) > [Operation Modes](#) for more introductions.
4. For other advanced settings, refer to [Chapter 7 Configuration with web Console](#) for more details.

4. Mapping COM Ports

A device server connects devices with RS-232, RS-422, or RS-485 serial interfaces to a local area network, allowing for serial data transmission over Ethernet. Device servers provide network access to connected devices by bridging a physically wired Ethernet network connection on one side and one or more serial ports on the other side, making them appear as if they were directly connected to the serial port. To achieve this, you may have to map a COM port on Windows or a Fixed TTY port on UNIX-like platforms. Once you've configured the IP address using the First-time Login Wizard (introduced in Chapter 3) and mapped the COM port settings, the device server is ready for use. This chapter provides instructions on how to install the driver and map a COM port.

Mapping COM Ports on Windows Platforms

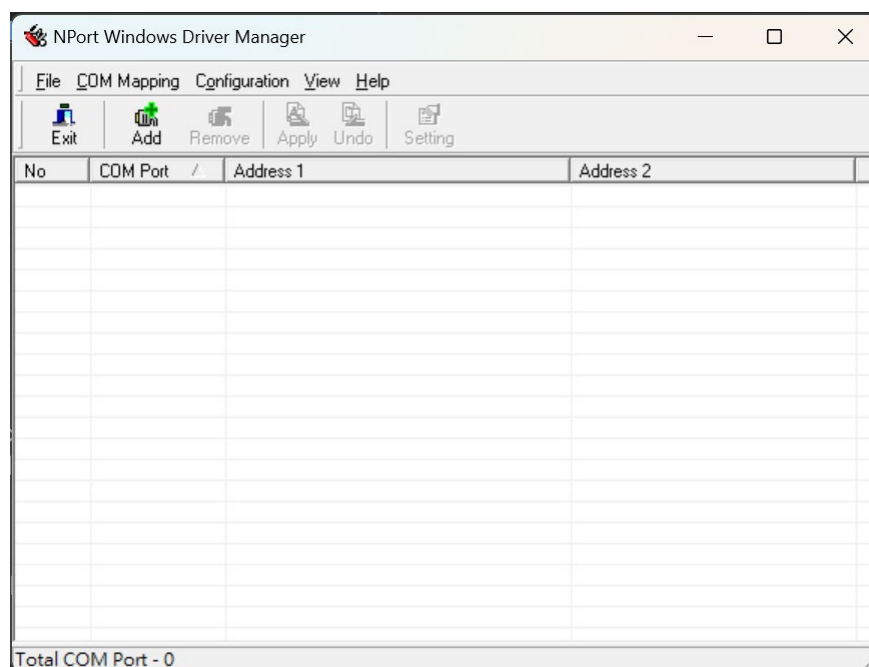
Mapping COM Ports With Real COM Mode

Refer to the "[COM Mapping](#)" section in Chapter 3 function triggers the NPort Windows Driver Manager when clicked. Once the software is installed, you can immediately run the NPort Windows Driver Manager.

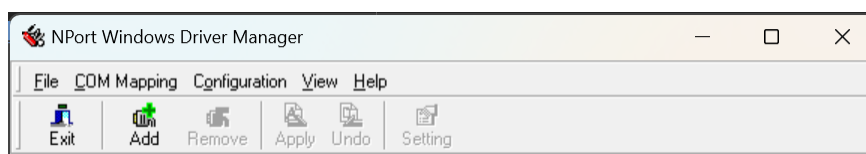


NOTE

Install Microsoft Visual C++ 2022 Redistributable to use COM mapping in NPort Windows Driver Manager.



1. Click the **Add** icon.



- Click the **Search** button to search for NPort device servers. Select the server from the list to map the COM ports before clicking **OK**.

Add NPort

Select From List

☐ Mapping IPv6 COM Port

Search Select All Clear All

No	Model	MAC 1	Address 1	MAC 2	Address 2

- Alternatively, you can select **Input Manually** and then manually enter the **NPort IP Address**, first **Data Port**, first Command Port, and **Total Ports** to which COM ports will be mapped. Click **OK** to proceed to the next step. Note the Add NPort page will automatically fill in the IP address field if a Fully Qualified Domain Name (FQDN) is used.

Add NPort

Select From List

☐ Mapping IPv6 COM Port

Search Select All Clear All

Input Manually

Real COM Redundant COM Reverse Real COM

NPort IP Address

MAC Address

First Mapping Port

Data Port

Command Port

Total Ports

☐ Enable Auto IP Report

? Help OK Cancel

- COM ports and their mappings will appear in blue until they are activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not use the COM port until the COM ports are activated. Click **Yes** to activate the COM ports at this time or click **No** to activate the COM ports later.
- Activated ports will be displayed in black.

NPort Windows Driver Manager

File COM Mapping Configuration View Help

Exit Add Remove Apply Undo Setting

No	COM Port	Address 1	Address 2
1	COM9	192.168.1.222 950:966 (Port1)	
2	COM10	192.168.1.222 951:967 (Port2)	
3	COM11	192.168.1.222 952:968 (Port3)	
4	COM27	192.168.1.222 953:969 (Port4)	
5	COM28	192.168.1.201 950:966 (Port1)	
6	COM50	192.168.1.201 951:967 (Port2)	
7	COM51	192.168.127.254 950:966 (Port1)	
8	COM52	192.168.127.254 951:967 (Port2)	
9	COM53	00:90:e8:12:fa:42 (Port1)	

Mapping COM Ports on Linux Platforms

Download the Real TTY Linux driver on Moxa website and install it. Remember to check the kernel version that is suitable for your host PC. Before installing it, make sure you've already configured the device server properly:

- The IP address of the device server must comply with the network topology. The default IP address of the NPort IA5000-G2 Series is <https://192.168.127.254>. Please log in to the device and change its location to the same subnet of the host PC.
- Make sure the Operation Mode is Real COM mode. Once the first administration user is set up, the default Operation Mode is Real COM mode. You may not need to change this. If you have a device server that has been modified by others, it's a good idea to double-check it.

When the IP address and Operation Mode settings are confirmed:

1. Get the driver file from Moxa's website, [waiting for support address]
2. Log in to the console of the host PC as a superuser (root).
3. Execute **# cd /** to go to the root directory.
4. Copy the driver file **npreal2xx.tgz** to the **/** directory.
5. Execute **# tar xvfz npreal2xx.tgz** to extract all files into the system.
6. Execute **# /tmp/moxa/mxinst.**

For RedHat AS/ES/WS and Fedora Core1, append an extra argument as follows:

/tmp/moxa/mxinst SP1

The shell script will install the driver files automatically.

7. After installing the driver, you will see several files in the **/usr/lib/npreal2/driver** folder:

```
> mxaddsvr      (Add Server, mapping tty port)
> mxdelsvr      (Delete Server, unmapping tty port)
> mxloadsvr     (Reload Server)
> mxmknod       (Create device node/tty port)
> mxrmnod       (Remove device node/tty port)
> mxuninst      (Remove tty port and driver files)
```

You are ready to map the NPort serial ports to the system tty port.

Mapping TTY Ports

Logging in as a superuser, enter the directory **/usr/lib/npreal2/driver** and then execute **mxaddsvr** to map the target NPort serial port to the host tty ports. The syntax of command **mxaddsvr** is as follows:

mxaddsvr [NPort IP Address] [Total Ports] ([Data port] [Cmd port])

The **mxaddsvr** command will perform the following actions:

1. Change **npreal2d.cf**.
The **npreal2d.cf** is the configuration file of the driver.
2. Create tty ports in directory **/dev** with major & minor number configured in **npreal2d.cf**.
3. Restart the driver.

To map the tty ports with default settings, execute **mxaddsvr** with the IP address and the number of ports, as in the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16
```

This example involves adding 16 tty ports, each with IP 192.168.3.4. The data ports will span from 950 to 965, while the command ports will go from 966 to 981.

To map the tty ports with preferred data ports and command ports, execute **mxaddsvr** with the following example:

```
# cd /usr/lib/npreal2/driver
# ./mxaddsvr 192.168.3.4 16 4001 966
```

This example involves adding 16 tty ports, each with IP 192.168.3.4. The data ports will span from 4001 to 4016, while the command ports will go from 966 to 981.

Removing Mapped TTY Ports

Logging in as root, enter the directory **/usr/lib/npreal2/driver** and then execute **mxdelsvr** to delete a server. The syntax of **mxdelsvr** is:

mxdelsvr [IP Address]

Example:

```
# cd /usr/lib/npreal2/driver
# ./mxdelsvr 192.168.3.4
```

The following actions are performed when executing **mxdelsvr**:

1. Change **npreal2d.cf**.
2. Remove the relevant tty ports in directory **/dev**.
3. Restart the driver.

If the IP address is not provided in the command line, the program will list the installed servers and total ports on the screen. Choose a server from the list for deletion.

Removing Linux Driver Files

A utility is included that will remove all driver files, mapped tty ports, and unload the driver. To do this, you only need to enter the directory **/usr/lib/npreal2/driver**, then execute **mxuninst** to uninstall the driver. This program will perform the following actions:

- Unload the driver.
- Delete all files and directories in **/usr/lib/npreal2**
- Delete directory **/usr/lib/npreal2**
- Change the system initializing script file.

Mapping COM Ports on macOS Platforms

To map an NPort IA5000-G2 serial port to a Mac host's tty port, follow these instructions:

1. Download the macOS driver from Moxa website and install the Mac driver files on the host.
2. Set up the NPort IA5000-G2. Verify the IP configuration works by using ping, telnet, etc.
3. Search or manually input the IP address of the NPort to set up a virtual COM port.

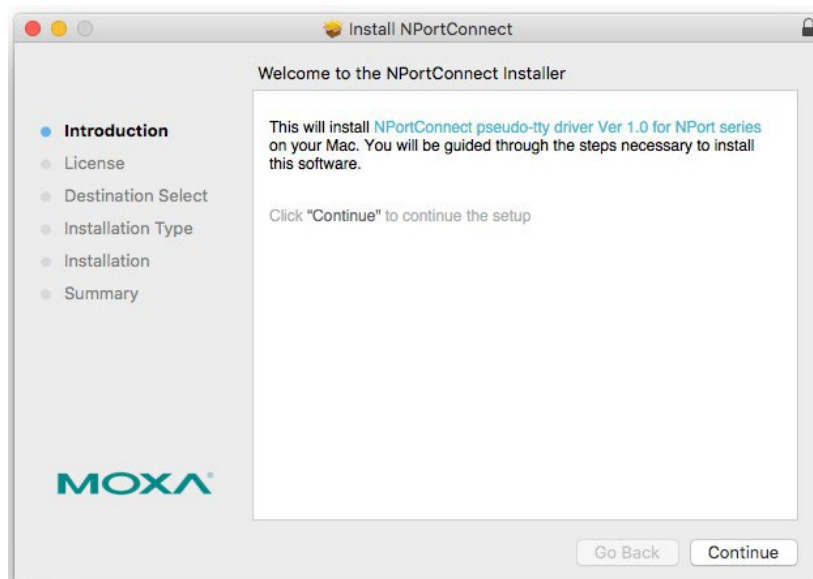
Installing macOS TTY Driver Files



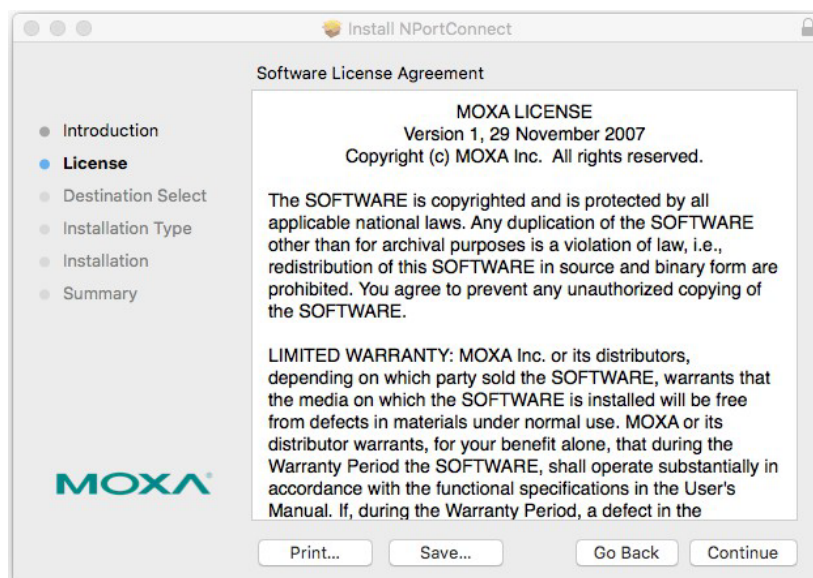
NOTE

For the newest information, please refer to readme.txt on Mac TTY Driver. Resources location of product information, release note, and readme file: /usr/local/share/NportConnect.

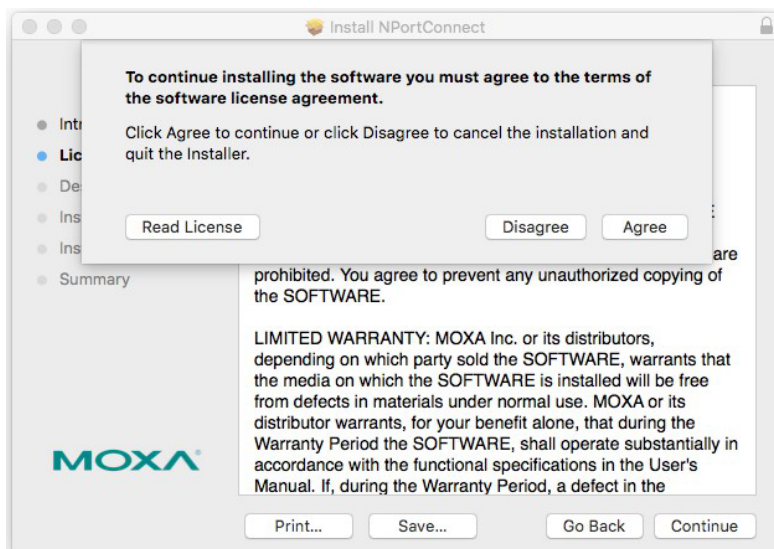
1. Get the driver file from Moxa's website, at <https://www.moxa.com>. It is in the Resource section under the product page.



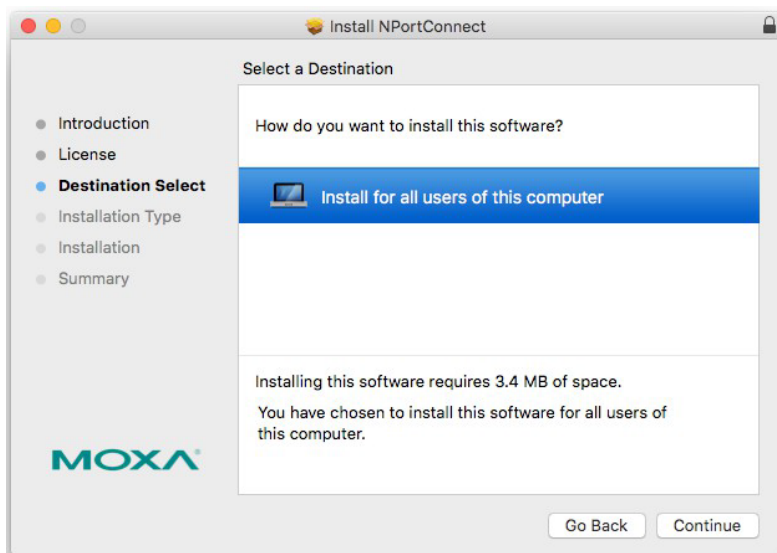
2. Execute the installer package 'moxa-macOS-tty-drivers-for-macOS-10.12-or-later-v1.0.pkg'.



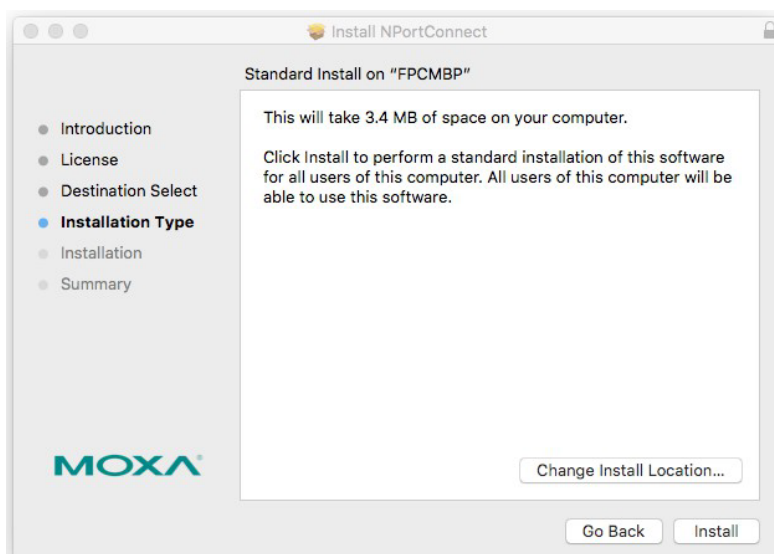
3. Press **Continue** when the **Introduction** window opens to proceed with installation.



4. Press **Continue** in the **Destination Select** window.



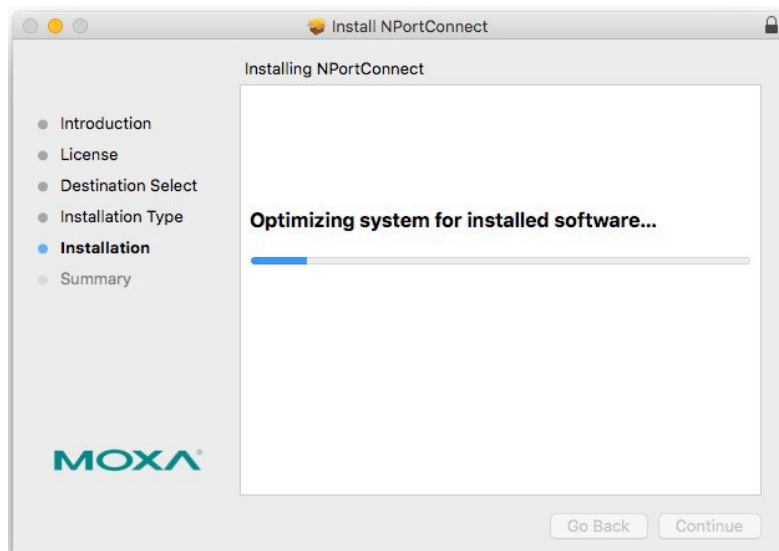
5. Click **Install** to start the installation in the default directory or select an alternative location.



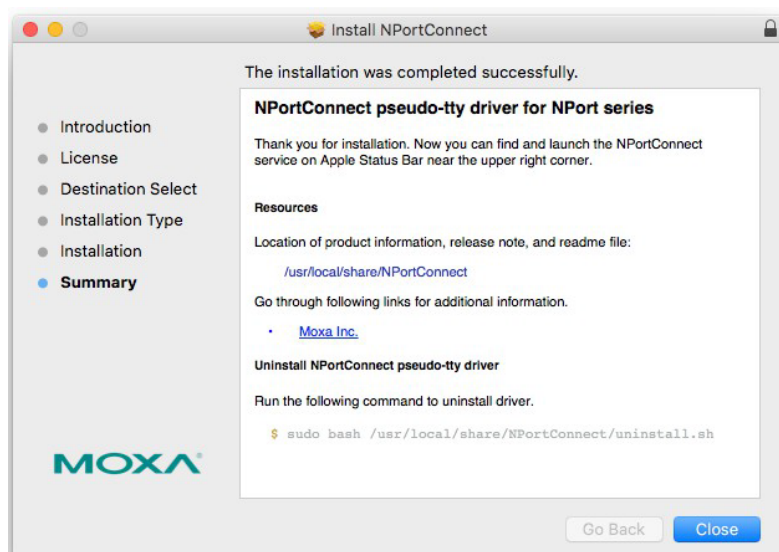
6. Key in your system login username and password to confirm the authentication.



7. The installation window reports the progress of the installation.



8. Click **Close** to complete the installation of the NPort macOS tty driver.



Mapping macOS TTY Port

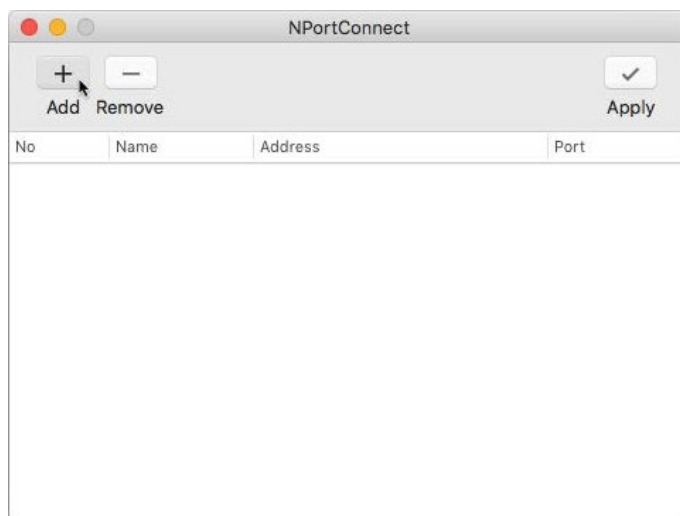
1. In the menu bar, a NPortConnect icon will appear after the installation is completed.



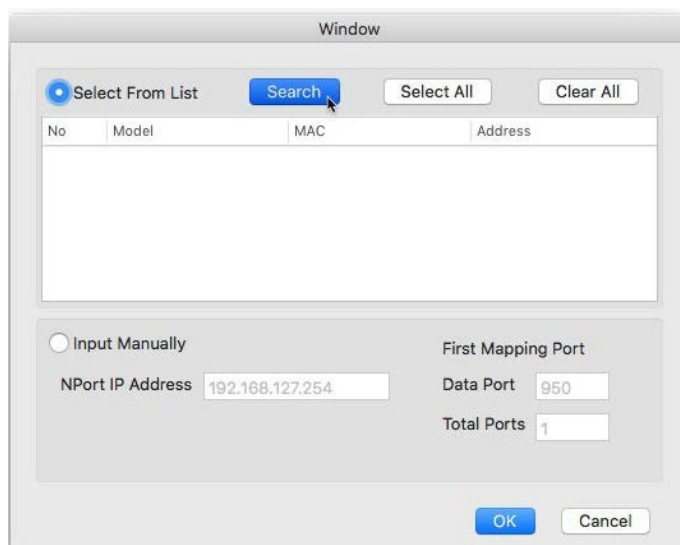
2. Click on the **NPortConnect** icon and select **NPort Mapping** for the port mapping function.



3. Click on **+ Add** to enter the tty port setup.



4. Click **Search** to find the NPort already set up in the **Hardware Setup** procedure. The **Search** function broadcasts a search to locate NPort units on the LAN that are connected to your Mac. The Broadcast Search function searches by MAC address and not IP address. The location of all NPort units connected to the LAN will be determined, regardless of their subnet. Alternatively, you can manually enter the IP address to locate the specific NPort.



- Once the search is completed, all the NPort found will appear on the list.

Window

☒ Select From List Search Select All Clear All

No	Model	MAC	Address
<input type="checkbox"/> 1	NPort 5110A	00:90:E8:51:72:90	192.168.127.254
<input type="checkbox"/> 2	NPort 5450	00:90:E8:48:F3:30	192.168.127.254

☐ Input Manually

NPort IP Address: 192.168.127.254

First Mapping Port: _____

Data Port: 950

Total Ports: 1

OK Cancel

- Select the model types that are for the tty port mapping and click **OK**.

Window

☒ Select From List Search Select All Clear All

No	Model	MAC	Address
<input type="checkbox"/> 1	NPort 5110A	00:90:E8:51:72:90	192.168.127.254
<input checked="" type="checkbox"/> 2	NPort 5450	00:90:E8:48:F3:30	192.168.127.254

☐ Input Manually

NPort IP Address: 192.168.127.254

First Mapping Port: _____

Data Port: 950

Total Ports: 1

OK Cancel

- NPortConnect auto assigns the tty name and corresponding port number to the IP address of the selected NPort.

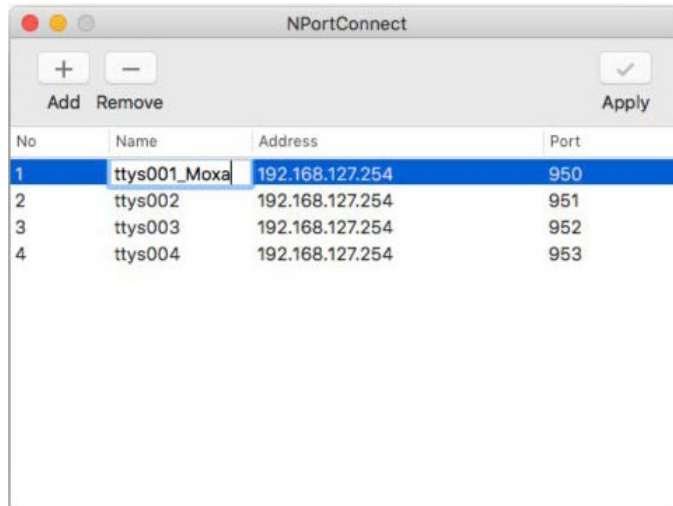
NPortConnect

+ - ✓

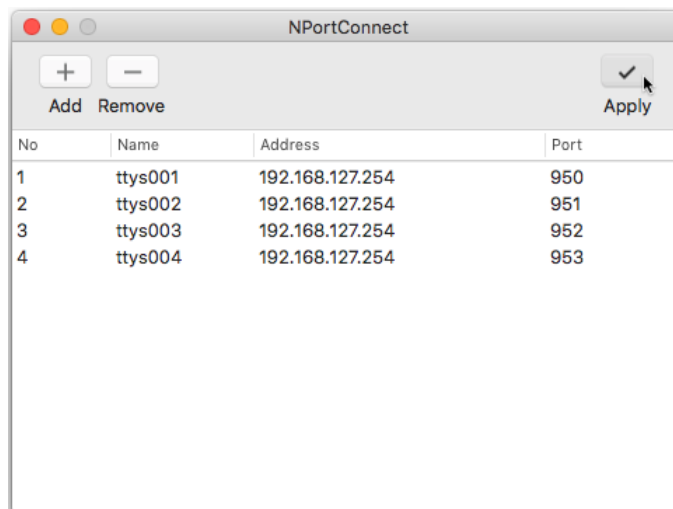
Add Remove Apply

No	Name	Address	Port
1	ttys001	192.168.127.254	950
2	ttys002	192.168.127.254	951
3	ttys003	192.168.127.254	952
4	ttys004	192.168.127.254	953

8. The tty name and port number are editable. Note these changed values are only for mapping configuration and would not change the values in the NPort settings.



9. When everything is set, click **Apply** to save the configuration.



Uninstalling the macOS Driver

Run the following command to uninstall driver:

```
$ sudo bash /usr/local/share/NPortConnect/uninstall.sh
```

Mapping COM Ports on UNIX-Like Platforms



NOTE

For the newest information, please refer to readme.txt on Fixed TTY Driver.

Installing the UNIX Fixed TTY Driver

1. Log in to UNIX and create a directory for the Moxa TTY driver. To create a directory named `/usr/etc`, execute the command:
mkdir -p /usr/etc
2. Copy `moxattyd.tar` to the directory you created. If you created the `/usr/etc` directory above, execute the following commands:
cp moxattyd.tar /usr/etc
cd /usr/etc
3. Extract the source files from the tar file by executing the command:
tar xvf moxattyd.tar
The following files will be extracted:
README.TXT
moxattyd.c --- source code
moxattyd.cf --- an empty configuration file
Makefile --- makefile
VERSION.TXT --- fixed tty driver version
FAQ.TXT
4. Compile and Link
 - For SCO UNIX:
make sco
 - For UnixWare 7:
make svr5
 - For UnixWare 2.1.x, SVR4.2:
make svr42

Configuring the UNIX Driver

Change the configuration:

The configuration used by the **moxattyd** program is defined in the text file **moxattyd.cf**, which is in the same directory that contains the program **moxattyd**. Use **vi** or any text editor to change the file, as follows:

ttyp1 192.168.1.1 950

For more configuration information, view the file **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.



NOTE

The "Device Name" depends on the OS. See the Device Naming Rule section in README.TXT for more information.

To start the **moxattyd** daemon after system bootup, add an entry into **/etc/inittab**, with the tty name you configured in **moxattyd.cf**, as in the following example:

ts:2:respawn:/usr/etc/moxattyd/moxattyd -t 1

Device naming rule

For UnixWare 7, UnixWare 2.1.x, and SVR4.2, use:

pts/[n]

For all other UNIX operating systems, use:

ttyp[n]

Starting moxattyd

Execute the command **init q** or reboot your UNIX operating system.

Adding an additional server

1. Change the text file **moxattyd.cf** to add an additional server. Use **vi** or any text editor to change the file. For more configuration information, refer to the file **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.
2. Find the process ID (PID) of the program **moxattyd**.
ps -ef | grep moxattyd
3. Update configuration of **moxattyd** program.
kill -USR1 [PID]
(e.g., if **moxattyd** PID = 404, kill -USR1 404)

This completes adding an additional server.

5. Cybersecurity Considerations

As cyberattacks increase and become more sophisticated, network device vendors are incorporating features to safeguard sensitive information. Moxa has made it a priority to develop measures that ensure all products meet security standards, so customers can use them with peace of mind. There are certain details that Moxa cannot do alone; customers and Moxa need to work together to build up a much-secured environment to defend against all kinds of cyberthreats. This chapter introduces the essential steps to enhance the cybersecurity of Moxa's products. Customers may need to refer to other sections in the user manual for the exact settings or commands.

Updating Firmware

Customers who buy products from Moxa or a reseller should be aware that Moxa might have already launched a newer firmware version with enhanced security features. Please check with Moxa's support website to see if there is a newer version of firmware. If so, we recommend upgrading the firmware to the newest.

Turn Off Unused Service and Ports

Imagine living in a house that has many entrances. If all the doors and windows are left unlocked or even open, it sends a message of welcoming to intruders out there. We always recommend turning off services and ports that are not in use to reduce the chances of being attacked.

Refer to the table below for all the ports, protocols and services that are provided to communicate between the NPort IA5000-G2 Series and other devices.

Service Name	Option	Default Settings	Type	Port Number	Description
Moxa services	Enable/Disable	Enable	TCP	443	For Moxa utility communication
			UDP		
SNMP agent	Enable/Disable	Disable	UDP	161	SNMP handling routine
HTTPS server	Enable/Disable	Enable	TCP	443	Secured web console
DHCP client	Enable/Disable	Disable	UDP	68	The DHCP client needs to get the system IP address from the DHCP server
SNTP	Enable/Disable	Disable	UDP	Random port	Synchronize the time settings with a time server

Operation Mode	Option	Default Settings	Type	Port Number
Real COM mode	Enable/ Disable	Disable (Changed to Enable after user set username/password)	TCP	949 + (serial port number) 965 + (serial port number)
RFC2217 mode	Enable/ Disable	Disable	TCP	4000 + (serial port number)
TCP Server mode	Enable/ Disable	Disable	TCP	4000 + (serial port number) 965 + (serial port number)
UDP mode	Enable/ Disable	Disable	UDP	4000 + (serial port number)
Pair Connection Server mode	Enable/ Disable	Disable	TCP	4000 + (serial port number)
Reverse Terminal – Telnet	Enable/ Disable	Disable	TCP	4000 + (serial port number)
Reverse Terminal – SSH	Enable/ Disable	Disable	TCP	4000 + (serial port number)
Disable mode	Enable/ Disable	Disable	N/A	N/A

Turn On Services That Are Necessary

Some services are recommended to be enabled because they are the key functions of the NPort IA5000-G2, and they face cybersecurity threats. The communication of these services are encrypted on the Ethernet network.

- Web console (HTTPS): This is the major management console of the NPort IA5000-G2 for configuring all the settings, and it also provides some diagnostic tools for an engineer to troubleshoot a problem.
- SNMPv3: The Simple Network Management Protocol is a popular tool for remote device monitoring and management. Enable SNMPv3 to encrypt communication data if needed.
- Moxa services (HTTPS): The Device Search Utility v3.0 is a good tool for first-time installation on the NPort IA5000-G2 Series, and the Moxa MXview can easily monitor all the NPorts in a network. All these tools work with the Moxa services.



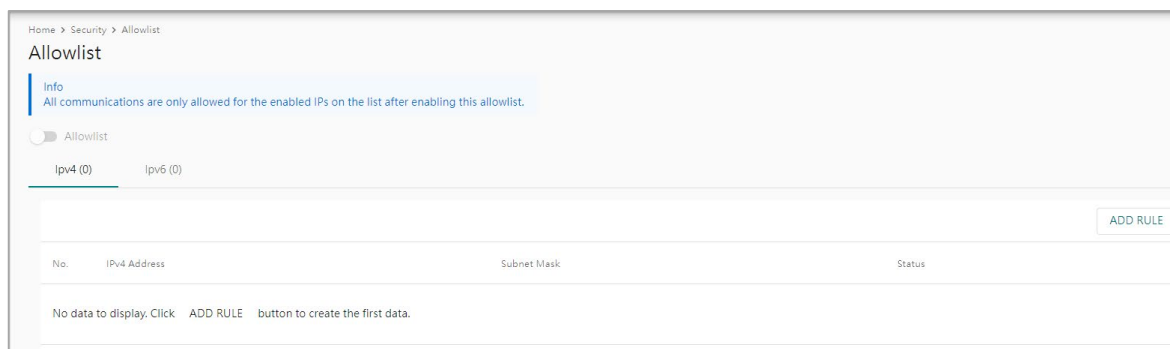
NOTE

If all HTTPS/SNMP/Serial consoles are turned off, then there is no other route to access the product. The only way to recover it is to reset the device and start from the beginning. For guidance on resetting the device, refer to the user manual.

Limited IP Access

Limiting the number of IP addresses that can access the product is one of the most effective ways of blocking unwanted intruders. If the product is accessed by a limited number of desktop/notebook/mobile devices, provide access to those IPs.

The NPort IA5000-G2 has the Allowlist function to grant an IP address or a range of devices to access the device server. You can **ADD RULE** for those granted IP addresses and then enable the Allowlist function to limit access to the specific NPort IA5000-G2 only to those IP addresses.



Account and Password

- There is no default username and password for NPort IA5000-G2 devices. You may need to follow up the first-time login process to set the username and password for the first user (who will also be the admin user) of this device to enhance the device's security.
- Use strong passwords. The devices support a function called **Password Policy** to check if passwords are strong enough. Enable the function to help you check whether the passwords are strong enough.
- Use the account login failure lockout feature to prevent unwelcome access (**Security > Login Settings > Login Lockout**).
- For central management purposes, set up an authentication server in the network. The NPort IA5000-G2 Series supports RADIUS and TACACS+ servers. Using an authentication server for account management can ease administrators' loads of repeatedly inputting the same account/password on multiple devices. Refer to **Account Management > Authentication Server** for more information.

System Log

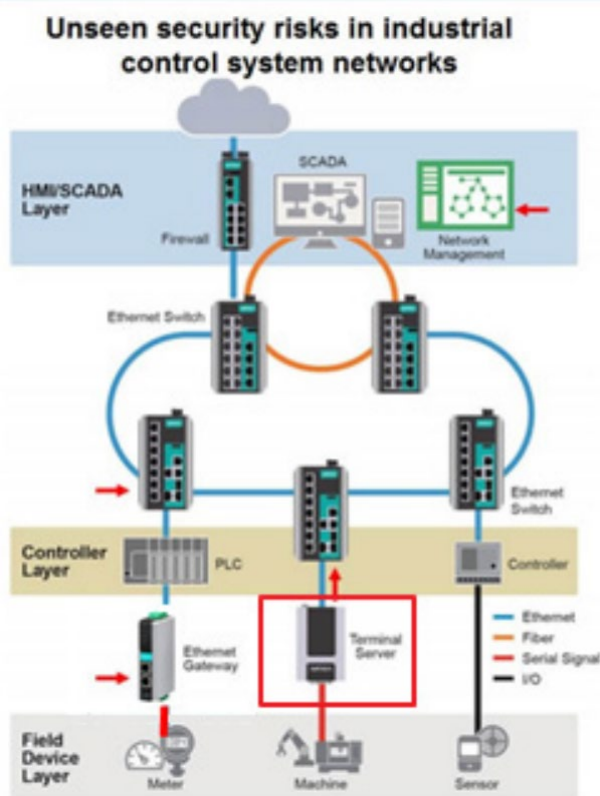
The system log usually records all kinds of activities that are happening on your NPort, such as Login Fail, IP Changed, Password Changed, Config Changed, etc. Check the log regularly to examine any abnormal behavior.

For central management purposes, set up a log server in the network to collect all the logs from different devices. The NPort IA5000-G2 Series supports syslog-ng protocol to deliver the logs securely to the log server. The events will be sent with the format defined by RFC3164 for the analyzer to read/analyze. Refer to **System Settings > Notifications > Channels Settings** for more information.

Deployment of the Device

Deploy the NPort IA5000-G2 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

Make sure that the physical protection of the NPort devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



Testing the Security Environment

Besides these devices that support these protective functions, network managers can follow several recommendations to protect their network and devices.

To prevent unauthorized access to a device, follow these recommendations:

- Testing tools for cybersecurity environment checks are available. Some may provide limited free use, for example, Nessus. These tools help identify probable security leaks in the environment.
- The device should be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
- Control access to the serial console as with any physical access to the device.
- Avoid using insecure services such as SNMPv1 or v2; the best way is to disable them completely.
- Limit the number of simultaneous web server sessions allowed. Periodically, change the passwords.
- Back up the configuration files periodically and check the CRC value of the run time settings to make sure the devices work properly.
- Audit the devices periodically to make sure they comply with these recommendations and/or any internal security policies.
- If there is a need to return the unit to Moxa, make sure encryption is disabled, and that you had already backed up the current configuration before returning it.



NOTE

DISCLAIMER: Please note that the above information and guide (the "information") are for your reference only. We do not guarantee a cyberthreat-free environment. These guidelines are to increase the security level to defend against cyber intrusions and do not guarantee that the above information will meet your specific requirements. The above information is provided "as-is", and we make no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

6. Management Consoles

If you're looking to open COM port applications, you can follow the steps in the **First-time Setup** and **Mapping COM Port** chapters to complete the basic settings. The NPort IA5000-G2 will work properly at the actual site. If you want to configure more advanced settings, like **Security** or **Account Management**, access the device with the different management consoles introduced in this chapter.

If you use other applications, finish the account and IP settings by **First-time Setup** process. There are more settings waiting for you. Access the device with different management consoles introduced in this chapter to complete the configuration.

Configuration Options

Device Search Utility

Configure your NPort IA5000-G2 with the bundled Device Search Utility (DSU) v3.0 and above for Windows. When you find the NPort IA5000-G2 with the default IP address 192.168.127.254 on DSU, set the username and password for the first user (it will also be the admin user) of this device to enhance the device security. Then **right-click** on the device to change the IP address for your network. Or, you can **double-click** on the device to directly open the Web console of the device for configuration.

Web Console

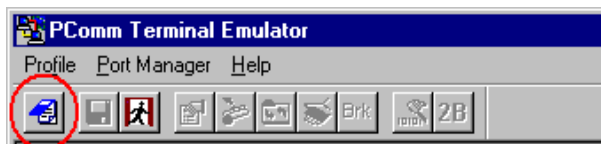
Configure your NPort IA5000-G2 using a standard web browser. The web console is the default management console of the device we recommend. Besides special reasons, we suggest keeping it enabled—not only for the first-time installation but also for maintenance and troubleshooting.

Serial Console

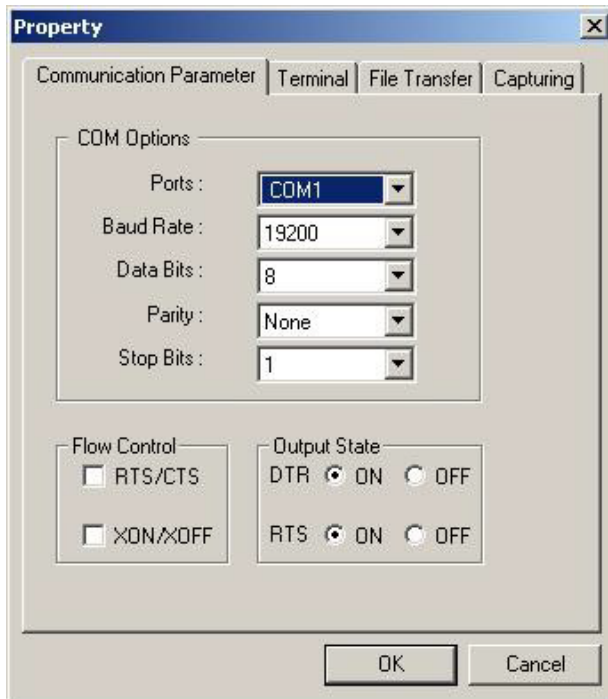
The NPort IA5000-G2 supports the serial console as the local access point through serial port 1. The serial console port only supports basic settings like network settings to change the IP address or when the Ethernet LAN port cannot be logged in.

The following instructions and screenshots show how to enter the serial console using PComm Terminal Emulator, which is available free as part of the PComm Lite suite. You may use a different terminal emulator utility, although your actual screens and procedures may vary slightly from the following instructions.

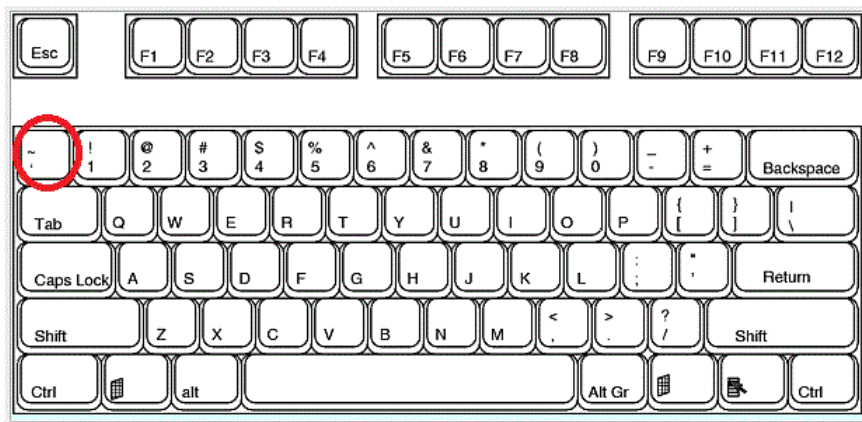
1. Turn off the power to the NPort IA5000-G2. Use a serial cable to connect the NPort IA5000-G2's serial console port to your computer's male RS-232 serial port.
2. From the Windows desktop, select **Start > All Programs > PComm Lite > Terminal Emulator**.
3. The PComm Terminal Emulator window will appear. From the Port Manager menu, select **Open**, or simply click the **Open** icon as shown below:



- The Property window opens automatically. Select the **Communication Parameter** tab; then, select the appropriate COM port for the connection (COM1 in this example). Configure the parameters for **19200**, **8**, **None**, **1** (**19200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits).



- From the Property window's Terminal page, select **ANSI** or **VT100** for **Terminal Type** and click **OK**.
- If you are using the NPort IA5000-G2, hold down the grave accent key (`) while powering it up, as shown below. Note the grave accent key (sometimes called backwards apostrophe) is NOT the apostrophe key—it is the key usually found next to the number **1** key.



The NPort IA5000-G2 will then automatically switch from data mode to console mode.

- When you see the "Login:" message, enter the username and password. You will be prompted to the command line mode.

```
Login: admin
Password: *****
NPort# █
```

- The serial console is a Command-line Interface. You may need to input commands to view or change the settings. Please find the [Appendix F Command List of the Serial Console](#) section for more details.

7. Configuration with the Web Console

To configure the NPort IA5000-G2, the web console is the easiest method to use. With a standard web browser, you can effortlessly navigate through all settings and options. Once you've completed the **First-time Setup** or used DSU-G2 to configure a new IP address for an NPort IA5000-G2, enter the new IP address to access the web console. This chapter covers the introduction of the web console and explores its configuration options.

Factory Default IP Address

The NPort IA5000-G2 is configured with the following default private IP address:

192.168.127.254

Note that IP addresses that begin with "192.168" are referred to as private IP addresses. Devices configured with a private IP address are not directly accessible from a public network. For example, you cannot ping a device with a private IP address from an outside Internet connection.

Using Your Web Browser

Opening the Web Console

Open your web browser and enter the IP address you've changed in the website address line. Press **ENTER** to load the page.



You may find the "Not secure" icon on the website address line. Click it to add the NPort as a trusted device to remove the icon. For more information, refer to the **Security Hardening Guide**. Enter the account name and password you've set to access the device.

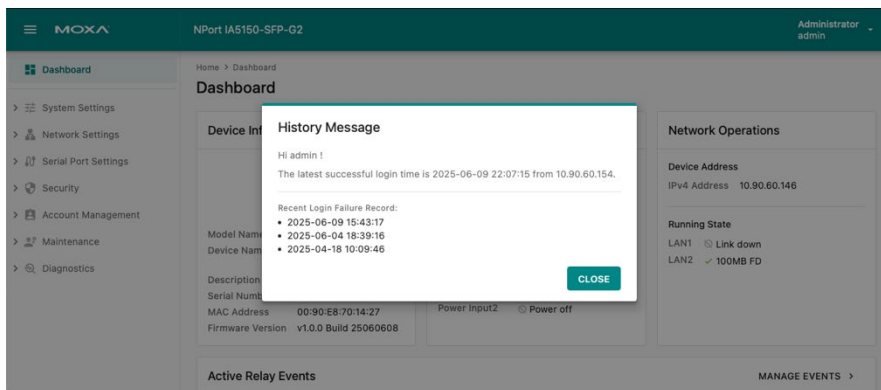


ATTENTION

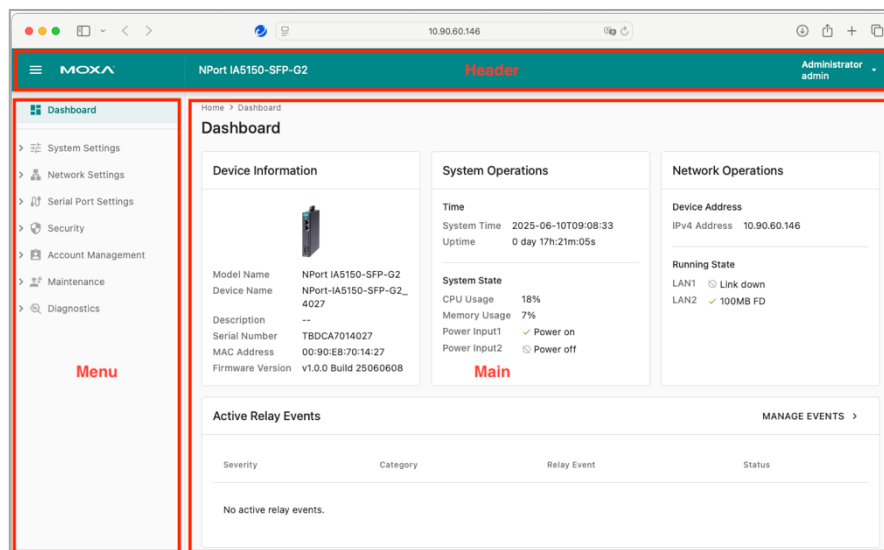
In case of a forgotten password, the reset button must be used to configure the NPort IA5000-G2 by resetting all settings and loading the factory defaults. Even if you disabled the reset button in your NPort IA5000-G2 configuration, you can still use it to restore factory defaults within the first minute of powering on the NPort IA5000-G2.

Remember to back up your configuration by exporting it to a file. Importing the file to the NPort IA5000-G2 will quickly restore your configuration. This will save time if you have forgotten the password and need to reload the factory defaults.

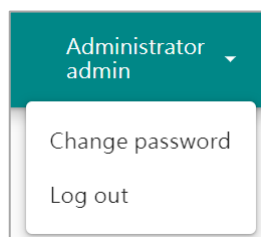
The NPort IA5000-G2's web console will appear after logging in and you may receive the history messages including the **Login Message** (can be configured at **Security > Login Settings > Login Message**) and account login history.




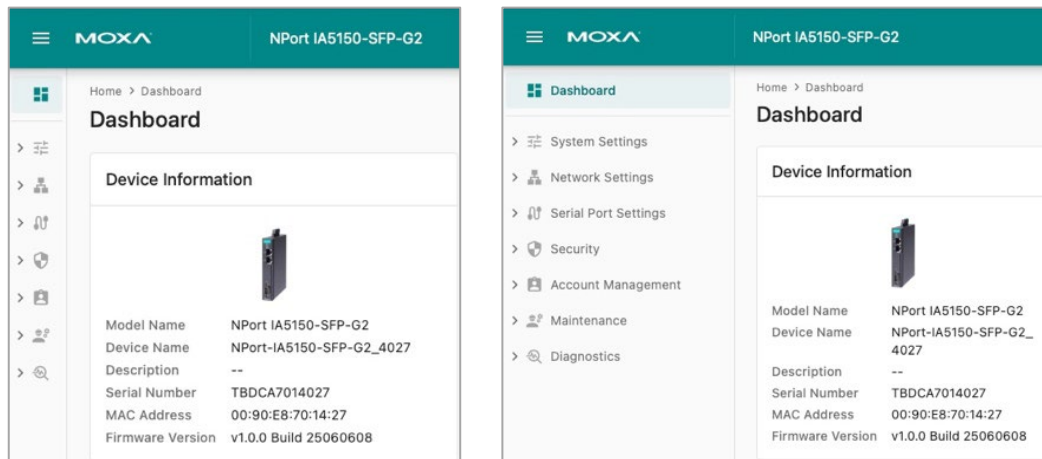
Click the **CLOSE** button and the Dashboard page will be displayed.



The Header shows who is logged in to the device. Click the account to change your password or log out the web console.



Click the  icon to hide or show the Navigation Panel.



How many categories you may see on the Navigation Panel depends on the privilege of the user group you belong to. The administrators will see all of them as in snapshot above.

Web Console Navigation

On the NPort IA5000-G2 web console, the left panel is the navigation panel and contains an expandable menu tree for navigating among the various settings and categories. When you click on a menu item in the navigation panel, the main window will display the corresponding options for that item. Configuration changes can then be made in the main window.

Changes will take effect immediately except for the network-related settings. If users add or remove devices after the NPort is online, they would want the new settings to immediately take effect without needing to reboot the device. Support for this function is provided by the NPort IA5000-G2 Series.


The IP address change for the NPort IA5000-G2 is a separate issue. It may require notifying all network devices and updating their tables. To make the NPort IA5000-G2 work after changing its IP address, a reboot is necessary.

Dashboard Introduction

Home > Dashboard

Dashboard

Device Information



Model Name NPort IA5150-SFP-G2
Device Name NPort-IA5150-SFP-G2_4027
Description --
Serial Number TBDCA7014027
MAC Address 00:90:E8:70:14:27
Firmware Version v1.0.0 Build 25060608

System Operations

Time
System Time 2025-06-10T09:28:18
Uptime 0 day 17h:40m:50s

System State
CPU Usage 5%
Memory Usage 7%
Power Input1 Power on
Power Input2 Power off

Network Operations

Device Address
IPv4 Address 10.90.60.146

Running State
LAN1 Link down
LAN2 100MB FD

Active Relay Events

MANAGE EVENTS >

Severity	Category	Relay Event	Status
No active relay events.			

System Log

Top 5 critical events within the past 30 days

VIEW MORE >

Severity	Category	Event Name	Timestamp
Warning	Security	Clear log	2025-06-10 09:28:11

Operation Mode State

VIEW MORE >

Port	Operation Mode	Connection Status	Serial Parameters	Serial Errors (count)
1	Real COM	Disconnected	RS-232, 19200, None, 8, 1	0

When you access the web console of an NPort IA5000-G2 device, it will take you to the Dashboard page to have an overview of the status of the unit. There are five sections:

Device Information: The section displays the basic/general information of the unit, including the Model Name, Serial Number, MAC address, and firmware version.

System Operations: This section displays some unique information about the unit, like when the device is powered up, the CPU, and memory usage.

Network Operations: In this section, it shows the network status of the unit. For example, the IP address and the Ethernet LAN speed.

Active Relay Events: In this section, it shows if there is a relay event happened.

System Log: You can check whether any critical events have happened since you last login to the device. It will remind if any abnormal events happened.

Operation Mode State: The key function of an NPort IA5000-G2 device is to provide communication between serial port(s) and the Ethernet LAN port(s). You will find the Operation Modes of each serial port in this section, and you can check the status here to see if it works properly.

System Settings

The first category of the navigation panel is System Settings, which includes three parts. The General page has the Identity and Date & Time settings of the device. The Notification page has the system events, emails, and SNMP Trap/Inform settings. The SNMP Agent has the SNMP Agent settings, which will be needed if you want to get information or settings from the NPort IA5000-G2 device via SNMP protocol.

General

The screenshot shows the 'General' settings page with the 'Identity' tab selected. The breadcrumb trail is 'Home > System Settings > General'. The left sidebar contains 'Dashboard', 'System Settings' (expanded), 'General' (selected), 'Notification', 'SNMP Agent', 'Network Settings', 'Serial Port Settings', 'Security', and 'Account Management'. The main content area has two tabs: 'Identity' and 'Date & Time'. Under 'Identity', there is a 'Device Name' field with the value 'NPort-IA5150-SFP-G2_4027' and a 'Description - Optional' text area. A 'SAVE' button is at the bottom.

Under the General page, the Identity tab provides the Device Name and Description column for you to identify which unit the NPort IA5000-G2 is using.

Device Name: This is an optional free text field for your own use. It does not affect the operation of the NPort IA5000-G2. It will be set as the Model Name of the device and the last 4 digits of the serial number. It helps differentiate one NPort IA5000-G2 server from another.

Description: This is an optional free text field for your own use. It does not affect the operation of the NPort IA5000-G2. It is useful for assigning or describing the location of an NPort IA5000-G2. In a network environment of multiple servers, this can be a valuable aid when performing maintenance.

The screenshot shows the 'General' settings page with the 'Date & Time' tab selected. The breadcrumb trail is 'Home > System Settings > General'. The left sidebar is the same as the previous screenshot. The main content area has two tabs: 'Identity' and 'Date & Time'. Under 'Date & Time', there are two sections: 'Current Date And Time' showing '2024-07-22 11:16:56' with an 'EDIT' button, and 'Time Zone' showing '(GMT+08:00) Taipei' with an 'EDIT' button.

The NPort IA5000-G2 has a built-in Real-Time Clock for time calibration functions. To change the time, please switch to the Date & Time tab. Click the **EDIT** button to change the current date and time and the time zone.

The NPort IA5000-G2 uses SNTP (RFC-1769) for auto time calibration. Enter a time server IP address or domain name in this optional field. Once the correct time server address is set, the NPort IA5000-G2 will regularly request time information from the time server every 10 minutes.

The screenshot shows the 'Edit Date And Time' dialog box. It has a 'Mode' section with 'Manual' selected (radio button) and 'Sync with NTP server' (radio button). Below is a 'Date' field showing '07/22/2024' with a calendar icon. At the bottom, there are three input fields for 'Hour' (11), 'Minute' (17), and 'Second' (29), separated by colons. 'CANCEL' and 'SAVE' buttons are at the bottom right.

To change the time zone, please click the **EDIT** button and select the location of the device. It will adjust the time zone automatically.

Edit Time Zone

Time Zone
(GMT+08:00) Taipei

☐ Enable daylight saving time by recurring

CANCEL
SAVE

If daylight saving time applies in the summer, enable the checkbox **Enable daylight saving time by recurring**.

☒ Enable daylight saving time by recurring

Offset (hour)
1

Start/End Date

From

Month
Jan

Week
First

Day
Sun

Hour
0

To

Month
Jan

Week
First

Day
Sun

Hour
0

CANCEL
SAVE

Daylight saving time (also known as **DST** or **summertime** involves advancing clocks (usually one hour) during the summer to provide an extra hour of daylight in the afternoon.

Offset

Setting	Description	Factory Default
User adjustable hour	The clock should be set forward by the number of hours specified in the offset parameter.	1

Start Date

Setting	Description	Factory Default
User adjustable date	The Start Date parameter allows users to enter the date that daylight saving time begins.	The Sunday of the First week of January

End Date

Setting	Description	Factory Default
User adjustable date	The End Date parameter allows users to enter the date that daylight saving time ends.	The Sunday of the First week of January



ATTENTION

A risk of an explosion exists if the real-time clock battery is replaced with the wrong type!

The NPort IA5000-G2's real-time clock is powered by a lithium battery. We strongly recommend that you do not attempt replacement of the lithium battery without help from a qualified Moxa support engineer. If you need to change the battery, please contact the Moxa RMA service team.

Notification

Home > System Settings > Notification

Notification

Select events and channels. Email and SNMP settings must be completed for notifications to work.

Events Settings
0 event(s) selected EDIT

Channels Settings

Email
🔇 Disabled EDIT
[More Information](#)

SNMP Trap/Inform
⚪ Not configured EDIT
[More Information](#)

Notification settings allow you to customize events that are logged by the NPort IA5000-G2. Events are grouped into five categories, known as event groups. Select which groups or events you want to log on the local memory space (up to 10,000 items will be saved in the flash). An email or SNMP Trap/Inform can also notify the administrator immediately of some of the events.

By default, the NPort will enable the event severity as Notice, Warning, and Error under the Security category and save them on the local flash memory. For the local log settings, find the diagnostics section.

The Categories of Notifications

Category	Description
System	The events related to the NPort itself, like firmware ready.
Network	The events related to the Ethernet interface, for example, the Ethernet link up.
Security	The events which may be considered security related; the administrator may need to figure out why it happened. For example, a Login fail event.
Maintenance	The events which usually happen at maintenance process, for example, firmware upgrade.
Serial	The events related to the serial interface(s), for example, Port connect.

The Severity of Events

Based on RFC5424, the severity of different events is categorized according to the following priority and description.

Priority	Severity	Description
1	Error	Events that indicate problems, but in a category that does not require immediate attention.
2	Warning	Events that provide forewarning of potential problems and indicate that some further actions could result in a critical error.
3	Notice	Events that are not error conditions, but that may require special handling.
4	Informational	Confirmation that the program works as expected.

The logs are essential for troubleshooting in case of errors. Refer to [Appendix E](#) for a detailed event list.

Event Settings

When clicking the **EDIT** button of the **Events Settings** column, you will see the event list, separated into different categories. Click the checkbox to enable the event for Email, SNMP Trap/Inform, or the Relay function. Only the enabled events will be recorded or trigger an email, SNMP Trap/Inform, or Relay output.

Home > System Settings > Notification > Events Settings

← Events Settings

Get notified by selecting the events and channels. Events can be sorted by various levels of severity.
[Refer to the specifics of the severity.](#)

Severity: ✓ Error ✓ Warning ✓ Notice ✓ Informational

SEARCH

System (5)

Network (5)

Security (9)

Maintenance (3)

Serial (5)

Severity	Event Name	<input type="checkbox"/> Syslog	<input type="checkbox"/> Email	<input type="checkbox"/> SNMP Trap/Inform	<input type="checkbox"/> Relay
Notice	User trigger reboot		<input type="checkbox"/>	<input type="checkbox"/>	
Warning	Power input failure		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Warning	NTP fail		<input type="checkbox"/>	<input type="checkbox"/>	
Notice	Email service is back		<input type="checkbox"/>	<input type="checkbox"/>	
Notice	SNMP inform service is back		<input type="checkbox"/>	<input type="checkbox"/>	

SAVE

System (5)

Network (5)

Security (9)

Maintenance (3)

Serial (5)

Severity	Event Name	<input type="checkbox"/> Syslog	<input checked="" type="checkbox"/> Email	<input checked="" type="checkbox"/> SNMP Trap/Inform	<input checked="" type="checkbox"/> Relay
Notice	User trigger reboot		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Warning	Power input failure		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Email

Home > System Settings > Notification > Email

← Email

☐ Enable SMTP service

Sever Settings

Server Address

TCP Port
25

☐ Enable secure connection

☐ Enable authentication

Contact Information

Sender Email (From)

Recipient Email (up to 4 Emails)

Recipient Email 1 (To)

+ Add Email

SAVE

Click the **EDIT** button in the Email column. You can enable the SMTP service so that the NPort will send an email if the selected events happen.

Server Settings

Setting	Description	Factory Default
Server Address	The IP address or domain name of the SMTP server.	N/A
TCP port	The TCP port to which the SMTP server receives SMTP messages.	25

If the SMTP server requires a secure connection (encrypt the email), click **Enable secure connection**. There are three options.

Setting	Description	Factory Default
TLS	Encrypts the entire communication channel between the client and the server from the beginning, ensuring that all data transmitted is secure.	N/A
STARTTLS	It is possible to start the connection in plain text and then switch to encrypted mode through STARTTLS. If the upgrade fails, the communication remains in plain text.	N/A
STARTTLS-None	No encryption. STARTTLS-None as an option helps system administrators clearly specify which connections should remain unencrypted.	N/A

If the SMTP server requires authentication verification, click **Enable authentication**, and input the username and password used to log into the SMTP server.

Setting	Description	Factory Default
Username	The name used to log into the SMTP server.	N/A
Password	The password used to log into the SMTP server.	N/A

Contact Information

Setting	Description	Factory Default
Sender Email (From)	The email address that the NPort will use to send the message. The user can easily figure out which NPort sends the message by this account.	N/A
Recipient Email 1 (To)	The email address that the NPort will send the message to. It shall be the administrator/manager of the NPort who manages/monitors the status of the NPort or the serial device connected to the NPort. There are 4 recipient emails at most.	N/A

SNMP Trap/Inform

Home > System Settings > Notification > SNMP Trap/Inform

← SNMP Trap/Inform

SNMP Trap/Inform service

SNMP Trap/Inform Server + ADD SERVER

There is no SNMP Trap/Inform server. Click + ADD SERVER button to create one.

Add Server

Server Settings | SNMP Settings

Server Address

UDP Port
162

CANCEL SAVE

Click the **EDIT** button at SNMP Trap/Inform column and click **ADD SERVER**. Set the Server Setting and the SNMP Settings.

Server Settings

Setting	Description	Factory Default
Server Address	The IP address or domain name of the SNMP server.	N/A
UDP port	The UDP port to which the SNMP server receives SMTP messages.	162

SNMP Settings

Add Server

Server Settings | SNMP Settings

SNMP Type
-- Select One --

SNMP Version
-- Select One--

CANCEL SAVE

SNMP Type	Description	Retry (Count)	Timeout (sec)	SNMP version
Trap	The NPort will send SNMP Trap and will not wait for acknowledgment	N/A	N/A	v1/v2c/v3
Inform	After sending an SNMP Inform, the NPort waits for the acknowledgment. The NPort will resend the Inform message until it gets a confirmation or times out.	Number of retries Default=3	The duration before a timeout occurs Default=5	v2c/v3

SNMP Inform messages requires acknowledgement of notifications. If you choose SNMP Inform as the SNMP type, you might have to specify the number of retries the NPort should attempt if it doesn't receive acknowledgments. Also, determine the time interval for the NPort to wait before sending the SNMP Inform message.

The screenshot shows the 'SNMP Settings' tab in a configuration interface. Under 'SNMP Type', 'Inform' is selected. Below this, there are two input fields: 'Retry (count)' with the value '3' and 'Timeout (sec)' with the value '5'.

SNMP Agent

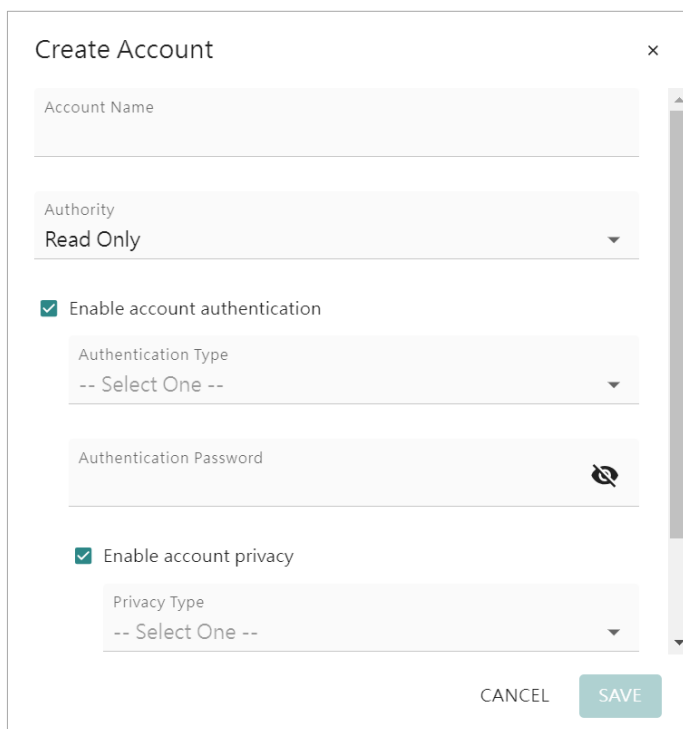
Simple Network Management Protocol (SNMP) is a widely used protocol/tool for network administrators to manage and monitor network devices. To meet this requirement, the NPort IA5000-G2 Series supports SNMPv1/v2c/v3 and includes a private MIB for device management and status monitoring of Ethernet or serial communication. For such purposes, enable the SNMP Agent service here (**System Settings > SNMP Agent**) and configure the proper settings introduced in the following sections.

The screenshot displays the 'SNMP Agent' configuration page. At the top, there's a breadcrumb 'Home > System Settings > SNMP Agent'. The main title is 'SNMP Agent'. Below it, a toggle switch for 'SNMP Agent service' is turned off. A note says 'Click "EDIT" button to select the SNMP version and fulfill the relevant configurations below.' There's a 'General' section with 'SNMP v3' selected and an 'EDIT' button. Below that, there's a 'V3 Account' section with a 'CREATE' button and a table with columns: Account Name, Authority, Status, Authentication Type, and Privacy Type. A note at the bottom says 'Set up at least one account to make the service work. Click CREATE button to create the account.'

Click the **EDIT** button under the General column. Select the SNMP Version and set the Device Details.

Setting	Description	Factory Default
SNMP Version	Select the SNMP Version. Use only SNMP v3/Use only v1, v2c/Use v1, v2c, and v3.	v3
Contact - Optional	This field usually includes an emergency contact name and telephone or pager number.	N/A
Location - Optional	Use this field to specify the location string for SNMP agents such as the NPort IA5000-G2. This string is usually set to the street address where the NPort IA5000-G2 is physically located.	N/A

When using SNMP v3, you need to create a V3 Account first. Click the **CREATE** button at V3 Account column.



The 'Create Account' dialog box contains the following fields and controls:

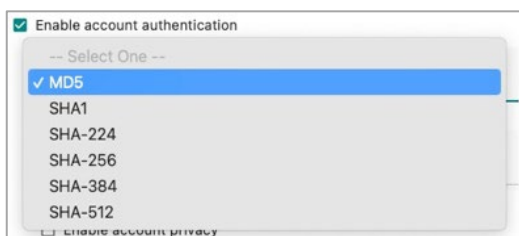
- Account Name:** A text input field.
- Authority:** A dropdown menu currently showing 'Read Only'.
- Enable account authentication:** A checked checkbox.
- Authentication Type:** A dropdown menu showing '-- Select One --'.
- Authentication Password:** A text input field with a toggle icon on the right.
- Enable account privacy:** A checked checkbox.
- Privacy Type:** A dropdown menu showing '-- Select One --'.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom right.

Account Name: Use this field to identify the username for the specified level of access.

Authority: Select authentication parameters for two levels of access: Read Only(default) and Read/Write.

When enabling account authentication, select the Authentication Type and input the Authentication Password.

Authentication Type: Use this field to select MD5 or SHA as the method of password encryption.

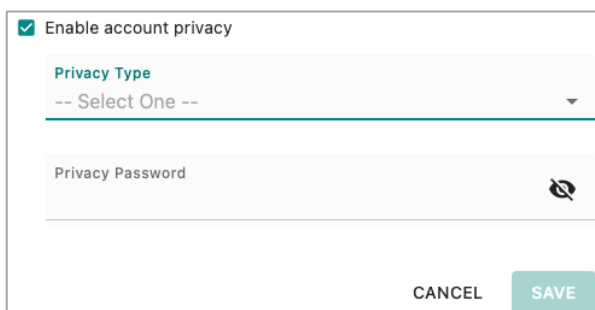


This image shows the 'Authentication Type' dropdown menu expanded. The options listed are:

- Select One --
- ✓ MD5
- SHA1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Authentication Password: Use this field to set the password.

When enabling account privacy, select the Privacy Type and input the Privacy Password.



This image shows the 'Privacy' section of the 'Create Account' dialog box:

- Enable account privacy:** A checked checkbox.
- Privacy Type:** A dropdown menu showing '-- Select One --'.
- Privacy Password:** A text input field with a toggle icon on the right.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom right.

Privacy Type: Use this field to enable DES_CBC or AES_128 data encryption when you enable account privacy.

Privacy Password: Use this field to set the password.

V3 Account
V3 Account Protection

To enhance the security of the v3 accounts, set the minimum password length for authentication and privacy passwords.

Min. Password Length
8

To prevent hackers from repeatedly logging into your account to crack passwords, you can enable v3 account protection and configure the settings accordingly.

☒ Enable v3 account protection

Max. Authentication Failure Retry(times)
5

☒ Enable reset login failure counter

The login failure counter will reset and be recalculated according to your designated reset period.

Reset Period(min)
10

Lockout Time (min)
5

SAVE

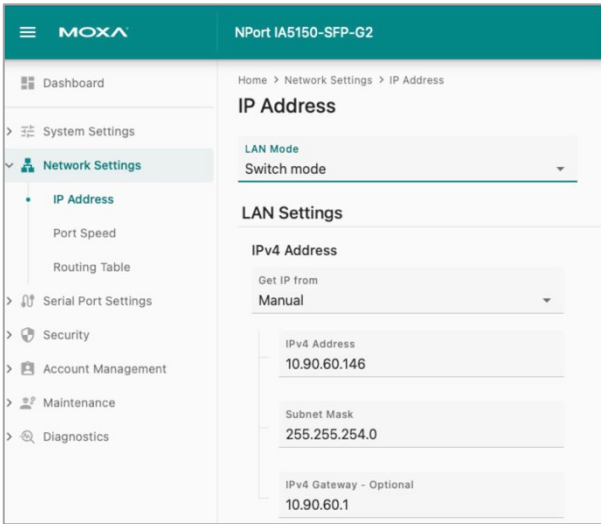
Click the V3 Account Protection to set the minimum password length for authentication and privacy passwords. Enable v3 account protection can set the maximum authentication failure times and lockout time. Additionally, you can enable the reset login failure counter to automatically reset and recalculate it within your designated reset period.

Network Settings

The second category of the Navigation Panel is Network Settings, which also includes three parts. The IP Address page is where you assign the NPort IA5000-G2 IP address, netmask, gateway, and other IP parameters. The Routing Table page allows you to configure the NPort IA5000-G2's connection to an external network. The Hosts & WINS page can make entering IP addresses on the NPort IA5000-G2 console easier by assigning a Host Name to an IP Address.

IP Address

A network device will need an IP address to communicate with other network devices. The IP address should have already been set up during the first-time login process. When accessing the Network Settings category, you may want to configure the advanced settings or change the existing IP address.



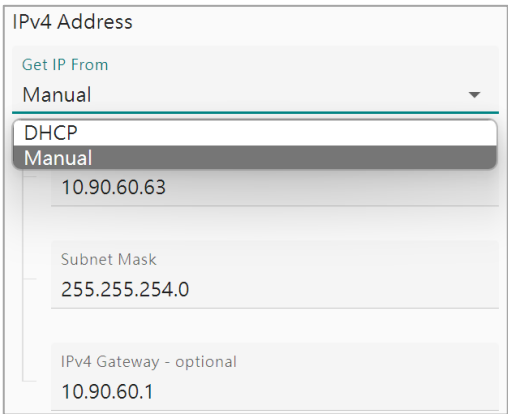
LAN Mode



Setting	Description
Switch mode	The default mode of LAN mode. The 2 Ethernet ports will share 1 IP address and work as a switch device.
Dual IP	The 2 Ethernet ports will use 2 different IP addresses in 2 different subnets, and 2 ports will active simultaneously. User can establish 2 independent networks for network redundancy with this Dual IP mode.
Redundant LAN	The 2 Ethernet ports will use 2 different IP addresses in same subnet, and the 2 ports will only active 1 port. If the primary port fails, it will switch to the backup port to keep the communication work.

IPv4 Address

Get IP From: DHCP or Manual. If there is a DHCP server in the network assigns the IP address automatically, then select **DHCP**. If not, select **Manual** and input the IPv4 address, subnet mask, and IPv4 gateway.

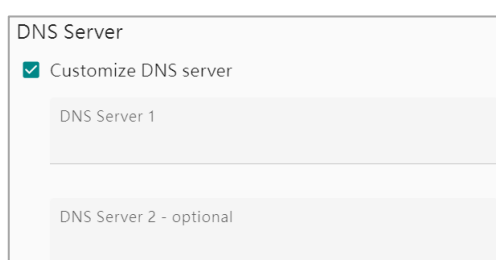


IPv4 Address (default=192.168.127.254): Enter the IP address that will be assigned to your NPort IA5000-G2. All ports on the NPort IA5000-G2 will share this IP address. An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment.

Subnet Mask (default=255.255.255.0): Enter the subnet mask. A subnet mask represents all the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort IA5000-G2 will use the subnet mask to check if the desired TCP/IP host specified in the packet is on the local network segment. If the address is on the same network segment as the NPort IA5000-G2, the NPort 6000 establishes a connection directly. Otherwise, the connection is established through the default gateway.

IPv4 Gateway: Enter the IP address of the gateway if applicable. A gateway is a network computer or device that acts as an entrance to another network. Usually, the devices that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort IA5000-G2 needs to know the IP address of the default gateway device to communicate with the hosts outside the local network environment. For correct gateway IP address information, consult the network administrator.

DNS Server



DNS Server

☒ Customize DNS server

DNS Server 1

DNS Server 2 - optional

Domain Name System (DNS) is responsible for translating internet domain names into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, which is easier to remember than the numerical IP address. A DNS server is a host that translates this kind of text-based domain name into the actual IP address used to establish a TCP/IP connection. When a user wishes to access a specific website, their computer sends the domain name (e.g., moxa.com) to a DNS server to obtain the website's IP address. The user's computer connects to the website's web server using the IP address obtained from the DNS server.


The NPort IA5000-G2 acts as a DNS client, actively querying the DNS server for domain name IP addresses. The following functions on the NPort IA5000-G2 web console support the use of domain names in place of IP addresses: Time Server, Destination IP Address (in TCP Client mode), Mail Server, SNMP Trap Server, Destination Address (in Pair Connection mode), Primary/Secondary Host Address (in Terminal mode), RADIUS Server, TACACS+ Server and SMTP Server.



DNS server 1: Choose Customize DNS server to enter the DNS server's IP address in this field. This allows the NPort IA5000-G2 to use domain names instead of IP addresses to access hosts.

DNS server 2: This is an optional field. The IP address of another DNS server can be entered in this field if DNS server 1 is unavailable.

Port Speed

If there is a legacy network device connects to the Ethernet port of the NPort IA5000-G2, user may need to configure the speed of the Ethernet port to be compatible with the device.

Click the  icon to modify the speed mode of each port.

Home > Network Settings > Port Speed		
Port Speed		
Overview		
Ethernet Port	Type	Speed Mode
LAN1	100 BASE-FX	100 Mbps full-duplex 
LAN2	100 BASE-TX	Auto-negotiation 

Setting	Description
Auto-negotiation	The default mode. The Ethernet port will negotiate with the device automatically to decide the speed this port will support.
100 Mbps full-duplex	User forces the Ethernet port to run with 100 Mbps with full-duplex mode.
10 Mbps full-duplex	User forces the Ethernet port to run with 10 Mbps with full-duplex mode.
100 Mbps half-duplex	User forces the Ethernet port to run with 100 Mbps with half-duplex mode.
10 Mbps half-duplex	User forces the Ethernet port to run with 10 Mbps with half-duplex mode.

Routing Table

If the NPort encounters an unknown IP address, it will check the routing table to determine the network interface for sending the Ethernet package. This is how network devices collaborate to ensure all Ethernet packets reach the target devices. The routing table in the NPort contains information about network routes and their associated metrics, for example, distances. The **routing table** also provides information about immediate network topology. You can configure the network connection for the NPort IA5000-G2 to an outside network. Edit the route settings and view the current routing status on this page.

Home > Network Settings > Routing Table

Routing Table

Edit the route settings and view the current routing status in the table below.

Refer to the definition of the flags.

Route Settings

EDIT

--

Refresh every 10 seconds ...

Destination	Subnet Mask	Gateway	Source Protocol	Flags	Metrics	Use	Interface
-------------	-------------	---------	-----------------	-------	---------	-----	-----------

To edit route settings, click the **EDIT** button.

Route Settings-Static

← Route Settings

Static

Dynamic

CREATE

No	Destination	Subnet Mask	Gateway	Metric	Interface
No data to display.					

In the static page, click the **CREAT** button to create a routing entry. You must provide information on the Destination, Subnet Mask, Gateway, Metric, and Interface.

Create Routing Entry

Create Routing Entry

Destination

Subnet Mask

Gateway

Metric

10

Interface

-- Select One --

CANCEL

SAVE

Destination: This is the target device's IP address of the route's destination.

Subnet Mask: This is the destination network's netmask.

Gateway: This is the IP address of the next-hop router.

Metric: You may use this optional field to enter the number of hops from the source to the destination. This allows the NPort IA5000-G2 to prioritize the routing of data packets if more than one router is available.

Interface: This is the network interface to which the packet must be sent. Select the Ethernet or serial port (Only for dial-in/out mode).

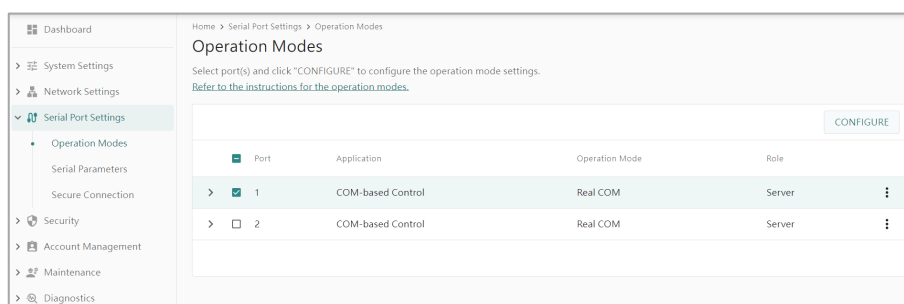
Serial Port Settings

The third section of the Navigation Panel is Serial Port Settings which is grouped into three categories: Operation Modes, Serial Parameters, and Secure Connection. To configure the operation mode and settings for a port, expand Serial Port Configurations in the navigation panel; then, expand the category that you would like to configure.

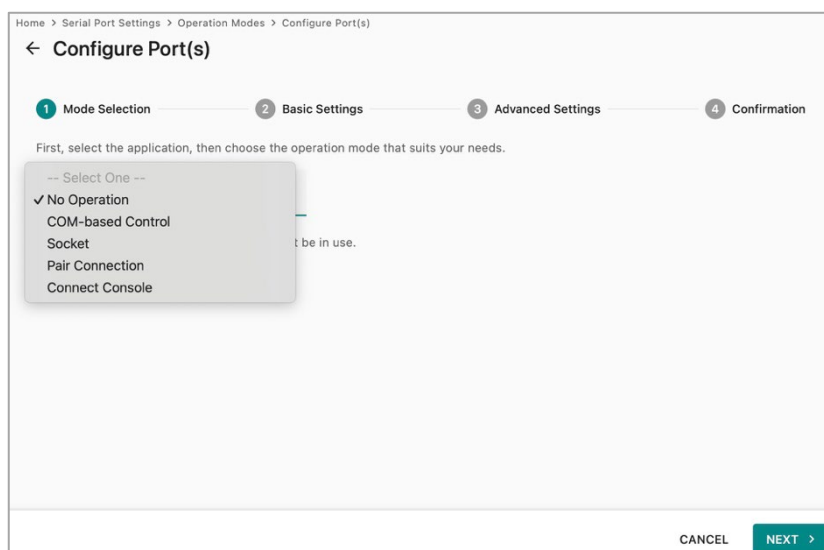
Operation Modes

NPort IA5000-G2 Series provides the capability to transfer the data from serial-to-Ethernet and vice versa. The setting of the Operation Modes sets the way how the data was packaged or how it is delivered on the Ethernet network. There are five popular applications: COM-based Control, Socket, Pair Connection, Connect Console and Connect Modem Application, They will be introduced one-by-one in the following sections.

- **COM-based Control:** For software using a COM port (Windows) or TTY port (Linux) to communicate with the serial device.
- **Socket:** For socket programs which communicate with NPort with IP address and TCP/UDP port.
- **Pair Connection:** To extend communication distance without changes to the host PC/HMI and serial device. This requires two NPort devices.
- **Connect Console:** For accessing a serial console via Telnet or SSH.



Select **Operation Modes** in the navigation panel to configure the mode for each serial port. For NPort IA5000-G2 models with two or more serial ports, use the checkboxes of the Port to apply the settings to one or more ports. Then, click the **CONFIGURE** button.



There is an Operation Mode Wizard to help you complete the settings. Select the application and operation mode as the first step. The next step involves configuring the basic settings for various scenarios. Set the advanced settings for a few scenarios during the third step. During the final step, go over all the settings mentioned earlier. If they're okay, confirm them and these settings will be activated immediately.

Application: Select an application for the serial port from among the choices. Your application will determine the modes that are available.

Operation Mode: Once you have chosen an application, select the operation mode. The configuration settings will vary depending on the mode that you have selected.

Application	Operation Mode	Description
No Operation	N/A	To decrease the risk of cyberattacks, select "No Operation" to disable the relative service if there are no serial devices connected to a specific port.
COM-based Control	Real COM mode	Installs the Moxa driver to simulate a real COM port over the network.
	RFC2217 mode	Installs a third-party driver to simulate a real COM port over the network.
Socket	TCP Server mode	Your application establishes a TCP connection to the NPort, providing access to connected serial devices.
	TCP Client mode	Your application listens to TCP connections from the NPort, providing access to connected serial devices.
	UDP mode	Your application sends and receives UDP packets for establishing communication with connected serial devices.
Pair Connection	Pair Connection Client mode	Connects to another NPort to enable two serial devices to communicate with each other.
	Pair Connection Server mode	Accepts connected NPort to enable two serial devices to communicate with each other.

Application	Operation Mode	Description
Connect Console	Reverse Terminal mode	Connects to a serial console server by connecting the NPort via Telnet/SSH.

COM-based Control Applications

The COM-based control application requires the installation of a Moxa or third-party driver to open a COM port (on Windows platform) or a TTY port (on Linux/UNIX-like platform) to start the communication with the remote serial devices. To keep the legacy software on the Windows or Linux/UNIX-like platform the same, Moxa provides the drivers on different operating systems. Please download them from Moxa website and refer to [Chapter 4 Mapping COM Ports](#), on how to use them.

Real COM Mode

Step 1. Mode Selection

Based on the scenario, select the application COM-based Control and Operation Mode Real COM. Then, click **NEXT** button to proceed to the next step.

Step 2. Basic Settings

In most scenarios, when configuring the Operation Mode to the Real COM mode, you have already completed the setup. Real COM mode does not have any basic settings. Click the **NEXT** button to go to Step 3.

Step 3. Advanced Settings—Connection Settings

In some scenarios, you may need to change the advanced settings to fulfill these special cases.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

✓ Mode Selection ✓ Basic Settings 3 Advanced Settings 4 Confirmation

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings Data Transmission Settings

Max. Connection
1

☒ Enable TCP alive check
Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)
7

☐ Enable port buffering
To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

< BACK CANCEL NEXT >

To communicate with multiple hosts on the NPort, enable **Max. Connection** and set the number to match the number of hosts. The NPort will now allow multiple hosts to connect at the same time. For example, let's suppose Host 1 is the primary computer, responsible for sending requests and receiving responses, while Host 2 is the backup computer, designated solely for receiving responses. Then, you should set the number to 2.

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings Data Transmission Settings

Max. Connection
2

Multiple Connections Settings

☐ Allow driver control
Enable NPort to accept commands from hosts to adjust the serial port settings.

Connection Process
Send serial data to all hosts

Congestion Handling
Wait until transmission succeeds

Max. connection (default=1): This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port of the NPort IA5000-G2, and the Real COM driver on that host will have full control over the port.

When the value is set to 2 or higher, multiple hosts' Real COM drivers can simultaneously open this port, up to the specified number. When several hosts' Real COM drivers open the port simultaneously, the COM driver only acts as a pure data tunnel and lacks control functionality. The serial port parameters will use firmware settings instead of depending on your application program (AP).

The firmware will only send data back to the driver on the host. When the data is received on the serial port and passed to the Ethernet side of the NPort, all the hosts will receive the same data. When the data is received on the Ethernet port and passed to the serial side of the NPort, the data will be sent first-in first-out.

If the situation described above doesn't match your site, there are several advanced functions at **Multiple Connection Settings** to do some modifications.

Allow driver control: As mentioned above, when **Max. connection** is set to 2 or higher, the serial port parameters will use firmware settings. If you want the serial parameters to still use the settings of your application program, enable the **Allow driver control** function. When you enable it, the serial port settings of your AP will overwrite the firmware settings while opening the COM port. Usually, you should only enable this function on one of the hosts. If you enable it on two or more hosts, then the serial parameters will be overwritten every time these hosts open the COM port.

To handle the unexpected data communication of multiple connections, there are different combinations for different scenarios.

Connection Control	Congestion Handling	Description
Send serial data to all hosts	-	This is the default data communication behavior for multiple connections. The serial data will be transmitted to the hosts. What happens if one host cannot receive the data?
	Wait until transmission succeeds	Wait until the host can receive data again. If the host cannot return, this option will store the serial data in the NPort's serial buffer as a side-effect. Once the serial data reaches 1,024 bytes, the buffer becomes full and can no longer receive data. Any new incoming data will be discarded.
	Keep sending data to other hosts	Ignore the abnormal host, keep sending data to other online hosts. The downside of this option is the communication seems OK when the user only checks the status on the succeed host(s). A mechanism might be necessary to alert the user when a host is unable to receive data.
Send serial data to the requested host	-	At times, the other hosts are unable to handle unrequested responses. In this scenario, choose to Send serial data to the requested host , ensuring that each host only receives the response specific to their request. What happens if the serial device fails to respond or responds too slowly in this situation?
	Discard	If the serial response times out, then the NPort will discard all the new incoming serial data before the NPort receives an Ethernet request.
	Send to the last request	If the serial response times out and new serial data arrives, the NPort will forward the data to the host that made the most recent request.
	Send to all open connections	If the serial response times out and new serial data is received, the NPort will distribute the data to all hosts that are still connected.
	Enable response timeout	To ensure smooth operation in this one-request-one-response application, you should specify the waiting time for the NPort to receive the serial response. The default timeout time is 10,000 ms. This value shall be less than the timeout time on user's AP. Make sure this value is smaller than the AP's timeout time. If not, this unusual situation could occur where AP identifies it as a timeout error, but the NPort is still waiting for a response.

☒ Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)

7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

Connection Settings Data Transmission Settings

☒ Enable port buffering
To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

Buffering Location
Memory (64K) ▼
Memory (64K)
SD card

If the port buffering is disabled, you may customize the RTS/DTR behaviors when TCP session is disconnected.

☒ RTS always on
☒ DTR always on

Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, you may enable the **Enable port buffering** function. The NPort can store serial data in its internal memory, which is 64 Kbytes.

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

RTS/DTR Behavior

If the port buffering is disabled, you may customize the RTS/DTR behaviors when TCP session is disconnected.

☒ RTS always on
☒ DTR always on

In a serial bus, the host and the serial device can use RTS/DTR signals to indicate their status to each other. Using the RTS/DTR Behavior function, the NPort can simulate the RTS/DTR behavior on Ethernet connections. When using legacy software, enable the RTS/DTR signal and keep it constantly on to prevent the host from entering sleep mode or shutting down. This will ensure the host is always ready for communication.

RTS/DTR Behavior (default=always on): Configures what happens to the RTS and DTR signals when the TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. If the serial devices detect the RTS or DTR is off, it may jump into sleeping mode or low-power mode. Then, it may take a while to come back from the sleeping/low-power mode, which will cause issues because the host PC will come back quicker. In this case, set the signal to always on.

When the Enable port buffering function is enabled, the RTS and DTS signals will be always be set to ON to keep the serial device sending data. This function may be disabled at the same time.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Mode Selection Basic Settings **3 Advanced Settings**

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
-- Select One --

☐ Delimiter (hex)
Allow the packaging and transmission of serial data until the specified force transmit time is met.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter (hex)**.

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
Delimiter (hex)

Delimiter 1
0x 0

Delimiter 2 - Optional
0x

Data Transmit Process

☒ **Default process**
Send data with delimiter characters.

☐ Delimiter + 1 byte
Send data with delimiter characters and following 1 byte.

☐ Delimiter + 2 bytes
Send data with delimiter characters and following 2 bytes.

☐ Strip delimiter
Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

- **Default process:** Data in the buffer and the delimiter(s) will be transmitted.
- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- **Strip delimiter:** Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.

☒ **Enable force transmit**
Allow the packaging and transmission of serial data until the specified force transmit time is met.

Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them effective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

✓ Mode Selection

✓ Basic Settings

✓ Advanced Settings

4 Confirmation

Selected Port: 1

Application: COM-based Control

Operation Mode: RealCOM

info

Confirm that Moxa driver has been installed. You may download it from the product page.
[Moxa official website](#)

Connection Settings

Max. Connection: 2

Allow driver control: Disabled

Connection Process: Send serial data to the requested host

Non-requested Data Handling: Discard

Response Timeout: Disabled

TCP Alive Check: Enabled

Check Time: 7 mins

Port Buffering: Enabled

Buffering Location: Memory (64K)

RTS Always On: Enabled

DTR Always On: Enabled

Data Transmission Settings

Data Packing: Disabled

Force Transmit: Disabled

← BACK

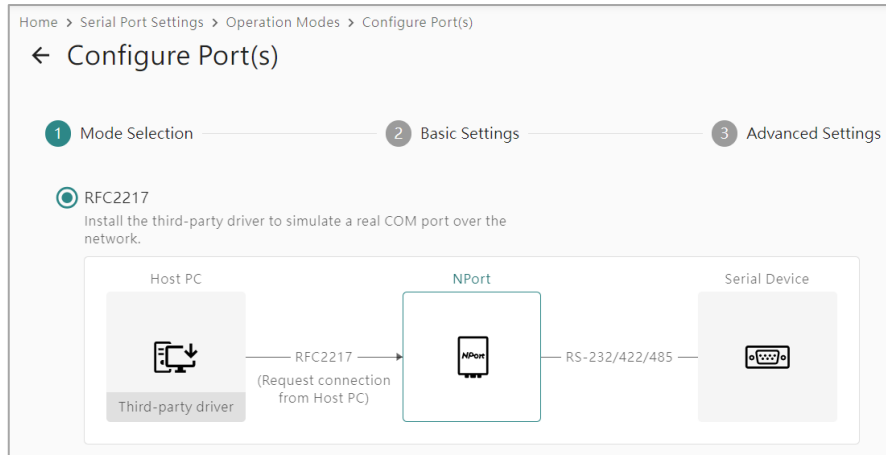
CANCEL SAVE

RFC2217 Mode

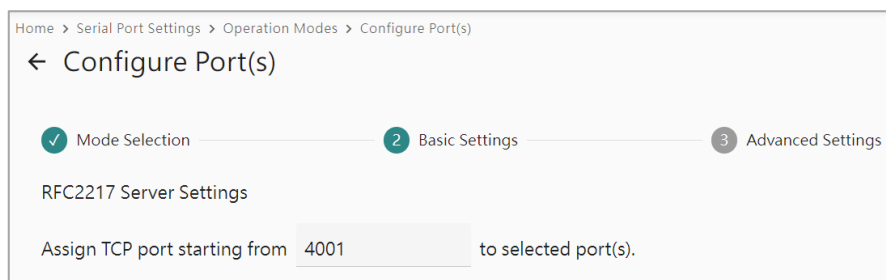
If you prefer a virtual COM driver or have different brands of serial device servers, install a third-party driver to communicate with the NPort and with all the other brands of device servers. In this case, please select the RFC2217 mode.

Step 1. Mode Selection

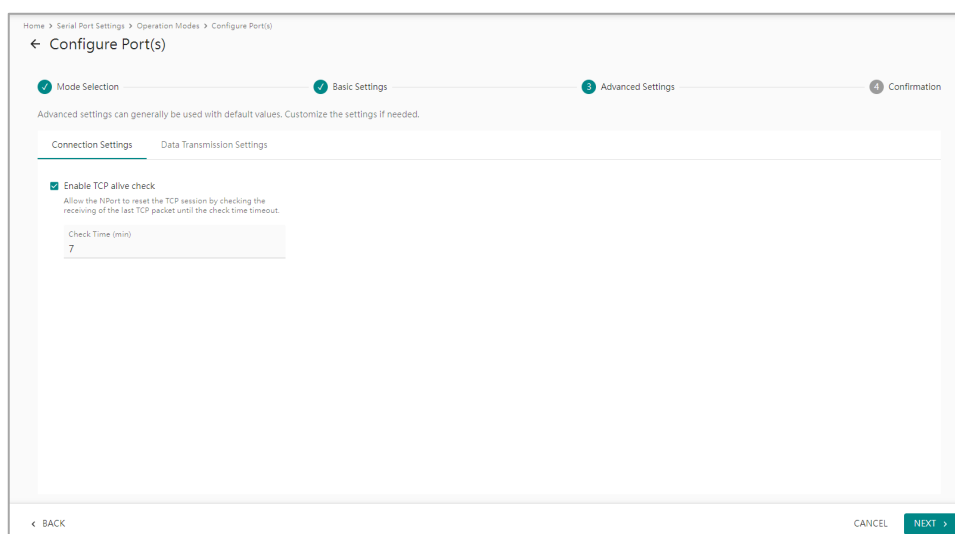
Select the COM-based control and select RFC2217 mode.



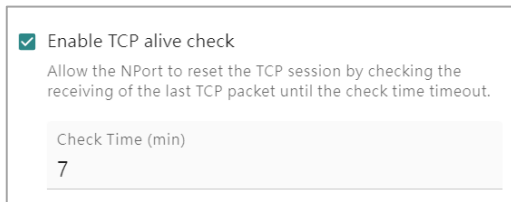
Step 2. Basic Settings



Assign TCP port starting from: This is the TCP port number assignment for the serial port on the NPort IA5000-G2. It is the port number that the serial port uses to listen. If more than two serial ports are configured as RFC2217 mode, the listen port will start from this assigned number (the first port will listen on TCP port 4001 and the second port will listen on TCP port 4002). For the host (or other network devices) this TCP port number is also the target TCP port for them to establish the TCP connection. To avoid conflicts with well-known TCP ports, set the default to 4001.



Step 3. Advanced Settings—Connection Settings



☒ Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)

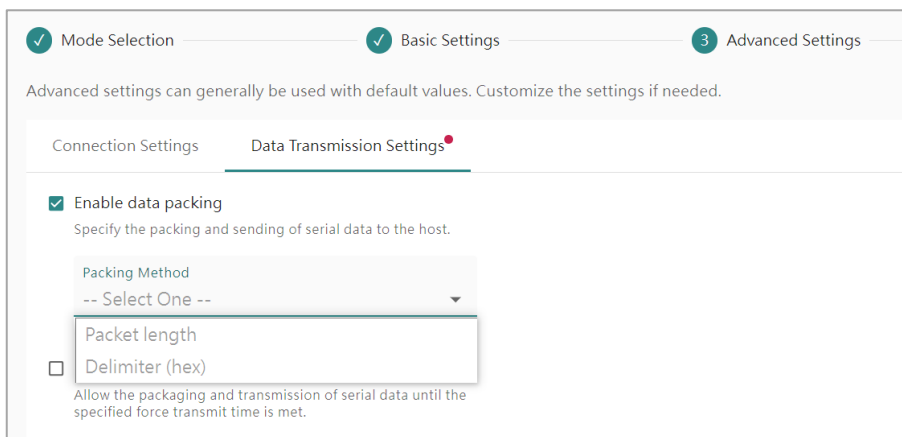
7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the Enable TCP alive check time function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.



Mode Selection Basic Settings 3 Advanced Settings

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings Data Transmission Settings

☒ Enable data packing

Specify the packing and sending of serial data to the host.

Packing Method

-- Select One --

Packet length

☐ Delimiter (hex)

Allow the packaging and transmission of serial data until the specified force transmit time is met.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter (hex)**.

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
Delimiter (hex) ▼

Delimiter 1
0x 0

Delimiter 2 - Optional
0x

Data Transmit Process

☒ **Default process**
Send data with delimiter characters.

☐ **Delimiter + 1 byte**
Send data with delimiter characters and following 1 byte.

☐ **Delimiter + 2 bytes**
Send data with delimiter characters and following 2 bytes.

☐ **Strip delimiter**
Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- **Strip delimiter:** Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field..

☒ **Enable force transmit**
Allow the packaging and transmission of serial data until the specified force transmit time is met.

Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them effective.

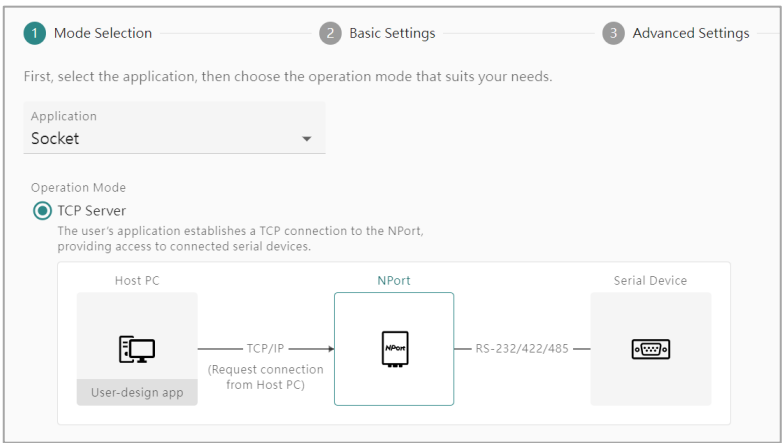
The screenshot shows the 'Configure Port(s)' window with the 'Confirmation' step selected. The progress bar at the top indicates four steps: 1. Mode Selection, 2. Basic Settings, 3. Advanced Settings, and 4. Confirmation. The 'Info' section states: 'Confirm that the third-party driver has been installed.' Below this, the 'RFC2217 Server Settings' are listed: 'TCP Port: 4001'. The 'Connection Settings' section shows 'TCP Alive Check: Enabled' and 'Check Time: 7 mins'. The 'Data Transmission Settings' section shows 'Data Packing: Disabled' and 'Force Transmit: Disabled'. At the bottom, there are 'BACK', 'CANCEL', and 'SAVE' buttons.

Socket Applications

The Socket application requires the user to have or create a socket program to establish the TCP session or send UDP packets to the destination NPort. Usually when the user wants to manage multiple brands of the network devices, he may have the resources to create or integrate a socket program to fulfill this need.

TCP Server Mode

If the user's program will initiate the TCP session actively, the NPort shall be a TCP Server to listen to a specific TCP port and wait for user's program to establish the TCP session. Please select **TCP Server** mode on NPort.



Step 1. Mode Selection

Select the **Socket** and select **TCP Server** mode.

The screenshot shows the 'Configure Port(s)' web interface. At the top, there is a breadcrumb trail: 'Home > Serial Port Settings > Operation Modes > Configure Port(s)'. Below this is a progress bar with four steps: 1. Mode Selection (active), 2. Basic Settings, 3. Advanced Settings, and 4. Confirmation. The main content area is titled 'TCP Port Settings'. It contains two input fields: 'Assign data port starting from' with the value '4001' and 'Assign command port starting from' with the value '966'. Both fields are followed by the text 'to selected port(s)'. At the bottom of the interface, there are three buttons: '< BACK', 'CANCEL', and 'NEXT >'.

Step 2. Basic Settings

Assign data port: This is the TCP port number assignment for the serial port on the NPort IA5000-G2. It is the port number that the serial port uses to listen to connections, and that other devices must use to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.

Assign command port: The Command port is the TCP port for listening to Moxa commands from the host. To prevent a TCP port conflict with other applications, the user can set the Command port to another port if needed.

The screenshot shows the 'Configure Port(s)' web interface, Step 2: Basic Settings. The progress bar at the top shows three steps: 1. Mode Selection, 2. Basic Settings (active), and 3. Advanced Settings. Below the progress bar, there is a note: 'Advanced settings can generally be used with default values. Customize the settings if needed.' There are two tabs: 'Connection Settings' (active) and 'Data Transmission Settings'. Under 'Connection Settings', there is a dropdown menu for 'Max. Connection' with the value '1'. Below this, there is a checkbox labeled 'Enable TCP alive check' which is checked. The text below the checkbox says: 'Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.' Below this text is a text input field for 'Check Time (min)' with the value '7'. At the bottom, there is a checkbox labeled 'Enable inactivity timeout' which is unchecked. The text below the checkbox says: 'If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.'

Step 3. Advanced Settings—Connection Settings

In some scenarios, the user may need to modify the advanced settings to fulfill his special cases.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

Mode Selection Basic Settings **Advanced Settings** Confirmation

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings Data Transmission Settings

Max. Connection
1

☒ Enable TCP alive check
Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)
7

☐ Enable port buffering
To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

< BACK CANCEL NEXT >

For those users who have more than one Hosts to communicate with the NPort, he will need to enable the Max. Connection by changing the number to the number of the Hosts. With this, the NPort will accept all these Hosts to connect simultaneously. For example, if Host 1 is the primary computer who will send requests and receive the responses and Host 2 is the backup computer to receive all the responses. The user shall set the number to 2.

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings Data Transmission Settings

Max. Connection
2

Multiple Connections Settings

☐ Allow driver control
Enable NPort to accept commands from hosts to adjust the serial port settings.

Connection Process
Send serial data to all hosts

Congestion Handling
Wait until transmission succeeds

Max. connection (default=1): This field is used if you need to receive data from different hosts simultaneously. When set to 1, only one specific host can access this port of the NPort IA5000-G2, and the Real COM driver on that host will have full control over the port.

When set to 2 or greater, up to the specified number of hosts' Real COM drivers may open this port at the same time. When multiple hosts' Real COM drivers open the port at the same time, the COM driver only provides a pure data tunnel—no control ability. The serial port parameters will use firmware settings instead of depending on your application program (AP).

The firmware will only send data back to the driver on the host. When the data is received on the serial port and passing to the Ethernet side of the NPort, all the Hosts will receive the same data. When the data is received on the Ethernet port and passing to the serial side of the NPort, the data will be sent first-in first-out.

If above scenario is not the case on your site, there are several advanced functions at **Multiple Connection Settings** to do some modifications.

Allow driver control: as mentioned above, when set **Max. connection** to 2 or greater, the serial port parameters will use firmware settings. If you want the serial parameters still use the settings of your application program, please enable the **Allow driver control** function. When you enable it, the serial port settings of your AP will overwrite the firmware settings while opening the COM port. Usually, you should only enable this function on one of the hosts. If you enable it on 2 or more hosts, then the serial parameters will be overwritten every time these hosts open the COM port.

To handle the unexpected data communication of multiple connections, there are different combinations for different scenarios.

Connection Control	Congestion Handling	Description
Send serial data to all hosts	-	This is the default data communication behavior for multiple connections, the serial data will be transmitted to all the hosts. What if there is one host cannot receive the data successfully?
	Wait until transmission succeeds	Just wait, until the host can receive data again. There is a side-effect on this option, if the host just cannot be back, the serial data will be stored on the serial buffer of the NPort. When the serial data is accumulated to 1,024 bytes, the serial buffer will full and cannot receive any data anymore. If there are new coming data, all of them will be dropped.
	Keep sending data to other hosts	Just ignored the abnormal host, keep sending data to other online hosts. The side-effect of this option is the communication seems OK when the user only checks the status on the succeed host(s). There may need a mechanism to notify the user there is an abnormal host cannot receive any data.
Send serial data to the requested host	-	Sometimes, the other hosts cannot handle the responses they don't request. For this case, please select Send serial data to the requested host then all the hosts will only receive the response based on their own request. For this scenario, what if the serial device doesn't respond the request or respond too late?
	Discard	If the serial response is timeout, then the NPort will discard all the new coming serial data before NPort receives an Ethernet request.
	Send to the last request	If the serial response is timeout and the NPort receives new coming serial data, it will send the data to the host who send the most recent request to NPort.
	Send to all open connections	If the serial response is timeout and the NPort receives new coming serial data, it will send the data to all the hosts who still connected to NPort.
	Enable response timeout	For this kind of one-request-one-response application, user may need to define how long time the NPort shall wait for the serial response? The default timeout time is 10,000 ms. This value shall be less than the timeout time on user's AP. Otherwise this abnormal scenario might happen, the AP consider it's a timeout error but NPort still waiting for a response.

☒ Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)

7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

☒ **Enable inactivity timeout**

If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.

Timeout Time (ms)

This setting is used for applications that may incur high costs for the connection between the remote host and the NPort, such as when it is connected with a cellular/satellite line. .

When the TCP session is established, the NPort will terminate the session actively if there is no new data for a while on the serial port. For the timing to terminate the TCP session, the user will need to set the Timeout time (ms) for this option.

☒ **Enable port buffering**

To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, you may enable the **Enable port buffering** function. The NPort can store serial data in its internal memory, which is 64 Kbytes.

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

RTS/DTR Behavior

If the port buffering is disabled, you may customize the RTS/DTR behaviors when TCP session is disconnected.

☒ RTS always on

☒ DTR always on

In a serial bus, the host and the serial device can use RTS/DTR signals to indicate their status to each other. Using the RTS/DTR Behavior function, the NPort can simulate the RTS/DTR behavior on Ethernet connections. When using legacy software, enable the RTS/DTR signal and keep it constantly on to prevent the host from entering sleep mode or shutting down. This will ensure the host is always ready for communication.

RTS/DTR Behavior (default=always on): Configures what happens to the RTS and DTR signals when the TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. This function may be disabled by enabling the Enable port buffering function.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. The software can receive the whole data by a simple "Read" command. When everything move to Ethernet based, it's another story. The Ethernet data might be separated to packets, and the receiver will assemble these packets to one complete frame to understand what the other device wants to transmit. But if it's a legacy serial software, it may not support the "assemble" function which is a basic function of a socket program. In this case, NPort provides Data Transmission function to deliver the correct frame at the beginning, then the legacy serial software doesn't need anything changed to read the correct data.

Mode Selection Basic Settings **3 Advanced Settings**

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
-- Select One --

☐ Delimiter (hex)

Allow the packaging and transmission of serial data until the specified force transmit time is met.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the dropdown menu Packing Method, select **Packet length** or **Delimiter (hex)**.

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
Delimiter (hex)

Delimiter 1
0x 0

Delimiter 2 - Optional
0x

Data Transmit Process

☒ **Default process**
Send data with delimiter characters.

☐ Delimiter + 1 byte
Send data with delimiter characters and following 1 byte.

☐ Delimiter + 2 bytes
Send data with delimiter characters and following 2 bytes.

☐ Strip delimiter
Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data then send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

- **Default process:** Data in the buffer and the delimiter(s) will be transmitted.
- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- **Strip delimiter:** Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.

☒ **Enable force transmit**
Allow the packaging and transmission of serial data until the specified force transmit time is met.

Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

Mode Selection

Basic Settings

Advanced Settings

Confirmation

Selected Port: 1

Application: Socket
Operation Mode: TCPServer

TCP Server Settings
Data Port: Start from 4001
Command Port: Start from 866

Connection Settings
Max. Connection: 1
TCP Alive Check: Enabled
Check Time: 7 mins
Inactivity Timeout: Disabled
Port Buffering: Enabled
Buffering Location: Memory (64K)
RTS Always On: Enabled
DTR Always On: Enabled

Data Transmission Settings
Data Packing: Disabled
Force Transmit: Disabled

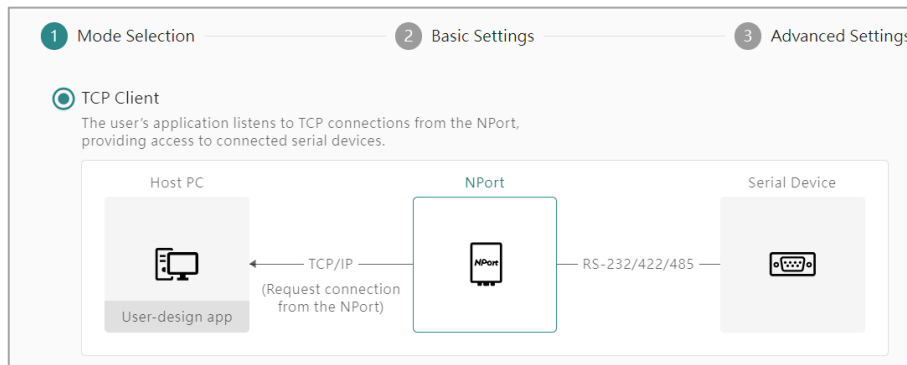
< BACK

CANCEL

SAVE

TCP Client Mode

When your program listens to a specific TCP port and wait for NPort to establish the TCP session. Please select **TCP Client** mode on the NPort.



Step 1. Mode Selection

Select the **Socket** and then **TCP Client** mode.

Step 2. Basic Settings

There are two types of the TCP Client application. If the serial device needs to connect to all the hosts (the TCP Servers) simultaneously, select **Connect to all servers**. Or, if the serial device will try to connect to all hosts but only needs to establish a connection with the first one, select **Connect to first available server**. With this setting, the NPort will connect the servers in the order they were entered.

Connect Method: Choose whether you want to **Connect to all servers** or **Connect to the first available server**.

Several parameters need to be set for each server:

Destination Address: Specifying an IP address allows the NPort IA5000-G2 to connect actively to the remote host. Provide the destination address for each server.

Assign the address port starting from: This is the TCP port number assignment on the remote host to listen to NPort's request. Please confirm that the port on the remote host matches the AP setting. The default port is set to 4001 to avoid conflicts with well-known TCP ports.

Assign local port starting from: Use these fields to specify the designated local port on the NPort.

ADD Server: Click **ADD Server** to add more remote servers for NPort to connect.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

Configure Port(s)

1 Mode Selection 2 Basic Settings 3 Advanced Settings 4 Confirmation

Advanced settings can generally be used with default values. Customize the settings if needed.

Connection Settings

Data Transmission Settings

When to Connect

Device starts up

When to Disconnect

Never

☒ Enable TCP alive check
 Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)

7

☒ Enable port buffering
 To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

Buffering Location

Memory (64K)

[< BACK](#)
[CANCEL](#)
[NEXT >](#)

Step 3. Advanced Settings—Connection Settings

For TCP Client mode, the NPort will start the TCP session. It's important to determine when the NPort shall start or end the session. Based on different scenarios, set the behavior on **When to Connect/ When to Disconnect** function.

When to Connect/Disconnect: This setting determines the parameters under which a TCP connection is established or disconnected. The following table provides the different options. In general, we provide both the Connect conditions and Disconnect conditions.

When to Connect	When to Disconnect	Description
Device starts up	Never	<p>This setting is used for those serial devices that may proactively update data and remain powered on at all times, so the NPort needs to start updating data as quickly as possible.</p> <p>The NPort will try to establish the TCP session when the firmware is ready. The NPort will not actively terminate the session once the TCP session is established. If the TCP session is disconnected by the remote host or by an accident, the NPort will try to reestablish it automatically.</p>
Receive any characters from serial	Never	<p>This setting is used for serial devices that may proactively update data, but they may not be powered at all the time or they may update data very frequently. Therefore, the NPort can wait until it receives new serial data, and then it starts to establish the TCP session.</p> <p>The NPort will try to establish the TCP session when it receives data on the serial port. The NPort will not actively terminate the session once it has established the TCP session. If the TCP session is disconnected by the remote host or by accident, the NPort will try to reestablish it automatically.</p>
	Reach the inactivity timeout time	<p>This setting is for applications that may incur high costs for the connection between the remote host and the NPort, such as when it is connected with a cellular/satellite line.</p> <p>The NPort will try to establish the TCP session when it receives data on the serial port. When the TCP session is established, the NPort will end the session actively if there is no new data for a while on the serial port.</p> <p>Set the Timeout time to determine when to end the TCP session.</p>

When to Connect	When to Disconnect	Description
DSR on	Never	This setting is used for serial devices that can notify the host of their readiness to update data by turning on the DTR signal. Once the NPort detects the DSR signal is on, it will establish the connection and be ready for serial data update. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will not terminate the session actively. If the TCP session is disconnected by the remote host or by accident, the NPort will try to reestablish it automatically.
	DSR off	This setting is used for those serial devices that can notify the host by changing the DTR signal to on when they are ready to update data. When the serial device finishes data update, it will also notify the host by changing the DTR signal to off. The NPort will try to establish the TCP session when it detects the DSR signal is on. When the TCP session is established, the NPort will only terminate the session actively when detecting the DSR signal is off.
DCD on	Never	This setting is used for serial devices that can notify the host of their readiness to update data by turning on the DCD signal. So, when the NPort detects the DCD signal is on, it shall establish the connection and be ready for serial data update. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will not terminate the session actively. If the TCP session is disconnected by the remote host or by accident, the NPort will try to reestablish it automatically.
	DCD off	This setting is used for those serial devices that can notify the host by changing the DCD signal to on when they are ready to update data. When the serial device finishes the data update, it will also notify the host by changing the DCD signal to off. The NPort will try to establish the TCP session when it detects the DCD signal is on. When the TCP session is established, the NPort will only terminate the session actively when detecting the DCD signal is off.

☒ Enable TCP alive check

Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)

7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

☒ Enable port buffering

To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.

Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, user can enable the **Enable port buffering** function. The NPort can store serial data in its internal memory, which is 64 Kbytes.

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

On a serial bus, the Host and the serial device may based on turning on/off the RTS/DTR signals to notify the serial device that the Host is alive or not, and vice versa. The NPort supports RTS/DTR Behavior function to simulate above behavior on the Ethernet connections. Some legacy software on the Host may switch to sleep mode or shutdown itself based on the RTS/DTR signal, when enable this function and keep these two signal always on, it can prevent this to happen and keep the Host is ready for communication.

RTS/DTR Behavior (default=always on): You can configure what happens to the RTS and DTR signals when TCP session is disconnected. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent via the serial port. This function may be disabled by enabling the Enable port buffering function.

Step 3. Advanced Settings—Data Transmission Settings

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the Enable data packing function..

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter (hex)**.

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When you specify a packet length between 1 and 1024 bytes, the data in the buffer will be sent as soon as it reaches the specified length.

Connection Settings **Data Transmission Settings**

☒ **Enable data packing**
Specify the packing and sending of serial data to the host.

Packing Method
Delimiter (hex) ▼

Delimiter 1
0x 0

Delimiter 2 - Optional
0x

Data Transmit Process

☒ **Default process**
Send data with delimiter characters.

☐ **Delimiter + 1 byte**
Send data with delimiter characters and following 1 byte.

☐ **Delimiter + 2 bytes**
Send data with delimiter characters and following 2 bytes.

☐ **Strip delimiter**
Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data. Then, send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two bytes will be transmitted after two additional bytes are received following the delimiter.
- **Strip delimiter:** Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.

☒ **Enable force transmit**
Allow the packaging and transmission of serial data until the specified force transmit time is met.

Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them effective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

1 Mode Selection 2 Basic Settings 3 Advanced Settings 4 Confirmation

Selected Port: 1

Application: Socket

Operation Mode: TCPClient

Remote Server Settings

Connect Method: Connect to all servers

Server 1

Destination Address: 10.0.0.10

Address Port: Start from 4001

Designated Port: Start from 5010

Connection Settings

When to Connect: Device starts up

When to Disconnect: Never

TCP Alive Check: Enabled

Check Time: 7 mins

Port Buffering: Enabled

Buffering Location: Memory (64K)

Data Transmission Settings

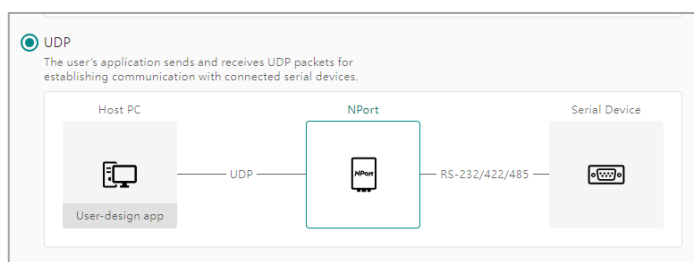
Data Packing: Disabled

Force Transmit: Disabled

← BACK CANCEL SAVE

UDP Mode

If your application requires faster data arrival at the device without the need for guaranteed data reception, then he may choose to use UDP packets for the application. For example, at the train station, the message displayed on the LCM could be missed because there are so many displays. If the passenger misses the message on one display, they can find it on the others. The train arrival message may be useless if it arrives on the display one minute after the train has already arrived. This is the typical application of the UDP mode.



Step 1. Mode Selection

Select the **Socket** and then **UDP** mode.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

1 Mode Selection 2 Basic Settings 3 Advanced Settings 4 Confirmation

Destination Address Settings Listen Port Settings

Destination Mode

Static destination

Specify the destination address to transmit data, and up to 4 sets of destination can be added.

Destination 1

Address Type

Single address

Destination Address

Assign the address port starting from 4001 to selected port(s).

+ ADD DESTINATION

← BACK CANCEL NEXT >

Step 2. Basic Settings

There are two types of UDP applications. The data may be sent to static destinations, or it may depend on different serial data going to different destinations.

Destination Mode	Address Type	Description
Static destination	Single address	This setting allows serial devices to proactively update data to specific remote hosts. You can input the target IP address and listen UDP port with this option.
	Address range (up to 16 addresses)	This setting allows users to proactively update data from serial devices to specific remote hosts. You can input a range of the IP addresses and listen UDP port with this option.
Dynamic learning	Learning by packet	This setting is used for the one- request, one-response scenario. The NPort will record the source IP address and UDP port as the destination IP address and UDP port when the NPort receives serial data. Every time the NPort receives an Ethernet request, it will update the destination IP address and UDP port.
	Learning when reaching the timeout	Until the timeout time is reached, the NPort will remove the old destination IP address and UDP port and update the information of the next UDP request to the table.

Destination Address Settings Listen Port Settings

Destination Mode
Static destination

Specify the destination address to transmit data, and up to 4 sets of destination can be added.

Destination 1

Address Type
Single address

Destination Address

Assign the address port starting from 4001 to selected port(s).

+ ADD DESTINATION

Destination Mode: Specify the way the determines the destination address to transmit data. There are two options, the **Static destination** or **Dynamic learning**. This snapshot shows the parameters for the Static destination.

The parameters for Destination 1 are:

Address Type: Specify **Single address** or **Address range (up to 16 addresses)** as the destination for communication.

Destination Address: Input unicast, multicast IP addresses or domain names as the destination address. At least one destination range must be provided.

Assign the address port starting from: This is the UDP port number assignment for the serial port on the NPort.

ADD DESTINATION: Click the button to add more destinations.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

Mode Selection (1) Basic Settings (2)

Destination Address Settings Listen Port Settings

Destination Mode
Dynamic learning

Learning Method
Learning by packet

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

Mode Selection (1) Basic Settings (2)

Destination Address Settings Listen Port Settings

Destination Mode
Dynamic learning

Learning Method
Learning when reaching the timeout

Timeout Time (ms)

Destination Mode: Specify the way the determines the destination address to transmit data. There are two options, the **Static destination** or **Dynamic learning**. This snapshot shows the parameters for the Dynamic learning.

Learning Method: Under **Dynamic learning** mode, the NPort will record the source IP address and UDP port from the UDP packet. Depends on different user scenarios:

- The different UDP hosts may send the requests frequently, and the NPort (also the serial device) needs to reply to every request. Select **Learning by packet**. With this setting, the NPort will update the Destination IP address and UDP port for each UDP packet, so all the UDP hosts can receive the expected results.
- The different UDP hosts may take turns to send requests and get responses. Only when one host has finished its turn for updating, the token will pass to the second host to start another turn for requesting/responding. Here, set **Learning when reaching the timeout** and a specific timeout time (ms) for the hosts to exchanging the token. The NPort can learn the new host's IP address and UDP port.

No matter which Destination Mode was selected, assign the local listen port at Listen Port Settings tab:

Mode Selection (1) Basic Settings (2) Advanced Settings (3)

Destination Address Settings Listen Port Settings

Assign the local listen port starting from 4001 to selected port(s).

Assign the local listen port from (default=4001): This is the UDP port that the NPort IA5000-G2 listens to and that other devices must use. To avoid conflicts with well-known UDP ports, the default is set to 4001.

Step 3. Advanced Settings

Mode Selection (1) Basic Settings (2) Advanced Settings (3)

Advanced settings can generally be used with default values. Customize the settings if needed.

Data Transmission Settings

☒ Enable data packing
Specify the packing and sending of serial data to the host.

Packing Method
Packet length

Packet Length (Byte)

☐ Enable force transmit
Allow the packaging and transmission of serial data until the specified force transmit time is met.

When the serial data is transmitted on the serial bus, it's continuous data. A "Read" command allows the software to receive all of the data. When everything switches to Ethernet, it's a different story. Ethernet data can be divided into packets, which are then assembled by the receiver into a complete frame to interpret the transmission request from the other device. However, a legacy serial software might lack support for the fundamental "assemble" function found in socket programs. Here, the NPort enables the Data Transmission function to deliver the correct frame at the beginning, requiring no changes to the legacy serial software for reading accurate data.

Like a bar code reader, serial data has a fixed length, and the fixed length data is read at once. A second common application is a serial protocol with specific ending character(s), which makes it easier for the engineer to read the data. In these two scenarios, please enable the **Enable data packing** function.

Enable data packing: With the drop-down menu Packing Method, select **Packet length** or **Delimiter (hex)**.

Packet length (Byte): The packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.

Connection Settings Data Transmission Settings

☒ Enable data packing
Specify the packing and sending of serial data to the host.

Packing Method
Delimiter (hex) ▼

Delimiter 1
0x 0

Delimiter 2 - Optional
0x

Data Transmit Process

☒ Default process
Send data with delimiter characters.

☐ Delimiter + 1 byte
Send data with delimiter characters and following 1 byte.

☐ Delimiter + 2 bytes
Send data with delimiter characters and following 2 bytes.

☐ Strip delimiter
Send data without delimiter characters.

Delimiter (hex): The delimiter refers to the ending character(s) of data. When the specific character(s) is received, the NPort will execute the Data Transmit Process to handle the serial data then send it out on the Ethernet side.

Delimiter 1 and Delimiter 2: If Delimiter 1 is configured in hex format, the NPort will treat the designated character as the end character. If there are two ending characters, use Delimiter 2 and ensure they are received in the correct order (Delimiter 1 first, then Delimiter 2). The NPort will package all the data in the serial buffer and follow the Data Transmit Process to handle the delimiter(s) before transmitting the data to the Ethernet port.

Data Transmit Process: This field determines how to handle the serial data and the delimiter(s) when receiving the delimiter(s). If both Delimiters 1 and 2 are set up, the process will only occur when both characters are received in the correct order.

Default process: Data in the buffer and the delimiter(s) will be transmitted.

- **Delimiter+1 byte:** Data in the buffer and the delimiter(s) plus one byte will be transmitted after one additional byte is received following the delimiter(s).
- **Delimiter+2 bytes:** Data in the buffer and the delimiter(s) plus two byte will be transmitted after two additional bytes are received following the delimiter.
- **Strip delimiter:** Data in the buffer will be transmitted and the delimiter(s) will be dropped.

Some protocols, like Modbus, may separate different messages from the idle time between two messages. For this case, please enable the **Enable force transmit** function and input the idle time at the **Force Transmit Time (ms)** field.

☒ Enable force transmit

Allow the packaging and transmission of serial data until the specified force transmit time is met.

Force Transmit Time (ms)

Enable force transmit: The NPort will monitor the idle time between two characters. If the time is reached and there are no new characters being received, the NPort will package all the data in the serial buffer and then send it on the Ethernet side. The number of this field is between 1 and 65535.

Step 4. Confirmation

Please review and **SAVE** above settings to make them effective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

1 Mode Selection

2 Basic Settings

3 Advanced Settings

4 Confirmation

Selected Port: 1
 Application: Socket
 Operation Mode: UDP
 Destination Address Settings
 Destination Mode: Static destination
 Destination 1
 Address Type: Single address
 Destination Address: 10.0.0.5
 Address Port: Start from 4001
 Listen Port Settings
 Listen Port: 4001
 Data Transmission Settings
 Data Packing: Disabled
 Force Transmit: Disabled

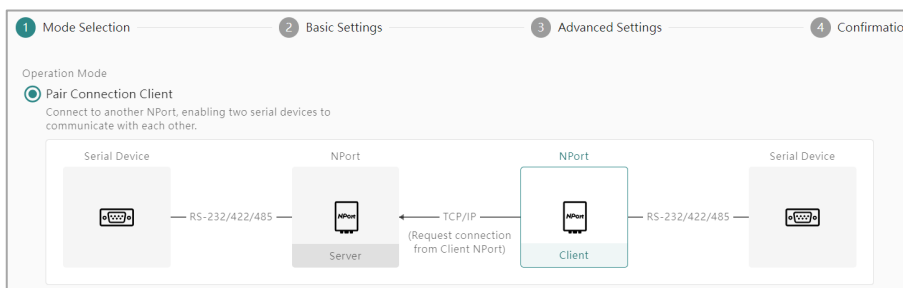
< BACK
 CANCEL
 SAVE

Pair Connection Applications

The Pair Connection application is designed for serial applications that keep the serial host and serial device. Here, the serial host cannot install any driver or socket program since it might not have Ethernet ports. But let's say the factory refurbishes, and the distance between the serial host and serial device increases significantly or maybe the network transitions to an Ethernet-based network. In this scenario, buying two NPorts with the Pair Connection application is a good fit.

Pair Connection Client Mode

With Pair Connection Application, set one NPort to Pair Connection Client mode to establish the connection and set the other NPort to Pair Connection Server mode to receive the request.



Step 1. Mode Selection

Select **Pair Connection** and **Pair Connection Client** mode.

The screenshot shows the 'Mode Selection' step of the NPort configuration. At the top, there are three tabs: '1 Mode Selection' (active), '2 Basic Settings', and '3 Advanced Settings'. Below the tabs, the section is titled 'NPort Server Settings'. It contains a text input field labeled 'Server Address'. Below this, there is a label 'Assign server port(s) starting from' followed by a text input field containing '4001', and then 'to selected port(s)'.

Step 2. Basic Settings

Server Address: The Pair Connection Client will try to establish the TCP session with this IP address. Input an IP address or a domain name.

Assign server port(s) starting from: This is the TCP port number assignment for the serial port on the NPort. It is the TCP port number on the remote NPort to listen to the request from the Pair Connection Client. To avoid conflicts with well-known TCP ports, set the default to 4001.

Step 3. Advanced Settings

The screenshot shows the 'Advanced Settings' step of the NPort configuration. At the top, there are three tabs: '1 Mode Selection', '2 Basic Settings', and '3 Advanced Settings' (active). Below the tabs, a note states: 'Advanced settings can generally be used with default values. Customize the settings if needed.' The section is titled 'Connection Settings'. It contains two checked checkboxes: 'Enable TCP alive check' and 'Enable port buffering'. Under 'Enable TCP alive check', there is a text input field for 'Check Time (min)' with the value '7'. Under 'Enable port buffering', there is a dropdown menu for 'Buffering Location' with the selected option 'Memory (64K)'. A descriptive note for port buffering is also present: 'To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.'

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

This is a close-up of the 'Enable port buffering' checkbox, which is checked. Below the checkbox, the text reads: 'To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.'

Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, you may enable the **Enable port buffering** function. The NPort can store serial data in its internal memory, which is 64 Kbytes.

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them effective.

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

1 Mode Selection

2 Basic Settings

3 Advanced Settings

4 Confirmation

Selected Port: 1

Application: Pair Connection

Operation Mode: PairConnectionClient

NPort Server Settings

Server Address: 10.0.0.1

Server Port: Start from 4001

Connection Settings

TCP Alive Check: Enabled

Check Time: 7 mins

Port Buffering: Enabled

Buffering Location: Memory (64K)

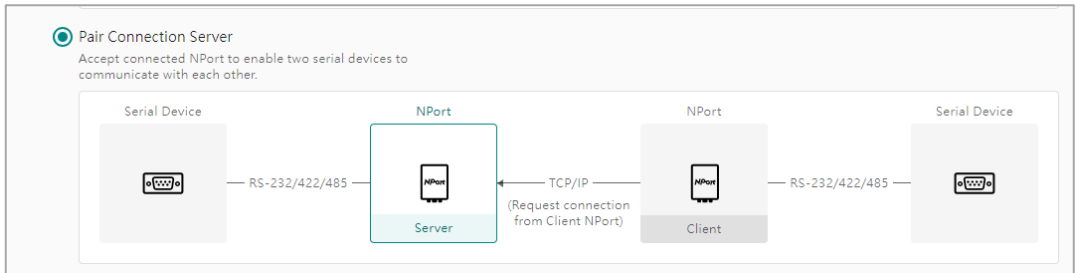
← BACK

CANCEL

SAVE

Pair Connection Server Mode

With Pair Connection Application, set one NPort to Pair Connection Client mode to establish the connection and set the other NPort to Pair Connection Server mode to receive the request.



Step 1. Mode Selection

Select the **Pair Connection** and **Pair Connection Server** mode.

1 Mode Selection

2 Basic Settings

3 Advanced Settings

Listen Port Settings

Assign TCP port starting from 4001 to selected port(s).

Step 2. Basic Settings

Assign TCP listen port starting from (default=4001): This is the TCP port that the NPort listens to, which shall match with the Pair Connection Client's setting. To avoid conflicts with well-known UDP ports, set the default to 4001.

The screenshot shows the 'Basic Settings' tab of the NPort configuration interface. At the top, there are three tabs: 'Mode Selection' (checked), 'Basic Settings' (active), and 'Advanced Settings' (3). Below the tabs, a note states: 'Advanced settings can generally be used with default values. Customize the settings if needed.' Under the 'Connection Settings' section, there are two checked options: 'Enable TCP alive check' and 'Enable port buffering'. The 'Enable TCP alive check' option has a description: 'Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.' Below this is a 'Check Time (min)' input field with the value '7'. The 'Enable port buffering' option has a description: 'To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.' Below this is a 'Buffering Location' dropdown menu with 'Memory (64K)' selected.

Step 3. Advanced Settings

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check** time function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

The screenshot shows a single checkbox labeled 'Enable port buffering' which is checked. Below the checkbox is a description: 'To prevent loss of serial data during an Ethernet disconnection, enable this function. Enabling port buffering means that RTS/DTR will always be set to on.'

Poor cable contact or a damaged switch/router could cause it to be disconnected or broken. When this happens, the serial data cannot transmit over Ethernet because the receiver does not exist. As time passes, the serial data could be discarded and lost. If the serial data is important, you may enable the **Enable port buffering** function. The NPort can store serial data in its internal memory, which is 64 Kbytes.

Enable port buffering (default=No): To prevent serial data loss when the Ethernet connection is down, check the checkbox to enable port buffering. If you enable port buffering, RTS/DTR will remain in the on position.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them effective.

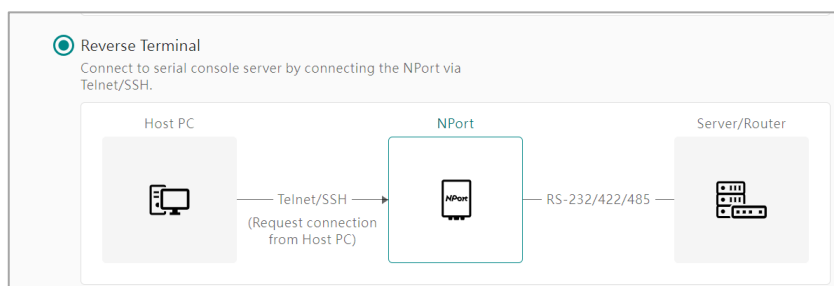
The screenshot shows the 'Configure Port(s)' web interface. At the top, there is a breadcrumb trail: Home > Serial Port Settings > Operation Modes > Configure Port(s). Below this is a progress bar with four steps: 1. Mode Selection (completed), 2. Basic Settings (completed), 3. Advanced Settings (completed), and 4. Confirmation (current step). The main content area displays the following settings: Selected Port: 1, Application: Pair Connection, Operation Mode: PairConnectionServer, Listen Port Settings (TCP Port: Start from 4001), Connection Settings (TCP Alive Check: Enabled, Check Time: 7 mins, Port Buffering: Enabled, Buffering Location: Memory (64K)). At the bottom, there are 'BACK', 'CANCEL', and 'SAVE' buttons.

Connect Console Applications

Use the Connect Console application to connect to the console port of a server or a router/switch. The NPort IA5000-G2 Series supports a Ethernet-based terminal connects to the NPort with Telnet or the SSH protocol, and the NPort connects to the serial console of the server. Select the Reverse Terminal mode.

Reverse Terminal Mode

When a PC needs to establish a connection with the serial console of a server, router, or network device, but lacks a serial port (or doesn't have enough). The user might want to connect the serial console to an NPort's serial port. The NPort can then listen on TCP port 22 or 23 for SSH or Telnet connections respectively, allowing a terminal software on the PC to connect and provide the service. The PC can still use the Ethernet based software (supports Telnet or SSH) to connect the serial console of a network device. It's not necessary to increase the number of serial ports on the PC.



Step 1. Mode Selection

Select the **Connect Console** and **Reverse Terminal** mode.

The screenshot shows the 'Mode Selection' screen, which is the first step in a three-step process. The other steps are 'Basic Settings' and 'Advanced Settings'. The screen is titled 'Reverse Terminal Settings' and instructs the user to 'Select the service and assign TCP port to the selected serial port to accept the connection from terminal application.' Under the 'Service' section, there are two radio button options: 'Reverse Telnet' (which is selected) and 'Reverse SSH'. At the bottom, there is a text input field for 'Assign TCP port starting from' with the value '4001' entered, followed by the text 'to selected port(s)'.

Step 2. Basic Settings

It depends on which protocol the terminal software on the PC supports (or which protocol you prefer to use to connect to the NPort) for choosing the Service

Service	Description
Reverse Telnet	If the PC supports Telnet protocol, then select Reverse Terminal mode on the NPort. The Telnet protocol or the Reverse Telnet mode of NPort is widely used for device management in control rooms. The system waits for a host on the network to start a connection. Since TCP Server mode does not assist with conversion of CR/LF commands, if the management of the serial console of the device requires these CR/LF commands, the user shall use Reverse Telnet mode.
Reverse SSH	Since the Telnet is a plaintext protocol, you may have cybersecurity concerns. In this case, select the Reverse SSH mode to encode the communication between the PC and the NPort.

Assign TCP port starting from (default=4001): This is the TCP port that the NPort listens to, which shall match with the TCP port of the terminal software such as PuTTY on the PC. To avoid conflicts with well-known UDP ports, set the default to 4001.

The screenshot shows the 'Advanced Settings' screen, which is the third step in a three-step process. The other steps are 'Mode Selection' and 'Basic Settings'. The screen has a title bar with two tabs: 'Connection Settings' (which is active) and 'Preference Settings'. Below the tabs, there is a note: 'Advanced settings can generally be used with default values. Customize the settings if needed.' Under the 'Connection Settings' tab, there are three checked checkboxes with their respective descriptions and input fields: 1. 'Enable TCP alive check' with a description 'Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.' and a 'Check Time (min)' input field with the value '7'. 2. 'Enable idle timeout' with a description 'If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.' and a 'Timeout Time (min)' input field. 3. 'Enable terminal authentication' with a description 'Enable to authenticate the connection based on system account privileges. The operation mode permission setting is in Account Management > Groups.'

Step 3. Advanced Settings—Connection Settings

☒ **Enable TCP alive check**
Allow the NPort to reset the TCP session by checking the receiving of the last TCP packet until the check time timeout.

Check Time (min)
7

Service providers always have limited resources. By enabling Real COM mode, the NPort allows access to connected serial devices. In the event of an accidental TCP connection failure, the resource could be indefinitely occupied until the you restart the NPort. To prevent this from happening, the NPort will enable the **Enable TCP alive check time** function by default to verify if the existing connection is alive or not. If the session is not active and the timeout period (default value of 7 minutes) is reached, the NPort will end the session and make it available for other users/devices.

Enable TCP alive check time (default=7 min): The duration for which the NPort IA5000-G2 waits for a response to keep-alive packets before closing the TCP connection can be specified in this field. To verify connection status, the NPort IA5000-G2 sends keep-alive packets at regular intervals. If the packet goes unanswered by the remote host within the specified time, the NPort IA5000-G2 will terminate the TCP connection.

☒ **Enable idle timeout**
If there is no data from or to the serial device within the specified timeout time, allow the termination of both data and command connections.

Timeout Time (min)

Since the resources of the remote server is limited, the NPort as the session initiator can terminate the session. The duration of no data transmission or reception on the serial port determines it.

Enable idle timeout: You can specify the number of minutes with no data being sent or received from the serial port, and then the NPort will actively terminate the Telnet session to release the remote server's resources to other terminals.

☒ **Enable terminal authentication**
Enable to authenticate the connection based on system account privileges. The operation mode permission setting is in Account Management > Groups .

The administrator can use the **Enable the terminal authentication** function to verify if the user has the privilege to connect to the serial port of NPort and access the server. The NPort authenticates users for serial port access based on either the local username/password database or the remote RADIUS/TACACS+ server. Only users in the read/write privilege user group can access it in operation mode.

Step 3. Advanced Settings—Preference Settings

End-of-line Character (default=CR-LF): This specifies how the ENTER key is mapped at the serial console of the network device. If the terminal software on the PC has the limitation of sending the ENTER key, for example, it will always send <CR> to represent the ENTER key. But the serial console of the network device can only accept <LF> as the ENTER key. This mismatch may cause problems while using the terminal software to manage the network device. To solve this issue, set the end-of-line character as LF, then every time NPort receives the <CR> from the terminal software that will automatically change it to <LF> and then pass it to the network device. Everything will then work smoothly.

End-of-line Character	Description
<CR-LF>	Officially <CR-LF> represents carriage return + line feed (i.e., the cursor will jump to the next line and return to the first character of the line). This is the formal definition of the ENTER key.
<CR>	Officially <CR> represents carriage return (i.e., the cursor will return to the first character of the line). For some operation systems, this also represents the ENTER key.
<LF>	Officially <LF> represents line feed (i.e., the cursor will jump to the next line, but not move horizontally). For some operation systems, this also represents the ENTER key.

Step 4. Confirmation

Please review and **SAVE** the above settings to make them affective.

No Operation

To address cybersecurity concerns, users can set a serial port to No Operation if it is not connected to any serial devices. Disabling unused services can decrease cybersecurity risks.

Serial Parameters

Matching serial parameters between the serial device and the NPort device server is an essential factor for communication. Refer to the device manual to obtain its serial parameters. Then, navigate to **Serial Port Settings > Serial Parameters** to modify the serial parameters.

Only if the NPort is configured as a **COM-based Control** application, you can skip this step/section. The COM port software or TTY software will overwrite the serial parameters while it opens a COM port/TTY port.

Select Serial Port Settings > Serial Parameters in the navigation panel to configure the parameters for each serial port. You may click on the button and select **EDIT** to change the serial parameters on a specific serial port. The Edit Port window will open to change the existing parameters.

<input type="checkbox"/> Port	Interface	Baudrate	Parity	Data Bits	Stop Bit(s)	Flow Control	
> <input type="checkbox"/> 1	RS-232	115200	None	8	1	None	⋮
> <input type="checkbox"/> 2	RS-232	115200	None	8	1	None	⋮

Edit
Assign port alias
Copy port settings

Edit Port 1

Interface

RS-232

Basic Settings

Baudrate (bps)

115200

Parity

None

Data Bits

8

Stop Bit(s)

1

Flow Control

None

Advanced Settings

☒ Enable FIFO

Enabling FIFO results in increased throughput for serial communication.

CANCEL

SAVE

If you want to change multiple serial ports simultaneously, select the checkboxes of the target ports and click the **CONFIGURE** button. The Configure Port window allows you to set new values for all selected ports by displaying empty parameter fields.

<input checked="" type="checkbox"/> Port	Interface	Baudrate	Parity	Data Bits	Stop Bit(s)	Flow Control	
> <input checked="" type="checkbox"/> 1	RS-232	115200	None	8	1	None	⋮
> <input checked="" type="checkbox"/> 2	RS-232	115200	None	8	1	None	⋮

CONFIGURE

Configure Port(S)

Selected Port: 1, 2

Interface

-- Select One --

Basic Settings

Baudrate (bps)

-- Select One --

Parity

-- Select One --

Data Bits

-- Select One --

Stop Bit(s)

-- Select One --

Flow Control

-- Select One --

CANCEL

SAVE

Basic Settings

Interface (default=RS-232): You may configure the serial interface to RS-232, RS-422, RS-485 2-wire, or RS-485 4-wire

Baudrate (bps) (default=115200): This field configures the port's baudrate. Select one of the standard baudrates from the drop-down box or select Other and input the specific baudrate of the serial device in the Value box.

Parity (default=None): This field configures the parity parameter.

Data Bits (default=8): This field configures the data bits parameter; 5, 6, 7, or 8 are supported.

Stop Bits (default=1): This field configures the stop bits parameter; 1 or 2 are supported.

Flow control (default=None): This field configures the flow control type, including RTS/CTS, DTR/DSR, Xon/Xoff, RTS Toggle and None. When set interface as RS-232, it supports all above flow control mechanisms. When set interface as RS-422, RS-485 2-wire or RS-485 4-wire, it only supports None and Xon/Xoff.

Advanced Settings

Advanced Settings

☒ Enable FIFO
Enabling FIFO results in increased throughput for serial communication. Disabling FIFO reduces latency.

Enable FIFO:

The Enable FIFO function is enabled by default for improved data throughput. There are two situations where the user may choose to disable the Enable FIFO function by unchecking the checkbox.

- If the serial device does not have FIFO/buffer or does not support the flow control function. In this case, the serial device may not receive the serial data from the NPort on time, which means that some data might be dropped.
- If the data latency is more important than data throughput. To achieve higher data throughput, data can be temporarily stored in the buffer, allowing for larger amounts of data to be sent at once. The downside is that the latency of a single data may be slower. If the latency is important for the serial device to read data correctly, then you should consider disabling the Enable FIFO function.

This field enables or disables the 512-byte FIFO buffer. The NPort IA5000-G2 provides FIFO buffers for each serial port, for both the Tx and Rx signals.

☐ Enable terminator (120 Ω)
For RS-422/485, especially for long distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.

Resistor ⓘ
150 K Ω

When configuring the interface as RS-422, RS-485 2-wire, or RS-485 4-wire, you can choose to enable the terminator (120 Ω) and set the resistor. Because these interfaces can handle communication distances of over 1 km and accommodate more than 10 serial devices on the same bus, there are more factors that need to be taken into account.

Enable terminator (120 Ω): For RS-422/485, especially for long-distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.

Resistor: If the remote devices are unable to receive data correctly for RS-422/485, try adjusting the pull high/low resistors which can strengthen the serial signal, and it might help on this. Two values are selectable, 1 K Ω or 150 K Ω .

Secure Connection

To face the increasing cybersecurity threats, user may want to consider how you can protect important data on the serial device. The communication distance on the serial bus is short and hard to steal (usually in a factory with a security guard). When using a device server to pass the serial data to an Ethernet network, it is another story. An Ethernet network is more vulnerable than a serial bus. The NPort device server provides the ability to communications on the Ethernet network.

Select **Serial Port Settings > Secure Connection** in the navigation panel to configure the **TCP Connection Type** for each serial port. You can also select multiple serial ports and click the **CONFIGURE** button to change them simultaneously.

Dashboard

Home > Serial Port Settings > Secure Connection

Secure Connection

Secure connection supports Real COM, Reverse Real COM, TCP Server, TCP Client, and Pair Connection modes in TCP connection. Configure the TCP connection type as needed.
[Refer to the cipher suites for an encrypted connection.](#)

TCP Connection Type Remote Device Certificate

Select port(s) and click "CONFIGURE" to configure the TCP connection type.

CONFIGURE

<input type="checkbox"/> Port	Application	Operation Mode	TCP Connection Type
<input type="checkbox"/> 1	COM-based Control	Real COM	Unencrypted connection
<input type="checkbox"/> 2	COM-based Control	Real COM	Unencrypted connection

TCP Connection Type

Configure Port(S)

Info
If you set the port(s) as an encrypted and authenticated connection, upload the remote device certificate for authentication.

TCP Connection Type

☒ Unencrypted connection
☐ Encrypted connection
☐ Encrypted and authenticated connection

CANCEL SAVE

Option	Description
Unencrypted connection	Data sent through the Ethernet will not be encrypted. This is the default value.
Encrypted connection	Data sent through the Ethernet will be encrypted with TLS v1.2.
Encrypted and authenticated connection	Data sent through the Ethernet will be encrypted with TLS v1.2, and the connection will be authenticated by certificate before the connection is established. Please upload the certificate at Remote Device Certificate tab for authentication if you choose this type.

Remote Device Certificate

Dashboard

> System Settings

> Network Settings

> Serial Port Settings

- Operation Modes
- Serial Parameters
- Secure Connection

> Security

> Account Management

> Maintenance

> Diagnostics

Home > Serial Port Settings > Secure Connection

Secure Connection

Secure connection supports Real COM, Reverse Real COM, TCP Server, TCP Client, and Pair Connection modes in TCP connection. Configure the TCP connection type as needed.
[Refer to the cipher suites for an encrypted connection.](#)

TCP Connection Type Remote Device Certificate

The port(s) with encrypted and authenticated connections will verify the uploaded certificates.

UPLOAD

File Name	Issued to	Issued by	Status
No certificate to display. Click UPLOAD button to upload the certificate.			

Encrypting the TCP session safeguards the confidentiality of the serial data, but how can we ensure the authenticity of the network device being communicated with? It's possible that the server is fake and attempting to extract valuable data from the serial device. To avoid this, it is recommended to enable certificate-based authentication. The NPort will verify the user-uploaded certificate and request verification of the remote server's certificate before establishing a secure connection. Once both devices are confirmed as correct, they will establish an encrypted TCP session to safeguard the crucial serial data. To enable it, remember to select **TCP Connection Type** to **Encrypted and authenticated connection** and upload the certificate at **Remote Device Certificate** tab.

When switching to the **Remote Device Certificate** tab, click the **UPLOAD** button to upload your certificate for authentication.

Upload Certificate

Choose one or multiple certificates to upload. The number of certificates that can be uploaded is limited to 10.

Choose Files

No file chosen

CANCEL

UPLOAD

Security

With cyberattacks growing in number and sophistication, device server vendors are adding functions geared towards protecting sensitive business and personal information. All the relative functions are listed under the **Security** category.

Services

Based on different user scenarios, you may need different services to meet these requirements. Click **Security > Services** to enable/disable the services he needs or no need.

Home > Security > Services

Services

Set the software and hardware services by toggling the buttons or editing the options below.

Software Services

Web Console
TCP: Port 443

Serial Console
Command-Line Interface

SNMP Agent ⓘ
UDP: Port 161

MOXA Service ⓘ
RESTful API(TCP: Port 443), mDNS(UDP: Port 5353), LLDP.

Gratuitous ARP
Periodic to send gratuitous ARP ✎

Hardware Services

Beeper

Reset Button on Device

Only enable within 60s after booting [EDIT](#)

Software Services	Value	Default Value	Description
Web Console	Enable/Disable	Enable	This setting is to enable/disable the web console. To ensure security, the NPort IA5000-G2 device server only supports HTTPS console using TLS v1.2 or newer. The web console provides all the settings that the NPort IA5000-G2 supports. We don't recommend a user to disable it.
Serial Console	Enable/Disable	Enable	This setting is to enable/disable the serial console on the serial port 1 of the NPort 6150-G2/6250-G2. Log in the serial console while the device server is booting up to configure the network settings like the IP address. After setting the network settings, it is advisable to disable the serial console. This prevents accidental triggering of the console by the serial device during simultaneous boot-up.
SNMP Agent	Enable/Disable	Disable	This setting is to enable/disable the SNMP Agent service. If you want to use the SNMP protocol to monitor the status or change some configuration settings of the NPort IA5000-G2, enable the service. If your site doesn't match this scenario, please disable it.
Moxa Service	Enable/Disable	Enable	This setting is to enable/disable Moxa proprietary service. NPort Windows Driver Manager, DSU-G2, and MXStudio are based on this service to work. This software cannot be used when Moxa Service is disabled.
Gratuitous ARP	Enable/Disable	Disable	This setting is to enable/disable the Gratuitous ARP service. In some applications, you may need the NPort IA5000-G2 to send broadcast packets to update the ARP table on the server. If you enable this function and set the send period, the NPort IA5000-G2 will periodically send broadcast ARP packets at the specified time interval.

Gratuitous ARP
Periodic to send gratuitous ARP

When click the edit button  of Gratuitous ARP service, set the time for the ARP packets. The default value is 300 seconds.

Edit Periodic Time

Periodic Time (sec)
300

CANCEL SAVE

Hardware Services	Value	Default Value	Description
Beeper	Enable/Disable	Enable	This setting is to enable/disable the beeper of the device. You will hear the beeper when the device is ready after a power cycle. If you don't want to hear the sound, you may disable the service.
Reset Button on Device	Only enable within 60s after booting up/Always enable	Only enable within 60s after booting up	By default, the device disables the reset button after booting up for 60 seconds to prevent someone from accidentally pushing the button and resetting the device to its default settings.

Reset Button on Device
Only enable within 60s after booting
EDIT

The EDIT button in the Reset Button On Device service allows you to specify when the reset button should be enabled. Either the button is enabled for just one minute after the device boots up, or it stays enabled indefinitely.

Reset Button On Device

Considering the possibility of an accidental operation, there are two modes for the reset button on device. You may set it according to your needs.

Mode

☒ Only enable within 60s after booting

☐ Always enable

CANCEL SAVE

Allowlist

An allowlist is a list of IP addresses or domains that are provided privileged access. Enabling this function limits the number of the IP addresses that can access the device server, which can prevent unauthorized access from an untrusted network.

Home > Security > Allowlist

Allowlist

Info

All communications are only allowed for the enabled IPs on the list after enabling this allowlist.

☐ Allowlist

ADD RULE

No.	IPv4 Address	Subnet Mask	Status
No data to display. Click ADD RULE button to create the first data.			

Before you enable Allowlist, add at least one rule on the table. And remember to make sure the host PC's IP address is on the list, or you may not access the web console of the device server.

Add IPv4 Rule

IPv4 Address

Subnet Mask

☒ Enable this rule

CANCEL SAVE

Click the ADD RULE button to add a new rule. You may fill an IP Address or a domain name in the IP Address column, and then input the subnet mask to allocate a range of IP addresses. We recommend you enable this function, so the new rules will be enabled while adding a new rule. If you don't want to enable it, remember to uncheck the checkbox **Enable this rule**.

Certificate

The NPort IA5000-G2 will automatically generate a self-certification for all the TLS sessions, including web console (HTTPS) and secure operation modes service.

If you have company generated or a third-party verified certification, click the MANAGE button to import the certification to mitigate the cybersecurity risks to the network.

Home > Security > Certificate

Certificate

The device automatically generates a certificate based on its IP address for system identification.
The user certificate can be imported to replace the system's default certificate.

System Certificate

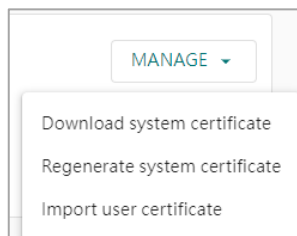
Valid

MANAGE

Issued to: 10.90.60.63
Issued by: 10.90.60.63
Start Time: 2024/8/6
Expiration Time: 2025/9/8

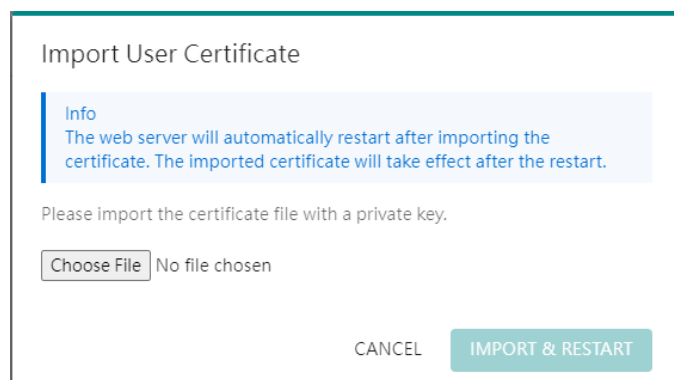
When access the **Security > Certificate** page, it shows the status of the system certificate:

- Is the system certificate still valid? Or has it expired?
- Who requested the system certificate?
- Who issued the system certificate? If it is a self-certification, the IP address will be NPort's IP address.
- When was the system certificate issued?
- When will the system certificate expire?



When you click the MANAGE button, there are three actions:

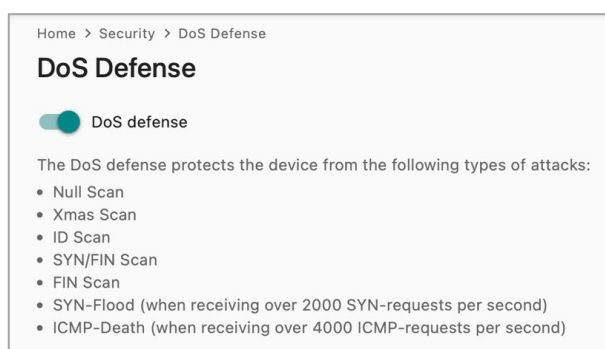
- **Download system certificate:** The browser or the software on a PC may request the target device to provide a valid certificate before establishing a secure connection. In this case, download the system certificate from the NPort, and then upload it to the browser or the software. Then the secure connection will be established.
- **Regenerate system certificate:** If the system certificate has expired or no longer secure, regenerate the system certificate for new secure connections.
- **Import user certificate:** If you have company generated or a third-party verified certification, import that certificate to the NPort to establish new secure connections.



When clicking the **MANAGE > Import user certificate**, click **Choose File** button to find the certification on the PC. Click the **IMPORT & RESTART** button to ensure the NPort will restart itself to use the imported certificate.

DoS Defense

To protect NPort IA5000-G2 from general DoS attack, it has DoS Defense function to identify the popular DoS attack types and to keep the normal function working. This function will be default enabled.



Login Settings

The NPort device server administrator may need to send messages to a user upon successful or failed login attempts. The administrator can edit related messages or functions here.

When you successfully log in to an NPort IA5000-G2 device server, the Login Message column will be shown. The message input by the administrator can be up to 256 characters long.

To communicate with users who couldn't login, the administrator can opt for Customized message mode and enter the message in the Message Text column. When the mode is set to Default message, the NPort IA5000-G2 also offers a recommended message for the administrator to refer to.

To prevent hackers from repeatedly attempting to log in and crack passwords, we recommend you enable the Login Lockout function. It will be enabled on default.

Name	Value	Default Value	Description
Enable login failure lockout	Checked/uncheck	Checked	When checked, the Login Lockout function will be enabled.
Max. Failure Retry (times)	1 - 10	5	If the Login Lockout function is enabled, it sets the number of attempts a user has before being locked out. Let's say the value is 5, then five password attempts are allowed. Regardless of whether the password is right or wrong on the sixth attempt, access to the device will be denied.
Enable reset login failure counter	Checked/uncheck	Unchecked	If this function is enabled, the user can wait a bit and then retry logging in. If this feature is turned off, the only option is to contact the administrator and request an account unlock.
Lockout Time (min)	1 - 60	5	If the option to reset the login failure counter is turned on, it sets the waiting time for the user before another login attempt.

Home > Security > Login Settings

Login Settings

Login Message Login Lockout **Session Control**

Max. Login User for HTTPS (count)

5

Session Timeout (min)

60

SAVE

For security and resource arrangement reasons, the NPort will limit the usage of the HTTPS sessions.

Name	Value	Default Value	Description
Max. Login User for HTTPS (count)	1 - 10	5	The number of users with different user accounts that can establish a HTTPS connection to the NPort.
Session Timeout (min)	1 - 1440	60	The time the NPort allows for inactivity when a user logs in before ending the HTTPS session.

Account Management

For security concerns, different users need different accounts and privileges on one device. With the Account Management function of the NPort IA5000-G2 Series, administrators can easily add, delete, or change user account names. They can also assign access to specific function categories based on different user groups. Furthermore, administrators can effectively manage passwords and login policies to ensure that only authorized users can use the device.

Accounts

In the NPort IA5000-G2 Series, the categories that you can access have a strong correlation with the user groups defined by the administrator(s) (for managing the groups, please refer to the next section, Groups). Administrators are allowed to add user accounts to the NPort IA5000-G2 device by clicking the Create button on the **Accounts** page.

Dashboard

> System Settings

> Network Settings

> Serial Port Settings

> Security

> **Account Management**

• Accounts

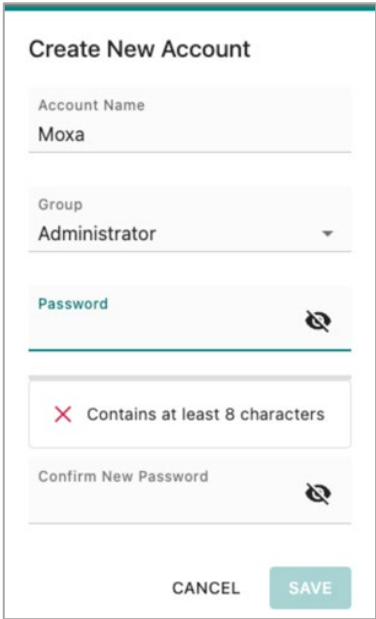
Home > Account Management > Accounts

Accounts

CREATE

Account Name	Group	Status	Date of Creation	
admin	Administrator	Active	2024-08-06	

The **Create New Account** window will pop up for you to input account information and assign a password to the user. Also, the Administrator(s) shall assign a proper **Group** to users to limit their privileges of using the NPort IA5000-G2. To add/delete/edit the **Group**, please go to the **Groups** section in the menu. The **Password** rules can be set up in **Password Policy** section.



The 'Create New Account' window contains the following fields and controls:

- Account Name:** A text input field with the value 'Moxa'.
- Group:** A dropdown menu with 'Administrator' selected.
- Password:** A text input field with a toggle icon to show/hide the password.
- Validation:** A message box indicating 'Contains at least 8 characters' with a red 'X' icon.
- Confirm New Password:** A text input field with a toggle icon to show/hide the password.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom.

You may also click more menu button on an existed user to edit the account’s above information/settings.)



admin	Administrator	Active	2024-08-06	⋮
Users	Viewer	Active	2024-08-26	⋮

Change password

Change group

Deactivate

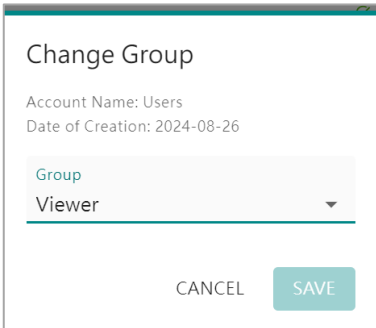
Delete

Change password

As an administrator, you can change every user’s password. The Change Password window will appear. Input the new password twice and **SAVE** the new password. The password will be changed.

As a general user, you can only change your password. Click the More menu button in your account name and select **Change password** so that the Change password window opens. Input the new password twice and **SAVE** the new password. The password will be changed.

Change group



The 'Change Group' window contains the following fields and controls:

- Account Name:** Displays 'Users'.
- Date of Creation:** Displays '2024-08-26'.
- Group:** A dropdown menu with 'Viewer' selected.
- Buttons:** 'CANCEL' and 'SAVE' buttons at the bottom.

Only the administrator can change the group of a user account. Click the More menu button in the target account name and select **Change group** to open the Change Group window. On te drop-down menu, select the group you want to move click the **SAVE** button. The user account will move to the new group.

Deactivate

Deactivate Account

Deactivating the account will result in the account being blocked from accessing the system.

Are you sure you want to deactivate the account "Users" ?

CANCELDEACTIVATE

Only the administrator deactivate a user account. When deactivating an user, the user account still exists on the NPort, but the user cannot log in to the device. Only when the administrator activates the user account can the user lock in. Click the More menu button on the target account name and select **Deactivate** to open the Deactivate Account window. Click the **DEACTIVATE** button and the user account will be deactivated.

Delete

Delete Account

Deleting the account will remove the account permanently from the system and revoke all access.

Are you sure you want to delete the account "Users" ?

CANCELDELETE

Only the administrator can delete a user account. When deleting a user account, it will be removed from the NPort. Click the More menu button on the target account name and select **Delete** to open the Delete Account window. Click the **DELETE** button to delete the user account.

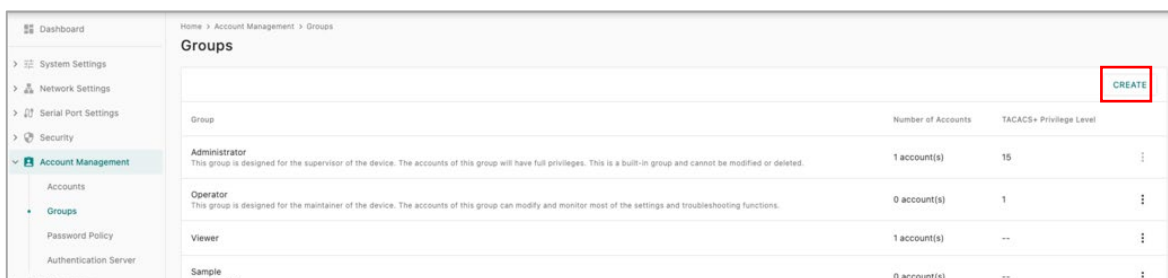
Groups

Users can access different function categories with the NPort IA5000-G2 based on their group affiliation. Customizing access permissions for different groups is restricted to the group administrator by default, or any group which is granted with Read/Write permission on Account Management category.

A maximum of four user groups can be created, with up to four user accounts per group. By default, the NPort IA5000-G2 has the Administrator, Operator, and Viewer user groups built in.

- The Administrator group cannot be removed, and the name cannot be changed.
- The Operator group can be removed, and the name can be changed.
- The Viewer group cannot be removed , but the name can be changed.

Clicking the Create button on the Groups page to create a new group.



Group Name: The name of the group user is going to create. You need to give the group name. When the NPort enables a central account management mechanism with RADIUS, the group name shall match the Filter-ID parameter on the RADIUS server.

Group Description – Optional: Describe the group to understand the purpose for creating this group. For example, creating a group named "Operator" with the description: "This group is designed for the maintenance of the device. The accounts of this group can change and monitor most of the settings and troubleshooting functions." This is an optional column.

Operation Mode Permission: When the serial port(s) is configured with these operation modes—Terminal, Reverse Terminal or Dial-in/out PPP mode—can check if the remote user has the necessary privilege to access the serial port. For these users, add them to a group that enabled this function.

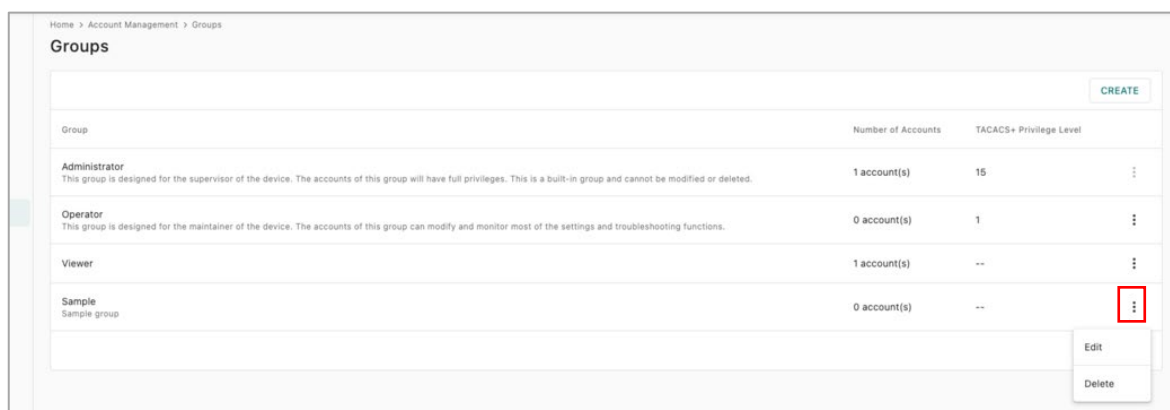
Console Permissions: Assign the privileges for different categories using the drop-down menu. There are three types of the permissions:

- **No Display:** The user in this user group will not see this function group when accessing the NPort IA5000-G2.
- **Read Only:** The user in this user group can only view the function/setting in this function group but cannot make modifications.
- **Read Write:** The user in this user group can view the function/setting in this function group and make modifications.

There are totally seven categories:

- **System Settings:** Includes all the settings for the NPort itself, like the server's name and notification.
- **Network Settings:** Includes all the settings related to the Ethernet port, like the IP address and subnet mask.
- **Serial Port Settings:** Includes all the settings related to the serial port, like the operation mode and serial parameters.
- **Security:** Includes all the settings related to cybersecurity, like the allowlist and login settings.
- **Account Management:** Includes all the settings related to account and group, like create/modify/delete an account or group.
- **Maintenance:** Includes all the settings related to routine maintenance jobs, like firmware upgrade and configuration import/export.
- **Diagnostics:** Includes all the functions which help the user troubleshoot, like device status and traffic monitoring.

Click the More menu button on an existing group to edit its access privilege or delete the group.



Password Policy

With the PC platform becoming increasingly powerful, users worry about the risk of password brute-force attacks. The administrator can mitigate cybersecurity risk by enabling the Password Policy function to boost password complexity.

Home > Account Management > Password Policy

Password Policy

You have the option to enhance password security by selecting a minimum length and strength policy.

Min. Password Length
8

Password Strength Policy

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

You can enhance account security by setting a password lifetime. When an account reaches the lifetime threshold and a user logs in, the system will mandate password changes.

☒ Enable password lifetime

Password Lifetime (day)
90

SAVE

Parameter	Setting	Default	Description
Password minimum length	8 to 256 characters	8	Define the minimum length of the login password for NPort IA5000-G2.
At least one digit (0-9)	Enable/Disable	Disable	The password must contain at least one number (0 to 9) when enabling this parameter.
Mixed upper- and lowercase letters (A~Z, a~z)	Enable/Disable	Disable	The password must contain an upper- and a lowercase letter when enabling this parameter.
At least one special character (~!@#\$%^&*~+=`'(){}[];~<>.,?/)	Enable/Disable	Disable	The password must contain at least one special character when enabling this parameter.
Enable password lifetime	Enable/Disable	Enable	Enhancing account security by setting a password lifetime.
Password Lifetime (day)	1 to 180 days	90 days	Users can set a specific lifetime for their passwords, and receive system notifications to change them if the option is enabled.

On completion of the settings, click the **SAVE** button to save the changes and make them effective.

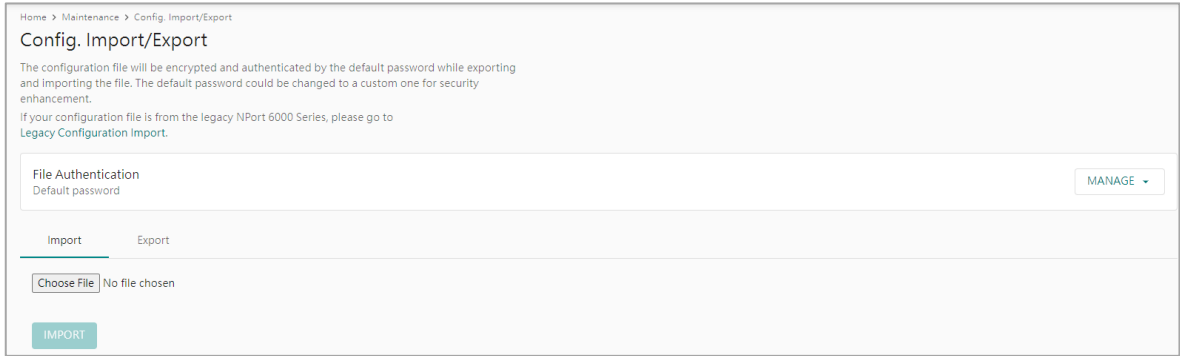
For setting related to failure logins, for example, to lock out an IP address after five failure password inputs, find the **Security > Login Settings > Login Lockout** section.

Maintenance

Operators may have to perform routine tasks every month or quarter to maintain the system when it is online. NPort categorizes these actions as Maintenance to simplify their completion for the user.

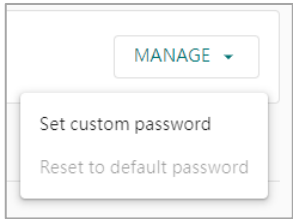
Config. Import/Export

You may want to back up the configuration settings of the NPort to access the **Maintenance > Config. Import/Export** to accomplish it.



File Authentication

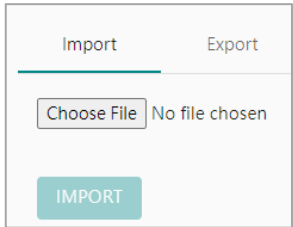
Because of security concerns, the NPort IA5000-G2 can no longer export a configuration file without a password. Click the MANAGE button to set a password for the exported configuration file.



When clicking the **Set custom password**, give a customized password for the exported configuration file. The NPort IA5000-G2 will use this password to decode the imported configuration file. The password policy for the configuration file allows for 8 to 64 characters and does not have any complex requirements.

When clicking the **Reset to default password**, the NPort IA5000-G2 will use the default password to encode or decode a configuration file.

Import/Export the Configuration File



At the **Import** tab, click the **Choose File** button to select the configuration file you want to import.

The screenshot shows a web interface with two tabs: 'Import' and 'Export'. The 'Export' tab is active. Below the tabs, a message states: 'The exported configuration file is not included:'. This is followed by a bulleted list:

- System log
- Certificate on the system
- Custom password of the file authentication
- Custom profile of the default setting

 At the bottom of this section is a teal button labeled 'EXPORT'.

At the **Export** tab, click the **EXPORT** button to select where you want to save the configuration file to.

Firmware Upgrade

It's highly advised to always upgrade to the latest firmware version due to the increasing number of cybersecurity threats. Consistently using the latest firmware helps reduce cybersecurity risks.

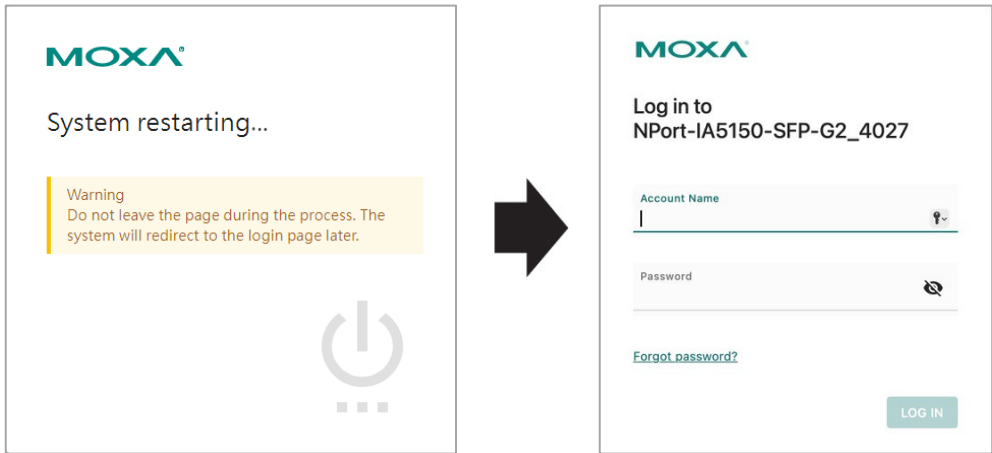
When you want to upgrade the firmware, click **Maintenance > Firmware Upgrade**, and click the **Choose File** button to find the firmware file. Click the **UPLOAD** button to proceed.

The screenshot shows the 'Firmware Upgrade' page. At the top is a breadcrumb: 'Home > Maintenance > Firmware Upgrade'. The title 'Firmware Upgrade' is prominent. Below it, the text reads: 'Current Firmware Version: v1.0.0 Build 24080808'. A paragraph follows: 'Choose the firmware file and upload it to the device. You can download the firmware file from the product page of [Moxa official website](#).' Below this is a 'Choose File' button next to the text 'No file chosen'. At the bottom left is a teal 'UPLOAD' button.

Ensure the device remains powered on and click the **UPLOAD & RESTART** button. The device will upgrade to the new firmware version and restart itself.

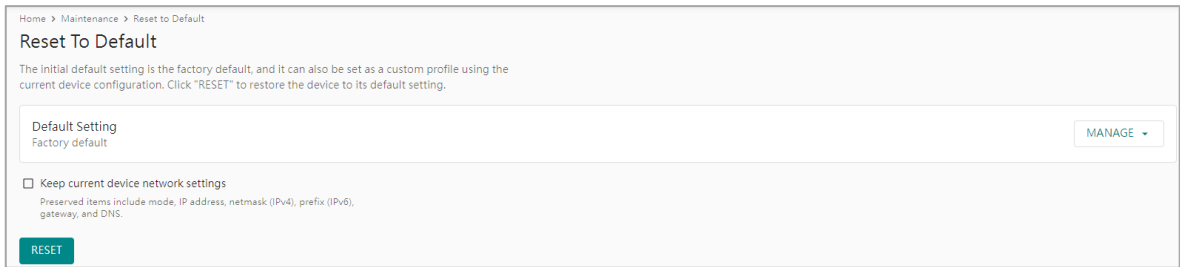
This screenshot shows the 'Firmware Upgrade' page after a file has been selected. The breadcrumb is 'Home > Maintenance > Firmware Upgrade'. The title is 'Firmware Upgrade'. The text now reads: 'Current Firmware Version: v1.0.0 Build 24081513'. The paragraph below is the same: 'Choose the firmware file and upload it to the device. You can download the firmware file from the product page of [Moxa official website](#).' The 'Choose File' button is now next to the filename 'nport6000g2_r...ld_24081513.bin'. The 'UPLOAD' button is now teal. A modal dialog box titled 'Upload File' is open in the bottom right. It contains the text: 'Please ensure that the device remains powered on during the process. The new firmware version will come into effect after restarting.' At the bottom of the dialog are two buttons: 'CANCEL' and 'UPLOAD & RESTART'.

When the login page appears, it means that the firmware upgrade process has been completed.

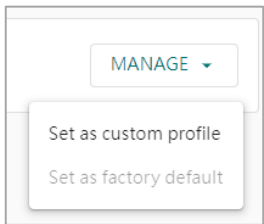


Reset to Default

This function will reset all the NPort IA5000-G2's settings to the factory default values. All previous settings, including the console password, will be lost. If you wish to keep the NPort IA5000-G2 IP address, netmask, and other network settings, make sure **Keep current device network settings** is checked before loading the factory defaults.

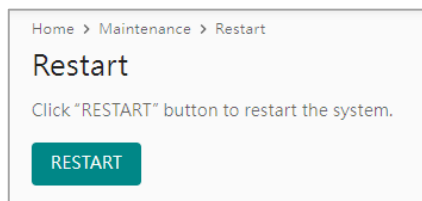


Machine builders or system integrators may have their preferred default values on the NPort. The NPort IA5000-G2 provides **Set as custom profile** function to allow users to set the settings as the default setting. In this case, when the customer triggers the Reset to Default function, the device will restore the custom default settings. The hardware reset button is the only way to reset it to the Moxa factory default. Clicking the **MANAGE** button and selecting the **Set as custom profile** will enable this function. The configuration file will be saved as default when the customer initiates a reset using the web console, DSU-G2, or MCC Tool.



Restart

If you want to restart the device, access **Maintenance > Restart** and click the **RESTART** button. The device will restart itself.



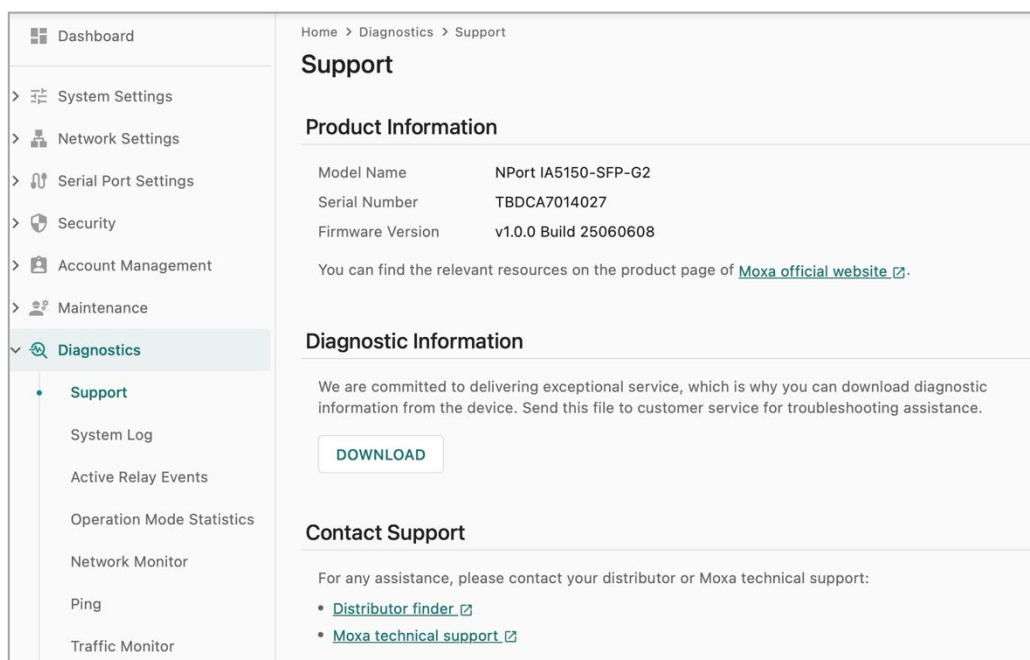
Diagnostics

System integrators and technical engineers may encounter issues when configuring a new application or receiving error reports during system operation. When that happens, you might find it helpful to have some diagnostic tools for troubleshooting.

In the Navigation Panel, the Diagnostics section brings together all the necessary functions for quick troubleshooting.

Support

If users need direct support from Moxa, they can find it on the Diagnostics à Support page. There, we provide a list of recommended information to collect before contacting Moxa, as well as contact information for seeking assistance.



Product Information

Find here the basic information of the NPort device server, including the Model Name, Serial Number, Firmware Version of the NPort IA5000-G2 device.

Diagnostic Information

Diagnostic Information

We are committed to delivering exceptional service, which is why you can download diagnostic information from the device. Send this file to customer service for troubleshooting assistance.

[DOWNLOAD](#)

Previously, users would typically reach out to Moxa customer service initially, and the engineer would then request additional information for problem analysis. For the NPort IA5000-G2 Series, we advise users to gather Diagnostic Information and send it along with their inquiry to Moxa customer service. This can make it simpler for the customer service engineer to pinpoint the root cause of the problem.

Download Diagnostic Information

Info

To maintain security, please delete the file after it has been sent to avoid any potential leaks of information.

By accepting this privacy announcement, you consent to the automatic collection of the following information:

- Model name
- Firmware version
- Serial number
- System uptime
- RTC time
- Log file
- Configuration file
- Monitor data (serial-to-network connection, serial port statistics, network connections, and network statistics)

If you agree, the data will be collected and made available in a file for download. The file is intended solely for troubleshooting assistance. For your security, please be aware that the file will be encrypted, and the device won't keep a copy after downloading.

☐ I consent to the collection of the data and understand its purpose.

[CANCEL](#) [DOWNLOAD](#)

The Download Diagnostic Information window will open and list what information on the NPort device server will be collected/downloaded. Click **DOWNLOAD** to save the data after providing your consent for collection. The diagnostic information is encrypted to ensure it is secure when delivered on the Internet and can only be unzipped by Moxa engineers for troubleshooting purposes. Access will not be granted with the password.

To verify this information, please use the NPort device server's web console.

Contact Support

Contact Support

For any assistance, please contact your distributor or Moxa technical support:

- [Distributor finder](#)
- [Moxa technical support](#)

After downloading the Diagnostic Information, you can find the contact window by clicking the **Distributor finder** or **Moxa technical support**, which will guide you to the corresponding resources on the official website.

System Log

It is very important to record the activities of a device. At the System Settings > Notification page, configure which events will be recorded. Under the **Diagnostics > System Log > Log View** tab, find the recorded events on the NPort device server. Under the **Log Settings** tab, set the advanced settings for the local system log.

Home > Diagnostics > System Log

System Log

Log View

Log Settings

FILTER

CLEAR

EXPORT

REFRESH

No	Severity	Category	Event Name	Timestamp
> 1	Informational	Security	Login success	2025-06-10 13:05:03
> 2	Warning	Security	Clear log	2025-06-10 09:28:11

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

An event will be recorded under these columns: Severity, Category, Event Name, and Timestamp. You may find more information at **System Settings > Notification** section. also, there is the event list in the appendix.

Home > Diagnostics > System Log

System Log

Log View

Log Settings

FILTER


CLEAR

EXPORT

REFRESH

No	Severity	Category	Event Name	Timestamp
1	Informational	Security	Login success	2024-09-20 14:56:12

Source: nport-pm 10.123.124.200
Message: A web user 'nport-pm' from 10.123.124.200 login the device successfully.

Click the arrow icon  to read more details about the event.


The NPort device server provides some management functions for you to easily read the events.


Home > Diagnostics > System Log

System Log

Log View Log Settings

▼ FILTER

 CLEAR

 EXPORT

REFRESH

No	Severity	Category	Event Name	Timestamp
> 1	Informational	Security	Login success	2024-09-16 15:02:51
> 2	Informational	Security	Login success	2024-09-16 11:23:59
> 3	Informational	Security	Login success	2024-09-12 10:12:59

FILTER: Filter the event by Severity, Category, Event Name, or Timestamp.

▼ Severity

Severity

+ Category

Event Name

Timestamp (Date)

APPLY

CLEAR: Delete all system logs on the device.

Clear System Log

This action is irreversible and will result in the deletion of all system logs on the device. Are you sure that you want to proceed?

CANCEL CLEAR

EXPORT: Export the system log for troubleshooting.

REFRESH: Refresh the logs on the panel.

Under the Log Settings tab, you will see the Current Log Capacity displayed as a percentage for reference. Since the events are stored on the local flash memory, there is a limitation on the number of events that can be saved. Click the **EDIT** button to manage the settings.

System Log

Log View Log Settings

Log Settings

✔ 50 enabled event(s)

Current Log Capacity: 3%

Log Capacity Policy: Overwrite the oldest log

EDIT

Events Settings

Log Capacity Settings

Events Settings

Select the events you will like to save in the local system log.

Home > Diagnostics > System Log > Events Settings

← Events Settings

Select the events you would like to save in the system log. The events can be sorted by severity.
[Refer to the details of the severity.](#)

Severity:

✓ Error

✓ Warning

✓ Notice

✓ Informational

SEARCH

System (16)

Network (7)

Security (23)

Maintenance (8)

Serial (8)

<div>Event Name</div>	<div>Severity</div>
<div><input checked="" type="checkbox"/> Firmware ready</div>	<div>Notice</div>
<div><input type="checkbox"/> Detect SD card</div>	<div>Informational</div>
<div><input checked="" type="checkbox"/> SD card removed</div>	<div>Warning</div>
<div><input checked="" type="checkbox"/> No SD card inserted</div>	<div>Error</div>
<div><input checked="" type="checkbox"/> User trigger reboot</div>	<div>Notice</div>

SAVE

Find more information in the **System Settings > Notification** section. Also, there is the event list in the appendix.

Log Capacity Settings

Home > Diagnostics > System Log > Log Capacity Settings

← Log Capacity Settings

Capacity Management

Current Log Capacity: 3%

The maximum number of system logs that can be stored on the device is 10,000. You may manage the log capacity by clearing all system logs.

CLEAR

Policy Settings

Please select the overwrite policy when the log capacity reaches its limit.

Overwrite Policy

☒ Overwrite the oldest log

☐ Stop recording the log

The system will notify or log the "log threshold reached" event according to the value set below.

Capacity Threshold (%)

80

SAVE

Capacity Management: The NPort IA5000-G2 provides 10,000 audit records. Click the CLEAR button to clear the local system log when it's getting full.

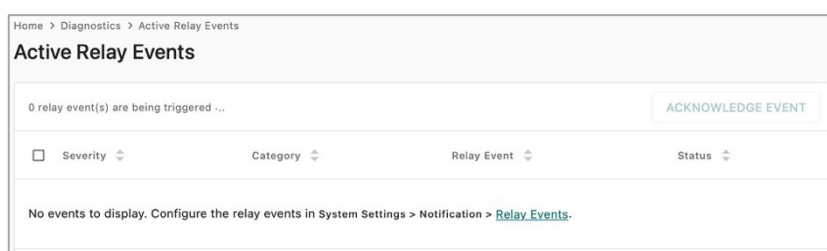
Policy Settings: When the log capacity reaches its limit, decide what action the NPort should take due to limited recording system log capacity.

- Overwrite the oldest event log
- Stop recording events

Capacity Threshold (%): The system will notify you or record an event "log threshold reached" when the log capacity reaches the value set here. The default value is 80.

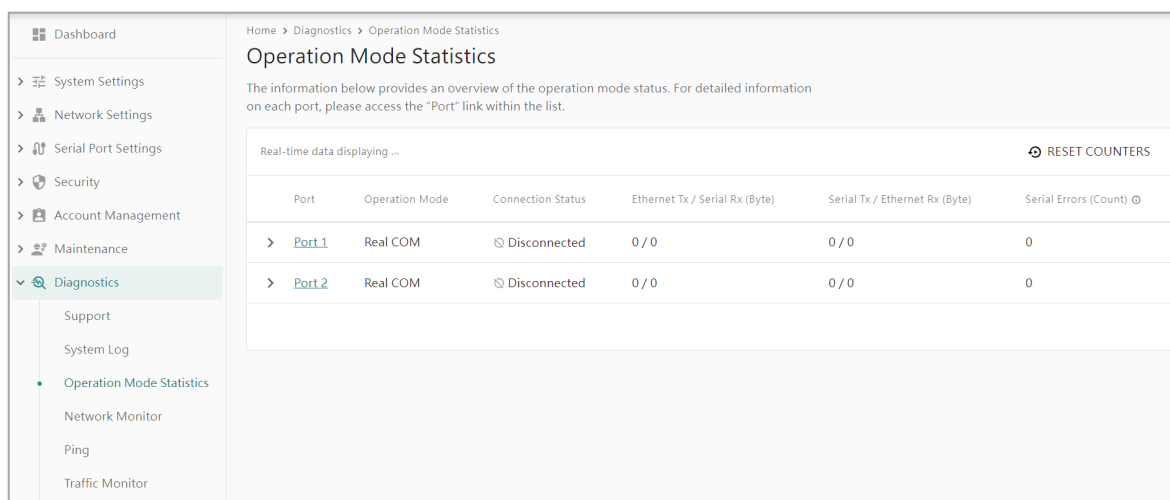
Active Relay Events

The NPort IA5000-G2 supports active relay to alert the operators that the device might have something wrong. User can configure what Relay Events need to be monitored/alerted. If the event happens, the operator can login to the NPort IA5000-G2 and click the **ACKNOWLEDGE EVENT** button to disable the relay after the situation is removed.



Operation Mode Statistics

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. Everything that happens on the serial interface will be recorded here, **Diagnostics > Operation Mode Statistics**, to help the user understand the serial data transmitted/received or the modem status changes.



- The Operation Mode Statistics contains the operation mode, connection status, the transmitted/received packets on Ethernet and serial connections, and the serial errors. The status or numbers for each port and column are shown here.
- Port: The serial port number of this NPort. When clicking the Port, there are more details.
- Operation Mode: The operation mode which is set a the specific serial port.
- Connection Status: Whether or not the Ethernet session is connected
- Ethernet Tx / Serial Rx (Byte): The Ethernet port and the serial port recorded a total of transmitted bytes and received bytes, respectively. Normally, these two numbers ought to match. If the Ethernet session disconnects, the number will reset.

- **Serial Tx / Ethernet Rx (Byte):** The serial port and the Ethernet port recorded a total of transmitted bytes and received bytes, respectively. Normally, these two numbers ought to match. If the Ethernet session disconnects, the number will reset.
- **Serial Errors (Count):** If the NPort detects an error in the received serial data (1 byte), for example, a frame error or parity error, it increments this column by 1.

Home > Diagnostics > Operation Mode Statistics > Port 1

← Port 1

Operation Mode: Real COM (Secure)

Serial Parameters

Serial Connections

Ethernet Connections

Real-time data displaying ...

Interface	RS-232
Baudrate	115200
Parity	None
Data Bits	8
Stop Bit(s)	1
Flow Control	None
FIFO	Enabled

When clicking a specific port number, the Port window will open with the information below.

Serial Parameters tab:

This tab displays the current settings of the serial parameters like the interface, baudrate, and so on.

Home > Diagnostics > Operation Mode Statistics > Port 1

← Port 1

Operation Mode: Real COM (Secure)

Serial Parameters

Serial Connections

Ethernet Connections

Real-time data displaying ...

Serial Total Tx ⓘ 746219520 byte(s)

Serial Total Rx ⓘ 746213992 byte(s)

Serial Statistics

Serial Tx (Byte) ⓘ	Serial Rx (Byte) ⓘ	Frame Error (Count)	Parity Error (Count)	Overrun Error (Count)	Break Error (Count)
0	0	0	0	0	0

Serial Signal

DSR	DTR	RTS	CTS	DCD
● Off	● On	● On	● Off	● Off

Serial Connections tab:

This tab displays the current statistics of the serial port:

- **Serial Total Tx:** The total amount of data transmitted on the serial port since the device was powered up. The number resets when performing a power cycle.
- **Serial Total Rx:** The total amount of data received on the serial port since the device was powered up.. The number resets when performing a power cycle.
- **Serial Tx (Byte):** The total amount of data transmitted on the serial port since the TCP session is connected. The number resets when the TCP session disconnects.
- **Serial Rx (Byte):** The total amount of data received on the serial port since the TCP session is connected.. The number resets when the TCP session disconnects.
- **Frame Error (Count):** When NPort receives a byte of serial data, it will check if the frame format matches the serial parameters. If not, it will count one frame error.
- **Parity Error (Count):** When NPort receives a byte of serial data, it will check if the parity value is correct. If not, it will count one parity error.
- **Overrun Error (Count):** If the serial device sends data too quickly for the NPort to read, resulting in dropped data bytes, it will be considered an overrun error.
- **Break (Count):** When the NPort receives a break signal, it will count it as one break.
- **Serial Signal:** Displays the current status of all modem signals, including DSR, DTR, RTS, CTS and DCD.

Home > Diagnostics > Operation Mode Statistics > Port 1				
← Port 1				
Operation Mode: Real COM (Secure)				
Serial Parameters Serial Connections <u>Ethernet Connections</u>				
Real-time data displaying ...				
Overview				
Connections	Ethernet Tx (Byte) ⓘ	Ethernet Rx (Byte) ⓘ	Buffering (Byte) ⓘ	Strip Delimiter (Byte) ⓘ
0	0	0	0	0
Connections				
IP Address	Connection Tx (Byte)	Connection Rx (Byte)	TCP State	Cipher Suite
No data to display.				

Ethernet Connections tab:

This tab displays the current statistics of the Ethernet port, related to serial communications:

- **Connections:** The number of TCP sessions established on this serial port.
- **Ethernet Tx (Byte):** The amount of data transmitted on the Ethernet port since the TCP session was established. The number will reset when TCP session disconnects. The number needs to match the Serial Rx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **Ethernet Rx (Byte):** The amount of data received on the Ethernet port since the TCP session was established. The number will reset when TCP session disconnects. The number needs to match the Serial Tx (Byte).. It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **Buffering (Byte):** Byte numbers are still stored in the NPort buffer. If the numbers above don't match (Ethernet Tx & Serial Rx or Ethernet Rx & Serial Tx), it could be because there are still some data bytes in the buffer.
- **Strip Delimiter (Byte):** If you enable the Delimiter function with the Strip delimiter process, the total dropped delimiters will be recorded here.

The Connections sheet displays more detailed information about the TCP sessions:

- **IP Address:** This column displays the IP address connected to the NPort.
- **Connection Tx (Byte):** The amount of data transmitted on the Ethernet port since the TCP session was established. The number resets when the TCP session disconnects. The number needs to match the Serial Rx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **Connection Rx (Byte):** The amount of data received on the Ethernet port since the TCP session was established. The number resets when the TCP session disconnects. The number needs to match the Serial Tx (Byte). It is easy to check this on the **Diagnostics > Operation Mode Statistics** page.
- **TCP State:** Displays the status of this TCP session, which may be CLOSED, LISTEN, ESTABLISHED, CLOSING and TIME-WAIT.
- **Cipher Suite:** If the TCP session has the Encrypted connection feature enabled (Serial Port Settings > Secure Connection), this column will show the cipher suite used for the TCP session.

Network Monitor

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. Everything that happens on the Ethernet interface will be recorded here, **Diagnostics > Network Monitor**, to help you understand the Ethernet data transmitted/received.

Home > Diagnostics > Network Monitor				
Network Monitor				
Network Statistics Network Connections Fiber Check				
Real-time data displaying ...				
Ethernet Packet Count				
Direction	Unicast	Broadcast	Multicast	Error
Sent	20890 (+2/s)	8 (+0/s)	17 (+0/s)	0 (+0/s)
Received	1714290 (+33/s)	553747 (+10/s)	1145859 (+21/s)	80740 (+1/s)
Protocol Packet Count				
✓ TCP UDP ICMP IPv4				
Sent	Received	Drop	Retransmitted	Receive RST
15948 (+2/s)	27964 (+4/s)	253 (+0/s)	4 (+0/s)	41 (+0/s)

Network Statistics tab:

The Ethernet Packet Count sheet separates the Ethernet data in two directions, Send and Received, to count the number of unicasts, broadcasts, and multicasts. If there are any error bytes, the Error column will count them.

The Protocol Packet Count sheet separates the Ethernet data by different protocols to count the numbers of TCP, UDP, ICMP, IPv4, IPv6 and PPP.

Network Connections tab:

This tab displays the status of all the TCP sessions.

Home > Diagnostics > Network Monitor

Network Monitor

Network StatisticsNetwork ConnectionsFiber Check

Real-time data displaying ...

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
UDP	0	0	0.0.0.0:64667	0.0.0.0:0	
UDP	0	0	0.0.0.0:55602	0.0.0.0:0	
	0	0	AF_PACKET		
	0	0	AF_PACKET		
TCP	0	0	0.0.0.0:38872	0.0.0.0:0	LISTEN
TCP	0	0	0.0.0.0:64763	0.0.0.0:0	LISTEN

Fiber Check tab:

This tab displays the status of the fiber module. With Moxa fiber module, this tab can provide you the health of the fiber module and depends on the information to schedule when to purchase a new one for predictable maintenance.

Home > Diagnostics > Network Monitor

Network Monitor

Network StatisticsNetwork ConnectionsFiber Check

Info
This fiber module is not provided by Moxa. The following information is for reference only and may be incomplete or inaccurate.

Real-time data displaying ...

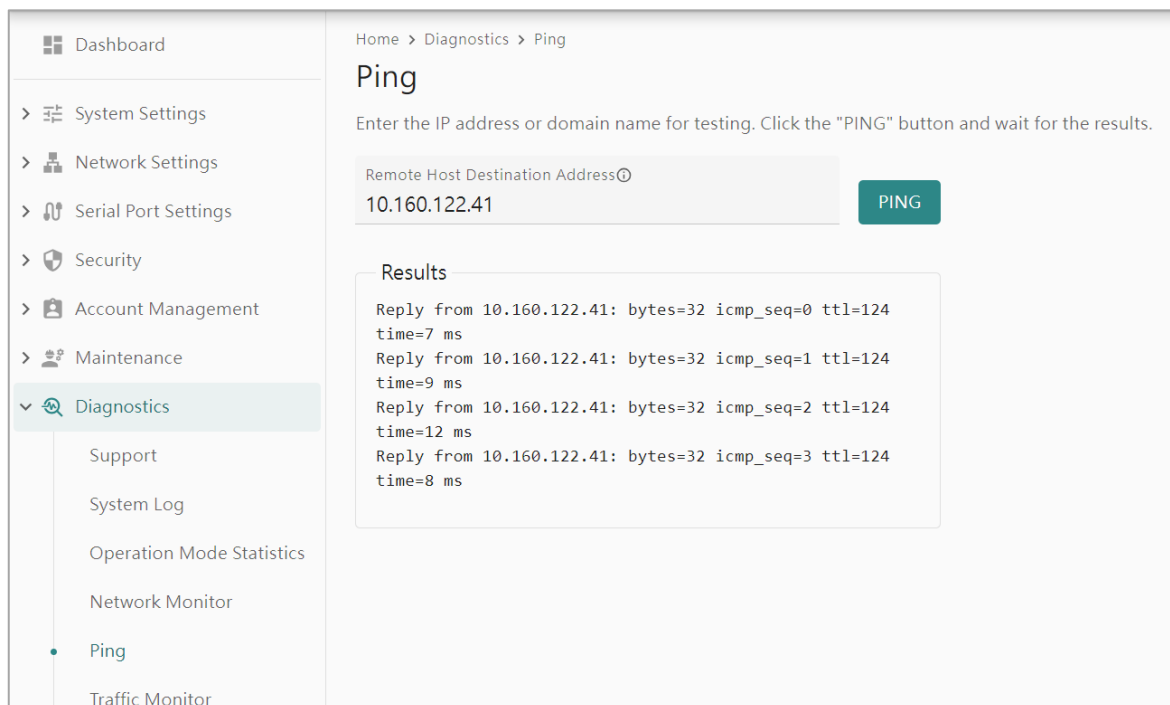
⚙

Fiber Port	Wavelength (nm)	Voltage (V)	Temperature (°C)	Tx Power (dBm)	Rx Power (dBm)
> 1	850	0	0 Reference range: < 0	-- Reference range: 0 ~ 0	-- Reference range: 0 ~ 0

Ping

The Ping function is a good tool for troubleshooting. Engineers can use the NPort device server in this tool to verify the status of network nodes.

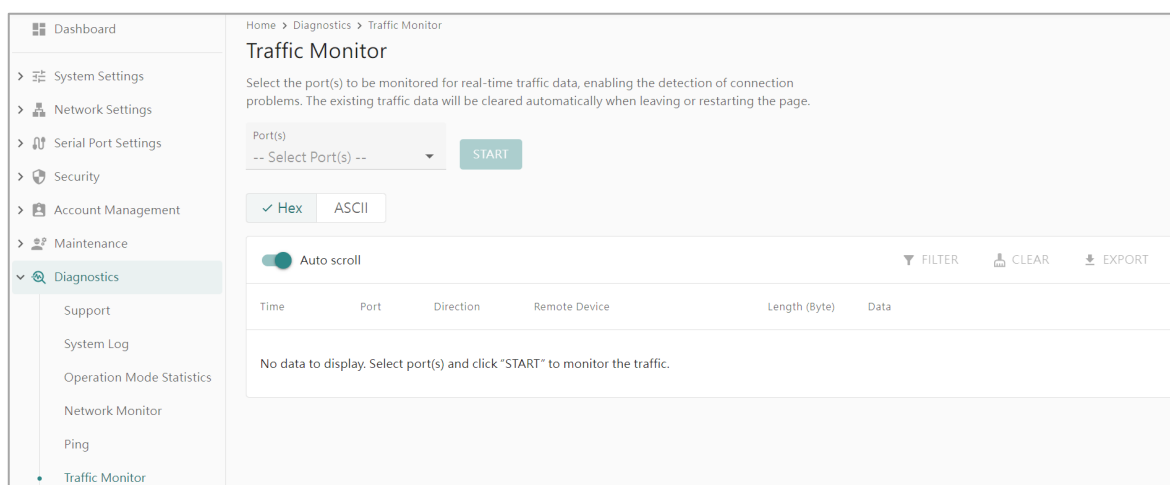
Directly input the IP address and click the PING button. The NPort will check if the target node can respond to the ping request and display the result.



Traffic Monitor

The key feature of an NPort device server is to transmit serial data to the Ethernet network and vice versa. To troubleshoot, it's crucial to check if the serial data is transferred correctly to the Ethernet side.

Previously, the customer service engineer had the option to use a third-party tool to indirectly check the data and provide an answer. Engineers can now use the Traffic Monitor function to compare recorded serial and Ethernet data.



As a troubleshooting tool, it may not be proper to monitor normal communication for a very long time because of the limited local memory size. Moxa recommends that the engineer use this tool to capture both abnormal and normal communication for a few minutes, allowing them to compare and analyze them.

To initiate capturing, choose the target port and click the START button; the transactions captured will be shown below. You can decide whether to view the data as HEX or ASCII.

After finishing the capturing, you have the option to click the FILTER button to narrow down the data for analysis or click the EXPORT button to save the transactions for further analysis by Moxa customer service.

8. Mass Deployment/Maintenance

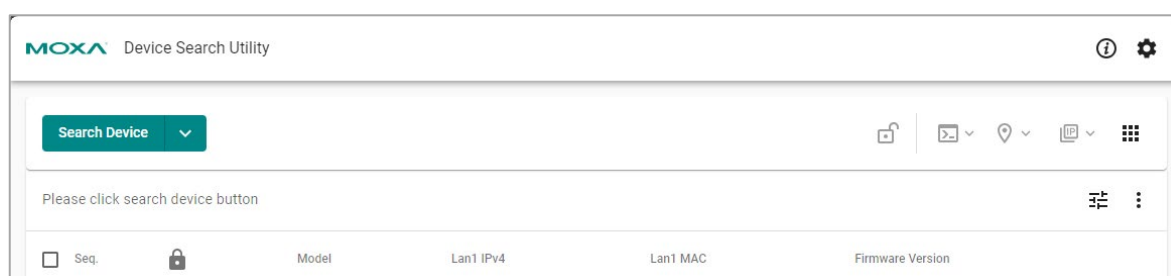
Once a user completes the settings on a device server, they may need to deploy those settings to multiple devices or sites. Moxa provides the GUI tool Device Search Utility v3.0 or the CLI tool Moxa CLI Command Tool, MCC Tool, to meet this requirement.

After the devices were set up at the locations, the maintainer might need to perform routine tasks on a regular basis to run the system. This includes tasks such as firmware upgrades or password updates. The Device Search Utility v3.0 and MCC Tool can assist the maintainer in carrying out these tasks effortlessly.

Mass Configuration With GUI Tool: Device Search Utility v3.0 or Newer


The Device Search Utility v3.0 is a web-based utility. Make sure the operation system and browser version are compliant with the below version before using the tool:

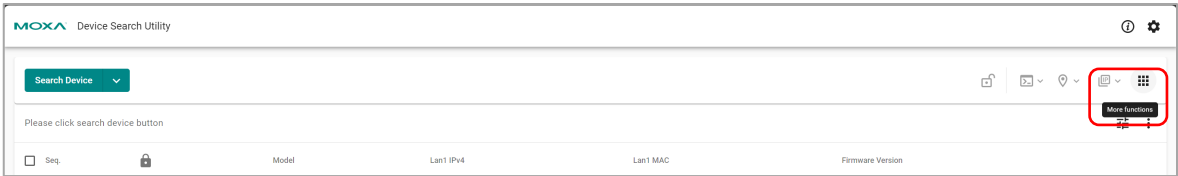
- Chrome:
 - For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
 - For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions
- Edge:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions



Execute the Device Search Utility and click the Search Device button to find the target NPort(s). Remember to unlock them before any further actions.

Import/Export Configuration

Select the NPort device server(s) to import/export configuration and then move the mouse to the More functions to choose the  Import Configuration function.



Import Configuration is to import one configuration file to one or more devices of the same model. Click the BROWSER... button to find out where the configuration file is saved.

Import Configuration

Choose the configuration file to upload and import.

Configuration File

BROWSE...

☐ Keep current device network settings
Preserved items include mode, IP address, netmask (IPv4), prefix (IPv6), gateway, and DNS.

CANCELIMPORT & RESTART

Keep the Current Device Network Settings

If the target NPort device server(s) already has the proper IP address(es) configured, you may choose to retain the existing network settings for the device(s). Select the option.

After importing the configuration, Device Search Utility will display success or failure in the Status & Message columns for each device.

Info: It may take a while to execute this process, please wait for it to end before performing other actions.

Execution is completed !

Device Name	Model Name	Status	Message	Last Updated Time
NP5210A_8205	NPort 5210A	Failed	File format incorrect.	Feb 06, 2024 10:08:59
NP5210A_8295	NPort 5210A	Success	Success.	Feb 06, 2024 10:08:59


Items per page: 101 ~ 2 of 2

Your device may restart again to make the configuration effective, and it will stop your work in progress.



NOTE

For the cause of failure, please refer to the **DSU** User Manual Appendix: Error Messages.

For exporting the configuration file(s), you can also find the  Export Configuration function under the More functions button.

Export Configuration is to export the configuration file from one or more devices with the same model. When exporting one device only, the file format may be *.ini, *.dat, *.txt, *.cfg, *.dec. The filename will be [ModelName] - [IP] _ [Date] .xxx, e.g., NPort6150-10.123.10.1_220724.ini.

When exporting multiple devices, the system will zip the configuration files.

Import Certificate

To build a more secure or a zero-trust network environment, you may want to set up a public key infrastructure (PKI). The certificate needs to be imported into all network devices for this scenario. To simplify the loading process, the Device Search Utility supports importing certificates to multiple NPort device servers.

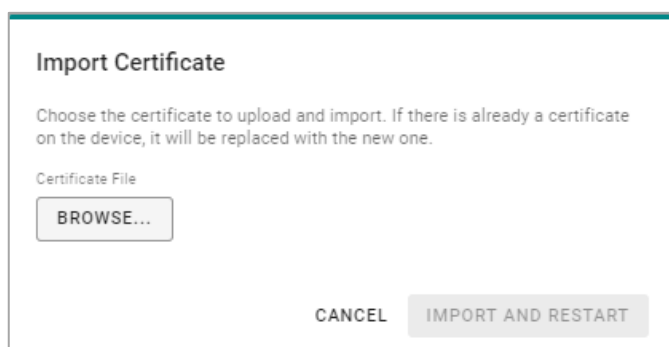
You can find the  Import Certificate function under the More functions button.

Import Certificate is to exchange certificate files to one or more devices to establish secured command/data transferring.

Step 1: Select NPort G2 models

Step 2: Import certificate file


Step 3: Import and restart



The dialog box titled "Import Certificate" contains the following text: "Choose the certificate to upload and import. If there is already a certificate on the device, it will be replaced with the new one." Below this text is a label "Certificate File" and a "BROWSE..." button. At the bottom right of the dialog are two buttons: "CANCEL" and "IMPORT AND RESTART".

Firmware Upgrade

The increasing convergence of IT and OT poses a cybersecurity risk as more OT network devices connect to office networks. Upgrading the firmware version to the latest one is crucial for all network devices. In order to meet this requirement, the Device Search Utility supports firmware updates on multiple NPort device servers.

You can find the  Firmware Upgrade function under the More functions button. **Firmware Upgrade** is to send one firmware file to one or more devices with the same model. The firmware file extension normally comes with .ROM.

Step 1: Select NPort G2 models

Step 2: Import firmware file

Step 3: Imported and the device will restart.

Mass Configuration with CLI tool: MCC Tool

The MCC Tool is a command line utility based on Windows and Linux platforms. Make sure you have downloaded the correct file for your operating system.

Unzip the file and install the MCC Tool. Execute the MCC Tool under the command line to manage the NPort device servers in the network.

Import/Export Configuration

Import/Export the device configuration for a specific device or a range of devices through the device list file. The password must be specified by the parameter or by the device list file. Device configurations are stored in individual files, using device type, IP address, and file create date as the filename. The result log is directly printed on the screen, or you can specify a result_log file for it.

MCC_Tool -cfg -ex -i [ip_address] -u [user] -p [password] -dk [key] -l [result_log]

MCC_Tool -cfg -ex -d [Device_list] -l [result_log]

MCC_Tool -cfg -ex -d [Device_list] -l [result_log] -t [timeout_value]

MCC_Tool -cfg -im -i [ip_address] -u [user] -p [password] -dk [key] -f [cfg_file] -l [result_log] -n -nr

MCC_Tool -cfg -im -d [Device_list] -l [result_log] -n -nr

MCC_Tool -cfg -im -d [Device_list] -l [result_log] -t [timeout_value]

Parameters Description:

Command	Function	Remark
-cfg	Execute actions for configuration related	
-ex	Export the configuration file	
-im	Import the configuration file	
-i	Device IP address (ex. 192.168.1.1)	
-d	Device list	
-u	Device's user account for login	
-p	Device's password for login	
-dk	When Exporting configuration: The command decrypts the exported file with the pre-shared key. <ul style="list-style-type: none">If this parameter is not used, the exported file will be encrypted by the pre-shared key set on the firmware of the device.If this parameter is used, the exported file will be decrypted to a clear-txt file for editing. When Importing configuration: If the configuration file that needs to be imported is encrypted, the command is needed with pre-shared key. <ul style="list-style-type: none">If the import configuration file is without -n, The MCC tool will ignore -dk (won't return -11).If the import configuration file is with -n, the MCC tool will use pre-shared key to decrypt the encrypted file. Therefore, if the key is wrong for decrypting the file, the MCC tool will return -10. However, if the file is in plain text, and you input the pre-shared key, it will ignore the key (won't return -10).* (by parameter -dk or the key column in the device list file)	
-f	The configuration file to be imported	Only for the import configuration function
-n	Keep original network parameters (includes IP, subnet mask, gateway, and DNS)	Only for the import configuration function
-nr	Do not reboot the device after importing the configuration file	Only for the import configuration function.
-l	Export result log file	
-t	Timeout (1 to 120 seconds) Export function Default value: 30 seconds Import function Default value: 60 seconds	

Example: Export the configuration using a device list and export the results to a result log

MCC_Tool -cfg -ex -d [DeviceList] -l [result_log]

The result_log will include the following items:

Model	ServerName	IP	MAC	FwVer	ExportCfgFile	Key	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	NP6650_192_168_1_1_20170622.ini;	moxa;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	NP6650_192_168_1_2_20170622.ini;	moxa;	0;

Example: Import the configuration to a device list (with restarting the units) and export the results to a result log.

MCC_Tool -cfg -im -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwVer	CfgFile	Key	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	NP6650_192_168_1_1_20170622.ini	moxa;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	NP6650_192_168_1_2_20170622.ini	moxa;	0;

Example: Import the configuration to a device list without restarting the units and export the results to a result log.

MCC_Tool -cfg -im -d [DeviceList] -nr -l [result_log]

Firmware Upgrade

With the IT/ OT convergence trend, office networks may see an increase in OT network devices, posing cybersecurity risks. Upgrading the firmware version is crucial for all network devices. The MCC Tool allows users familiar with the command line interface to update the firmware on multiple NPort device servers to fulfill this need.

The NPort IA5000-G2 Series supports password protection by default and cannot be disabled. The password(s) must be specified by a command parameter or by the DeviceList file before upgrading the firmware and restarting a specific device (or multiple devices simultaneously).

MCC_Tool -fw -up -i [ip_address] -u [user] -p [password] -f [firmware_file] -l [result_log]

MCC_Tool -fw -up -d [Device_list] -l [result_log]

MCC_Tool -fw -up -d [Device_list] -l [result_log] -t [timeout_value]

Parameters Description:

Command	Function	Remark
-fw	Execute actions for firmware related	
-up	Upgrade firmware version	
-i	Device's IP address (192.168.1.1)	
-u	Device's user account for login	
-p	Device's password for login	
-d	Device list	
-f	Firmware file to be upgraded	
-l	Export result log file	
-t	Timeout (1~1200 seconds) Default value: 800 seconds	
-print	Print upgrade process status message	

Example: Upgrade firmware using a device list and capture the results in an import log.

MCC_Tool -fw -u -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwFile	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	NP6000_V1.3.rom;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	NP6000_V1.3.rom;	0;

Change Password

Due to the IT/OT convergence trend, an increasing number of companies require their employees to regularly update their login passwords, as do the network devices. The owner/maintainer of the network devices may need to update the password regularly. The MCC Tool helps you to ease this routine job by generating a small script to update the password.

Set the password of the target device specified by an IP address. The current password must be specified by a parameter or by the Device List file.

MCC_Tool -pw -ch -i [ip_address] -u [user] -p [old_password] -npw [new_password]

MCC_Tool -pw -ch -d [Device_list] -nd [device_list_new_password] -l [result_log]

MCC_Tool -pw -ch -d [Device_list] -nd [device_list_new_password] -l [result_log] -t [timeout_value]

Parameters Description:

Command	Function	Remark
-pw	Execute actions for password	
-ch	Change password	
-npw	The new password for the specific user	
-i	Device's IP address (192.168.1.1)	
-u	Device's user account for login	
-p	Device's password for login (old password)	
-d	Device list	
-nd	The Device list with new password settings	You will need to assign a new password in the Device List when using -nd command.
-l	Export result log file	
-nr	Don't reboot the device after changing the password	
-t	Timeout (1 to 120 seconds) Default value: 60 seconds	

Example: Set the new password as "5678" and restart the device to make it effective. Print the result on the screen.

MCC_Tool -pw 5678 -i 192.168.1.1 -u admin -p moxa

Example: Set the new password from a device list and then restart the device to make it effective. Export the results to a result log

MCC_Tool -pw DeviceList_New -d [DeviceList] -l [result_log]

The result_log will include the items below:

Model	ServerName	IP	MAC	FwVer	User	PWD	ErrCode
NPort6650;	NPort6650_123;	192.168.1.1;	00:90:e8:01:02:03;	1.3;	admin;	5678;	0;
NPort6150;	NPort6150_456;	192.168.1.2;	00:90:e8:04:05:06;	1.3;	admin;	moxa;	0;

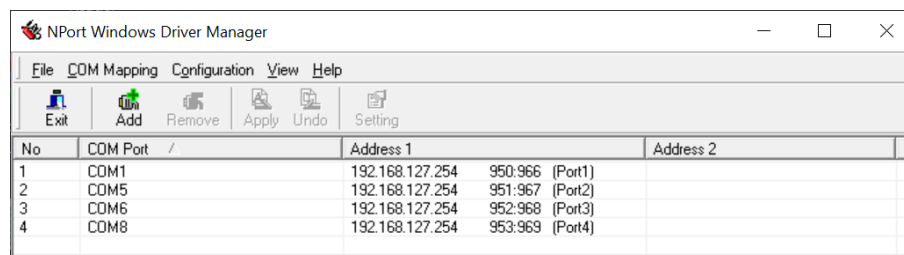
9. Advanced Settings of NPort Windows Driver Manager

The NPort Windows Driver Manager has additional capabilities apart from being a driver for the virtual COM application. There are many advanced settings to help you face different user scenarios. In this chapter, we will explain which functions/settings are useful in different scenarios.

Configure the Mapped COM Ports

After mapping the COM ports, refer to Chapter 4 for instructions. In many instances, the legacy COM port software can establish communication with the serial devices by opening either the COM port or the TTY port. In specific cases, the user may need to modify the advanced settings of the NPort Windows Driver Manager for certain applications.

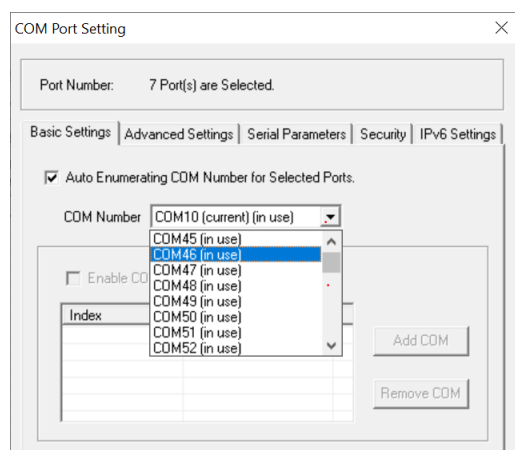
To reconfigure settings for a specific serial port on the NPort device server, select the corresponding row and click the **Setting** icon in Real COM Mode/Reverse Real COM Mode.



No	COM Port	/	Address 1	Address 2
1	COM1		192.168.127.254 950:966 (Port1)	
2	COM5		192.168.127.254 951:967 (Port2)	
3	COM6		192.168.127.254 952:968 (Port3)	
4	COM8		192.168.127.254 953:969 (Port4)	

Change the Number of a Mapped COM Port

Some legacy COM port software is restricted to using specific COM ports like COM1 or COM2. Nevertheless, the NPort Windows Driver Manager has the capability to automatically assign COM ports starting from COM3. To modify the COM port number, click on the **Setting** button and locate the **COM Number** drop-down menu in the Basic Settings. Simply select the COM port requested by the legacy COM port software.



To assign the serial ports of the NPort device server to COM port numbers in sequence, choose **Auto Enumerating COM Number** option for selected ports.

COM Splitting

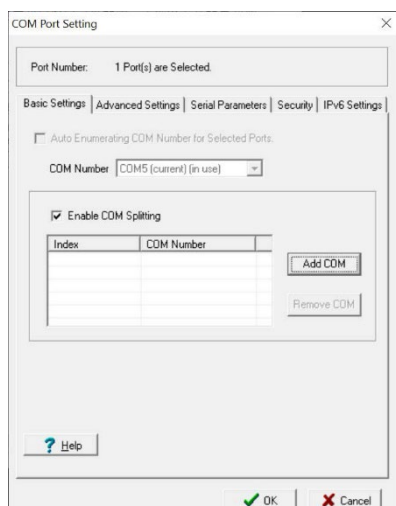
When you activate COM Splitting, you can use multiple COM port software to communicate with the same serial device. Only one software can open/occupy a COM port, causing others to wait until it is closed. The COM Splitting function allows multiple COM port numbers to be assigned to the same serial port on the NPort device server. The first software accesses COM1, while the second software uses COM2, but both communicate with the same serial device.

Since both softwares will be using the same serial port and device, they must coordinate when the first software sends a command and when the second one does. Or there may be a data collision. Using this feature could be a better option for enabling one-way communication from the serial device to multiple host PCs on the Ethernet network. Let's say there's a serial temperature sensor that constantly updates temperature data to the control servers. If the temperature gets too high or too low, one of the servers will send a request to activate the fan or heater. The purpose of the second server might be to serve as the database for recording temperature readings.

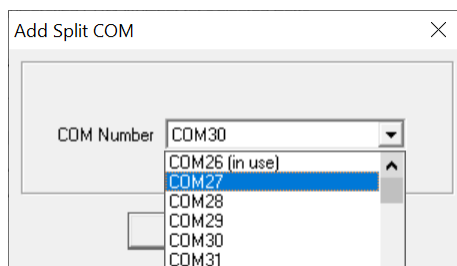
The COM Splitting function will group all the selected COM ports into one COM port. Even if you use varying software to communicate via different COM port numbers, all the software will receive identical data from the serial device.

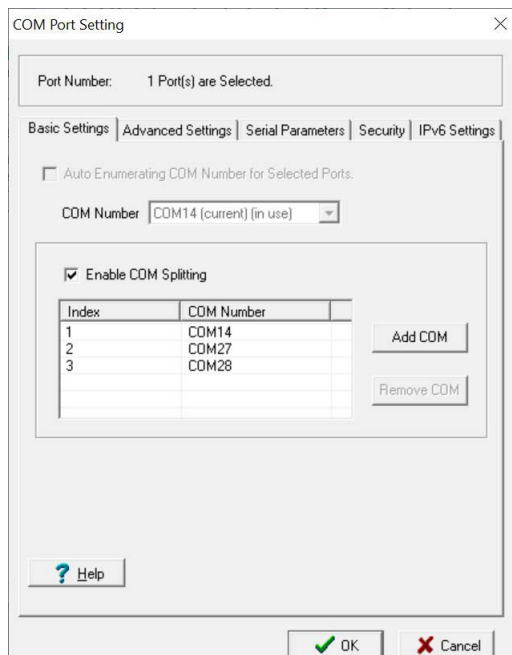
In order to handle various host PCs connecting to the same serial port, it is necessary to modify the **Max. Connection** setting according to the number of ports grouped in your NPort. For example, if you split to two COM ports, **Max. Connection** needs to be adjusted to 2. The grouped serial ports must be directed to the same NPort device server; they cannot be combined from different NPorts.

Enabled COM Splitting

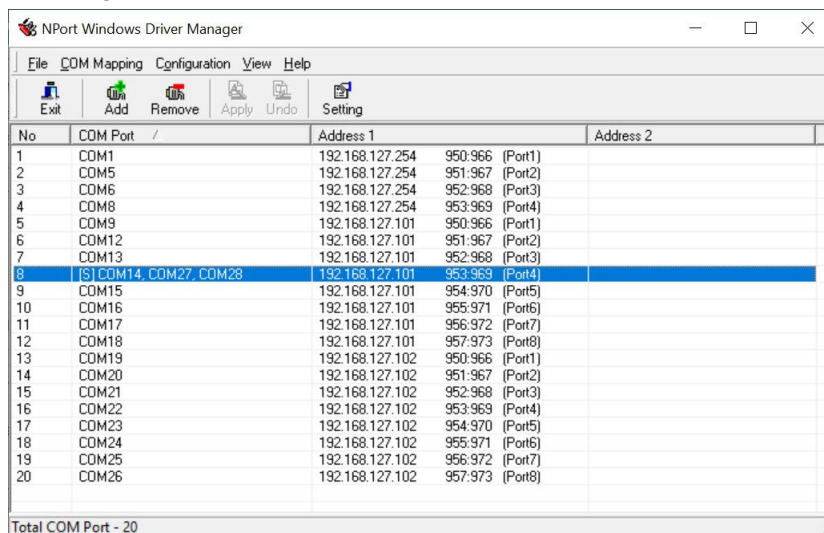


1. Select the target COM port number and click the **Setting** button.
2. Select to enable the Enable COM Splitting function.
3. **Add COM** to select target COM ports for splitting; the COM port must be available.





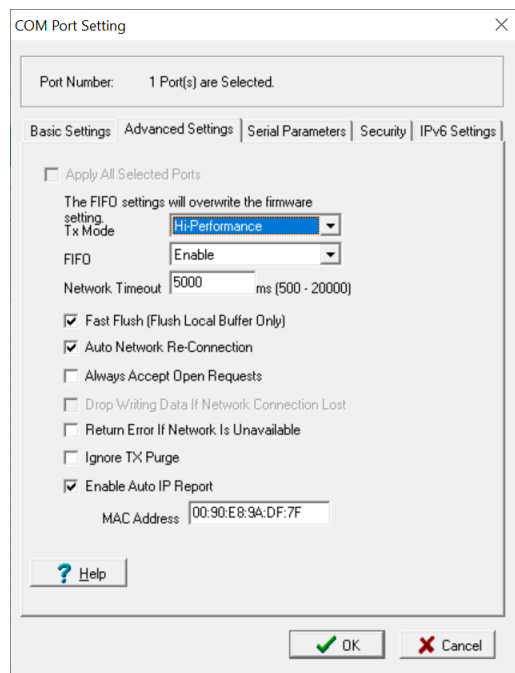
4. After pressing **OK**, check if the COM ports you just selected are grouped together. Click **Apply** to save the change.



5. Once the COM port number changes to black text, the software can open multiple COM Splitting ports to receive serial data.

Advanced Setting

Transferring serial data to an Ethernet network can result in timing differences and variations in behavior compared to TCP socket behavior. The NPort Windows Driver Manager offers various advanced settings to accommodate these differences, ensuring that your original software remains unchanged and communication functions properly.



Tx Mode

Because Ethernet and serial technology have significantly different speeds, the serial line's maximum baudrate is only 921,600bps, while Ethernet's minimum speed is 10Mbps. The Tx Mode offers two options for the driver to mimic either Ethernet or serial bus behavior more closely.

The default setting for the Tx Mode is **Hi-Performance** mode, which sends as much data as possible to the serial side. This behavior will be closer to Ethernet. The driver buffer will temporarily store the data before sending it all at once over Ethernet, resulting in higher data delivery throughput.

This might pose issues for older serial applications or devices that lack sufficient buffer or performance to handle large amounts of data quickly. To handle these situations, switch the Tx Mode to **Classical** mode. In Classical mode, the NPort sends the serial data one byte at a time, eliminating the need for a large buffer size in the serial device. This is designed to work with serial devices like these. Additionally, the **Classical** mode allows for quicker data delivery by minimizing latency. The serial data can bypass the driver buffer's waiting time.

FIFO

This FIFO setting is the same setting on the NPort device server. If they're not the same, the value in the NPort Windows Driver Manager will overwrite the setting on the firmware and apply either Real COM mode or Reverse Real COM mode.

The Enable FIFO function is enabled by default for improved data throughput. There are two scenarios you may consider disabling the Enable FIFO function (uncheck the checkbox).

- The serial device does not have FIFO/buffer or does not support flow control function. In this case, the serial device may not be able to receive the serial data from NPort on time, which means that some data might be dropped.
- The data latency is more important than data throughput. Higher data throughput involves temporarily storing data in the buffer to enable sending larger amounts of data at once. This behavior may result in slower latency for individual data. If maintaining low latency is a priority for reading data correctly on the serial device, it is recommended to disable the Enable FIFO function.

This field enables or disables the 512-byte FIFO buffer. The NPort IA5000-G2 provides FIFO buffers for each serial port, for both the Tx and Rx signals.

Network Timeout

This function shares similarities with the **TCP alive check time** function on the NPort device server. The only difference is the source of each function. The source of the **TCP alive check time** is the NPort device server; it will check if the remote host PC is alive or not. The source of the **Network Timeout** function is the host PC (which installed the NPort Windows Driver Manager); it will check if the remote NPort is alive or not. Use this option to prevent blocking when the target NPort is unavailable.

Fast Flush (only flushes the local buffer)

For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. Following the execution of the PurgeComm() function, the NPort driver persists in querying the firmware of the NPort multiple times to ensure the absence of queued data in the firmware buffer, instead of solely flushing the local buffer on the host PC. The purpose of this design is to meet specific requirements. The additional time required for Ethernet communication means it may take longer (about several hundred milliseconds) than a native COM1. PurgeComm() is noticeably faster on native COM ports than on mapped COM ports on the NPort IA5000-G2. In order to support applications with faster response requirements, the new NPort driver incorporates a Fast Flush option. This function is enabled by default.

If you disable Fast Flush and notice a significant decrease in performance for COM ports mapped to the NPort IA5000-G2, check if your application uses "PurgeComm()" functions. If so, try enabling the Fast Flush function and see if there is a significant improvement in performance.

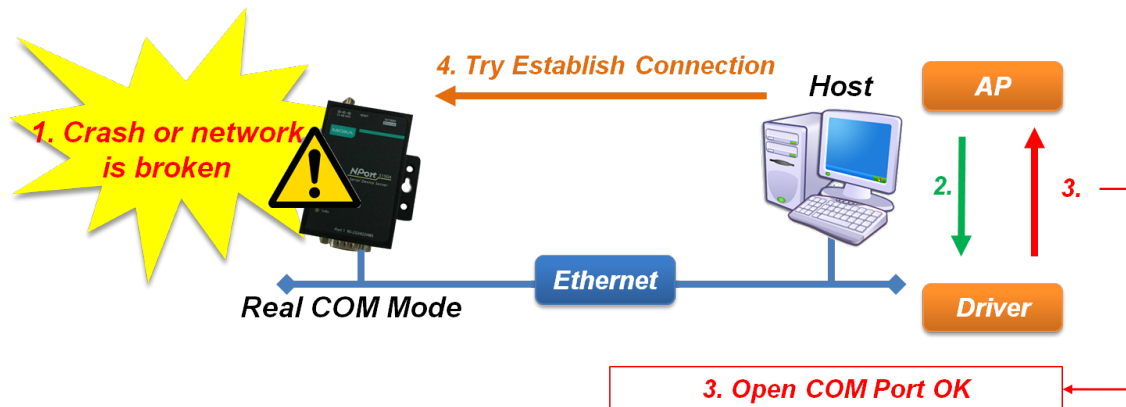
Auto Network Reconnection

While serial communication is always connected, Ethernet communication is not. The NPort Windows Driver Manager offers Auto Network Reconnection for automatic re-establishment of connections, ensuring the serial device is always considered connected and capable of sending data.

If this option is turned on, the driver will keep trying to reconnect the TCP connection if the NPort IA5000-G2 doesn't respond to "check-alive" packets, which are sent in the background. The Network Timeout function, which cannot be disabled, determines the timing of these packets..

Always Accept Open Requests

When the driver cannot establish a connection with the NPort, your software can still open the mapped COM port, like an onboard COM port.



Return Error If Network Is Unavailable

We discovered that some legacy COM port software always opens a fixed range of COM ports, from COM1 to COM10, when executed by the user. For the real application, only COM3, COM5 and COM7 are available, so the software will always return failure since it cannot open the COM1 to COM10 successfully. To temporarily resolve this issue with the outdated software, you can deactivate the **Return error if network is unavailable** option..

Disabling this option will prevent the driver from reporting errors for failed connections to the NPort IA5000-G2. Enabling this option will result in the Win32 Comm function returning the error code "STATUS_NETWORK_UNREACHABLE" if a connection to the NPort IA5000-G2 cannot be established. Typically, this indicates that your host's network connection is offline, possibly due to a disconnected cable. But if you're able to access other network devices, it's likely that the NPort IA5000-G2 is either disconnected or not powered on. To use this feature, make sure **Auto Network Re-Connection** is turned on.

Ignore TX Purge

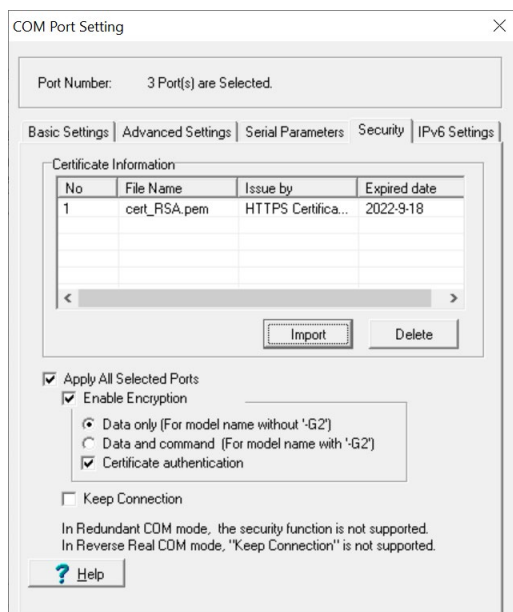
When programming for legacy COM port software, it is common practice to clear the buffer before and after writing data, to prevent any unwanted data from being present. In the past, there were no troubles, making it an effective method to avoid sending incorrect data to the serial device.

Due to advancements in technology, PCs now have significantly improved performance compared to the past. There's a possibility that the clear buffer command might be sent to the NPort device server prematurely, following the write command. The NPort may still have correct data in its buffer, but it will be lost when the clear buffer command, which is the Win32 API PurgeComm command, is received. You might notice that the received serial data is missing the last few bytes. Enabling the **Ignore TX Purge** function might be the solution when this occurs.

Security

When addressing the growing cybersecurity threats, it is crucial to devise ways to protect vital data on serial devices. The serial bus has a short communication distance and is difficult to steal, especially in secure manufacturing facilities with guards. However, it's a different situation when it comes to using a device server to transmit serial data over an Ethernet network. The Ethernet network is much more vulnerable than the serial bus. The NPort device server enables encryption of Ethernet network communications. With the NPort Windows Driver Manager, you can encrypt communications on the host PC.

Select target serial port, click the **Setting** button, and switch to **Security** tab:



Enable Encryption

Enable the SSL encryption for data and command transmission of the selected COM port.

Data Only

The NPort 6000 Series supports data encryption only. Select this option if you are using the NPort 6000 Series.

Data and Command

The NPort IA5000-G2 Series supports both data and command encryption. Select this option if you are using NPort G2 models.

Certification Authentication

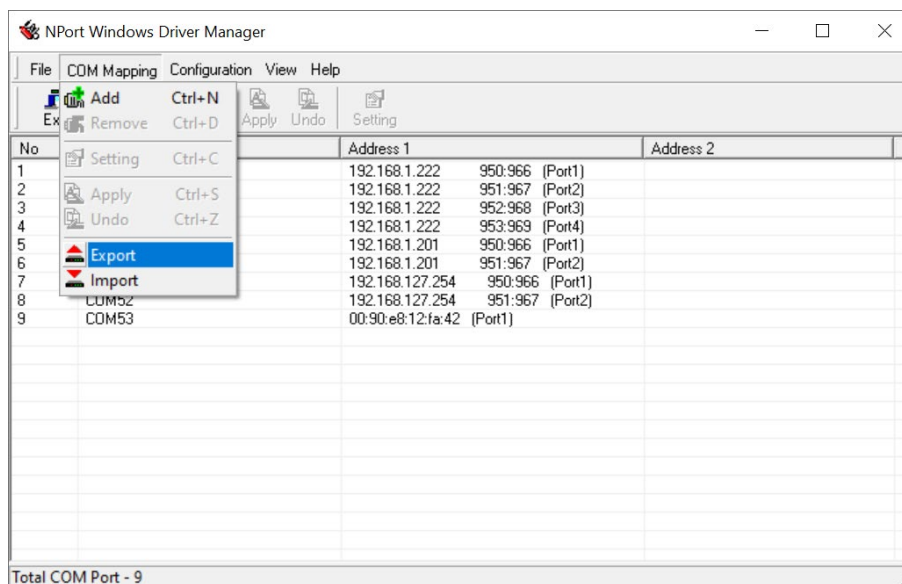
This security enhancement allows you to verify the server and client using an imported certificate from a trusted Certificate Authority (CA). Click the **Import** button above to import the certification of your own.

Keep Connection

For quicker operations, it is recommended to enable this option if the COM port software frequently opens and closes the COM port with data encryption and the NPort is dedicated to one host. The opening time of a COM port with encryption enabled will be brief (300 to 500ms) due to the SSL protocol. By enabling these options, you can ensure a continuous SSL connection for the COM port. The opening and closing of the COM port will be faster here. The Keep Connection feature is not supported in Reverse Real COM mode.

Importing/Exporting COM mapping

To load/save the configuration to a text file, select Import/Export from the **COM Mapping** menu. You will then be able to use this configuration file on another host and use the same COM Mapping settings in the host.

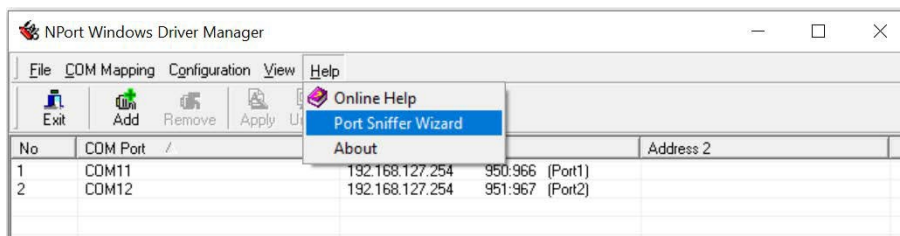


Port Sniffer Wizard

At times, engineers may require an analyzer to track the commands and responses exchanged between the Windows platform and the NPort Windows Driver Manager to diagnose communication issues. The Port Sniffer Wizard is a tool that tracks and records activity on all serial ports of a system. Its advanced filtering and search capabilities make it a powerful tool for exploring Windows functionality, monitoring port usage, and troubleshooting system or application configurations.

How to Use the Port Sniffer

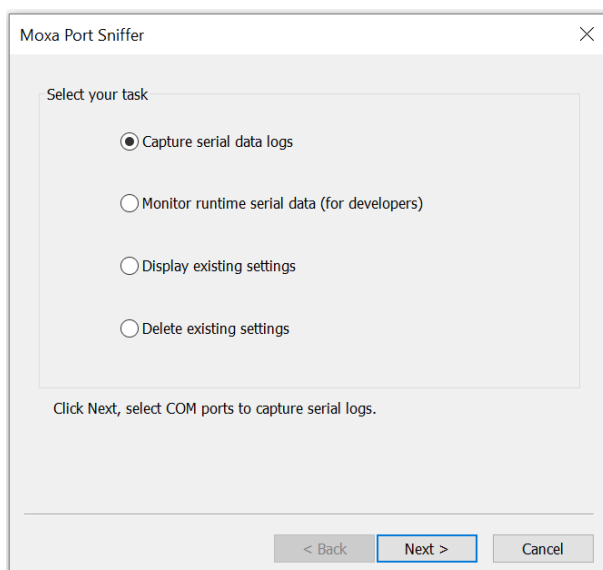
Click **Port Sniffer Wizard** in the drop-down menu under Help.



Task Page

Select the task you need, and click **Next**:

- Capture serial data logs
- Monitor runtime serial data (for developers)
- Display existing settings
- Delete existing settings



Capture Serial Data Logs

If errors occur, you can capture serial data logs from specific ports and send the logs back to Moxa. We can help you check the problems. Select this function to export log files.



NOTE

Enabling the capture serial data logs function may cause slight latency.

Step 1: COM port setting

- Select one or more COM ports to capture.
- Turn on the function you need.
 - Display IRP direction
IRP will inform users whether an error occurs when issuing a command or returning a response.
 - Hide sensitive data
The system will hide the data, so that you don't need to worry about data leakage. Used specifically for sensitive data.

The screenshot shows a 'Port Sniffer' dialog box with a close button (X) in the top right corner. The main area is titled 'Select COM ports to capture' and contains a list of COM ports with checkboxes: COM5, COM6, COM7, COM8, COM11, and COM12. COM12 is selected. To the right of the list are three checked checkboxes: 'Display IRP direction', 'Log to file', and 'Hide sensitive data'. Below these is a 'Refresh' button. At the bottom of the dialog, there are instructions: 'Click Next, set the parameters of logging files.' and 'Click Back, return to the task page.' At the very bottom are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

Step 2: Set the parameters of logging files

- Enable log service.



NOTE

Disabling the log service will not capture the serial data.

- Choose the location of log files.
- Set the max. number of log files and max. file size (MB).

The screenshot shows a dialog box titled "Port Sniffer" with a close button (X) in the top right corner. The main area is titled "Set the attribute of logging file". It contains the following settings:

- Log Service :** A dropdown menu set to "ENABLED".
- Location of log files :** A dropdown menu showing "C:\mxportsf".
- Max. number of log files :** A text input field containing "10".
- Max. file size (MB) :** A text input field containing "30".

A red rectangular box highlights the "Max. number of log files" and "Max. file size (MB)" fields. Below these fields, there is instructional text: "Click Finish, Sniffer will start/stop to log serial data in the background." and "Click Back, return to check the COM port settings." At the bottom of the dialog, there are three buttons: "< Back", "Finish" (which is highlighted with a blue border), and "Cancel".

- Click finish and check log files at the locations you set.

Monitor Runtime Serial Data (for developers)

The difference between the "Capture serial data logs" and "Monitor runtime serial data" functions is that the latter presents the status in real time.

Step 1: COM port setting

- Select one or more COM ports to monitor the serial log in the runtime.
- Turn on the function you need.
 - Display IRP direction
IRP will inform users whether the error occurs when issuing a command or returning a response.
 - Log to file
Export log files simultaneously. (Exporting log files simultaneously will cause latency)



NOTE

Monitor runtime is usually used by developers or serial driver programmers to troubleshoot. Download debug tools like "DebugView" from a third party to view the real-time status.

- Hide sensitive data

The system will hide the data. Used specifically used for sensitive data.

Step 2: Set the parameters of logging files. Skip this step if you disabled **Log to file** function

- Enable log service.
- Choose the location of log files.
- Set the max. number of log files and max. file size (MB).

The screenshot shows the 'Port Sniffer' window with the 'Set the attribute of logging file' tab selected. The 'Log Service' is set to 'ENABLED'. The 'Location of log files' is set to 'C:\mxportsf'. The 'Max. number of log files' is set to '10' and the 'Max. file size (MB)' is set to '30'. These two fields are highlighted with a red rectangle. Below the input fields, there is a note: 'Click Finish, Sniffer will start/stop to log serial data in the background. Click Back, return to check the COM port settings.' At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

Step 3: Set the environment settings.

- Enable the Debug Print Filter to dump messages from the kernel. The setting will take effect after the system restarts.

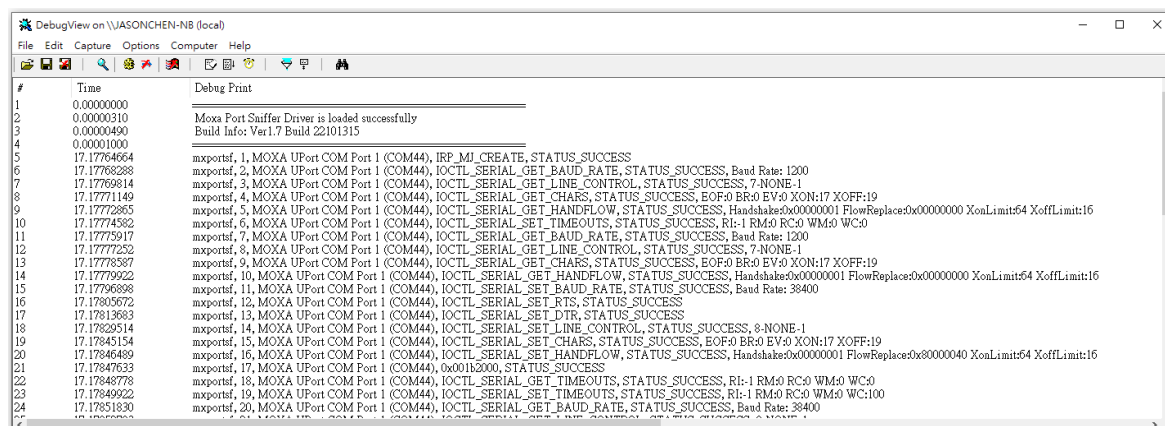


NOTE

1. Disabling the Debug Print Filter will not output the serial data to the monitor.
2. You can see the runtime serial data from the debug output monitor.

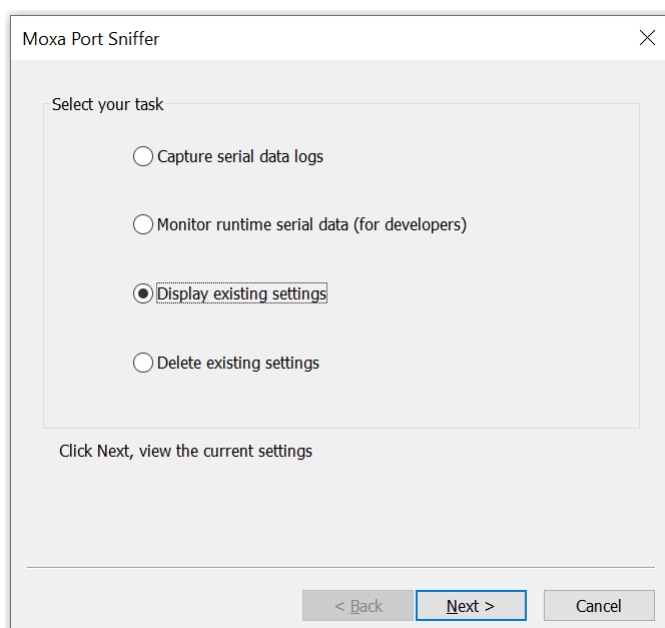
The screenshot shows the 'Port Sniffer' window with the 'Environment settings' tab selected. The 'Sniffer Service' is set to 'ENABLED'. The 'Debug Print Filter' is set to 'ENABLED'. Below this, there is a note: 'In Windows Vista or later versions, you must enable the Debug Print Filter to dump messages from kernel. This setting will take effect after system restart. Then, you can see the run-time serial data from the debug output monitor, like DebugView. (DebugView is an application distributed by Sysinternals ®)'. At the bottom, there is a note: 'Click Finish, Sniffer will enable the service and apply the filter. Then, the sniffer will output serial data to the debug monitor. Click Back, return to check the COM port settings.' At the bottom, there are three buttons: '< Back', 'Finish', and 'Cancel'.

- Click **finish** and open "DebugView" to Monitor runtime serial data.



Display existing settings

- Step 1:** Click **Display existing settings** to view the current setting.



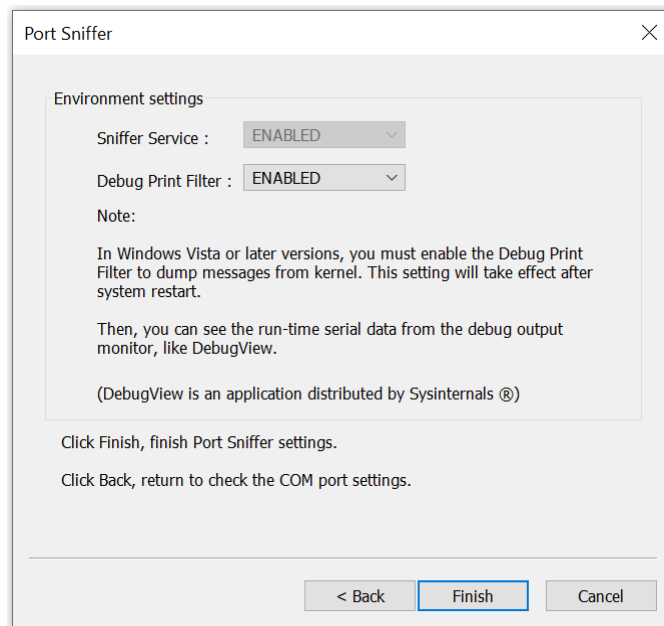
Step 2: Check the COM port settings.

The 'Port Sniffer' dialog box is shown with the title bar and a close button. The main area is titled 'Select COM ports to capture'. It contains a list box labeled 'COM Number' with 'COM12' selected and checked. To the right of the list box are three checkboxes: 'Display IRP direction' (checked), 'Log to file' (unchecked), and 'Hide sensitive data' (checked). Below these checkboxes is a 'Refresh' button. At the bottom of the dialog, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. Below the main area, there is instructional text: 'Click Next, check the parameters of logging files.' and 'Click Back, return to the task page.'

Step 3: Check the parameters for logging files.

The 'Port Sniffer' dialog box is shown with the title bar and a close button. The main area is titled 'Set the attribute of logging file'. It contains four settings: 'Log Service' is set to 'ENABLED' in a dropdown menu; 'Location of log files' is set to 'C:\mxportsf' in a dropdown menu; 'Max. number of log files' is set to '10' in a text box; and 'Max. file size (MB)' is set to '30' in a text box. At the bottom of the dialog, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. Below the main area, there is instructional text: 'Click Next, check the environment settings.' and 'Click Back, return to check the COM port settings.'

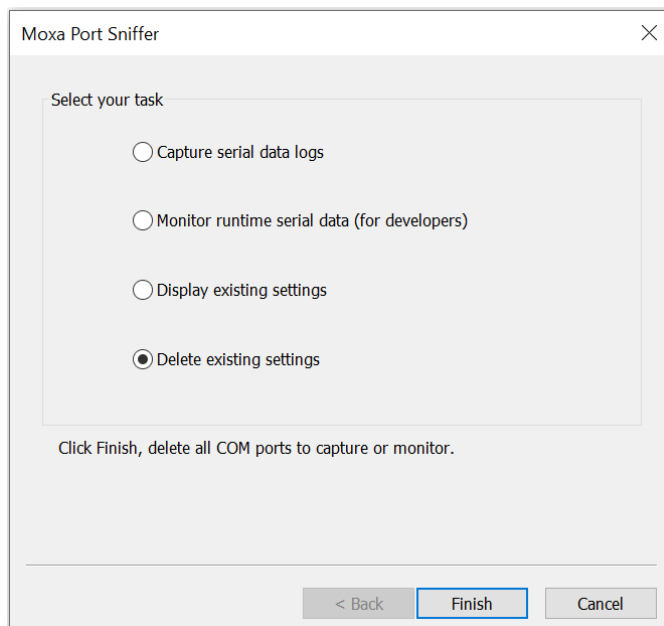
Step 4: Check the environment settings.



Step 5: Click **Finish** to finish Port Sniffer settings.

Delete existing settings

Step 1: Select **Delete existing settings**.



Step 2: Click **Finish** to delete existing settings.

10. Frequently Asked Questions

We have designed this section to list the Frequently Asked Questions so that users can solve their own questions.

Q1. If I disable the Web console, how can I change the settings?

The web console is the major management console of the NPort IA5000-G2. It configures all the functions of the NPort IA5000-G2 and monitors the status of the device server. We don't recommend you to disable the web console service.

When operating in an extremely high-risk cybersecurity environment, you may opt to disable the web console service after completing the configuration and confirming that no further adjustments are needed. The web console service can be enabled through SNMP private MIB in this scenario.

If the SNMP Agent service is also turned off, the only way to reset the device to factory settings and re-enable the web console service is to use the hardware reset button.

Q2. Can different users use the same account to log in to the device server?

Different connections are not allowed for one user account on the device server because of cybersecurity measures.

For example, the administrator is already logged into the NPort as account "admin". And, now a second user uses "admin" to log in to the same device server:

- If the password is wrong, the device server will record a login failed event on the syslog. The administrator can check the syslog to notice this failure.
- If the password is correct, the user will log in to the device and the former connection will be terminated. The administrator will be notified by this unexpected behavior. By logging in again, the administrator can find the IP address from the syslog to prevent the user to try again.

Q3. Why Device Search Utility v3.0 and later cannot be executed on my Windows 7 or Windows 2008 R2?

Since the Device Search Utility v3.0 is a web-based application, it has the minimum requirements for the browser version and operating system:

- Chrome:
 - For Windows 7, 8/8.1, Server 2012 and Server 2012 R2: Chrome 109 and newer
 - For Windows 10 and newer, Server 2016 and newer: All Chrome versions
- Firefox:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions
- Edge:
 - For Windows 7 and newer versions, Server 2012 and newer versions: All Firefox ESR versions

Q4. How can I check the CRC value of the runtime settings?

The NPort IA5000-G2 provides private MIB for the CRC value of the runtime settings, the OID is configCRC32. Use a MIB browser or send a SNMP command to get the CRC value.

Q5. Is there an easier way to copy the settings of a NPort IA-5000/IA5000A device server to a NPort IA5000-G2?

If you have NPort IA-5000/IA5000A device servers on site, you may wonder how to transfer the same settings to the NPort IA5000-G2 device servers. Is it possible to configure each setting individually, one page at a time, even if it takes a lot of time?

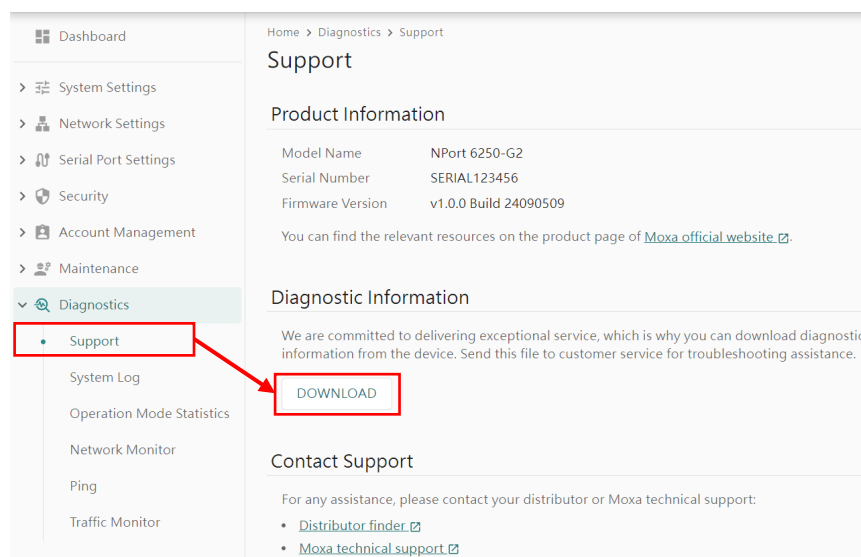
The NPort IA5000-G2 device servers have the capability to import the configuration file directly from a NPort IA-5000 or NPort IA5000A. Export the NPort IA-5000/IA5000A settings and import them into the NPort IA5000-G2. The NPort IA5000-G2 can then replace the device server on site.

Q6. If there is a power outage during a firmware upgrade, how can I recover the device?

The NPort IA5000-G2 supports a fail-safe mechanism during firmware upgrade. If there is a power outage, just power up the device. The device will be ready with the previous version of firmware. Try again or arrange another proper time to upgrade the firmware.

Q7. Before calling Moxa customer service, is there anything I can prepare to save both of us time?

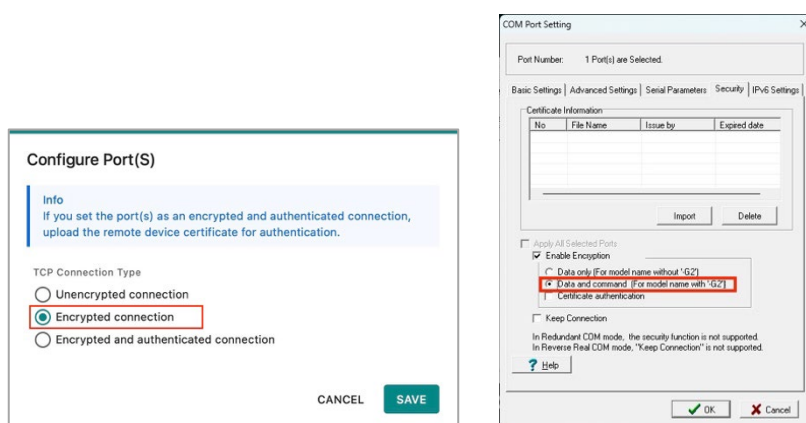
Please find the **Support > Diagnostic Information** and click the **DOWNLOAD** button to collect all the settings and logs for troubleshoot. This will help Moxa customer service to understand the case background and try to replicate the issue you are experiencing.



Q8. How to set up a Secure Connection of Real COM mode?

In general, most of the serial data is plaintext and it will be directly passed to the Ethernet side for the host to monitor or control the serial device. Nowadays, the network becomes bigger and bigger, and user may concern if the data may be sniffed on the Ethernet. To fulfill this need, the NPort IA5000-G2 Series supports Secure Connection to encode the data. Furthermore, the NPort can also verify if the remote host is the correct server or not.

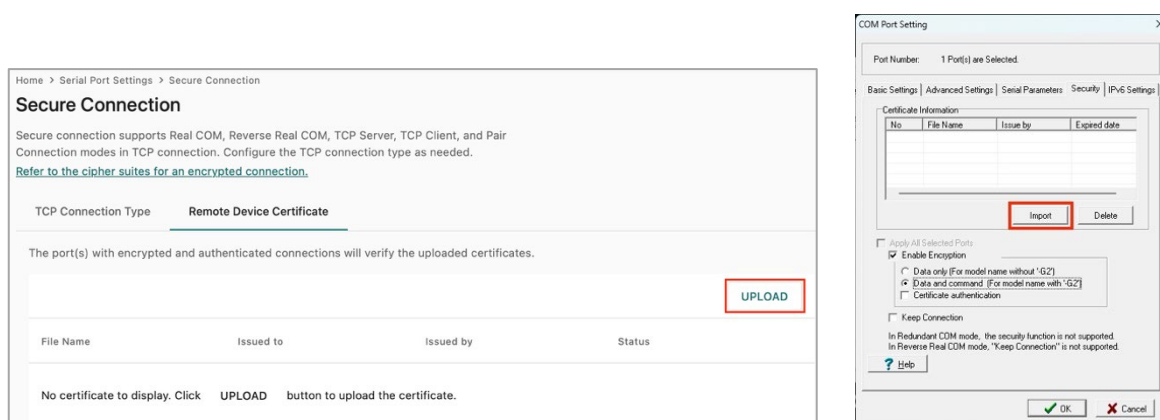
Please find the **Serial Port Settings > Secure Connection** and click the **CONFIGURE** button to select "Encrypted connection" to start the negotiation with the remote host how to encode the TCP session between each other. And on the host side, user need to execute the NPort Windows Driver Manager and click the COM **Setting** button then switch to the **Security** tab. Enable the Enable Encryption and select Data and command (For model name with '-G2'). Then the NPort IA5000-G2 and the host will select a strongest cipher suite to encode the connection.



If user would like to verify the NPort IA5000-G2 and remote host are the correct targets, he can select "Encrypted and authenticated connection" on NPort and "Certificate authentication" on the NPort Windows Driver Manager.

On NPort, he also need to switch to the Remote Device Certificate tab to click the UPLOAD button to upload the remote host's certificate for authentication.

On NPort Windows Driver Manager, at the same Security tab and click Import button to import the NPort's certificate for authentication.

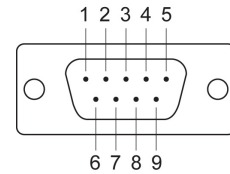


A. Pinouts and Cable Wiring

As mentioned in Chapter 2, the pin assignment of NPort IA5000-G2 Series is as below:

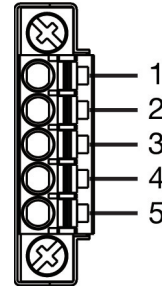
The serial port RS-232/422/485 pin assignment (male DB9):

Pin	RS-232	RS-422 4-wire RS-485	2-wire RS-485
1	DCD	TxD-(A)	-
2	RxD	TxD+(B)	-
3	TxD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	-	-
7	RTS	-	-
8	CTS	-	-
9	-	-	-



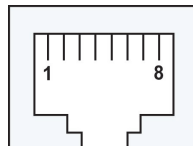
The 5-pin terminal block for the NPort IA5000-TB-G2 models pin assignments are as below:

Pin	RS-232	RS-422 4-wire RS-485	2-wire RS-485
1	GND	GND	GND
2	-	RxD-(A)	Data-(A)
3	TxD	RxD+(B)	Data+(B)
4	-	TxD-(A)	-
5	RxD	TxD+(B)	-



The Ethernet port pin assignment (RJ45):

Pin	RJ45
1	Tx+
2	Tx-
3	Rx+
4	-
5	-
6	Rx-
7	-
8	-

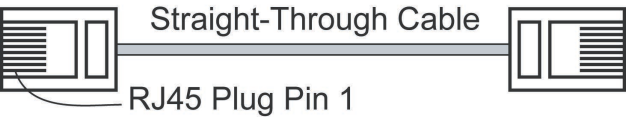


Cable Wiring Diagrams

To connect dserialhe serial devices/Ethernet devices, customize the connecting cable to connect the NPort and the serial/Ethernet devices. Here are some of most popular cable wiring for your reference.

Ethernet Cables

There are two major types of the RJ45 Ethernet cable, straight-through and crossover cables.



Cable Wiring

3	_____	3
6	_____	6
1	_____	1
2	_____	2



Cable Wiring

3	_____	1
6	_____	2
1	_____	3
2	_____	6

Serial Cables

Depending on different connectors on the serial devices, we provide several serial cables to connect easily to the NPort and the device.

CBL-RJ45F9-150

The CBL-RJ45F9-150 is a 150-cm long cable to connect the NPort's DB9 male connector to a serial device with RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

Pin on RJ45	RS-232 signal
6	DCD
4	RxD
5	TxD
1	DTR
3	GND
8	DSR
7	RTS
2	CTS
-	-



CBL-RJ45SF9-150

Industrial applications such as the factory floor are typically electrically noisy environments. The CBL-RJ45SF9-150 is a 150-cm long cable, shielded to protect the signals from the noise and connect the NPort's DB9 male connector to a serial device with a RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

Pin on RJ45	RS-232 signal
6	DCD
4	RxD
5	TxD
1	DTR
3	GND
8	DSR
7	RTS
2	CTS
-	-



CN-20070

The CN-20070 is a 150-cm long cable to connect the NPort's DB9 male connector to a serial device with a 10-pin RJ45 serial connector. The pin assignment of this cable is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-
10	-

Pin on 10-pin RJ45	RS-232 signal
1	DCD
5	RxD
6	TxD
2	DTR
7	GND
9	DSR
8	RTS
3	CTS
-	-
-	-



B. Accessory Introduction

Moxa provides different accessories for different user scenarios. The scenarios will be introduced with the appropriate accessory in this appendix.

Convert the DB9 Connector to Other Connectors

The DB9, RJ45 and terminal block are the most popular interfaces on serial communications. The NPort device server has built-in DB9 connector as the default. Moxa provides a connector to convert the DB9 interface to other connectors.

ADP-RJ458P-DB9F

The ADP-RJ458P-DB9F is a connector that transforms the NPort's DB9 male connector to an 8-pin RJ45 serial connector. The pin assignment of this connector is as below:

Pin on DB9 male	RS-232 signal
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	-

Pin on RJ45	RS-232 signal
6	DCD
4	RxD
5	TxD
1	DTR
3	GND
8	DSR
7	RTS
2	CTS
-	-



Mini DB9F-to-TB

The Mini DB9F-to-TB is a connector that transforms the NPort's DB9 male connector to a 5-pin terminal block serial connector. This connector usually is used on a RS-422/RS-485 application. The pin assignment of this connector is as below:

Pin on DB9 male	RS-422 signal	4w RS-485 signal	2w RS-485 signal
1	TxD-(A)	TxD-(A)	-
2	TxD+(B)	TxD+(B)	-
3	RxD+(B)	RxD+(B)	Data+(B)
4	RxD-(A)	RxD-(A)	Data-(A)
5	GND	GND	GND
6	-	-	-
7	-	-	-
8	-	-	-
9	-	-	-



LB-DB9F-G-01

The LB-DB9F-G-01 is a loop-back connector for the NPort's DB9 male connector. It shortens Pin2 and Pin3;;Pin4, Pin6, and Pin7; and Pin8 and Pin1, so the serial port can have a self-test to verify if the serial communication works properly. The pin assignment of this connector is as below:

Pin on DB9 male	RS-232 signal	Notes
1	DCD	Shorted with Pin7, Pin8
2	RxD	Shorted
3	TxD	
4	DTR	Shorted with Pin6
5	GND	-
6	DSR	Shorted with Pin4
7	RTS	Shorted
8	CTS	
9	-	-



Selecting Suitable Power Adapter Depends on the Environment

The standard temperature models (NPort IA5100-G2, NPort IA5200-G2, and NPort IA5400-G2) default will NOT be shipped with a power adapter. Since the product provides a terminal block power input, we assume most of the customers will use a DIN-rail type power supplies and directly connect the wire cables by their own.

In case some of the customer may prefer to use power adapters, here are the list of the power adapters we provide and please select one to suitable for your region.

- PWR-12050-AU-S1: with the Australia power plug
- PWR-12050-CN-S1: with the China power plug
- PWR-12050-EU-S1: with the European power plug
- PWR-12050-IN-S1: with the India power plug and certificate
- PWR-12050-KR-S1: with the Korea power plug and certificate
- PWR-12050-UK-S1: with the United Kingdom power plug and certificate
- PWR-12050-USJP-S1: with the United States and Japan power plug

With these power adapters, the operating temperature is from 0 to 40 degrees Celsius. Generally, the NPort device server may be set up in an indoor environment, like a control room. If the NPort device server may be set in an outdoor area or a cabinet without air conditioning, the temperature change may be big. Consider to buying the wide temperature models (NPort IA5000-G2-T models), and the power adapters may need to be ordered separately (it is not included in the box of NPort IA5000-G2-T).

- PWR-12150-AU-SA-T: with the Australia power plug
- PWR-12150-CN-SA-T: with the China power plug
- PWR-12150-EU-SA-T: with the European power plug
- PWR-12150-UK-SA-T: with the United Kingdom power plug and certificate
- PWR-12150-USJP-SA-T: with the United States and Japan power plug

With these wide temperature models and power adapters, the operating temperature is from -40 to 75 degrees Celsius. Generally, the NPort device server may be set up in an outdoor environment, like a cabinet at the remote site, where it may be really extremely hot in summer and extremely cold in winter.

For easy connections with a power adapter, Moxa provides a power cable: CBL-PJTB-10, which is a DC barrel jack at one side and with two bare wire V+ and V- at the other side to connect to the NPort IA5000-G2.



NPort IA5000-G2 series are designed as a default DIN-rail mounting device with terminal block power input connector, user can also select a DIN-rail power supply to provide the electricity. This product is intended to be supplied by an external power source (UL Listed/IEC 62368-1/EN 62368-1/BSMI), of which the output complies with ES1/SELV. The output rating is rated at 12 to 48 VDC and minimum current 583 mA. When using a Class I external power source, the power cord should be connected to an outlet with an earthing connection. Moxa has three DIN-rail power supplies user can select a proper one for field usage:

- HDR Power Supply Series: 60 W slim form factor power supplies for DIN-rail mounted products.



- MDR Power Supply Series: 40/60 W slim form factor power supplies for DIN-rail mounted products.



- NDR Power Supply Series: 120/240 W slim form factor power supplies for DIN-rail mounted products.



C. Well-known Port Numbers

In this appendix, we provide a list of well-known port numbers that may cause network problems if you set the NPort IA5000-G2 to one of these ports. Refer to RFC 1700 for well-known port numbers or to the following introduction from the IANA:

The port numbers are divided into three ranges: the Well-Known Ports, the Registered Ports, and the Dynamic and/or Private Ports.

The Well-known Ports range from 0 through 1023. The Registered Ports range from 1024 through 49151.

The Dynamic and/or Private Ports range from 49152 through 65535.

The Well-known Ports are assigned by the IANA, and on most systems, they can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the listed well-known port numbers. For more details, please visit the IANA website at <http://www.iana.org/assignments/port-numbers>.

TCP Socket	Application Service
0	Reserved
1	TCP Port Service Multiplexer
2	Management Utility
7	Echo
9	Discard
11	Active Users (sysstat)
13	Daytime
15	Netstat
20	FTP data port
21	FTP control port
23	Telnet
25	SMTP (Simple Mail Transfer Protocol)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)
53	Domain Name Server (domain)
79	Finger protocol (finger)
80	World Wide Web (HTTP)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use

UDP Socket	Application Service
0	Reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (sysstat)
13	Daytime
35	Any private printer server
39	Resource Location Protocol
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (login)
53	Domain Name Server (domain)
69	Trivial Transfer Protocol (TFTP)
70	Gopher Protocol
79	Finger Protocol
80	World Wide Web (HTTP)
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	SNMP (Simple Network Management Protocol)
162	SNMP Traps
213	IPX (used for IP Tunneling)

D. SNMP MIB List

The NPort IA5000-G2 has built-in SNMP (Simple Network Management Protocol) agent software that supports SNMP Trap, RFC1317 and RS-232-like groups, and RFC 1213 MIB-II. The following table lists the standard MIB-II groups and the variable implementation for the NPort IA5000-G2.

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

Moxa-NPIA5000-G2-MIB

overview	basicSetting	networkSetting	opModeSetting
modelName	serverName	ipConfiguration	portIndex
serialNumber	serverLocation	sysIpAddress	portApplication
firmwareVersion	timeZone	netMask	portMode
macAddress	localTime	defaultGateway	
viewLanSpeed	timeserver	dnsServer1IpAddr	
viewLanModuleSpeed		dnsServer2IpAddr	
upTime		pppoeUserAccount	
moduleType		pppoePassword	
configCRC32		winsFunction	
		winsServer	
		lan1Speed	
		routingProtocol	
		gratuitousArp	
		gratuitousArpSendPerios	

deviceControl Mode	socket Mode
deviceControlTcpAliveCheck	socketTcpAliveCheck
deviceControlMaxConnection	socketInactivityTime
deviceControlIgnoreJammedIp	socketMaxConnection
deviceControlAllowDriverControl	socketIgnoreJammedIp
deviceControlSecure	socketAllowDriverControl
deviceControlLocalTcpPort	socketSecure
deviceControlConnectionDownRTS	socketLocalTcpPort
deviceControlConnectionDownDTR	socketCmdPort
	socketTcpServerConnectionDownRTS
	socketTcpServerConnectionDownDTR
	socketTcpClientDestinationAddress1
	socketTcpClientDestinationPort1
	socketTcpClientDestinationAddress2
	socketTcpClientDestinationPort2
	socketTcpClientDestinationAddress3
	socketTcpClientDestinationPort3
	socketTcpClientDestinationAddress4
	socketTcpClientDestinationPort4
	socketTcpClientDesignatedLocalPort1
	socketTcpClientDesignatedLocalPort2
	socketTcpClientDesignatedLocalPort3
	socketTcpClientDesignatedLocalPort4
	socketTcpClientConnectionControl
	socketUdpDestinationAddress1Begin
	socketUdpDestinationAddress1End
	socketUdpDestinationPort1
	socketUdpDestinationAddress2Begin
	socketUdpDestinationAddress2End
	socketUdpDestinationPort2
	socketUdpDestinationAddress3Begin
	socketUdpDestinationAddress3End
	socketUdpDestinationPort3
	socketUdpDestinationAddress4Begin
	socketUdpDestinationAddress4End
	socketUdpDestinationPort4
	socketUdpLocalListenPort

pairConnection Mode	ethernetModem Mode
pairConnectionTcpAliveCheck	ethernetModemTcpAliveCheck
pairConnectionSecure	ethernetModemTcpPort
pairConnectionDestinationAddress	
pairConnectionDestinationPort	
pairConnectionTcpPort	

terminal Mode	reverseTerminal Mode
terminalTcpAliveCheck	reverseTerminalTcpAliveCheck
terminalInactivityTime	reverseTerminalInactivityTime
terminalAutoLinkProtocol	reverseTerminalTcpPort
terminalPrimaryHostAddress	reverseTerminalAuthenticationType
terminalSecondHostAddress	reverseTerminalMapKeys
terminalTelnetTcpPort	
terminalSshTcpPort	
terminalType	
terminalMaxSessions	
terminalChangeSession	
terminalQuit	
terminalBreak	
terminalInterrupt	
terminalAuthenticationType	
terminalAutoLoginPrompt	
terminalPasswordPrompt	
terminalLoginUserName	
terminalLoginPassword	

printer Mode	dial Mode	dataPacking
printerTcpAliveCheck	dialTERMBINMode	portPacketLength
printerTcpPort	dialPPPDMode	portDelimiter1 Enable
printerGroup	dialSLIPDMode	portDelimiter1
printerQueueNameRaw	dialAuthType	portDelimiter2 Enable
printerQueueNameASCII	dialDisconnectBy	portDelimiter2
printerAppendFromFeed	dialDestinationIpAddress	portDelimiterProcess
	dialSourceIpAddress	portForceTransmit
	dialIpNetmask	
	dialTcpIpCompression	
	dialInactivityTime	
	dialLinkQualityReport	
	dialOutgoingPAPID	
	dialPAPPassword	
	dialIncomingPAPCheck	

comParamSetting	dataBuffering	modemSetting
portAlias	portBufferingEnable	portEnableModem
portInterface	portBufferingLocation	portInitialString
portBaudRate	portBufferingSDFileSize	portDialUp
portBaudRateManual	portSerialDataLoggingEnable	portPhoneNumber
portDataBits		
portStopBits		
portParity		
portFlowControl		
portFIFO		
portOnDelay		
portOffDelay		

welcomeMessage	sysManagement
portEnableWelcomeMessage	enableAccessibleIpList
portMessage	accessibleIpListIndex
	activeAccessibleIpList
	accessibleIpListAddress
	accessibleIpListNetmask
	snmpEnable
	snmpContactName
	snmpLocation
	dDNSEnable
	dDNSServerAddress
	dDNSHostName
	dDNSUserName
	dDNSPassword
	hostTableIndex
	hostName
	hostIpAddress
	routeTableIndex
	gatewayRouteTable
	destinationRouteTable
	netmaskRouteTable
	metricRouteTable
	interfaceRouteTable
	userTableIndex
	userNameUserTable
	passwordUserTable
	phoneNumberUserTable
	radiusServerIp
	radiusKey
	udpPortAuthenticationServer
	radiusAccounting
	sysLocalLog
	networkLocalLog
	configLocalLog
	opModeLocalLog
	mailWarningColdStart
	mailWarningWarmStart
	mailWarningAuthFailure
	mailWarningIpChanged
	mailWarningPasswordChanged
	trapServerColdStart
	trapServerWarmStart
	trapServerAuthFailure
	alarmServerEthernet1LinkDown
	alarmServerEthernet2LinkDown
	alarmServerEthernet3LinkDown
	mailDCDchange
	trapDCDchange
	alarmDCDchange
	mailDSRchange
	trapDSRchange
	alarmDSRchange
	emailWarningMailServer
	emailRequiresAuthentication
	emailWarningUserName
	emailWarningPassword
	emailWarningFromEmail
	emailWarningFirstEmailAddr
	emailWarningSecondEmailAddr

welcomeMessage	sysManagement
	emailWarningThirdEmailAddr
	emailWarningFourthEmailAddr
	snmpTrapReceiverIp
	trapVersion
	httpConsole
	httpsConsole
	telnetConsole
	sshConsole
	lcmReadOnlyProtect
	resetButtonFunction
	loadFactoryDefaultSetting
	maxHttpLoginUsers
	autoLogoutSetting
	loginNotificationMessage
	loginFailureMessage
	userAccountIndex
	activeUserAccount
	accountName
	accountGroupName
	groupName
	networkConfig
	serialConfig
	systemConfig
	adminConfig
	monitorLogWarning
	commonSetting
	pwdMinLength
	pwdComplexityCheckEnable
	pwdComplexityCheckDigitEnable
	pwdComplexityCheckAlphabetEnable
	pwdComplexityCheckSpecialCharEnable
	pwdLifetime
	loginFailureLockoutEnable
	loginFailureLockoutRetrys
	loginFailureLockoutTime

sysStatus	saveConfiguration	restart
remoteIpIndex	saveConfig	restartPorts
monitorRemoteIp		restartSystem
monitorTxCount		
monitorRxCount		
monitorTxTotalCount		
monitorRxTotalCount		
monitorDSR		
monitorDTR		
monitorRTS		
monitorCTS		
monitorDCD		
monitorErrorCountFrame		
monitorErrorCountParity		
monitorErrorCountOverrun		
monitorErrorCountBreak		
monitorBaudRate		
monitorDataBits		
monitorParity		
monitorRTSCTSFlowControl		
monitorXONXOFFFlowControl		
monitorFIFO		

sysStatus	saveConfiguration	restart
monitorInterface		
monitorRTSToggleFlowControl		
relayOutputEthernet1LinkDown		
ethernet1LinkDownAcknowledge		
relayOutputEthernet2LinkDown		
ethernet2LinkDownAcknowledge		
relayOutputEthernet3LinkDown		
ethernet3LinkDownAcknowledge		
portDCDChangedStatus		
portDCDChangedAcknowledge		
portDSRChangedStatus		
portDSRChangedAcknowledge		

E. Event List

The NPort IA5000-G2 provides event logs to help users to troubleshoot. All the events that may be recorded are listed below.

Item	Category	Severity	Default Setting	Event Name	Description
1	System	Notice	Disable	Firmware ready	The system is ready for operation.
2		Informational	Disable	Detect SD card	Mount SD card successfully.
3		Warning	Disable	SD card removed	Detect SD card is removed.
4		Error	Disable	No SD card inserted	No SD card in the system when Port Buffering is enabled and targeting to save in the SD card.
5		Notice	Disable	User trigger reboot	The device was rebooted by the user.
6		Informational	Disable	Configuration changed	A user changed the configuration setting, and the new settings are activated.
7		Notice	Disable	Configuration changed failed	A user changed the configuration setting, but the new settings activated failed.
8		Warning	Disable	Power input failure	The device detects Power Input doesn't provide the electricity (only happens on multiple power inputs models).
9		Informational	Disable	NTP success	The device synchronizes the time with NTP server successfully.
10		Warning	Disable	NTP fail	The device failed to synchronize the time.
11		Informational	Disable	Manual setting time success	Manual setting time success.
12		Notice	Disable	Email fail	The device failed to deliver the email message.
13		Notice	Disable	SNMP inform fail	The device failed to deliver the SNMP Inform message.
14		Notice	Disable	Syslog fail	The device failed to deliver the Syslog message.
15		Notice	Disable	Email service is back	Email service resumed; the event recorded for successfully sending after a failure.
16		Notice	Disable	SNMP inform service is back	SNMP information service resumed; the event recorded for successfully sending after a failure.
17		Notice	Disable	Syslog service is back	Syslog service resumed; the event recorded for successfully sending after a failure.
18		Informational	Disable	LCM display ready	The system detects the LCM display, and it's ready for use.
19		Notice	Disable	LCM display not work	The system detects the LCM display, but it doesn't work.
20	Network	Informational	Disable	Ethernet link up	The Ethernet port is linked up.
21		Notice	Disable	Ethernet link down	The Ethernet port is linked down.
22		Notice	Disable	IP changed	A user changed the network configuration setting, and the new settings are activated.
23		Error	Disable	IP conflict	The device detects an IP conflict, this may make the device malfunctioned.
24		Warning	Disable	Not get IP from DHCP server	The device shall get an IP address from the DHCP server, but it failed.
25		Warning	Disable	Connect DHCP server fail	The device cannot find a DHCP server in the network.
26		Notice	Disable	Using 169.254.x.x IP	The device is using 169.254.x.x IP address, which is abnormal.
27		Informational	Disable	IP renew	IP of the device is renewed (with DHCP enabled).
28		Notice	Disable	Topology change	When Redundant protocol (RSTP or TurboRing) enabled, the Slave port is blocked to prevent data loop. When the master path is broken and the

Item	Category	Severity	Default Setting	Event Name	Description
					network communication is working with the Slave path (only for the models which supports Redundant protocols).
29		Informational	Disable	Network module ready	The network module is detected and ready for communication (only for the models which can plug-in a network module).
30		Informational	Disable	No network module	There is no network module detected (only for the models which can plug-in a network module).
31		Notice	Disable	Network module not work	The system detects the network module, but it doesn't work (only for the models which can plug-in a network module).
32	Security	Warning	Enable	Clear log	Clear all the system logs on the device.
33		Informational	Disable	System log export	The system log is exported.
34		Notice	Enable	Log threshold reached	The number of the log events reached the number of the threshold setting.
35		Informational	Disable	Login success	A user from the IP address login the device successfully.
36		Notice	Enable	Login fail	A user from the IP address try to login the device but failed.
37		Informational	Disable	Account/group changed	A user changed the configuration setting of username, password or group privilege.
38		Warning	Enable	Account lockout	An account is locked out because he failed to login too many times.
39		Informational	Disable	Service enabled	The device enables the service successfully.
40		Notice	Enable	Service disabled	The device disables the service successfully.
41		Warning	Enable	Service enabled/disabled failed	The device tries to enable/disable service failed.
42		Informational	Disable	Syslog certificate export	The Syslog certificate was exported.
43		Notice	Enable	Syslog certificate import	The Syslog certificate was imported.
44		Notice	Enable	Syslog certificate deleted	The Syslog certificate was deleted.
45		Notice	Enable	Syslog certificate expired	The Syslog certificate was expired.
46		Informational	Disable	Syslog certificate will expire	The Syslog certificate will expire in one month.
47		Warning	Enable	Connect authentication server fail	The device failed to connect to the RADIUS/TACACS+ server.
48		Error	Enable	Authentication fail	A user failed to pass the authentication process.
49		Informational	Disable	SSL certificate export	The SSL certificate was exported.
50		Notice	Enable	SSL certificate import	The SSL certificate was imported.
51		Notice	Enable	SSL certificate deleted	The SSL certificate was deleted.
52		Notice	Enable	SSL certificate expired	The SSL certificate was expired.
53		Notice	Enable	SSL certificate regenerated	The SSL certificate was regenerated.
54		Warning	Enable	DoS Defense is triggered	The DoS Defense functions were triggered.
55		Informational	Disable	Password reached lifetime	Account's password reached the lifetime.
56	Maintenance	Informational	Disable	Firmware upgrade	The firmware is upgraded.

Item	Category	Severity	Default Setting	Event Name	Description
57		Warning	Disable	Firmware upgrade fail	A user tried to upgrade the firmware, but the device rejects to upgrade it because of the wrong file format/checksum error.
58		Notice	Disable	Configuration import	The config file was imported.
59		Warning	Disable	Configuration import fail	The device failed to import a config file because of the wrong file format or invalid authentication.
60		Informational	Disable	Configuration export	The config file was exported.
61		Notice	Disable	Load factory default	Load factory default.
62		Notice	Disable	Load customized default	Load customized default.
63		Notice	Disable	Log collection	When use click One-click data collection function to collect the event logs and relative information for diagnostics purpose, the device will record this event.
64	Serial	Informational	Disable	Serial port CTS changed	The CTS signal of the serial port is turned ON from OFF or is turned OFF from ON.
65		Informational	Disable	Serial port DSR changed	The DSR signal of the serial port is turned ON from OFF or is turned OFF from ON.
66		Informational	Disable	Serial port DCD changed	The DCD signal of the serial port is turned ON from OFF or is turned OFF from ON.
67		Notice	Disable	Port OP mode disabled	The Operation mode of the port is disabled; the port cannot be connected by any network devices.
68		Informational	Disable	Port connect	The session is connected on the port.
69		Notice	Disable	Port disconnect	The session is disconnected on the port.
70		Error	Disable	Port authentication fail	A user failed to login on the port in terminal, Reverse Terminal. or dial-in/out operation modes.
71		Notice	Disable	Port restart	The serial port is restarted.
72		Notice	Disable	Serial data error	There is an error happened on the received serial data of the Port, for example, a framed error, parity error, or overrun error.

F. Command List of the Serial Console

The NPort IA5000-G2 provides a serial console as a command-line interface for the user who prefers to log in with the serial port. The serial console only supports limited configuration settings. View the basic information and configure the network settings.

When you first enter the serial console, input ? to view a list of basic commands and the description of each command.

```
#  
# ?  
show          - Show running system information  
configure     - Enter configuration mode  
reload        - Halt and perform a cold restart  
quit          - Exit command line interface  
# _
```

For the users with READ privilege of the serial console, execute the **show** command to view relative settings. For the users with WRITE privilege, execute the **configure** command to set or modify relative settings.

Input # configure to access the subcategory to show or change the network related settings.

Set statis ip address of the network interface:

Syntax Description	ip	Configure IP parameters
	address	Configure IPv4 address parameters
	static	Configure static IPv4 address
	<i>ipv4-address</i>	The IPv4 address
	<i>ipv4-netmask</i>	The IPv4 subnet mask
	dhcp	Assign the IPv4 address by DHCP
Defaults	IPv4 Address: 192.168.127.254 IPv4 Netmask: 255.255.255.0 IPv4 Gateway: 0.0.0.0	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	# configure (config)# ip address static 192.168.127.254 255.255.255.0	
Related Commands	no ip address	

Set the default gateway:

Syntax Description	ip	Configure IP parameters
	default-gateway	Configure IPv4 default gateway address
	<i>ipv4-address</i>	The IPv4 address
Defaults	N/A	
Command Modes	Global Configuration	
Usage Guidelines	N/A	
Examples	# configure (config)# ip default-gateway 192.168.127.1	
Related Commands	no ip address	

Show the network status:

Syntax Description	show	Display configuration/status information
	ip	Display IP information
	management	Display IP information
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	# show ip management	
	IPv4 IP configuration : DHCP IP address : 192.168.127.254 Subnet mask : 255.255.255.0 Default gateway : 0.0.0.0 DNS server : 0.0.0.0 #	
Related Commands	N/A	

User can input # reload to access the sub-category to show or modify the network related settings.

Restart the device:

Syntax Description	reload	Halt and perform a cold restart.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	# reload	
	Proceed with reload? [y/n] y Resetting system...	
Related Commands	N/A	

Reset the device to factory default settings:

Syntax Description	reload	Halt and perform a cold restart.
	factory-default	Halt and perform a cold restart with factory default.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	# reload factory-default	
	Proceed with reload to factory default? [y/n] y Reset to factory default...	
Related Commands	N/A	

Logout the serial console:

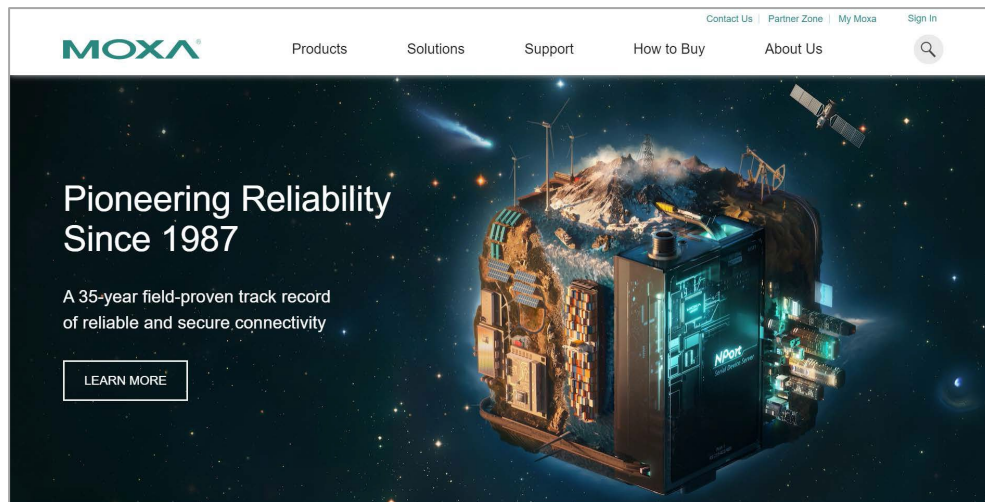
Syntax Description	quit	Logout from the command line interface.
Defaults	N/A	
Command Modes	Privileged EXEC	
Usage Guidelines	N/A	
Examples	# quit	
Related Commands	N/A	

G. How to Become a Registered User

By becoming a registered user on Moxa.com, you gain access to all updates for your purchased or interested products, including software and documentation. To become a registered user and receiving all updates, you need to do following:

Register a Moxa Account

1. Go to Moxa.com and click '**Sign in**' at the top-right corner.



2. In the Sign-in page, click "[Create your Moxa member account](#)" as below.'

Please sign in

Email*

Please input your email address

Password*

Forgot your password?

Password is required

SIGN IN

Not a member? [Create your Moxa member account](#)

3. Fill the necessary fields.

Create New Account

Work Email*

First Name* Last Name*

Company*

Phone*

Region*

--Select--

Please input a password*


Request for Product Updates

1. Go to the specific product page to receive updates. Click **"+FOLLOW UPDATE"**

Home > Products > Industrial Edge Connectivity > Serial Device Servers > Terminal Servers > NPort 6100/6200 Series

NPort 6100/6200 Series




1/2-port RS-232/422/485 secure terminal servers





Features and Benefits

- Secure operation modes for Real COM, TCP Server, TCP Client, Pair Connection, Terminal, and Reverse Terminal
- Supports nonstandard baudrates with high precision
- NPort 6250: Choice of network medium: 10/100BaseT(X) or 100BaseFX
- Enhanced remote configuration with HTTPS and SSH
- Port buffers for storing serial data when the Ethernet is offline
- Supports IPv6
- Generic serial commands supported in Command-by-Command mode
- Security features based on IEC 62443


Certifications





2. Once completes, see the FOLLOW UPDATES button changes.

GET A QUOTE

 FOLLOWING

