NPort 5000 Series User Manual

NPort 5000/5000A/IA5000/IA5000A/5000AI-M12 Series

Version 7.5, May 2025

www.moxa.com/products

NPort 5000 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

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual

Learn how to configure and use your Moxa NPort device server. The following products are covered by this manual:

NPort Family	Model Series	Introduction
NPort 5000	NPort 5110/5130/5150 Series NPort 5210/5230/5232 Series NPort 5410/5430/5450 Series NPort 5610/5630/5650 Series NPort 5610-8-DT/5650-8-DT Series NPort 5610-8-DTL/5650-8-DTL Series	NPort 5000 Series device servers make serial devices network-ready in an instant. The different form factors of the servers provide flexible options for users to connect legacy devices to an IP-based Ethernet LAN.
NPort 5000A	NPort 5110A/5130A/5150A Series NPort 5210A/ 5230A/5250A Series NPort 5150AI-M12/5250AI-M12/5450AI-M12 Series NPort P5150A Series	The NPort 5000A device servers make serial devices network-ready in an instant and give your PC software direct access to serial devices from anywhere on the network. The NPort 5000A device servers are ultra-lean, rugged, and user-friendly, making simple and reliable serial-to-Ethernet solutions possible.
NPort IA5000/IA5000A	NPort IA5150/IA5250 Series NPort IA5150A/IA5250A/IA5450A Series	NPort IA 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.

2. Getting Started

In this chapter, we explain how to install a Moxa NPort device server for the first time. There are four ways to access the Moxa NPort's configuration settings: Windows utility, web console, serial console, or Telnet console.

NPort products support the following configuration options:

- Windows Utilities: NPort Administrator; Device Search Utility and Windows Driver Manager
- Web Console
- Quick Setup Wizard*
- Serial Console**
- Telnet Console

* Does not support 5100/5200/IA5000 series

** Only available for the NPort Series that has RS-232 interface.

Installing Your NPort Device Server

This section describes how to connect an NPort device server to your serial devices for the first time. We cover Wiring Requirements, Connecting the Power, Grounding the NPort Device Server, Connecting to the Network, Connecting to a Serial Device, and LED Indicators.

Wiring Requirements

ATTENTION

Safety First!

Be sure to disconnect the power cord before installing and/or wiring your NPort Device Server.

Wiring Caution!

Calculate the maximum current allowed in each power wire and common wire. Observe all electrical codes dictating the maximum current allowed for each wire size. If the current goes above the allowed maximum, the wiring could overheat, causing serious damage to your equipment.

Temperature Caution!

Be cautious when handling the NPort device server. When plugged in, the NPort's internal components generate heat, and consequently, the casing may be too hot to the touch. When installed with other components, make sure that there is at least a 2-cm clearance on all sides of the NPort device server in order to allow proper heat dissipation.

You should observe:

- Use separate paths to route wiring for power and devices. If the 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.

- You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wires that share similar electrical characteristics can be bundled together.
- Keep input wiring and output wiring separately.
- Where necessary, we strongly advised that you label wires to all devices in the system.

Connecting the Power

Connect the power line with the NPort's power input. If the power is properly supplied, the "Ready" LED will show a solid red color until the system is ready, at which time the "Ready" LED will change to a green color.

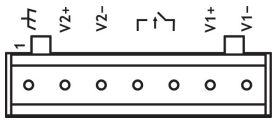
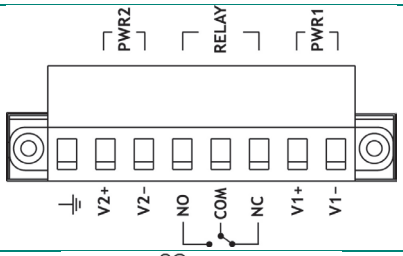
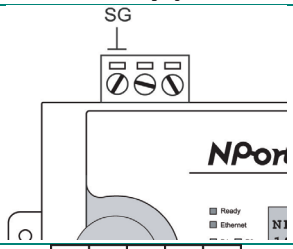
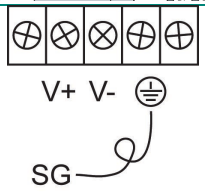
Grounding the NPort Device Server

Note: This section only applies if your NPort's power input is on a terminal block.

Grounding and wire routing help limit the effects of noise caused by electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface before connecting the devices.

WARNING

NPorts with a power terminal block are intended to be mounted to a well-grounded mounting surface, such as a metal panel.

Type of Power Terminal Block	Shielded Ground (SG)	Applicable Products
	The Shielded Ground (sometimes called Protected Ground) contact is the left most contact of the 7-pin power terminal block connector when viewed from the angle shown here. Connect the SG wire to an appropriate grounded metal surface.	NPort IA5000 Series
	The Shielded Ground (sometimes called Protected Ground) contact is the left most contact of the 8-contact power terminal block connector when viewed from the angle shown here. Connect the SG wire to an appropriate grounded metal surface.	NPort IA5000A Series
	The Shielded Ground (sometimes called Protected Ground) contact is the left most contact of the 3-pin power terminal block connector when viewed from the angle shown here. Connect the SG wire to an appropriate grounded metal surface.	NPort 5200/5400 Series NPort 5200A Series
	The Shielded Ground (sometimes called Protected Ground) contact is the second contact from the right of the 5-pin power terminal block connector on the rear panel of NPort 5600 VDC models. Connect the SG wire to the earth ground.	NPort 5600 Series

Connecting to the Network

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

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

ATTENTION

NPort IA5000/IA5000A/5600-8-DT Series of NPorts has two Ethernet ports that can create an open chain of NPort IA5000/IA5000A/5600-8-DT device servers. Be careful not to connect the Ethernet ports of the two device servers at the ends of the chain.

In other words, NPort IA5000/IA5000A/5600-8-DT Series of NPorts do NOT support closed chains.

Connecting to a Serial Device

Connect a serial data cable between the NPort and the serial device. Serial data cables must be purchased separately. They are not provided with the NPort.

LED Indicators

NPort 5100/5100A/P5150A Series

LED Name	LED Color	LED Function	
Ready	Red	Steady on:	Power is on, and the NPort is booting up.
		Blinking:	Shows an IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady on:	Power is on, and the NPort is functioning normally.
		Blinking:	The device server has been located by NPort Administrator's Location function.
	Off	Power is off, or a power error condition exists.	
Link	Orange	Steady on:	The device is connected to a 10 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 10 Mbps.
	Green	Steady on:	The device is connected to a 100 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 100 Mbps.
	Off	The Ethernet cable is disconnected or has a short.	
Tx/Rx	Orange	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	Data is NOT being transmitted or received through the serial port.	

NPort 5200/5200A/5400 Series

LED Name	LED Color	LED Function	
Ready	Red	Steady on:	Power is on, and the NPort is booting up.
		Blinking:	Shows an IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady on:	Power is on, and the NPort is functioning normally.
		Blinking:	The device server has been located by NPort Administrator's Location function.
	Off	Power is off, or a power error condition exists.	
Link (Ethernet)	Orange	Steady on:	The device is connected to a 10 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 10 Mbps.
	Green	Steady on:	The device is connected to a 100 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 100 Mbps.
	Off	The Ethernet cable is disconnected or has a short.	
P1, P2, (P3, P4)	Orange	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	Data is NOT being transmitted or received through the serial port.	

NPort 5600 Series (Rackmount)

LED Name	LED Color	LED Function	
Ready	Red	Steady on:	Power is on and the NPort is booting up.
		Blinking:	Shows an IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady on:	Power is on, and the NPort is functioning normally
		Blinking:	The device server has been located by NPort Administrator's Location function.
	Off	Power is off, or a power error condition exists.	
Tx/Rx, P1 to P16	Orange	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	Data is NOT being transmitted or received through the serial port.	
LAN	Green	The Ethernet port is connected, but data is NOT being transmitted.	
	Blinking	The Ethernet port is connected, and data is being transmitted.	
	Off	The Ethernet port is disconnected.	
PWR	Green	Power cable is connected and provides electricity properly.	
	Off	Power cable is disconnected.	

NPort 5600-8-DT/DTL Series

LED Name	LED Color	LED Function	
PWR	Red	Power is on.	
	Off	Power is off.	
Ready	Green	Steady on:	The NPort is operational.
		Blinking:	The NPort is responding to NPort Administrator's Location function, or the NPort is being reset to factory defaults.
	Off	Power is off, or power error condition exists.	
Fault	Red	Shows an IP conflict, or the DHCP or BOOTP server did not respond properly.	
	Off	No fault condition detected.	
	Off	Blinking:	Network is connected, data is being transmitted.
ETH 1, ETH2	Green	Steady on	Network is connected, no data is being transmitted.
	Off	Blinking	Network is connected, data is being transmitted.
In Use (P1 to P8)	Green	Serial port has been opened by server side software.	
	Off	Serial port is not currently opened by host side software.	
Tx/Rx (P1 to P8)	Green (Tx)	Serial device is transmitting data.	
	Orange(Rx)	Serial device is receiving data.	
	Off	No data is flowing to or from the serial port.	

NPort 5000AI-M12 Series

LED Name	LED Color	LED Function	
PWR	Green	Power is being supplied to the power input.	
Ready	Red	Steady on:	Power is on, and the NPort is booting up.
		Blinking:	Shows an IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady on:	Power is on, and the NPort is functioning normally
		Blinking:	The device server has been located by the NPort Administrator's Location function.
	Off	Power is off, or a power error condition exists.	
10M, 100M	Orange	Steady on:	The device is connected to a 10 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 10 Mbps.
	Green	Steady on:	The device is connected to a 100 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 100 Mbps.
	Off	The Ethernet cable is disconnected or has a short.	
P1, P2, P3, P4	Orange	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	Data is NOT being transmitted or received through the serial port.	

NPort IA5000/IA5000A Series

LED Name	LED Color	LED Function	
PWR1, PWR2	Red	Power is being supplied to power input PWR1, PWR2.	
Ready	Red	Steady on:	Power is on, and the NPort IA is booting up.
		Blinking:	Shows an IP conflict, the DHCP or BOOTP server did not respond properly, or a relay output was triggered. When the above two conditions occur at the same time, check the relay output first. If after resolving the relay output and the Ready LED is still blinking, then there is an IP conflict, or the DHCP or BOOTP server did not respond properly.
	Green	Steady on:	Power is on and the NPort IA is functioning normally.
		Blinking:	The device server has been located by the NPort Administrator's Location function.
	Off	Power is off, or a power error condition exists.	
E1, E2	Orange	Steady on:	The device is connected to a 10 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 10 Mbps.
	Green	Steady on:	The device is connected to a 100 Mbps Ethernet connection, but data is NOT being transmitted.
		Blinking:	The Ethernet port is connected, and data is being transmitted at 100 Mbps.
	Off	The Ethernet cable is disconnected or has a short.	
P1, P2, (P3, P4)	Orange	The serial port is receiving data.	
	Green	The serial port is transmitting data.	
	Off	Data is NOT being transmitted or received through the serial port.	
FX*	Orange	Steady on:	The fiber port is connected, but data is NOT being transmitted.
		Blinking:	The fiber port is connected, and data is being transmitted.

*Only applies to NPort IA5000 fiber models.

Beeper Definition

Beeper Timing	Frequency (Length/Intervals/Times)	Definition
Startup	100 ms / 100 ms / 2	When the NPort is ready to run
Locating	100 ms / 900 ms / when the user stops the function	When the NPort is located by a utility such as DSU

RS-485 Port's Adjustable Pull High/Low Resistor

For some applications, you may need to use termination resistors to prevent the reflection of serial signals. When using termination resistors, it is important to set the pull high/low resistors correctly so that the electrical signal is not corrupted. Refer to **Appendix B** for detailed instructions on how to set the pull high/low resistor values for different models.

Windows Utility for the NPort

Moxa provides a few types of software with the NPort 5000 Series:

- The Device Search Utility (also known as DSU) includes broadcast search for all the NPort 5000s accessible over the network and basic configuration for a quick start.
- The NPort Administrator Suite is for COM mapping, a full set of configuration and monitoring tools. It serves the NPort 5000 Series only.
- The NPort Windows Driver Manger is for COM mapping of Real COM operation mode.

All utilities are available to download from Moxa's website: https://www.moxa.com/en/support/product-support/software-and-documentation, and select your product and look for the driver for your OS platform.

For more detailed information on how to use these useful utilities, refer to **Chapter 7**.

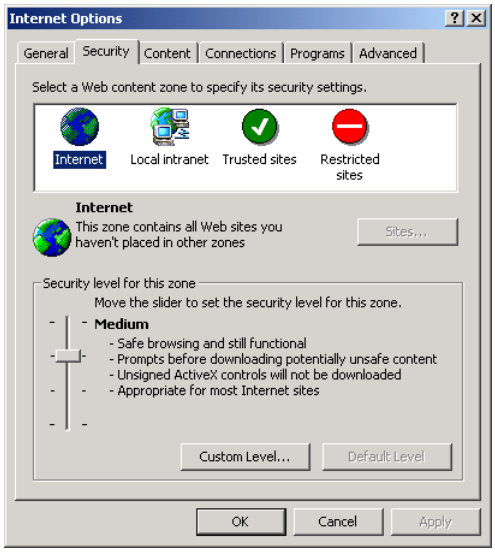
You may also use the web console, serial console, or Telnet to configure the device server. Refer to the section Configuration by Web Console, Configuration by Serial Console, and Configuration by Telnet Console for additional information on using these consoles.

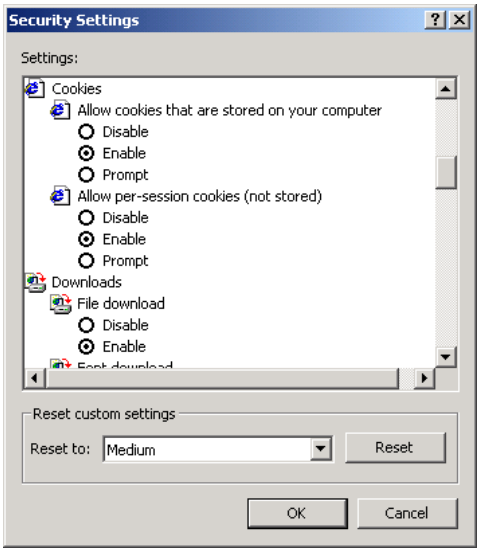
Configuration by Web Console

The Web Console is the most user-friendly way to configure NPort products. In this section, we cover a device server's general settings.

Opening Your Browser

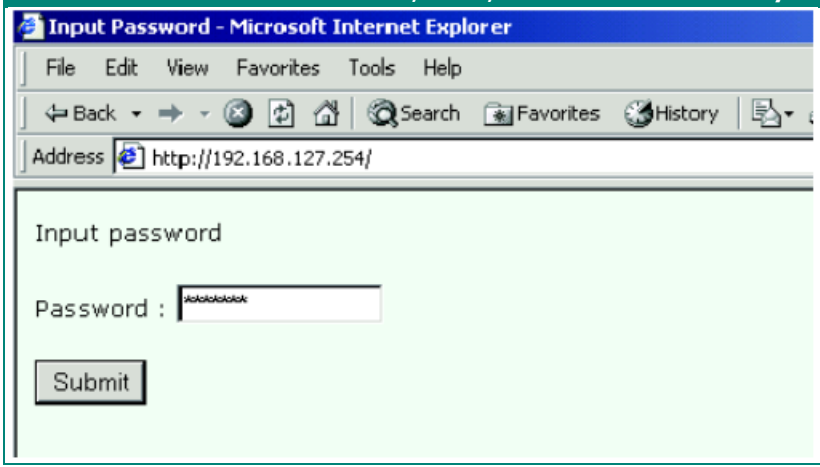
1. Open your browser with the cookie functionality enabled. (To enable your browser for cookies, right-click on your desktop's Internet Explorer icon, select **Properties**, click on the **Security** tab, and then select the three Enable options as shown in the figure below.)



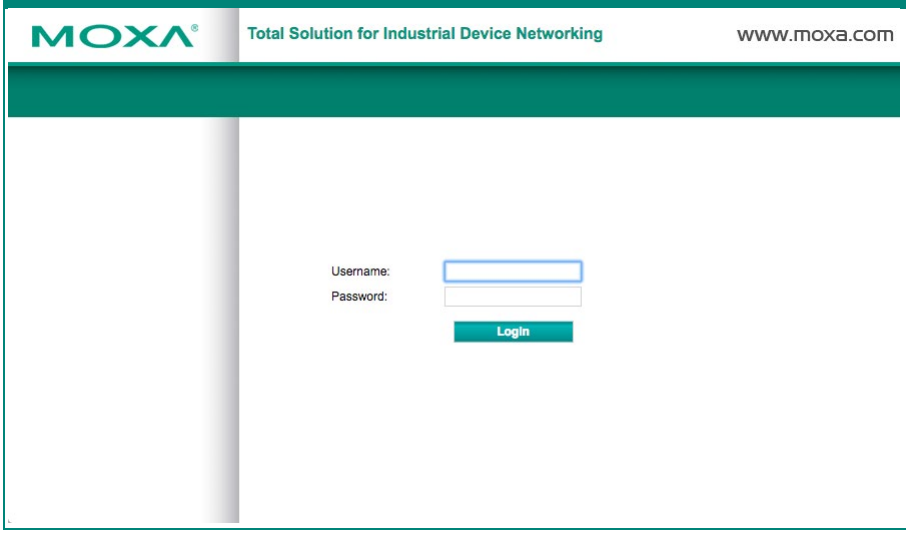


2. Type 192.168.127.254 in the **Address** input box (use the correct IP address if different from the default), and then press **Enter**.
3. For the overall NPort 5000 Series, you will be prompted to enter the username and password to access the NPort web console. Before configuring the NPort, you will need to unlock it first. Right-click the unit in the Configuration screen and select **Unlock** in the pop-up menu. The default username and password are **admin** and **moxa**, respectively. For the NPort 5100, 5200, and IA5000 Series, only the password is required to log in.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series

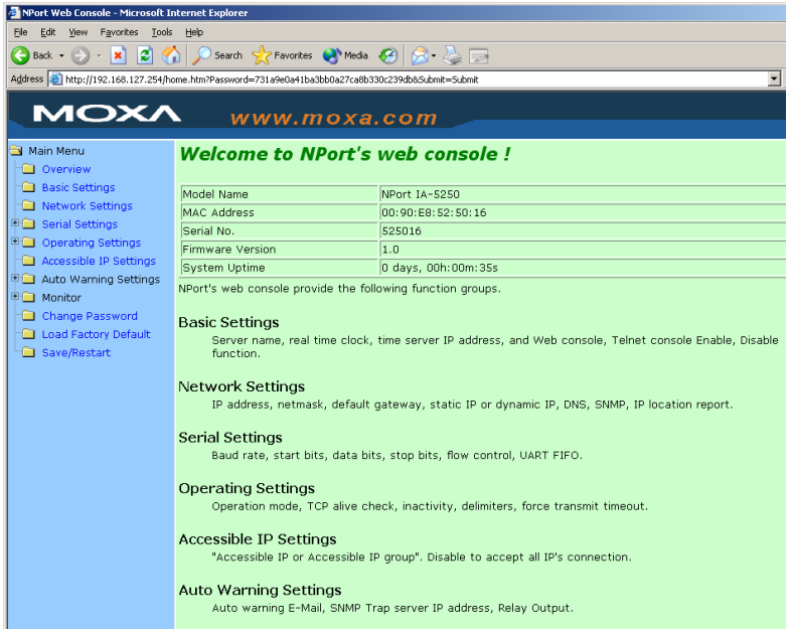


ATTENTION

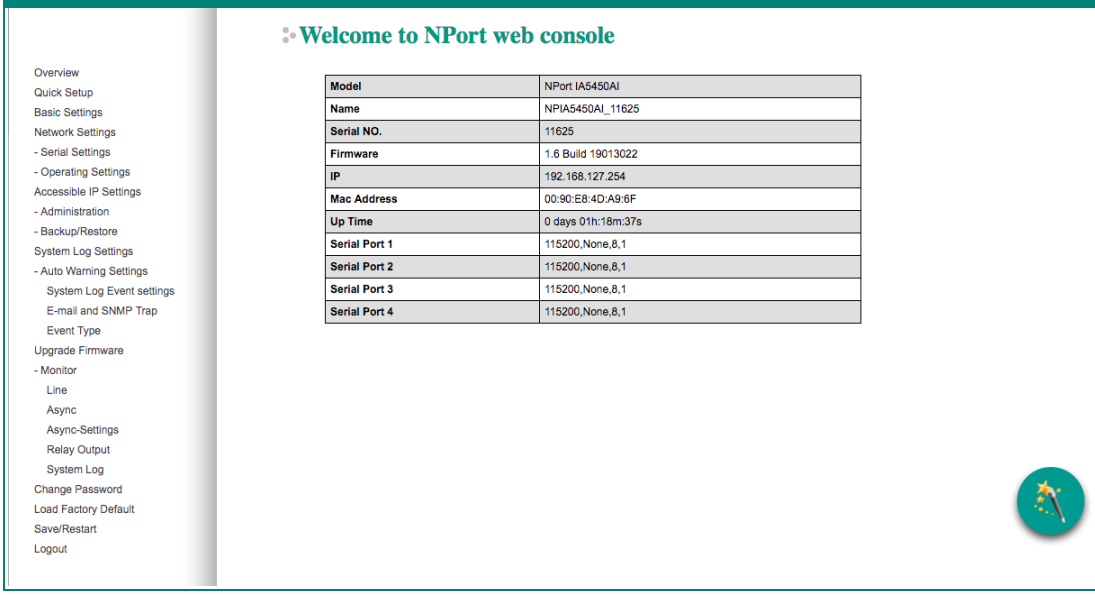
If you use other web browsers, remember to enable the functions to "allow cookies that are stored on your computer" or "allow per-session cookies." NPort device servers use cookies only for "password" transmissions.

The NPort home page will open. On this page, you can see a brief description of the Web Console's function groups.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series



ATTENTION

If you can't remember the password, the ONLY way to configure the NPort is to load factory defaults by using the **Reset** button near the NPort's Ethernet port.

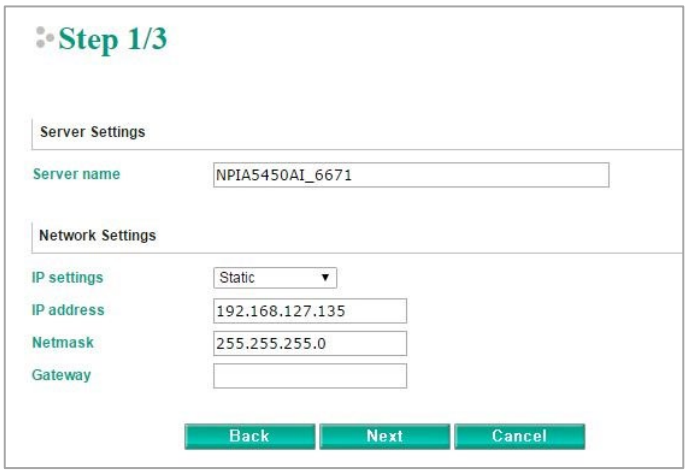
Remember to use NPort Administrator (for the NPort 5000 and the NPort IA5000 Series) to export the configuration file when you have finished the configuration. After using the **Reset** button to load factory defaults, your configuration can be easily reloaded into the NPort by using the NPort Administrator Import function. Refer to **Chapter 5** for details about using the Export and Import functions.

Quick Setup (available for the NPort 5000A Series only)

Quick Setup streamlines configuration of your NPort into three basic and quick steps that cover the most used settings. While in Quick Setup, you may click the **Back** button at any time to return to the previous step or click the **Cancel** button to reverse all settings. For more detailed settings, refer to the **Basic Settings**, **Network Settings**, **Serial Settings**, and **Operating Settings** sections later in this chapter.

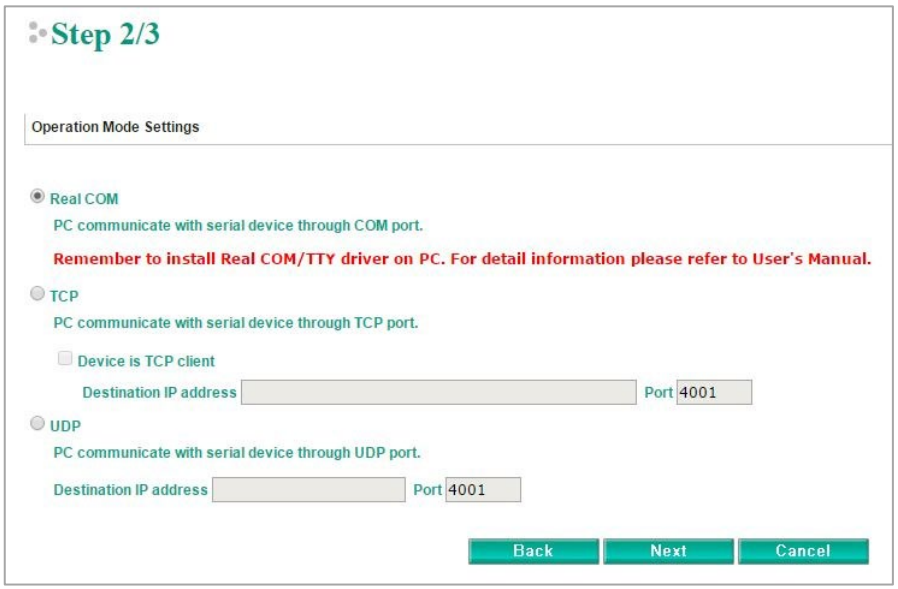
Step 1/3

In Step 1/3, you must assign a valid IP address to the NPort before it will work in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. In addition, the server name field is a useful way to specify the location or application of different NPort units.



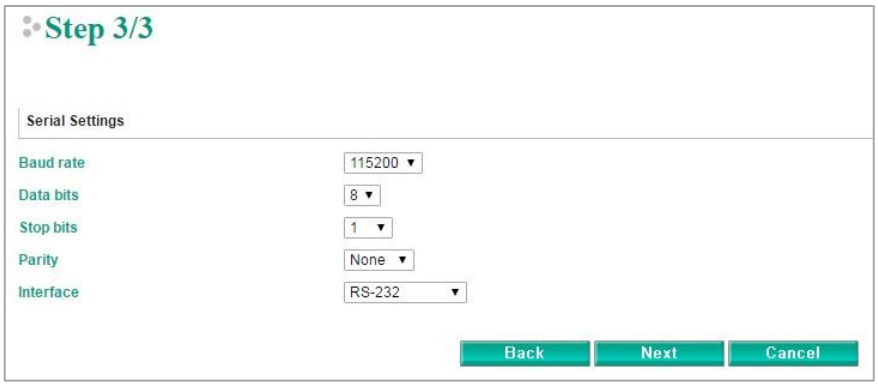
Step 2/3

In Step 2/3, you must specify which operation mode you will use. If your operation mode is not **Real COM**, **TCP Server, TCP Client**, or **UDP mode**, click **Cancel**, return to the main menu, and choose **Operating Settings** to select the correct settings.



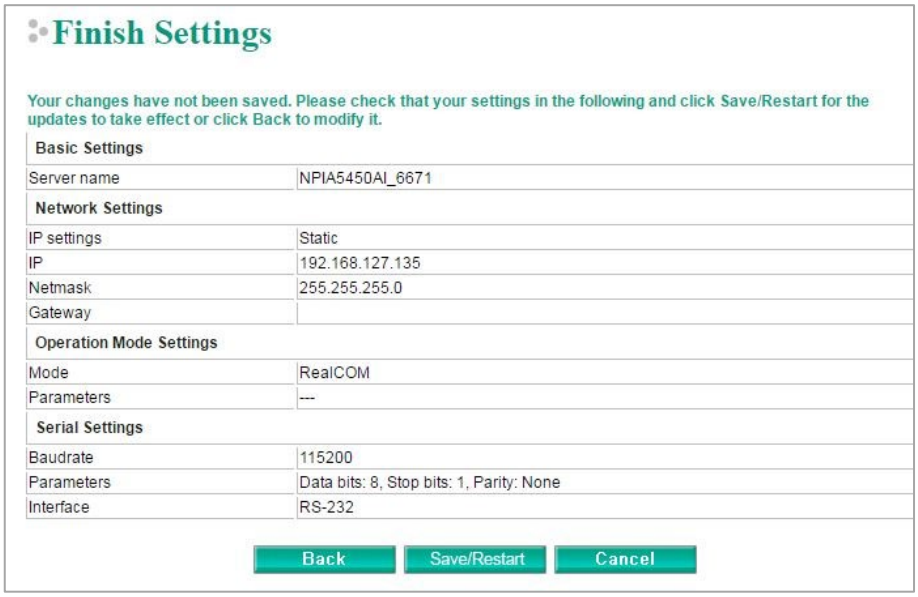
Step 3/3

In Step 3/3, change the **Serial Settings**.



Finish Settings

Review your settings on the **Finish Settings** page to confirm that they are correct and then click the **Save/Restart** button to restart the device with the new settings.

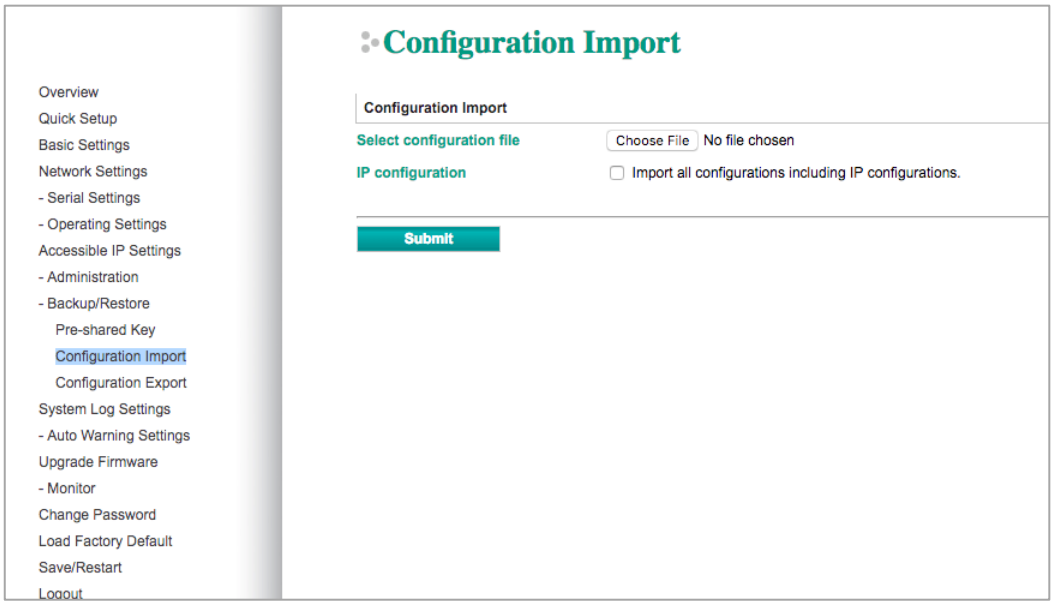


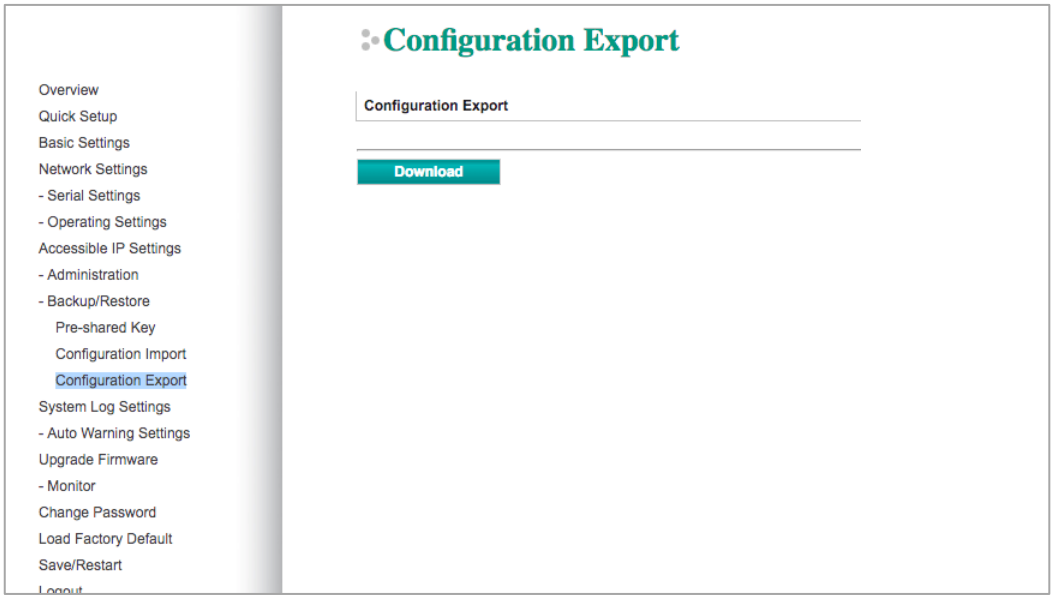
NOTE

If you change the IP address, you cannot use the **Home** button to return to the home page.

Export/Import (Excluding the NPort 5100, 5200, and IA5000 Series)

Export/Import allows you to back up and recover your settings.





The exported configuration file can be encrypted for security with a user-specified export password (the default password is **moxa**), which you may assign in **Pre-shared Key**. Click **Download** to write all configuration data to a fixed file name: **<Servername>.txt**.

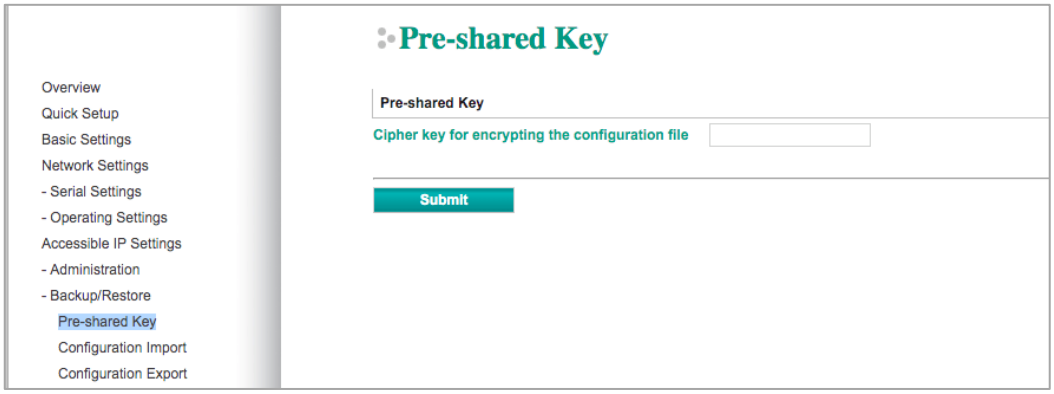
To import the configuration file, you will need to be sure that the pre-shared key stored in the system is the same as the configuration file (which is assigned when exporting the configuration file) to successfully import the configuration file.

If the firmware is not up to the version below, you may need to key in the password manually.

NPort 5100A Series Firmware v1.5
NPort 5200A Series Firmware v1.5
NPort 5150AI Series Firmware v1.4
NPort 5250AI Series Firmware v1.4
NPort 5450AI Series Firmware v1.4
NPort 5600 Series Firmware v3.9
NPort 5600 DT Series Firmware v2.6
NPort 5600 DTL Series Firmware v1.5
NPort IA5150A Series Firmware v1.4
NPort IA5450A Series Firmware v1.6

NOTE

The configuration encrypting function is not available in the NPort 5100, NPort 5200, and NPort IA5000 Series.

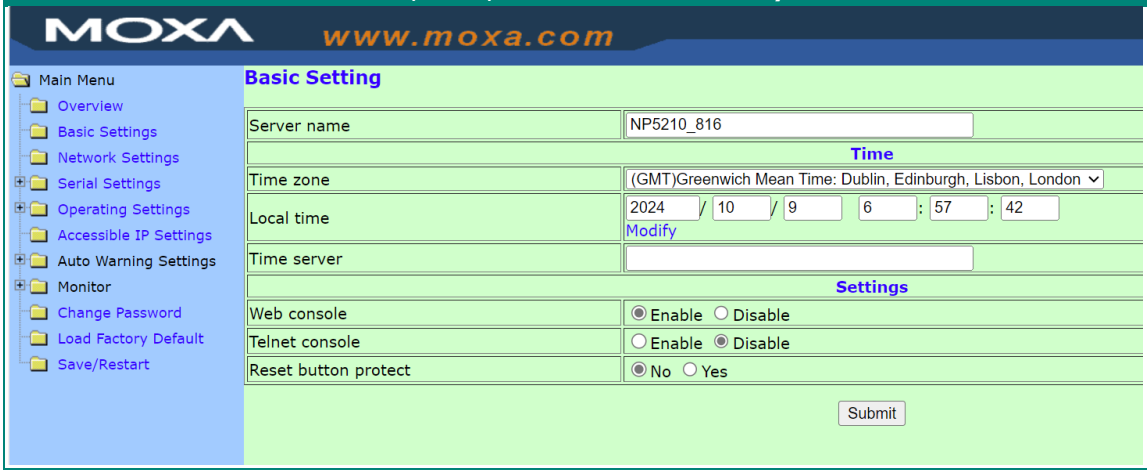


Refer to the table below for the firmware versions that support the encrypted configuration files in the Web Console.

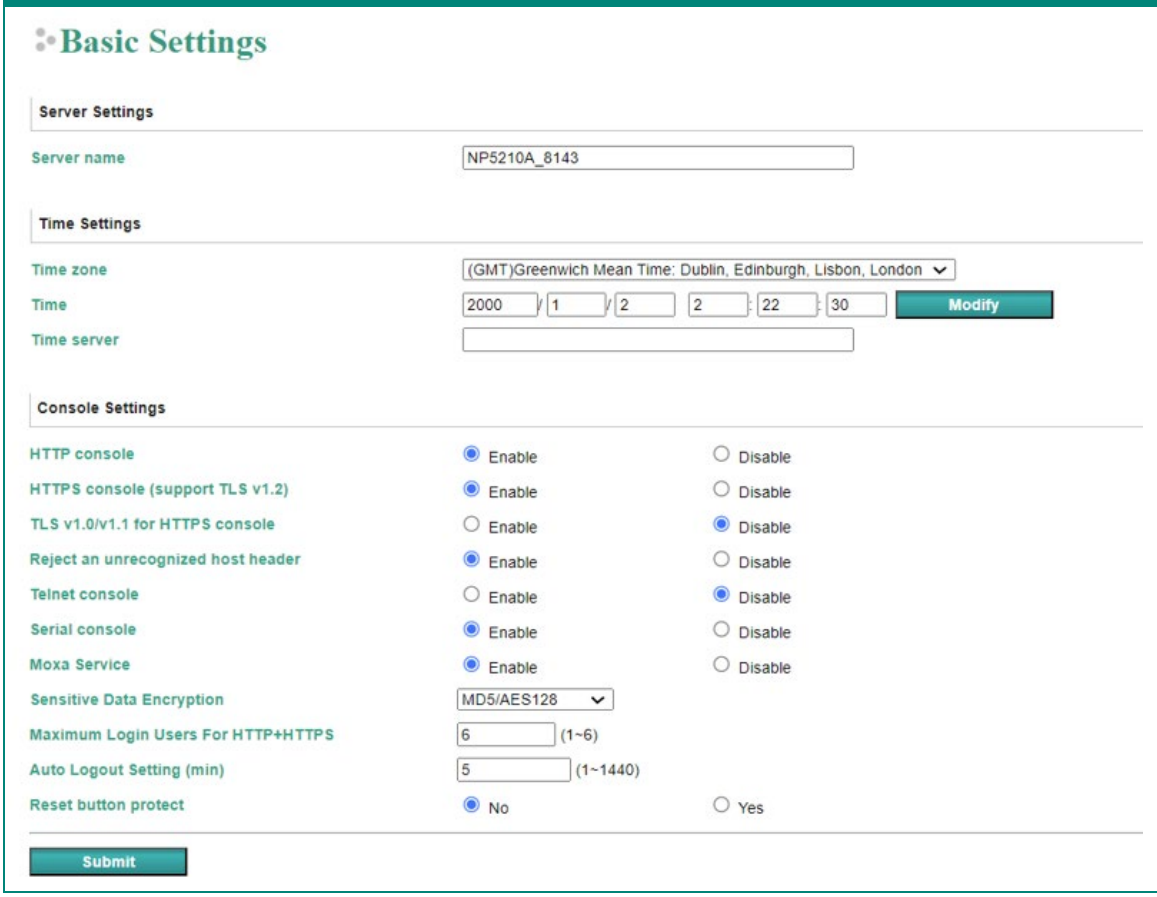
Model Name	Firmware version supporting encrypted configuration files.
NPort 5100A Series	Firmware v1.3 and up
NPort 5200A Series	Firmware v1.3 and up
NPort 5x50AI-M12 Series	Firmware v1.2 and up
NPort IA5150A, NPort IA5250A	Firmware v1.3 and up
NPort IA5450A	Firmware v1.4 and up

Basic Settings

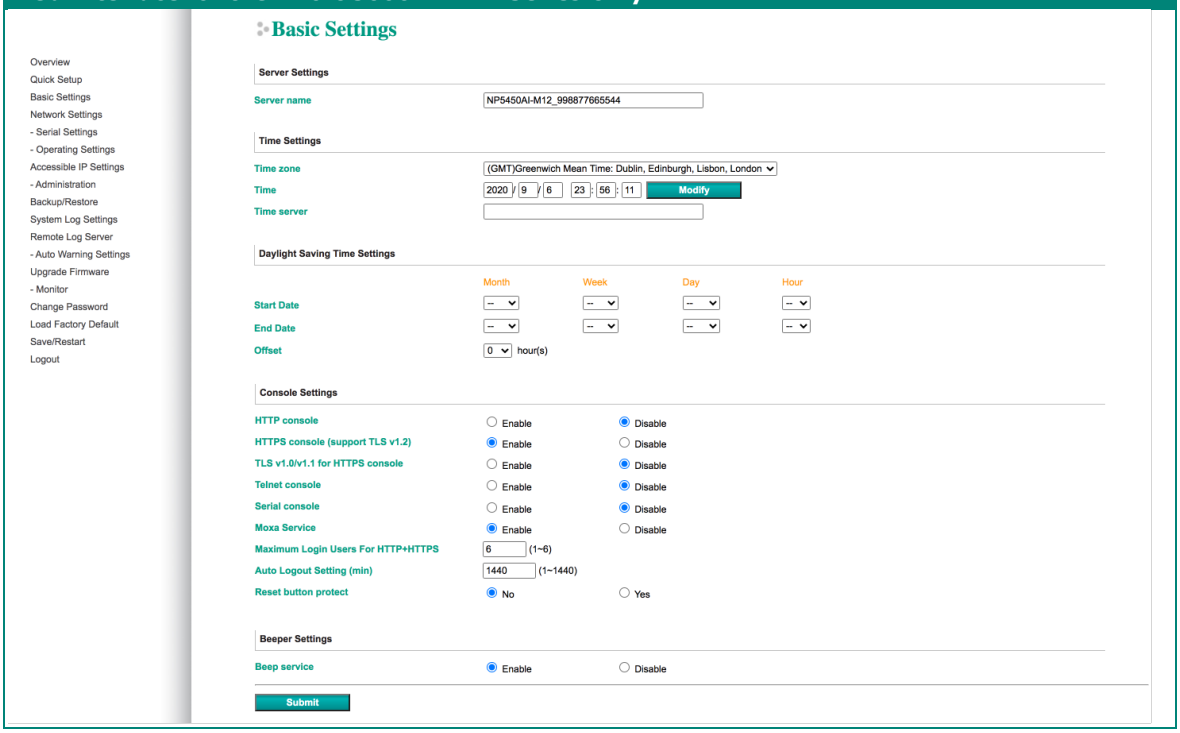
Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort Series



Web Interface for the NPort 5000AI-M12 Series Only



NOTE

The NPort 5100/5100A does not support **Time Settings**.

Parameter	Setting	Factory Default	Description	Necessity
Server name	1 to 39 characters	NP[model name]_[Serial No.]	This option is useful for specifying the location or application of different NPorts.	Optional
Time zone	User selectable time zone Not available in NPort 5100/5100A/5200/5200A Series	GMT (Greenwich Mean Time)	N/A	Required
Local time	User adjustable time (1900/1/1-2037/12/31) Not available in NPort 5100/5100A Series	GMT (Greenwich Mean Time)	Click the **Modify** button to open the change time settings window to input the correct local time.	Required
Time server	IP or Domain address (only available in 2/4/8/16 ports models) E.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov	None	NPorts use SNTP (RFC-1769) for auto time calibration. Input the correct **Time server** IP address or domain name. Once the NPort is configured with the correct Time server address, the NPort will request time information from the Time server every 10 minutes.	Optional
Daylight saving	Setting 1: "Start Date: Month, Week, Day, Hour" Setting 2: "End Date: Month, Week, Day, Hour" Setting 3: "Offset: hours"	None	The NPort can offset the system time to the values you have set in these settings. (This feature only applies to the NPort 5000AI-M12 Series.)	Optional
HTTP console	Enable or Disable	Enable	The options that are disabled by default—http Console, Telnet Console, and Serial Console—are for security reasons. In some cases, disable one or most of these console utilities as an extra precaution to prevent unauthorized users from accessing your NPort. Refer to **Chapter 3** "Cybersecurity Considerations" for detailed suggestions.	Required
HTTPS console	Enable or Disable	Enable		
TLS v1.0/v1.1 for HTTPS console	Enable or Disable	Disable		
Telnet console	Enable or Disable	Disable		
Serial console	Enable or Disable	Enable		
Moxa Service	Enable or Disable	Enable		
Reject an unrecognized host header	Enable or Disable	Enable	To prevent a HTTP Host header attack, its default enabled.	Required
Sensitive Data Encryption	MD5/AES128, SHA256/AES256	MD5/AES128	The password may be transmitted in the Moxa service on the network. In the past, we used MD5 or AES128 to protect it. Starting from firmware version 2.0, it can be protected by SHA256 or AES256. To achieve this, upgrade the DSU to v2.4 and NPort Windows Driver Manager to v2.1.	Required
Maximum Login Users For HTTP+HTTPS	1 to 6	6	Set the maximum number of users allowed on web console	Required
Auto Logout Setting (min.)	1 to 1440 minutes	5	Set the logout time	Required

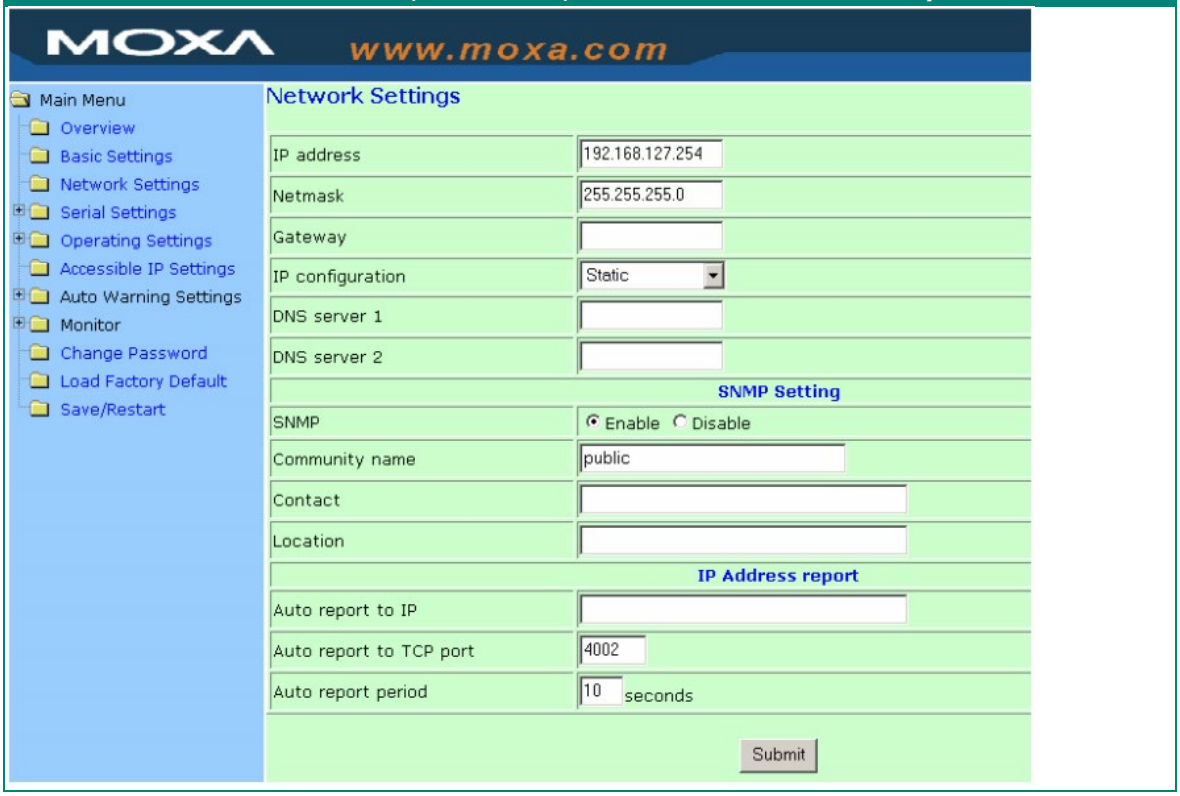
Parameter	Setting	Factory Default	Description	Necessity
Reset button protection	Yes or No	No	Select the **Yes** option to allow limited use of the Reset Button. In this case, the reset button can be used for only 60 seconds; 60 s. after booting up, the reset button will be disabled automatically.	Required
Beep Service	Enable or Disable	Enable	Beeper Service is to provide audio notification and warning according to the different situations. (This feature only applies to the NPort 5000AI-M12 Series.)	Optional
LCM read-only protection	Writeable/Read-only	Writeable	The NPort 5000 front panel, known as the LCM (Liquid Crystal Module), may be configured for read-only or writeable access. Read-only access allows settings to be viewed but not changed. Writeable access allows users in the Administration group to change the setting. This setting is only available for the model that has a font panel.	Optional

WARNING

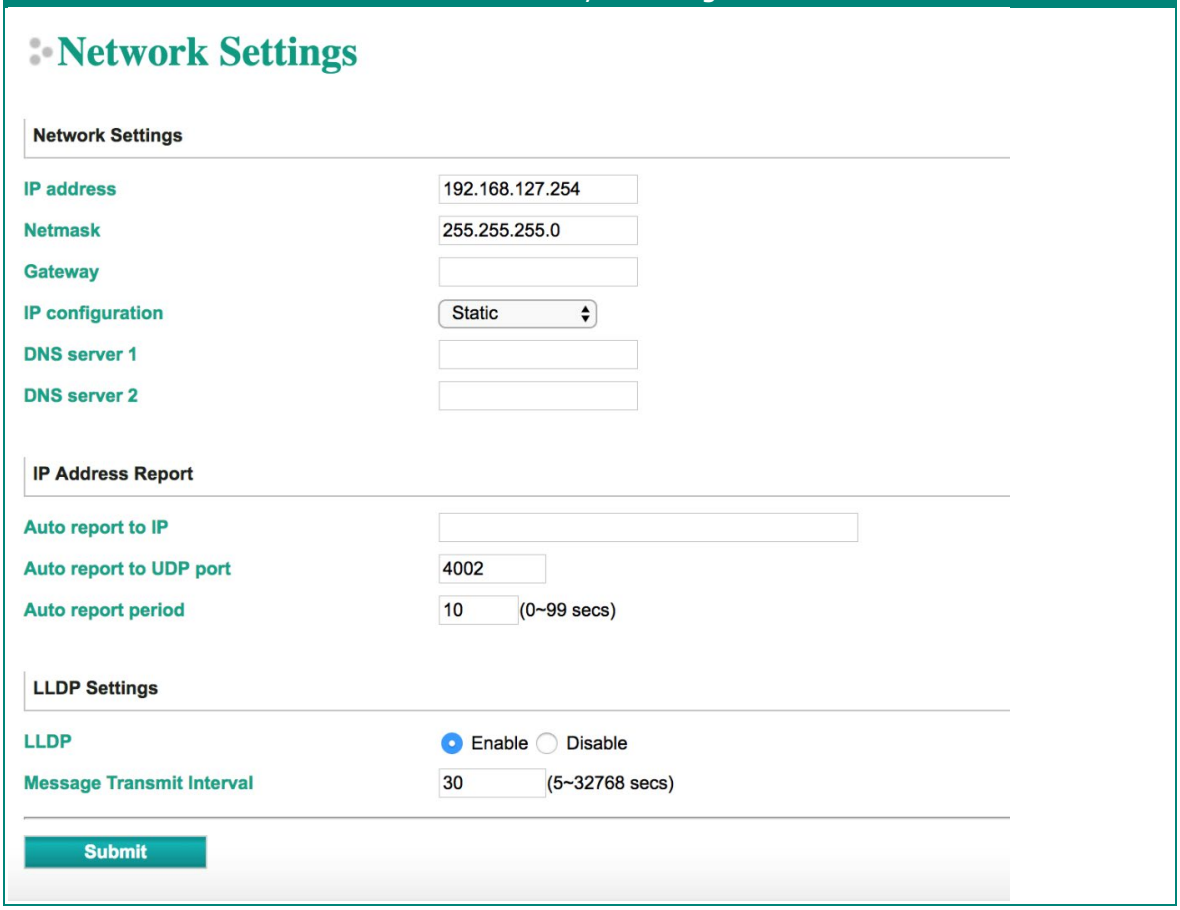
If you disable both the http/https console and Telnet console, you can still use NPort Administrator to configure the NPort device servers either locally or remotely over the network. Refer to **Chapter 5** for details. If you disable all the console and services, there is no alternative way to access the NPort device servers neither locally nor remotely. The only way to gain control is to reset to factory default settings.

Network Settings

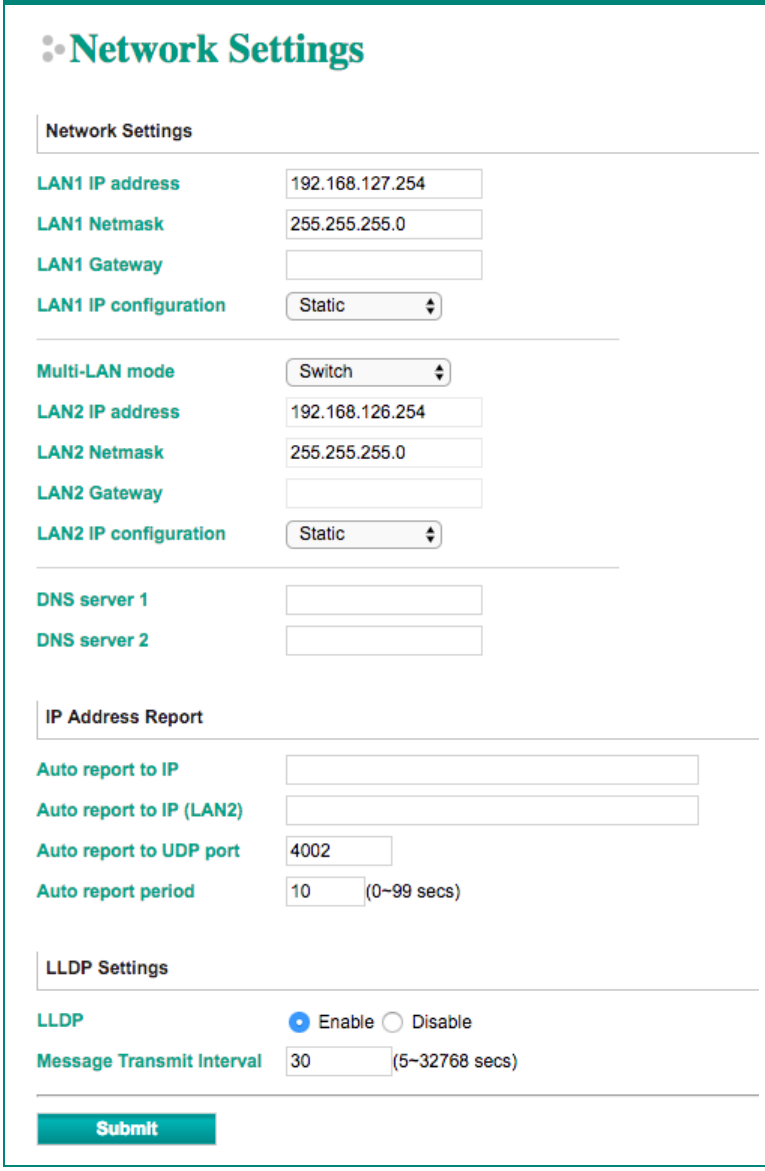
Web Interface for the NPort 5100, NPort 5200, and NPort IA5000 Series Only



Web Interface for the Overall NPort 5000 Series, excluding the NPort IA5000A Series



Web Interface for the NPort IA5000A Series



You must assign a valid IP address to the NPort before it works in your network environment. Your network system administrator should provide you with an IP address and related settings for your network. The IP address must be unique within the network (otherwise, the NPort will not have a valid connection to the network). You can choose from four possible **IP configuration** modes—Static, DHCP, DHCP/BOOTP, and BOOTP—located under the web console screen's IP configuration drop-down box.

Method	Function Definition
Static	The user must define the IP address, Netmask, and Gateway.
DHCP	The DHCP Server assigns the IP address, Netmask, Gateway, DNS, and Time Server
DHCP/BOOTP	The DHCP Server assigns the IP address, Netmask, Gateway, DNS, and Time Server, or the BOOTP Server assigns the IP address (if the DHCP Server does not respond).
BOOTP	The BOOTP Server assigns the IP address.

Network Settings

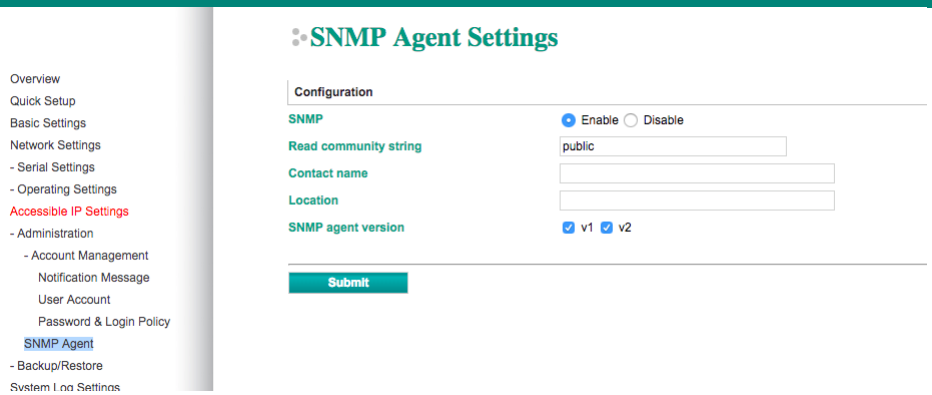
Parameter	Setting	Factory Default	Description	Necessity
IP Address	E.g., 192.168.1.1	192.168.127.254	An IP address is a number assigned to a network device (such as a computer) as a permanent address on the network. Computers use the IP address to identify and talk to each other over the network. Choose a proper IP address that is unique and valid in your network environment.	Required
Netmask	E.g., 255.255.255.0	255.255.255.0	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 will use the subnet mask to check whether 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, a connection is established directly from the NPort. Otherwise, the connection is established through the default gateway.	Required
Gateway	E.g., 192.168.1.1	None	A gateway is a network gateway that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort needs to know the IP address of the default gateway computer to communicate with the hosts outside the local network environment. For correct gateway IP address information, consult with your network administrator.	Optional
IP Configuration	Static DHCP DHCP/BOOTP BOOTP	Static	N/A	Required
Multi-LAN mode (for the NPort IA5000A Series only)	Switch Redundant LAN Dual IP	Switch	Dual LAN can be used as a redundant connection or dual IP. The scenario for redundancy is the NPort will automatically switch to working connection in case the other one loses connectivity (because of failed network component in the NPort, port at the switch/router stop working, etc.). As for dual IP scenario, each port will have its own IP address, but both will have the same MAC address, as it is convenient to connect the NPort to different network.	Optional
DNS server 1/ DNS server 2	E.g., 192.168.1.1	None	In order to use the NPort's DNS feature, you need to configure the DNS server. Doing so allows the NPort to use a host's domain name to access the host. The NPort provides DNS server 1 and DNS server 2 configuration items to configure the IP address of the DNS server. DNS Server 2 is included for use when DNS server 1 is unavailable. The NPort plays the role of DNS client, in the sense that the NPort will actively query the DNS server for the IP address associated with a particular domain name.	Optional
LLDP Settings	Enable or Disable	Enable	Not available for the NPort 5600DT Rev 1.5 or earlier	Optional

WARNING

In Dynamic IP environments, the firmware will be retried three times every 30 seconds until network settings are assigned by the DHCP or BOOTP server. The Timeout for each try increases from 1 second, to 3 seconds, to 5 seconds.

If the DHCP/BOOTP Server is unavailable, the firmware will use the default IP address (192.168.127.254), Netmask, and Gateway for IP settings.

Web Interface for the Overall NPort 5000 Series



SNMP Settings

Parameter	Setting	Factory Default	Description	Necessity
Community Name	1 to 31 characters (e.g., Moxa)	Public	A community name is a plain-text password mechanism that is used to weakly authenticate queries to agents of managed network devices.	Optional
Contact	1 to 31 characters (e.g., Support, 886-89191230 #300)	None	The SNMP contact information usually includes an emergency contact name and telephone or pager number.	Optional
Location	1 to 39 characters (E.g., floor 1, office 2)	None	Specify the location string for SNMP agents, such as the NPort. This string is usually set to the street address where the NPort is physically located.	Optional
SNMP Agent Version V1, V2, V3	V1, V2, V3 (V3 is available on 4/8/16 ports model)	V1, V2 checked for 1/2-port models. V1, V2, V3 checked for 4/8/16-port models.	The NPort 5000 1- and 2-port model supports SNMP V1 and V2, where the 4/8/16-port model supports V1, V2 and V3. Select the version according to your environmental needs. Note that the 4/8/16-port model only supports standard MIB such as RFC1213/1317, which supports Set server name, contact, location, whereas the 1/2-port model only supports Get, but not Set.	Optional
The following fields allow you to define usernames, passwords, and authentication parameters for two levels of access: read-only and read/write. The name of the field will show which level of access it refers to. For example, Read-only authentication mode allows you to configure the authentication mode for read-only access, whereas Read/write authentication mode allows you to configure the authentication mode for read/write access. For each level of access, you may configure the following:				
Read-only username	1 to 31 characters	None	Use this optional field to identify the username for the specified level of access.	Optional
Read-only authentication mode	MD5, SHA	Disable	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication	Optional
Read-only password	1 to 31 characters		Use this field to set the password for read only of access.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Read-only privacy mode	DEC, CBC	Disable	Use this field to enable or disable DES_CBC data encryption for the specified level of access.	Optional
Read-only privacy	1 to 31 characters	None	Use this field to define the encryption key for the specified level of access.	Optional
Read/write username	1 to 31 characters	None	Use this optional field to identify the username for the specified level of access.	Optional
Read/write authentication mode	MD5, SHA	Disable	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication	Optional
Read/write only password	1 to 31 characters		Use this field to set the password for read/write access.	Optional
Read/write only privacy mode	DEC, CBC	Disable	Use this field to enable or disable DES_CBC data encryption for the specified level of access.	Optional
Read/write only privacy	1 to 31 characters	None	Use this field to define the encryption key for the specified level of access	Optional

IP Address Report

When NPort products are used in a dynamic IP environment, users must spend more time on IP management tasks. For example, if the NPort works as a server (TCP or UDP), then the host, which acts as a client, must know the IP address of the server. If the DHCP server assigns a new IP address to the NPort, the host must have some way of determining the NPort's new IP address.

NPort products help by reporting their IP address periodically to the IP location server, in case the dynamic IP has changed. The parameters shown below are used to configure the Auto IP report function. There are two ways to develop an "Auto IP report Server" to receive the NPort's Auto IP report.

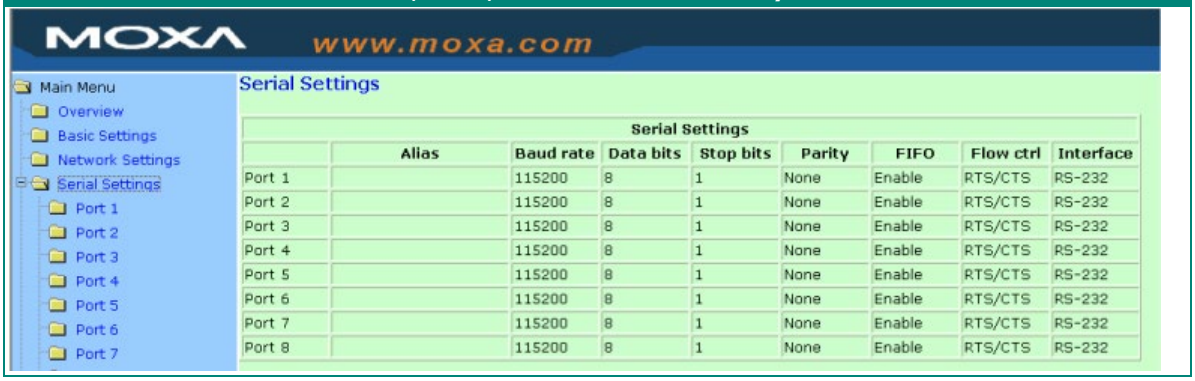
1. Use Device Server Administrator's **IP Address Report** function.
2. **Auto IP report protocol**, which can receive the Auto IP report automatically regularly, is also available to help you develop your own software. Refer to **Appendix E** for details about the **Auto IP report protocol**.

Parameter	Setting	Factory Default	Description	Necessity
Auto report to IP	E.g., 192.168.1.1 or URL	None	Reports generated by the Auto report function will be automatically sent to this IP address. In the multiple-LAN model version, two IPs can be set for the Auto report. The report will be sent to each IP when generated.	Optional
Auto report to UDP port	E.g., 4001	4002	In the multiple-LAN model version, two IPs can be set for Auto report. Report will be sent to each IP when generated.	Optional
Auto report period	Time interval (in seconds)	10	NA	Optional

Serial Settings

The **Serial Settings** page is where you set the serial communication parameters for each device port. Settings include baudrate, parity, and flow control. Each device port can be configured independently.

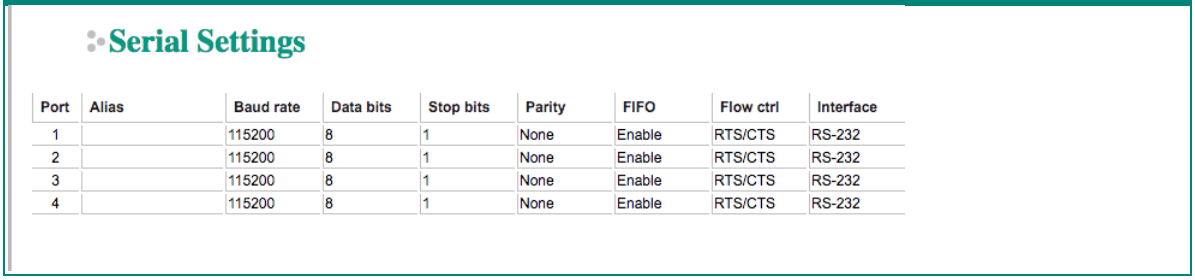
Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Serial Settings

	Alias	Baud rate	Data bits	Stop bits	Parity	FIFO	Flow ctrl	Interface
Port 1		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 2		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 3		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 4		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 5		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 6		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 7		115200	8	1	None	Enable	RTS/CTS	RS-232
Port 8		115200	8	1	None	Enable	RTS/CTS	RS-232

Web Interface for the Overall NPort 5000 Series



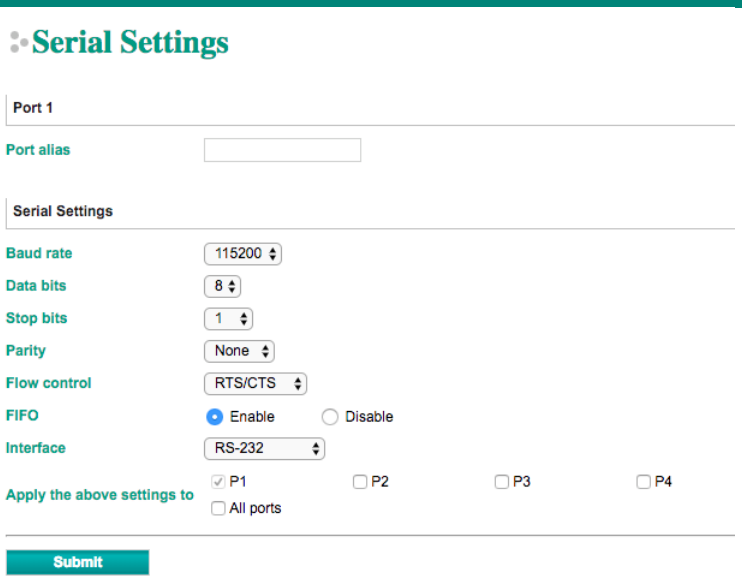
Serial Settings

Port	Alias	Baud rate	Data bits	Stop bits	Parity	FIFO	Flow ctrl	Interface
1		115200	8	1	None	Enable	RTS/CTS	RS-232
2		115200	8	1	None	Enable	RTS/CTS	RS-232
3		115200	8	1	None	Enable	RTS/CTS	RS-232
4		115200	8	1	None	Enable	RTS/CTS	RS-232

To change serial settings for a particular port, click on the **Port Number** under **Serial Settings**, located under **Main Menu** on the left side of the browser window.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

Web Interface for the Overall NPort 5000 Series



ATTENTION

It is critical that the device port's serial communication settings match the attached device. Refer to the user's manual for your serial device for the correct serial communication settings.

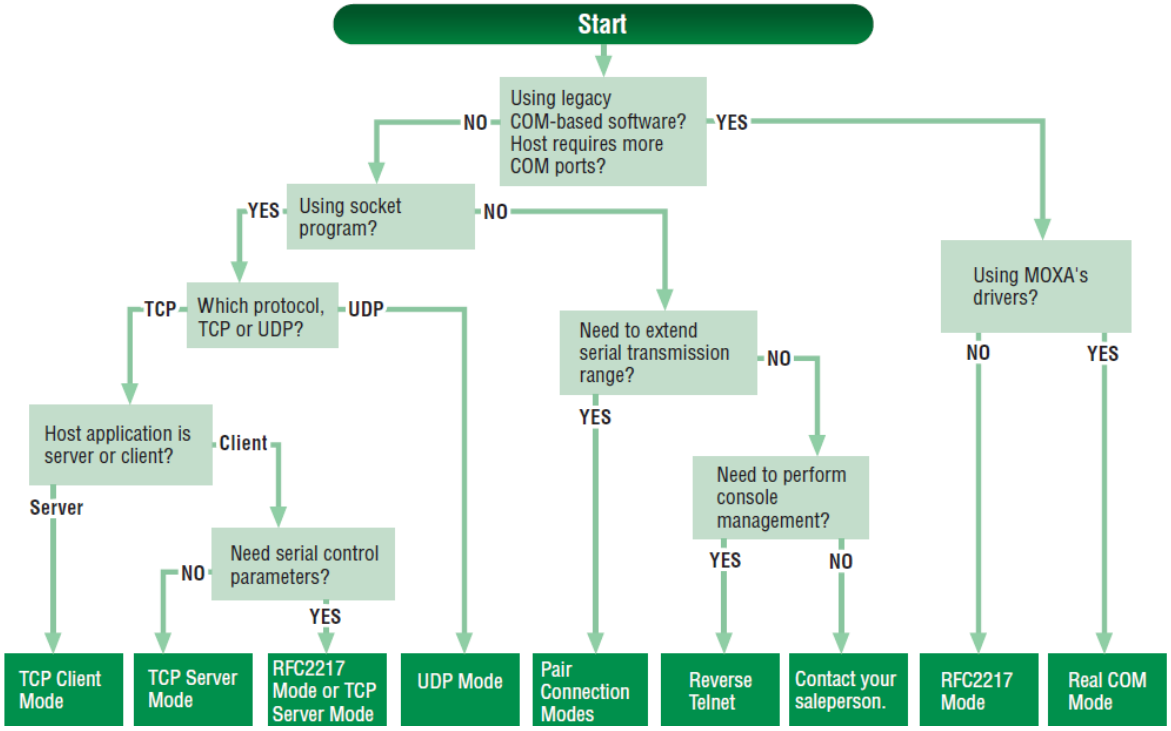
Parameter	Setting	Factory Default	Description	Necessity
Port Alias	1 to 15 characters (E.g., PLC-No.1)	None	Port Alias is specially designed to allow easy identification of the serial devices that are connected to the NPort's serial port.	Optional
Baud rate	Support standard baudrates (bps): 50/ 75/ 110/ 134/ 150/ 300/ 600/ 1200 1800/ 2400/ 4800/ 7200/ 9600/ 19200/ 38400/ 57600/ 115200/ 230.4k/ 460.8k/ 921.6k * The NPort 5110/5210/ 5230/5232I Series, and IA 5000 series are as low as 110 bps, and up to 230.4 kbps	115200 bps	The rate of data transmission to and from the attached serial device.	Required
Data bits	5, 6, 7, 8	8	When data bits is set to 5 bits, the stop bits setting will automatically change to 1.5 bits.	Required
Stop bits	1, 1.5, 2	1	The size of the stop character.	Required
Parity	None, Even, Odd, Space, Mark	None	Even and Odd parity provides rudimentary error-checking; Space and Mark parities are rarely used.	Required
Flow control	None, RTS/CTS, DTR/DSR, Xon/Xoff	RTS/CTS	The method used to suspend and resume data transmission to ensure that data is not lost. If you can use it, **RTS/CTS (hardware)** flow control is recommended.	Required
FIFO	Enable, Disable	Enable	Controls whether the device port's built-in 128-byte FIFO buffer is used. When enabled, the FIFO helps reduce data loss regardless of direction.	Required

Parameter	Setting	Factory Default	Description	Necessity
*Interface**	RS-232 RS-422 2-wire RS-485 4-wire RS-485	RS-232	The serial interface that will be used. The options that are available depend on the specific model of the device server.	Required

*Supported interfaces vary by model. Refer to the datasheet of your NPort device to see which serial interface it supports.

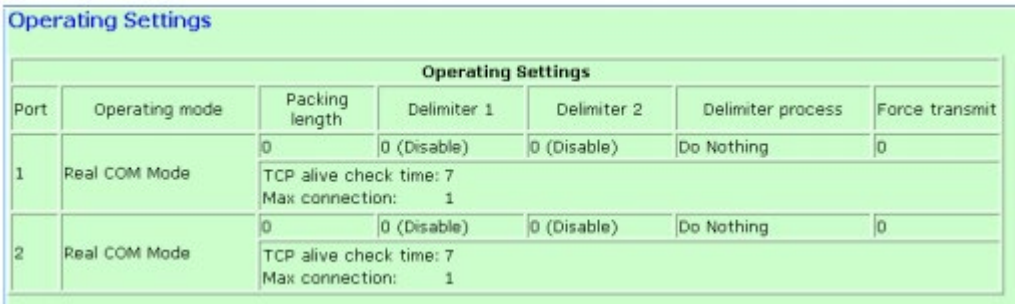
Operating Settings

Operating Settings is where each device port's operation mode and associated parameters are configured. Use the chart below to select the operation mode that is most suitable for your application and refer to **Chapters 4 and 5** for a detailed explanation of different operating modes and parameters.

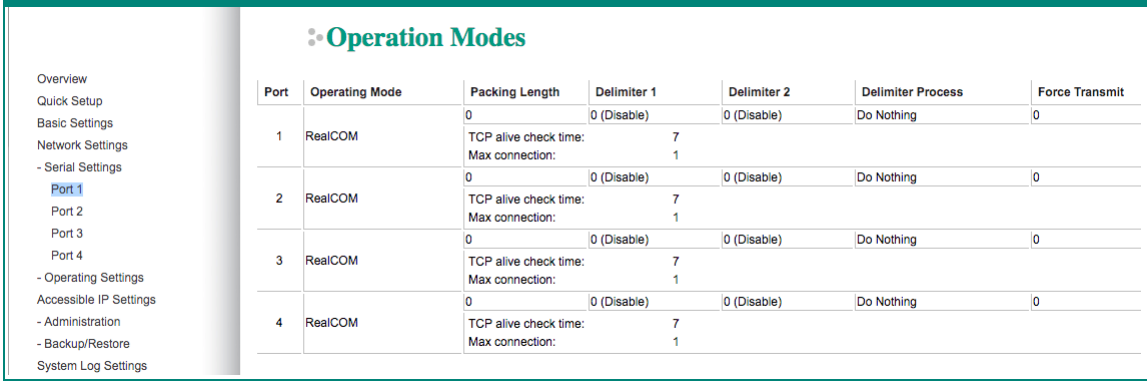


Click on **Operating Settings** under **Main Menu** to display the operating settings for the NPort's serial ports. To change operating settings for a particular port, click on the **Port Number** under **Operating Settings**, located under **Main Menu** on the left side of the browser window.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

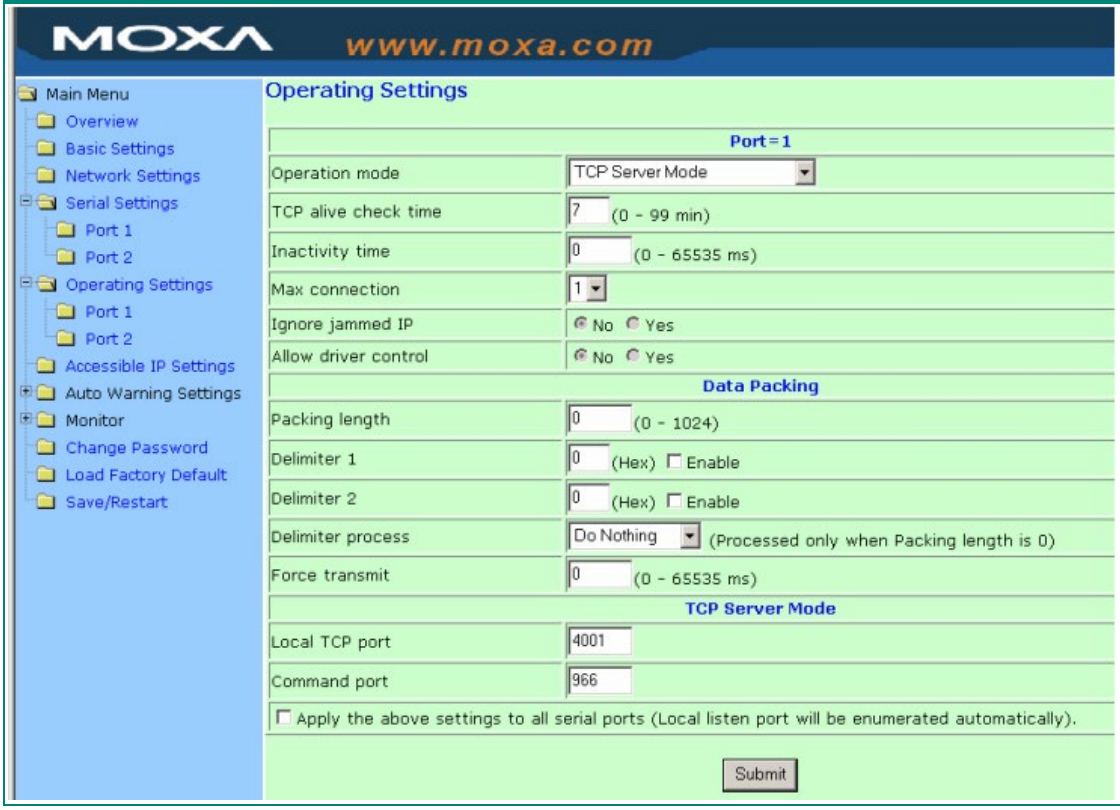


Web Interface for the Overall NPort 5000 Series

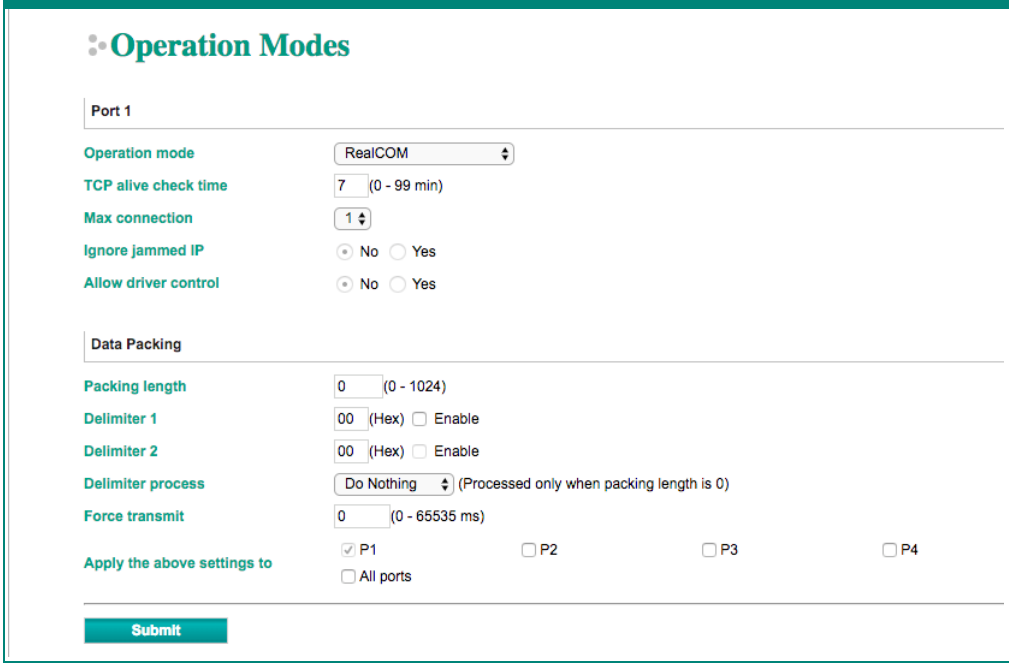


For each mode, the default settings should work for most applications. Change these settings only if necessary for your application. The operation mode and related parameters can be configured through the web console. The same parameters can also be configured using NPort Administrator, the Telnet console, or serial console. Refer to **Chapters 4 and 5** for details.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

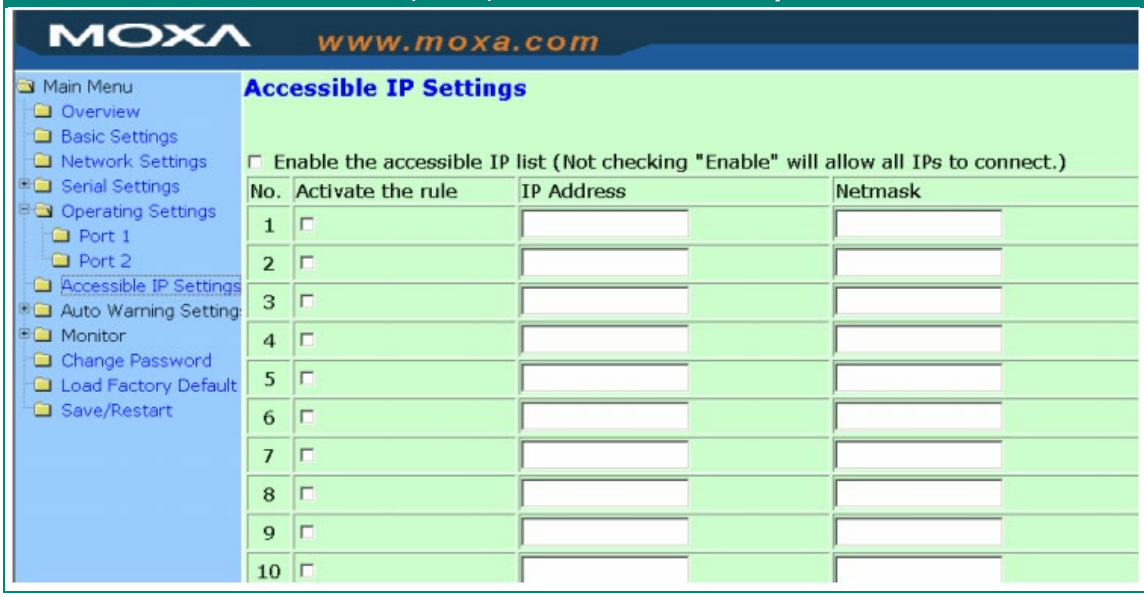


Web Interface for the Overall NPort 5000 Series

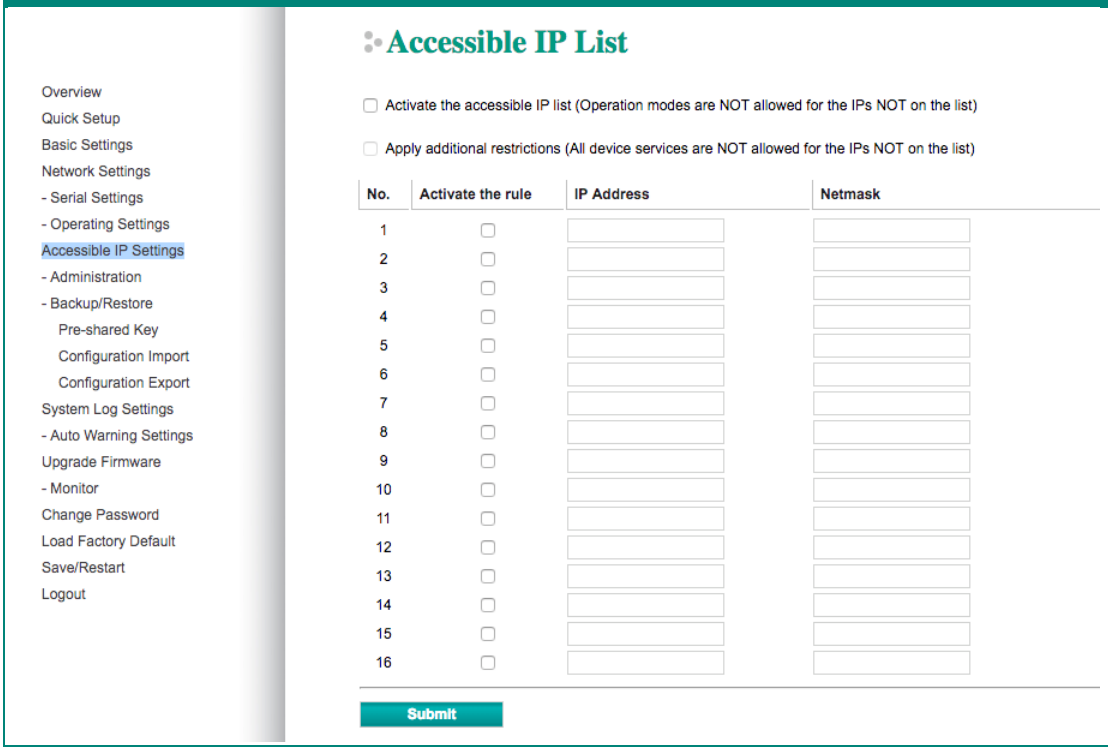


Accessible IP Settings

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series



Accessible IP Settings allow you to add or block remote host IP addresses to prevent unauthorized access. Access to the NPort is controlled by an IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed to access the NPort. Three setting types are described below:

- **Activate the Accessible IP list**

  Operation modes are NOT allowed for IPs NOT on the list. IPs that are not on the list will not be granted when communicating with the NPort via Operation mode.

- **Apply additional restrictions**

  All device services are NOT allowed for IPs NOT on the list. Services will not be granted for IPs that are not on the list. Note that all IPs will still have access if the IP list is empty, even though the function is enabled.

  Tip: For exact IP identification, the netmask needs to be 255.255.255.255.

- **Only one host with a specific IP address can access the NPort**
  Enter "[IP address]/255.255.255.255" (e.g., "192.168.1.1/255.255.255.255").
- **Hosts on a specific subnet can access the NPort**
  Enter "[IP address]/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0").
- **Any host can access the NPort**
  Disable this function. Refer to the following table for more details about the configuration.

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Firmware Upgrading

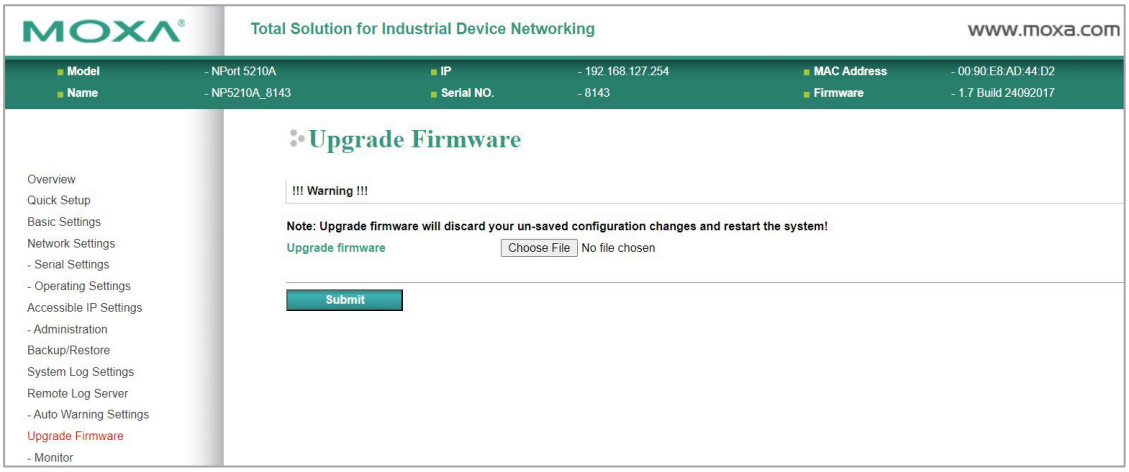
At times, Moxa needs to change the components within the NPort, which means the driver in the firmware needs to be updated. However, the firmware cannot always contain all the versions of the driver in one file; therefore, on some occasions, we need to separate the firmware for the older and newer versions of hardware. Before you decide to update the firmware to a newer or older version, make sure that the firmware is compatible with your NPort hardware version. In most cases, if a firmware does not specify for a particular hardware version, it is supposed to support all models in the series and for any hardware revision. If you are not sure, refer the product website to check for instructions or refer to the table below for specific cases, or otherwise, consult your region's technical support for confirmation.

Product Series	Models	Supporting Condition	Corresponding Firmware Version
NPort 5100	NPort 5110 Models	All revisions	v2.10
	NPort 5130/5150 Models	All revisions	v3.9
NPort 5400	NPort 5410/5430 Models	Rev 2.x and prior	v2.9
		Rev. 3.2 and later	v3.14
NPort 5600-DT	All	Supporting NPort 5600-DTL Series	v2.9
NPort IA5000A	NPort IA5150A/IA5250A models	All revisions	v1.5
	NPort IA5450A models	All revisions	v1.7
NPort IA5000	All	HW Rev 1.x	v1.7
		HW Rev 2.0 and after	v2.0
NPort 5000AI-M12	NPort 5150AI-M12 models	All	v1.5
	NPort 5250AI-M12 models	All	v1.5
	NPort 5250AI-M12 models	All	v1.5

Moxa will also roll out new firmware for feature/security enhancement, patches, etc. It may be necessary to visit the NPort product website frequently to check for the latest firmware. You may also register for Moxa's website and follow the product updates so that you will be notified automatically about any recent activity. Check for G. How to Become a Registered User on the Moxa Website.

Follow these steps to upgrade the firmware of an NPort through the web console:

1. Go to the web console and select the **Upgrade Firmware** function.



2. Click the **Choose File** and select the correct firmware file to load.
3. Click **Submit** and wait while the Upgrade Firmware action is processed.

NOTE

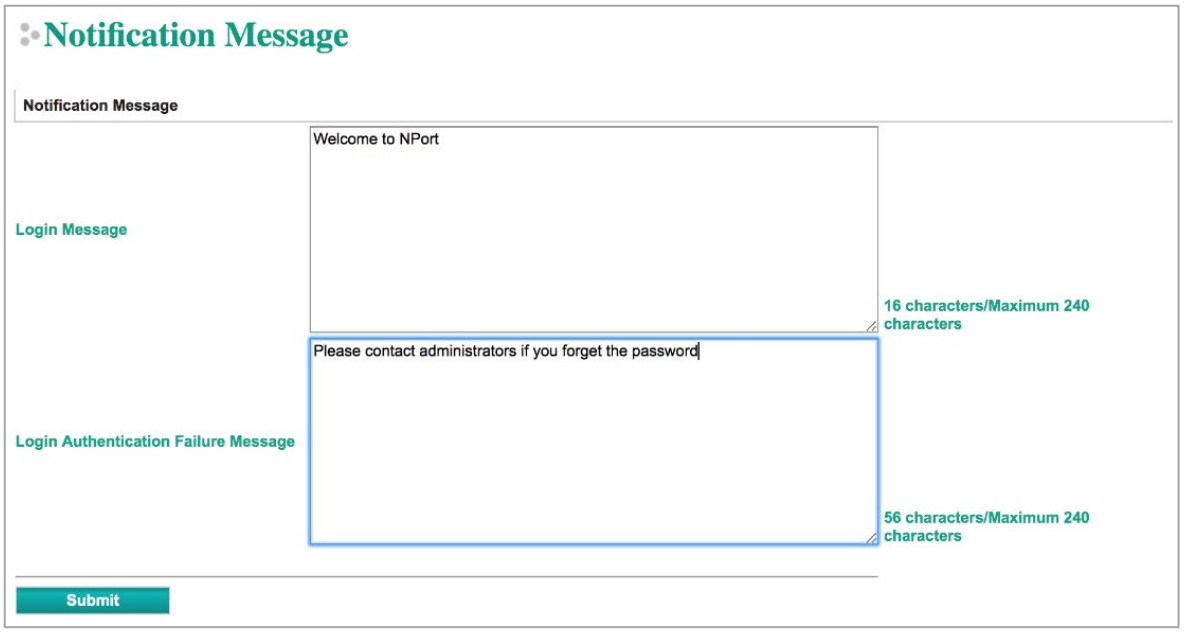
The NPort 5100, NPort 5200, and NPort IA5000 Series cannot upgrade firmware via the web console. To upgrade the firmware of the NPort 5100, 5200, and NPort IA5000 Series, refer to Chapter 7. Windows Utilities for NPort 5000 Models, and use either the Device Search Utility or NPort Administrator to complete the upgrade.

Account Management

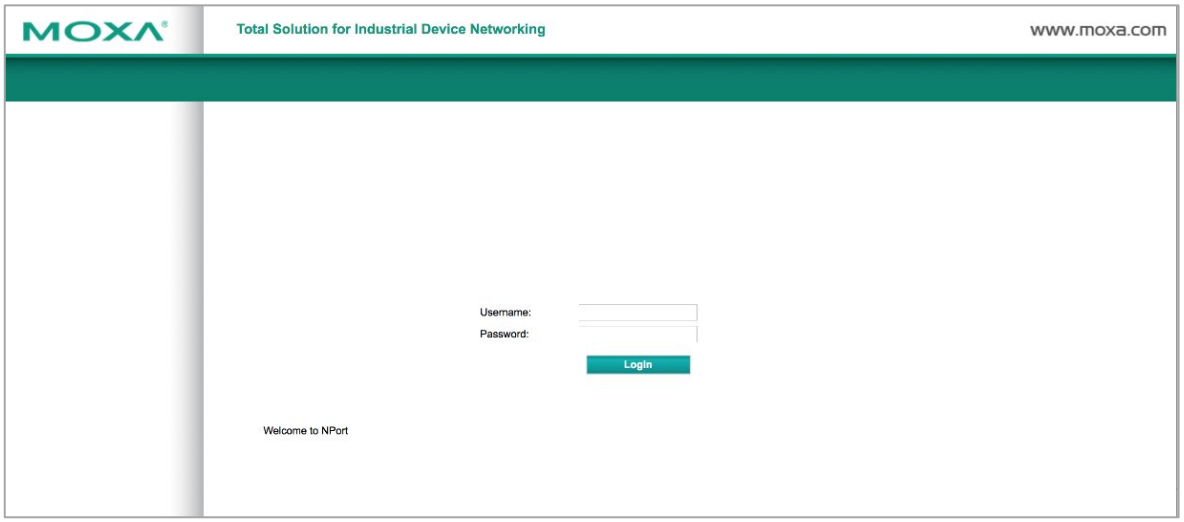
The Account Management setting provides administrators the authority to add/delete/modify a user account, grant access to the device users for specified function groups, and manage password and login policy to ensure device is used by a proper set of people.

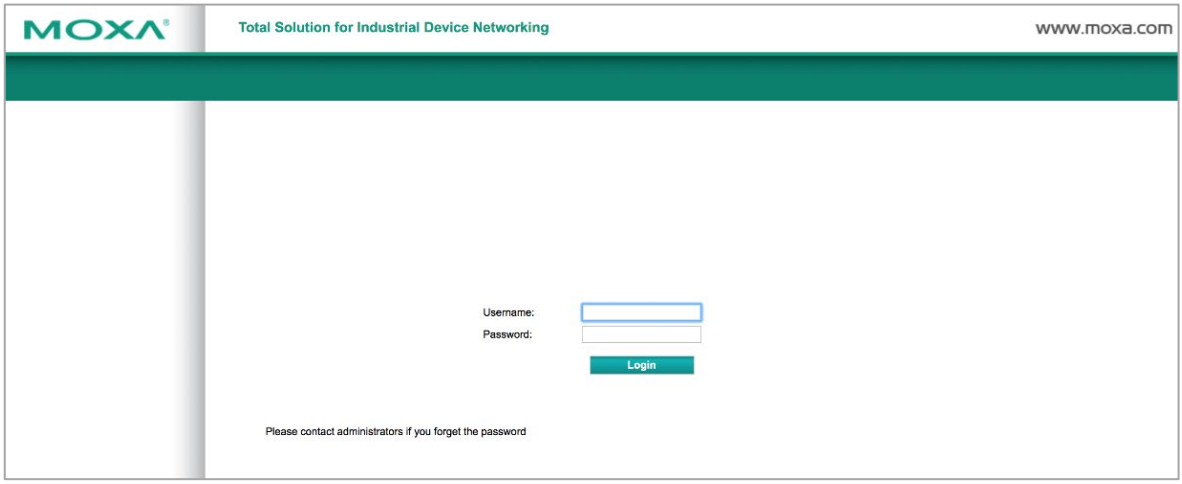
Notification Message

As an administrator, you may customize your **Login Message** and the **Login Authentication Failure Message** to notify users with information you would like to provide.



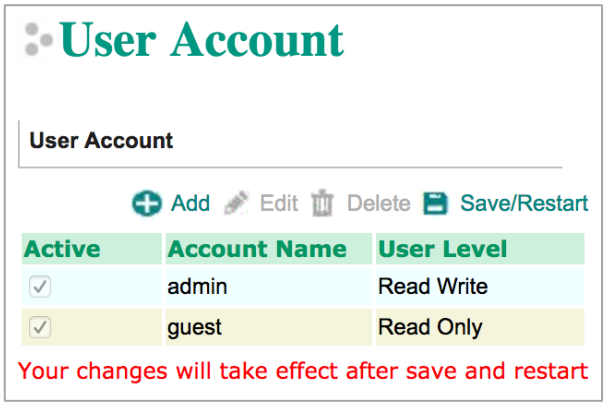
The message will appear on the login page at the time of a successful login or login failure. Examples are below.



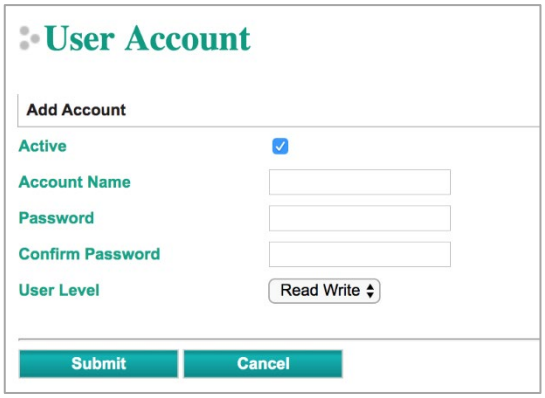


User Account

In the NPort 5000 Series, the main function groups are highly correlated with the **User Level** set by the administrator(s). Administrators are allowed to add user accounts to the NPort 5000 device by clicking the **Add** button on the **User Account** page. You may also click on the current user to **Edit** or Delete the selected account.

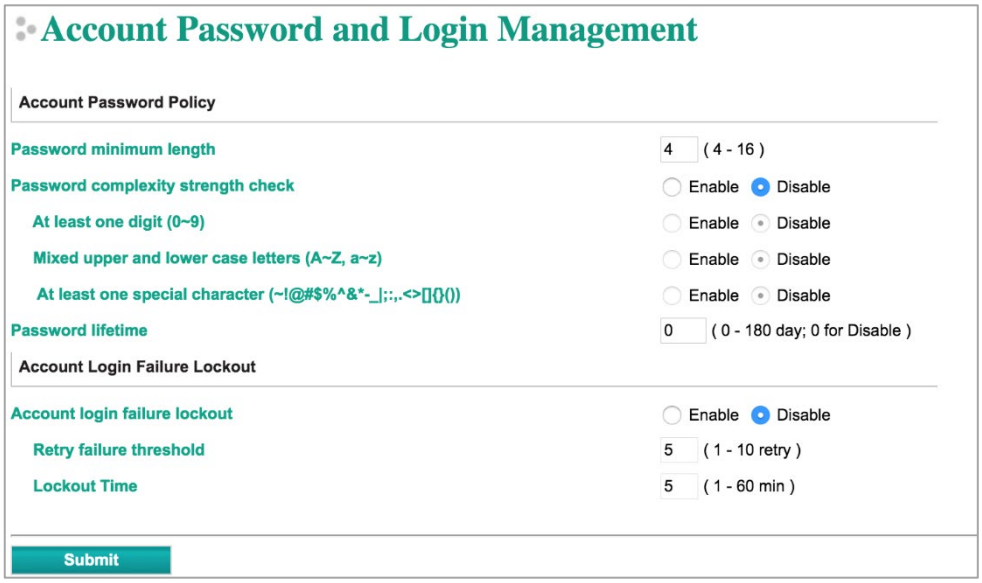


The **Add Account (Edit Account)** page will show up for you to enter (modify) account information and assign password to this user. Also, the Administrator(s) may assign a proper **User Level** to this user to limit his/her privileges of using NPort 5000.



Password and Login Policy

A user with an administrator role is authorized to determine the password and login policy of the NPort 5000 device.



Account Password Policy

Parameter	Setting	Default	Description
Password minimum length	4-16 characters	4	Define the minimum length of the login password
Password complexity strength check:	Enable/Disable	Disable	Enable password complexity strength check will enforce the password combination setting
• At least one digit (0-9)	Enable/Disable	Disable	The password must contain at least one number (0-9) when enabling this parameter
• Mixed upper- and lowercase letters (A to Z, a to 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
Password lifetime	0 to 180 days (0 for disable)	90 days	A password lifetime can be specified, and a system notification message will show up to remind users to change the password if the option is enabled.

Account Login Failure Lockout

Parameter	Setting	Default	Description
Account Login Failure Lockout	Enable/Disable	Disable	An account login failure lockout rule can be defined and enforced when enabled
• Retry failure threshold	1 to 10 retry	5 if enabled	Number of retries can be determined prior to the lockout
• Lockout time	1 to 60 minute(s)	5 if enabled	Lockout duration can be specified to determine time until the next retry

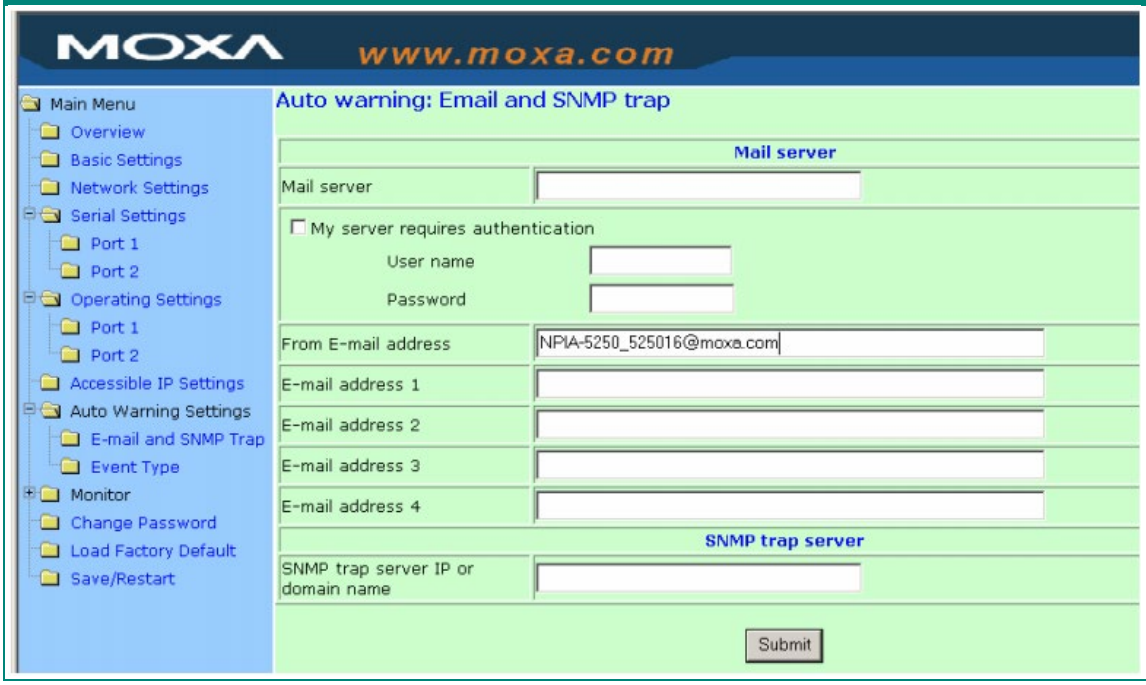
Auto Warning Settings

The NPort device server can automatically warn administrators of certain system, network, and configuration events. Depending on the event, different options for automatic notification are available. These options are configured in the Auto Warning Settings.

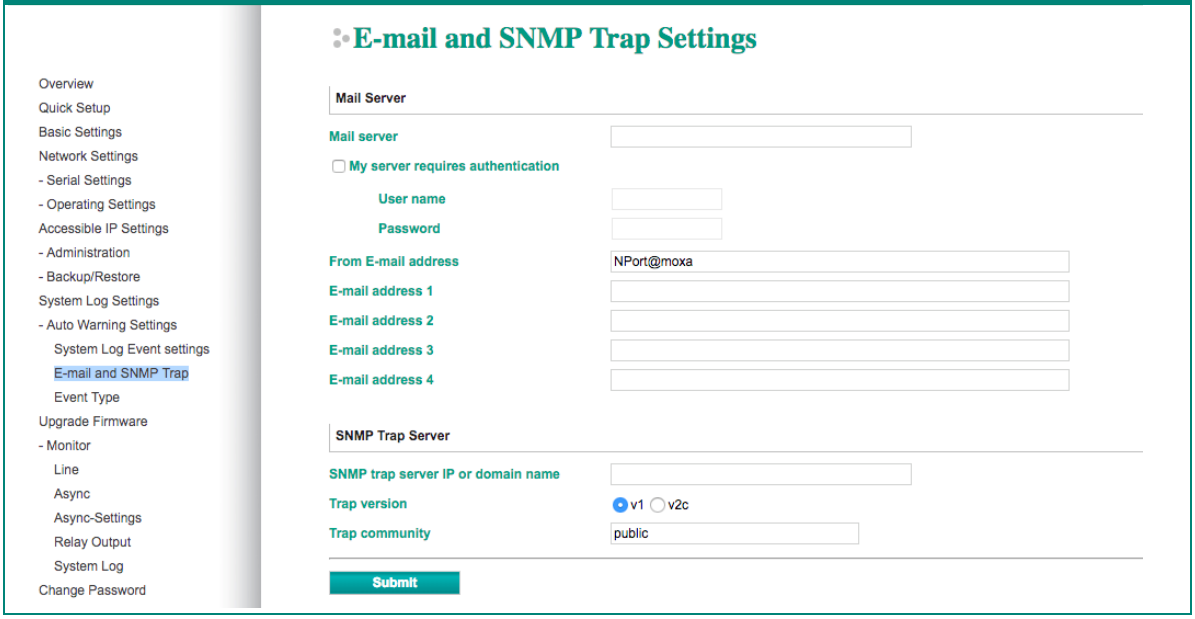
Auto warning: Email and SNMP trap

The Email and SNMP trap parameters are used to configure how email and SNMP traps are sent when an automatic warning is issued by the NPort device server.

Web Interface for the NPort 5100, 5200, IA5000 Series



Web Interface for the Overall NPort 5000 Series



Mail Server

Parameter	Setting	Factory Default	Description	Necessity
Mail server	IP or Domain Name	None	This optional field is for the IP address or domain name of your network mail server, if applicable. A mail server is required for the NPort to send email warnings about administrative events.	Optional
Username	1 to 15 characters	None	This optional field is used if your mail server requires it.	Optional
Password	1 to 15 characters	None	This optional field is used if your mail server requires it.	Optional
From Email address	1 to 63 characters	None	This optional field sets the "from" email address that will show up in an automatic warning email.	Optional
Email address 1/2/3/4	1 to 63 characters	None	These optional fields set the "destination" email address for automatic email warnings.	Optional

SNMP Trap Server

Parameter	Setting	Factory Default	Description	Necessity
SNMP trap server IP or domain name	IP address or Domain Name	None	Selecting the version based on your environmental needs. We strongly suggest to that you change the community name from the default **public** to another name; it is for security prevention reasons.	Optional

ATTENTION

Consult your network administrator or ISP for the proper mail server settings. The **Auto warning** function may not work properly if it is not configured correctly. NPort SMTP AUTH supports LOGIN, PLAIN, CRAM-MD5 (RFC 2554).

Event Type

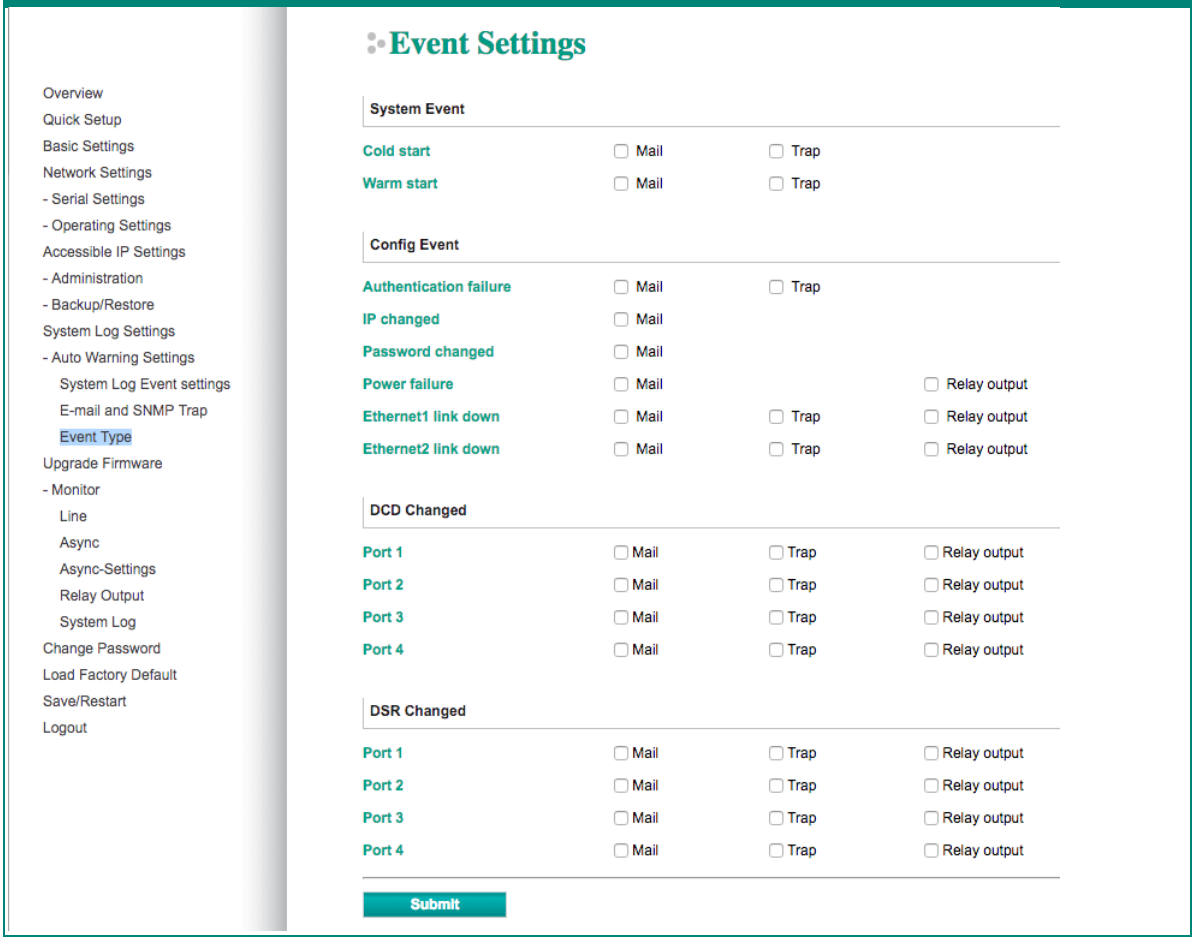
Web Interface for the NPort 5100, 5200 and IA5000 Series Only

Event Type

Cold start	☐ Mail	☐ Trap	
Warm start	☐ Mail	☐ Trap	
Authentication failure	☐ Mail	☐ Trap	
IP address changed	☐ Mail		
Password changed	☐ Mail		
Power failure	☐ Mail		☐ Relay Output
Ethernet1 link down	☐ Mail	☐ Trap	☐ Relay Output
Ethernet2 link down	☐ Mail	☐ Trap	☐ Relay Output
DCD changed			
Port 1	☐ Mail	☐ Trap	☐ Relay Output
Port 2	☐ Mail	☐ Trap	☐ Relay Output
DSR changed			
Port 1	☐ Mail	☐ Trap	☐ Relay Output
Port 2	☐ Mail	☐ Trap	☐ Relay Output

Submit

Web Interface for the Overall NPort 5000 Series



The Event Type parameters are used to configure which events will generate an automatic warning from the NPort device server, and how that warning will be issued. For each listed event, certain automatic warning options are available. If Mail is selected, an email will be sent. If Trap is selected, an SNMP trap will be sent. The **Relay Output** option is available for the NPort IA5000/IA5000A Series.

Cold start

Refers to starting the system from power off (contrast this with warm start). When performing a cold start, the NPort will automatically issue an auto warning message by email or send an SNMP trap after booting up.

Warm start

A warm start refers to restarting the computer without turning the power off. When performing a warm start, the NPort will automatically send an email, or send an SNMP trap after rebooting.

Authentication failure

An authentication failure event is triggered when the user inputs an incorrect password from the Console or Administrator. When an authentication failure occurs, the NPort will immediately send an email or SNMP trap.

IP address changed

An IP address changed event is triggered when the user has changed the NPort's IP address. When the IP address changes, the NPort will send an email with the new IP address before the NPort reboots. If the NPort cannot send an email message to the mail server within 15 seconds, the NPort will reboot anyway, and abort the email auto warning.

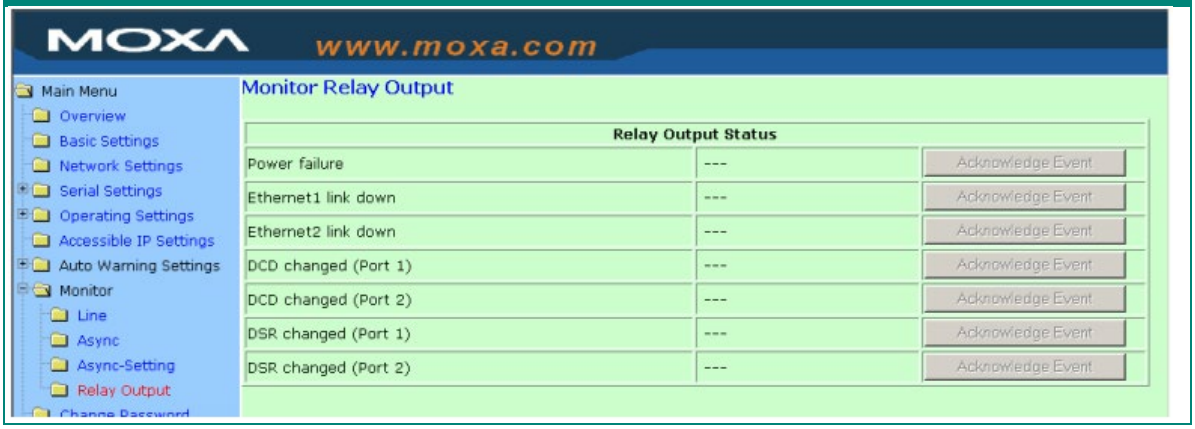
Password changed

A password changed event is triggered when the user has changed the NPort's password. When the password changes, the NPort will send an email with the password changed notice before the NPort reboots. If the NPort cannot send an email message to the mail server within 15 seconds, the NPort will reboot anyway, and abort the email auto warning.

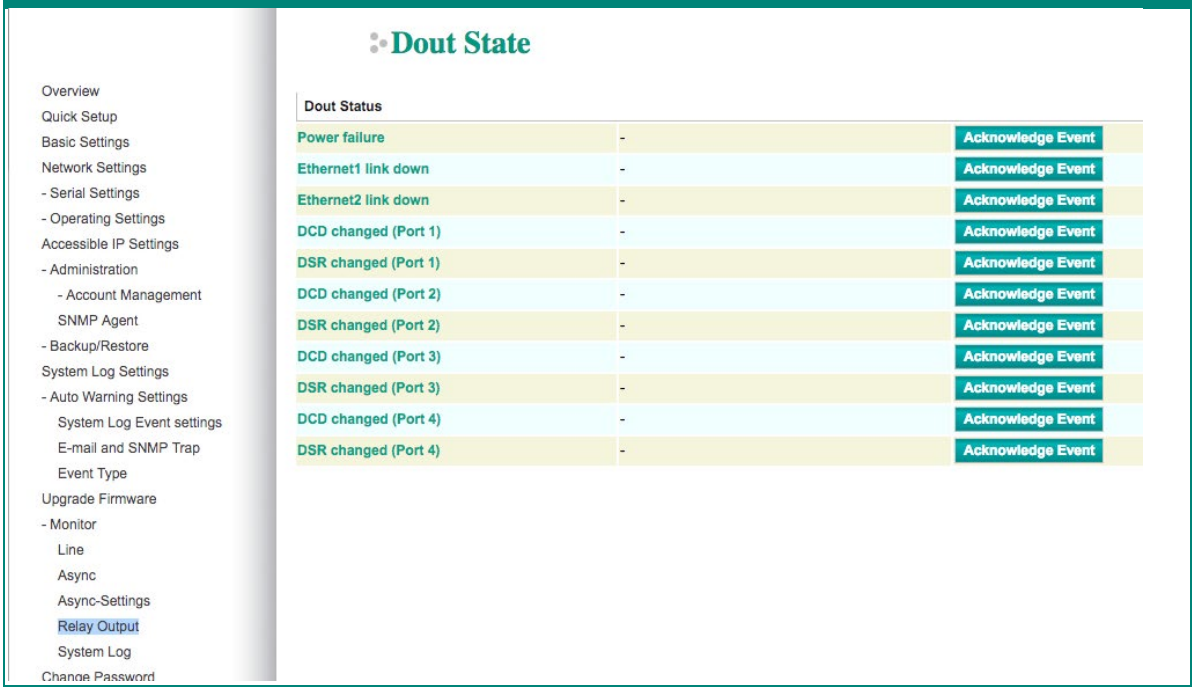
Power failure (this event type only applies to NPort IA5000/IA5000A Series)

The NPort IA5000/IA5000A Series has two DC power inputs for redundancy. Different approaches are used to warn engineers automatically, including by email and by relay output. Users can connect to **Monitor > Relay Output** from the web console to check which event caused the warning. The relay output will be canceled after the power recovers, or by selecting "acknowledge event" using the web console or Telnet. When the Relay Output is sending a warning, the Ready LED will flash red until the warning event ceases.

Web Interface for the NPort IA5000 Series



Web Interface for the NPort IA5000A Series



Ethernet link down

The NPort device server provides system maintainers with real-time alarm messages for Ethernet link down. Even when control engineers are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur. The NPort device server supports different methods for warning engineers automatically, such as by email, SNMP trap, and relay output*.

DCD changed

A DCD (Data Carrier Detect) signal change shows that the modem connection status has changed. For example, a DCD change to high shows that the local modem and remote modem are connected. A DCD signal change to low shows that the connection line is down. When the DCD changes, the NPort will immediately send an email, send an SNMP trap, or trigger the relay output*.

DSR changed

A DSR (Data Set Ready) signal change indicates that the data communication equipment's power is off. For example, a DSR change to high indicates that the DCE is powered ON. A DSR signal changes to low indicates that the DCE is powered off. When the DSR changes, the NPort will immediately send an email, send an SNMP trap, or trigger the relay output*.

*Relay output is only supported by the NPort IA5000/IA5000A Series.

NOTE

Relay Output is only available for the NPort IA5000/IA5000A Series. Users can connect to **Monitor > Relay Output** from the web console to check which event is causing the warning. The relay output will be canceled if the abnormal state is restored, or if **Acknowledge Event** is selected from the web or Telnet console. When the Relay Output is issuing a warning, the Ready LED will flash red until the warning event ceases.

Parameter	Setting	Factory Default	Description	Necessity
Mail	Enable, Disable	Disable	This feature helps the administrator manage how the NPort sends email to pre-defined email boxes when the enabled events (Cold start, Warm start, Authentication failure, etc.) occur. To configure this feature, click the **Event Type Mail** checkbox.	Optional
Trap	Enable, Disable	Disable	This feature helps the administrator manage how the NPort IA5000A sends an SNMP Trap to a pre-defined SNMP Trap server when the enabled events (Cold start, Warm start, Authentication failure, etc.) occur. To configure this feature, click the **Event Type Trap** checkbox.	Optional

ATTENTION

DCD and DSR signal changes only apply for the RS-232 interface.

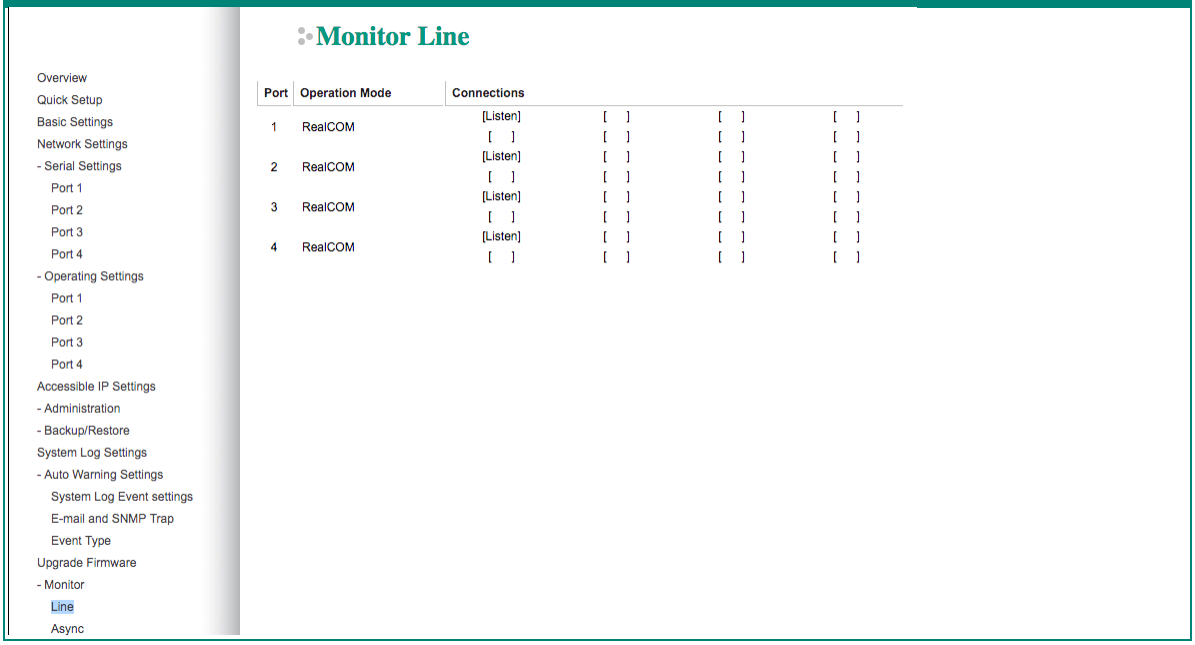
Monitor

Monitor Line

Click **Line** under **Monitor** to show the operation mode and status of each connection (IPx), for each of the four serial ports.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

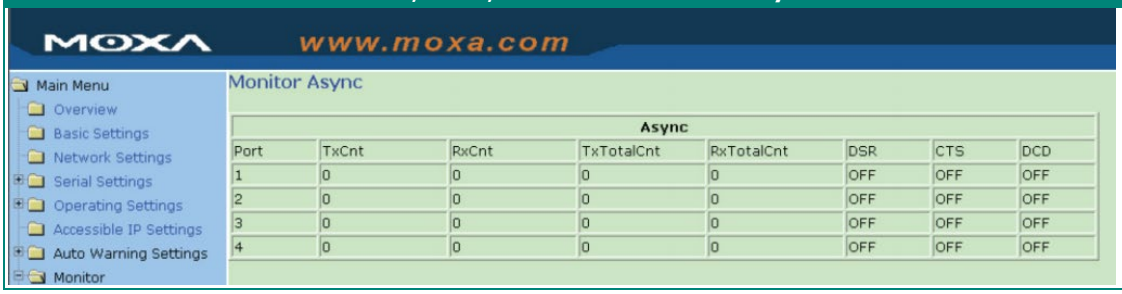
Web Interface for the Overall NPort 5000 Series



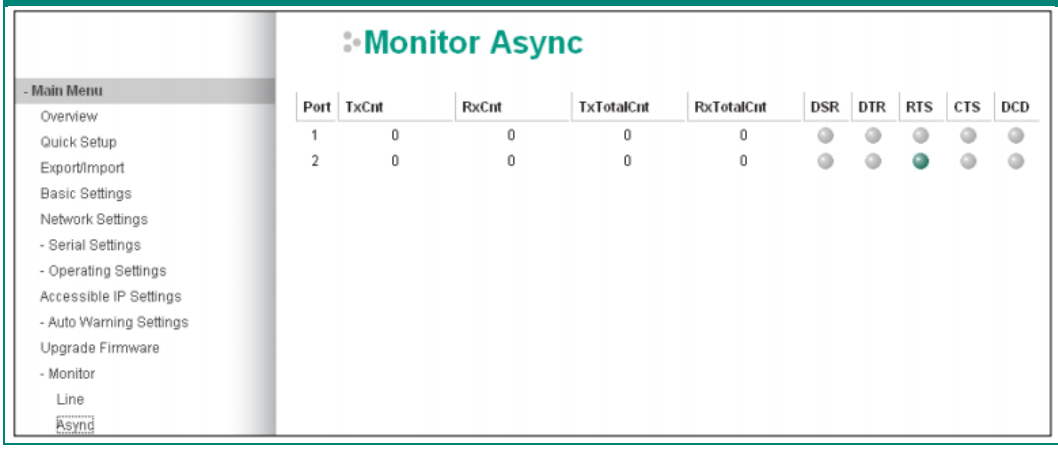
Monitor Async

Click **Async** under **Monitor** to show the status of each of the four serial ports.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



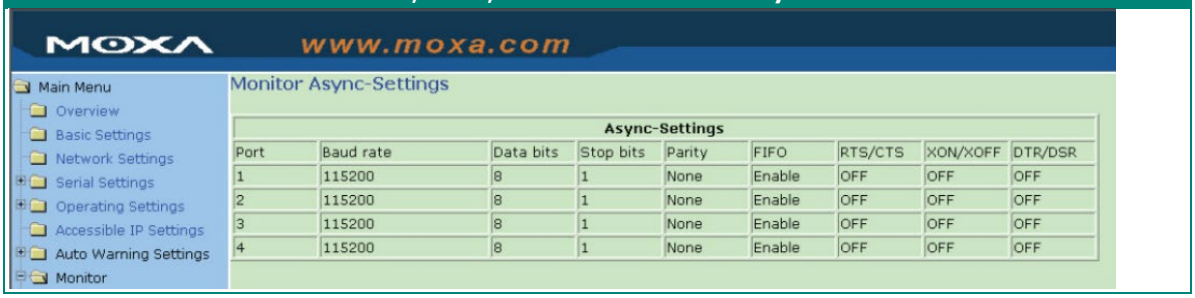
Web Interface for the Overall NPort 5000 Series



Monitor Async-Settings

Click **Async Setting** under **Monitor** to show the run-time settings for each of the four serial ports.

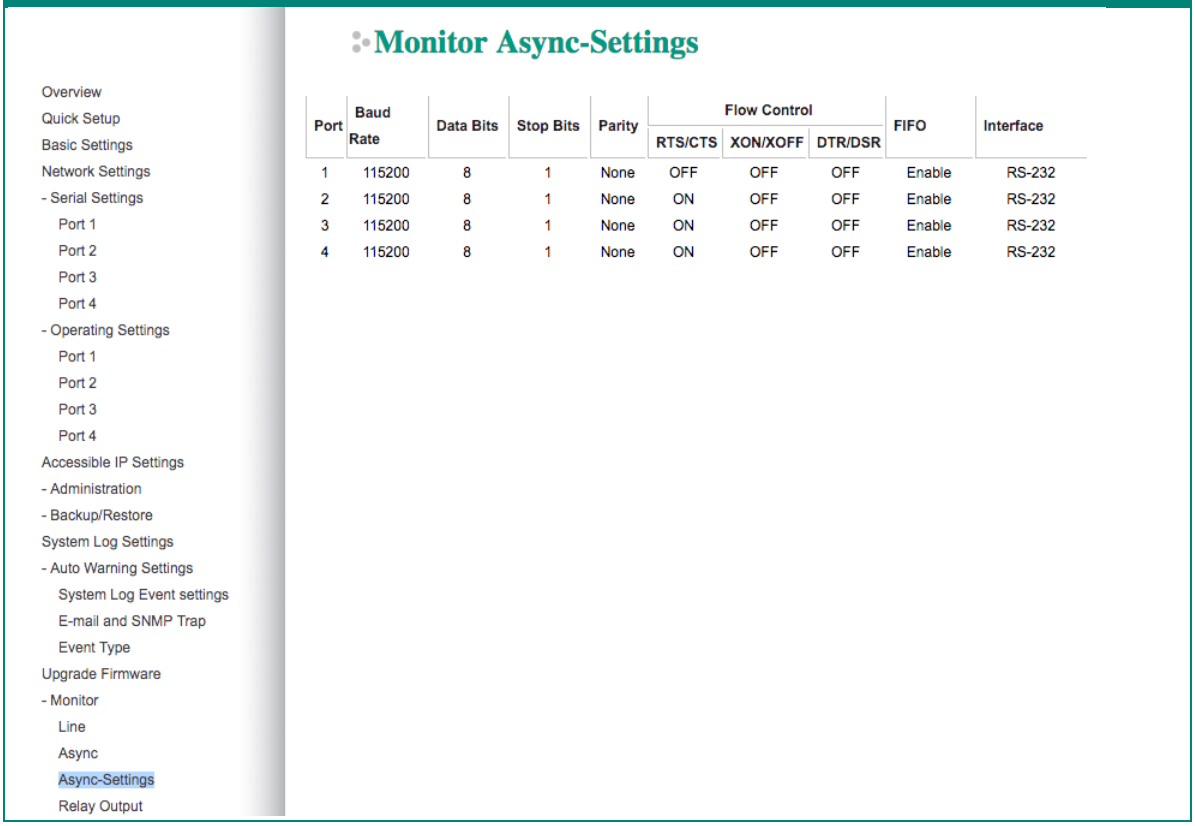
Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Async-Settings

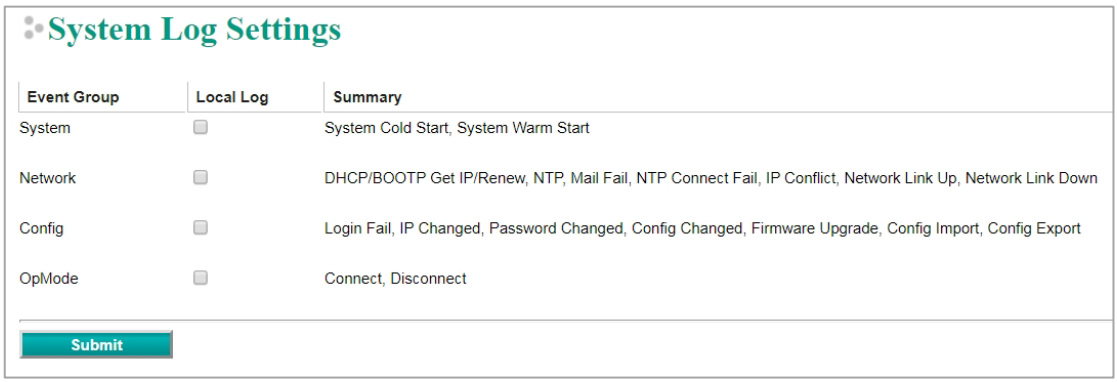
Port	Baud rate	Data bits	Stop bits	Parity	FIFO	RTS/CTS	XON/XOFF	DTR/DSR
1	115200	8	1	None	Enable	OFF	OFF	OFF
2	115200	8	1	None	Enable	OFF	OFF	OFF
3	115200	8	1	None	Enable	OFF	OFF	OFF
4	115200	8	1	None	Enable	OFF	OFF	OFF

Web Interface for the Overall NPort 5000 Series



Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control			FIFO	Interface
					RTS/CTS	XON/XOFF	DTR/DSR		
1	115200	8	1	None	OFF	OFF	OFF	Enable	RS-232
2	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
3	115200	8	1	None	ON	OFF	OFF	Enable	RS-232
4	115200	8	1	None	ON	OFF	OFF	Enable	RS-232

System Log Settings



NOTE

The NPort 5100, NPort 5200, and NPort IA5000 Series don't support this function.

System Log Settings allow NPort users to customize network events that are logged by the NPort 5000. Events are grouped into four categories, known as event groups, and the user selects which groups to log as Local Log (on the NPort 5000). The actual system events that would be logged for each system group are listed under the column "Summary". For example, if **System** was enabled, then System Cold Start events and System Warm Start events would be logged.

Local Log	Keep the log in the flash of NPort 5000 up to 512 items.

System

System Cold Start	NPort 5000 cold start.
System Warm Start	NPort 5000 warm start.

Network

DHCP/BOOTP/PPPoE Get IP/Renew	IP of the NPort 5000 is refreshed.
NTP	Time synchronization successful.
NTP Connect Fail	The NPort 5000 failed to connect to the NTP Server.
Mail Fail	Failed to deliver the email.
IP Conflict	There is an IP conflict on the local network.
Network Link Down	LAN 1 Link is down.

Config

Login Fail	
IP Changed	Static IP address was changed.
Password Changed	Administrator Password was changed.
Config Changed	The NPort 5000's configuration was changed.
Firmware Upgrade	Firmware was upgraded.
SSL Certificate Import	SSL Certificate was imported.
Config Import	Config was imported.
Config Export	Config was exported.

OpMode

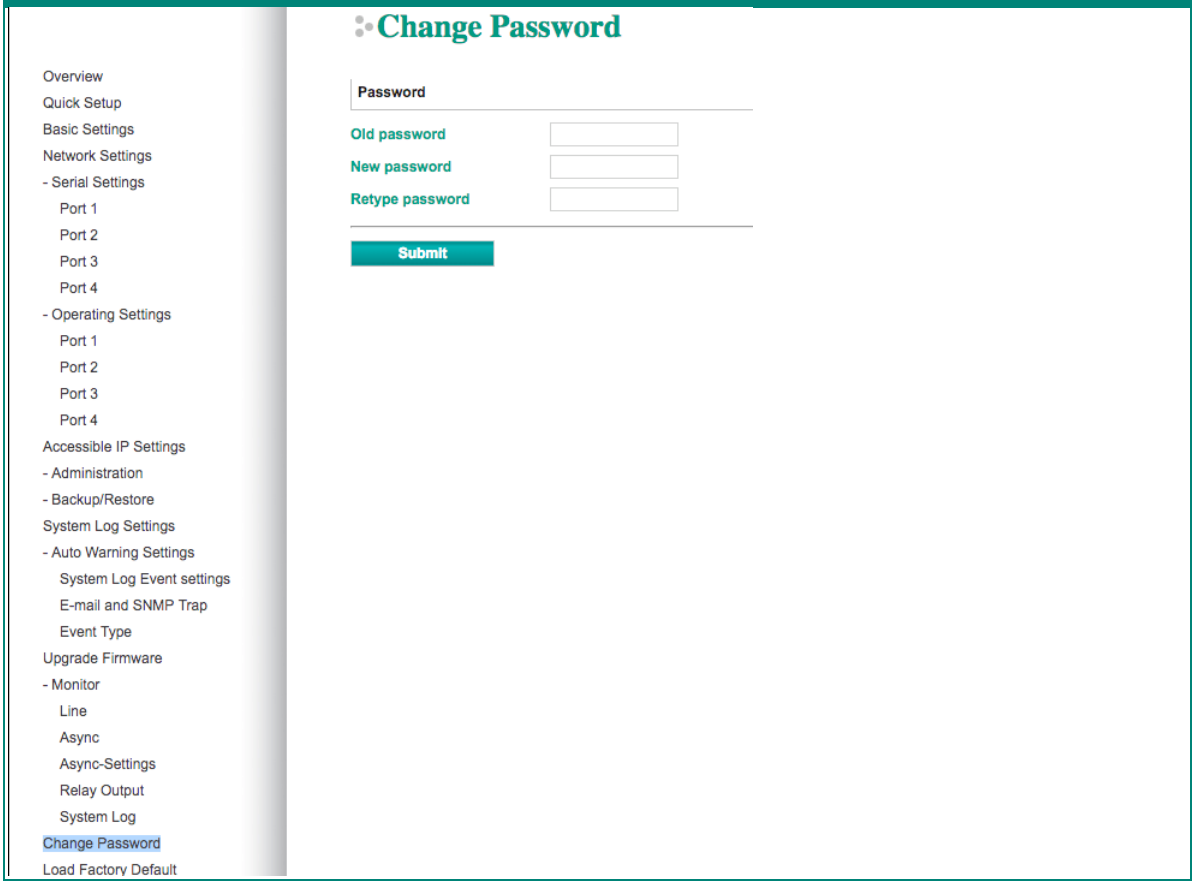
Connect	Op Mode is in use
Disconnect	Op Mode switched from in use to disconnect.
Authentication Fail	The Authentication failed in terminal; reverse terminal; or dial in/out operation modes
Restart	Serial port restarted.

Change Password

Set a password to restrict access to the NPort's configuration parameters. (The default password for NPort is **moxa**.) If a user does not enter the correct password when accessing the NPort through one of the consoles (e.g., web console), access to the NPort configuration settings will be denied.

Web Interface for the NPort 5100, 5200, IA5000 Series Only

Web Interface for the Overall NPort 5000 Series

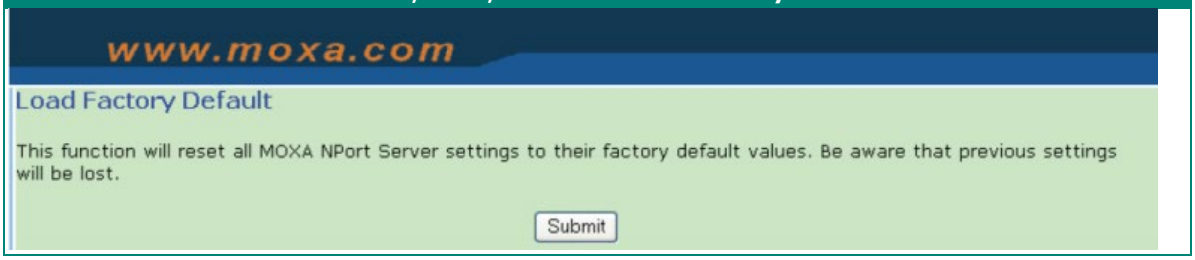


ATTENTION

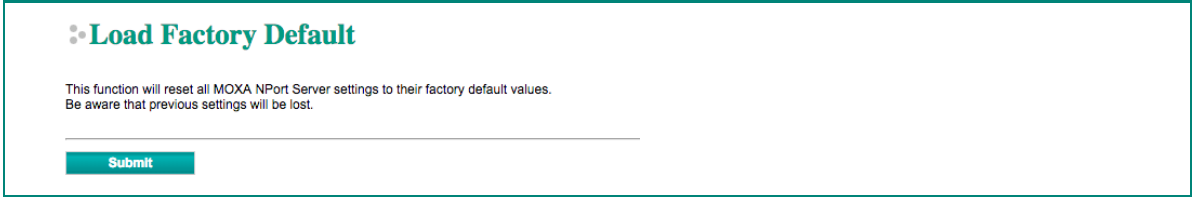
If you forget the NPort's password, the ONLY way to configure the NPort is by using the hardware reset button to load the factory defaults. Before you set a password for the first time, it is a good idea to export the NPort's complete configuration to a file. Your configuration can then be easily restored if necessary.

Load Factory Default

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series

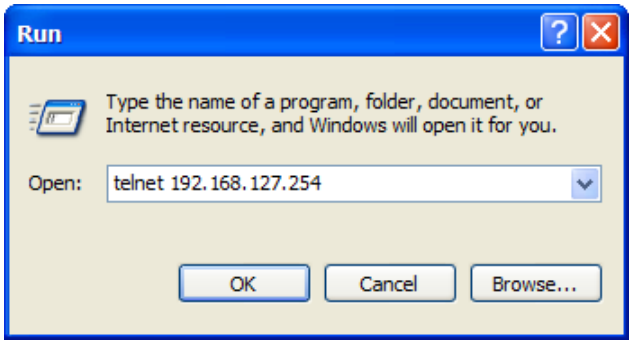


This function will reset all the NPort's settings to the factory default values. Be aware that previous settings will be lost.

Configuration by Telnet Console

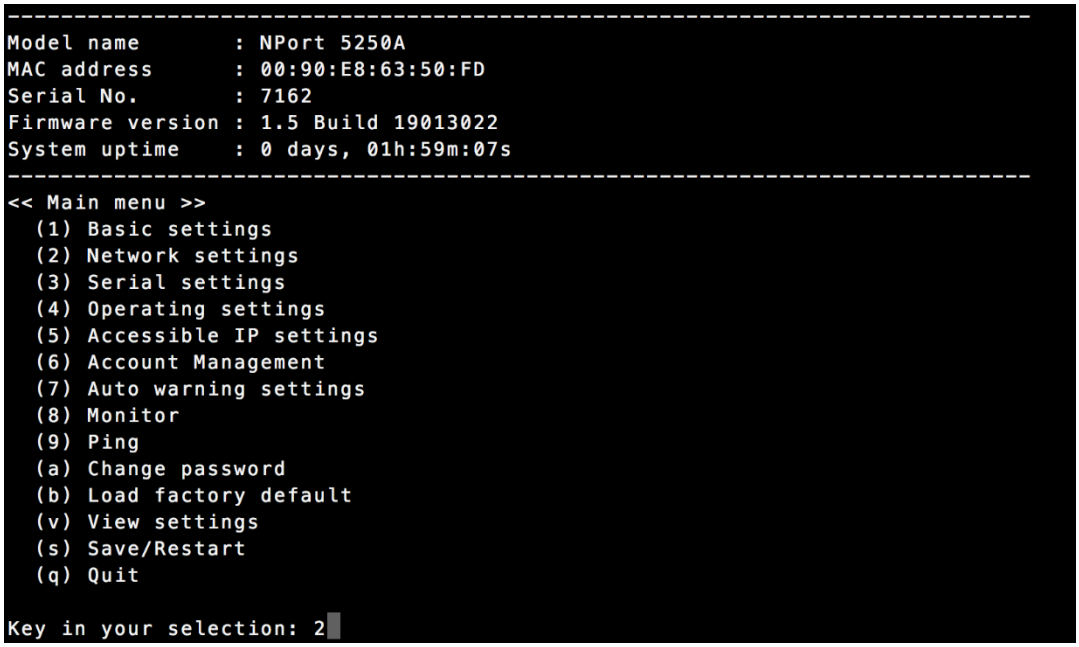
Update your NPort's IP address by using Telnet to connect to your NPort IA5000A over the network. (Figures in this section were generated using the NPort IA5450AI).

1. From the Windows desktop, click on **Start** and then select **Run**.
2. Type **telnet 192.168.127.254** (use the correct IP address if different from the default) in the **Open** text input box, and then click **OK**.

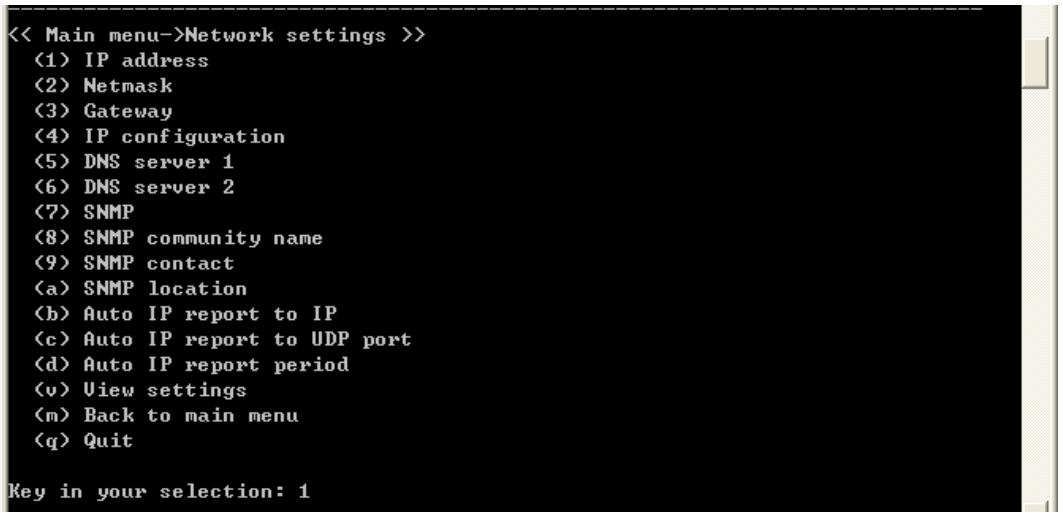


3. When the Telnet window opens, you will be prompted to input the Console password (the default username is **admin** and password is **moxa**; for the NPort 5100/5200/IA5000, it only requires the default password **moxa**); input the password and then press **Enter**.

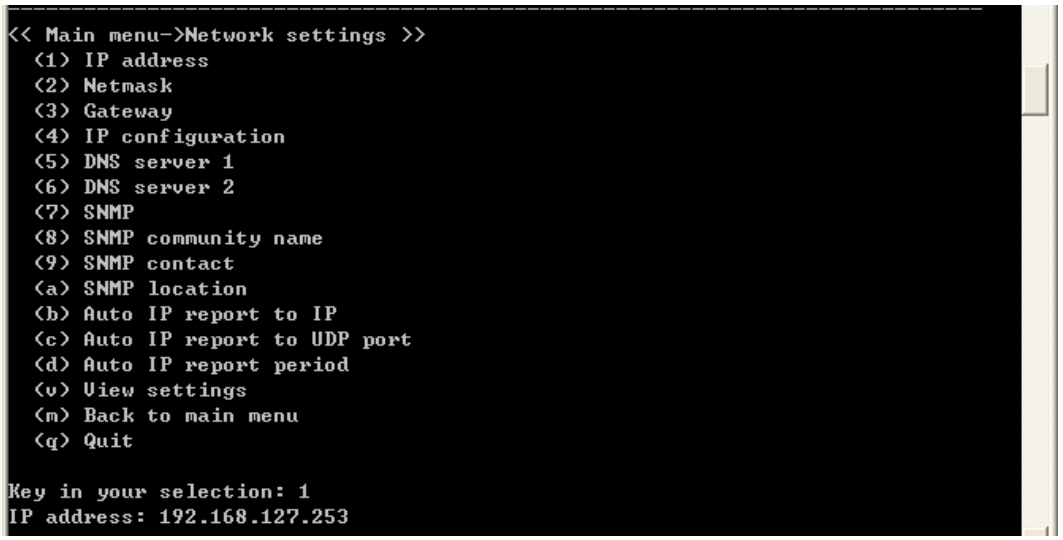
4. Type **2** to select Network settings, and then press **Enter**.



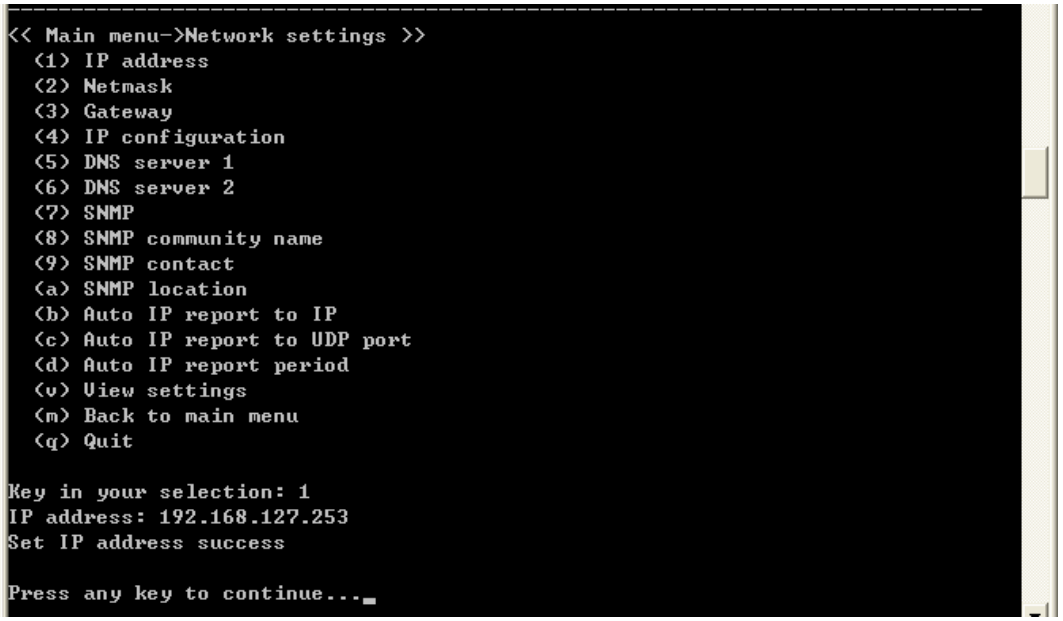
5. Type **1** to select IP address and then press **Enter**.



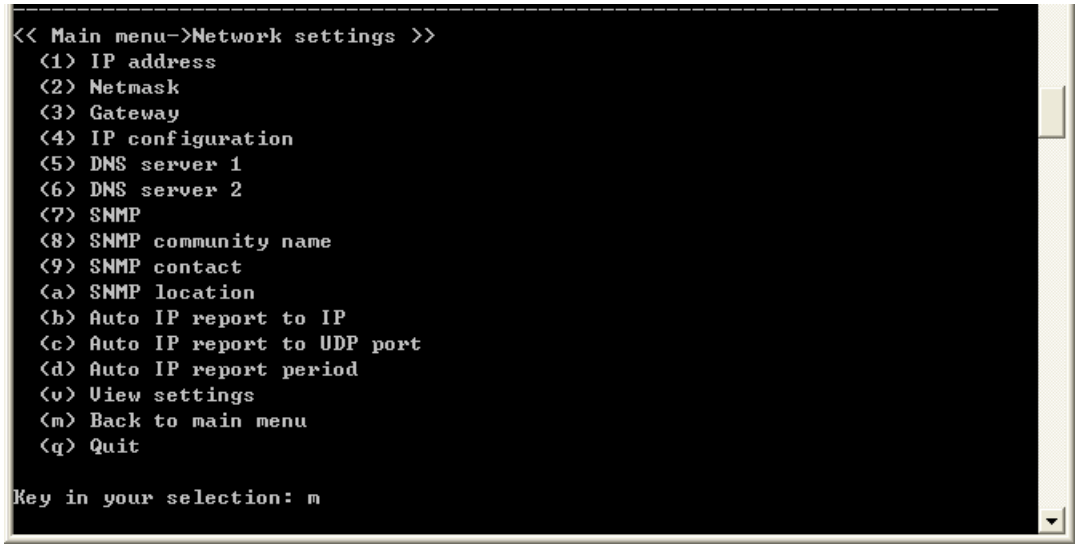
6. Use the **Backspace** key to erase the current IP address, type in the new IP address, and then press **Enter**.



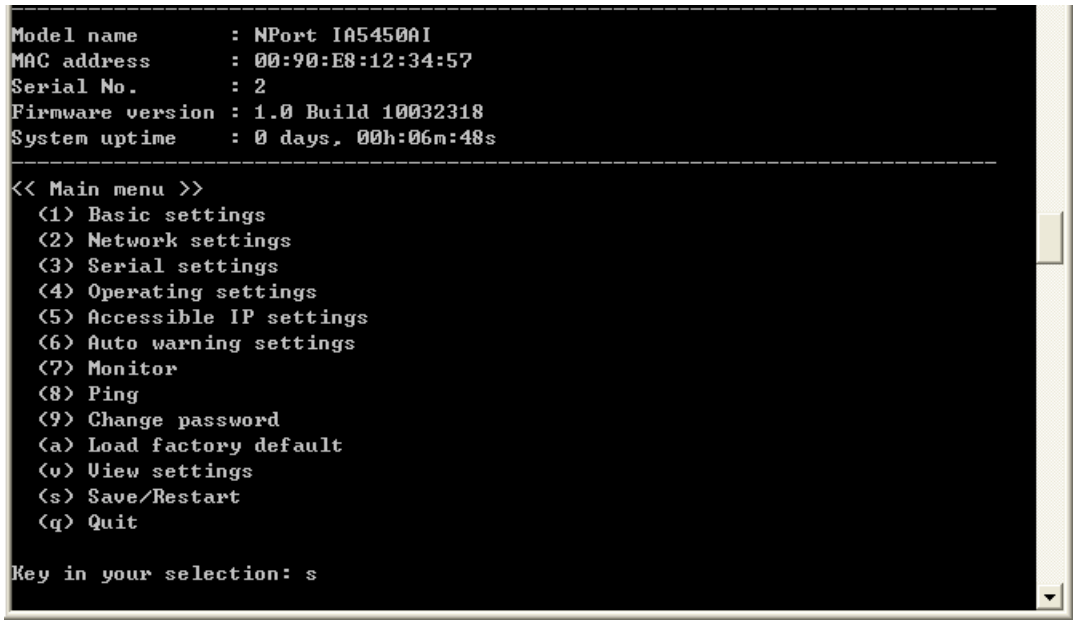
7. Press any key to continue…



8. Type **m** and then press **Enter** to return to the main menu.



9. Type **s** and then press **Enter** to **Save/Restart** the system.



10. Type **y** and then press **Enter** to save the new IP address and restart the NPort.

Configuration by Serial Console

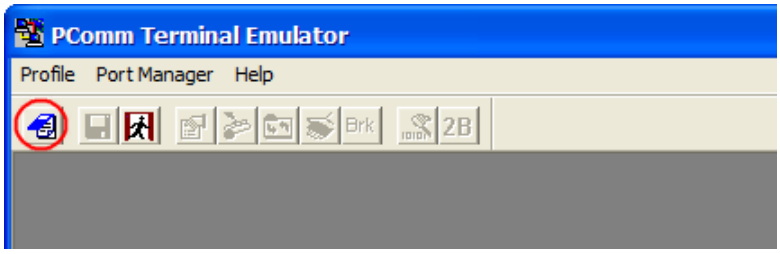
Serial Console (19200, n, 8, 1)

You may use the RS-232 console port to configure your NPort's IP address. We suggest using PComm Terminal Emulator, which is available free as part of the PComm Lite program suite, to carry out the installation procedure, although other similar utilities may also be used.

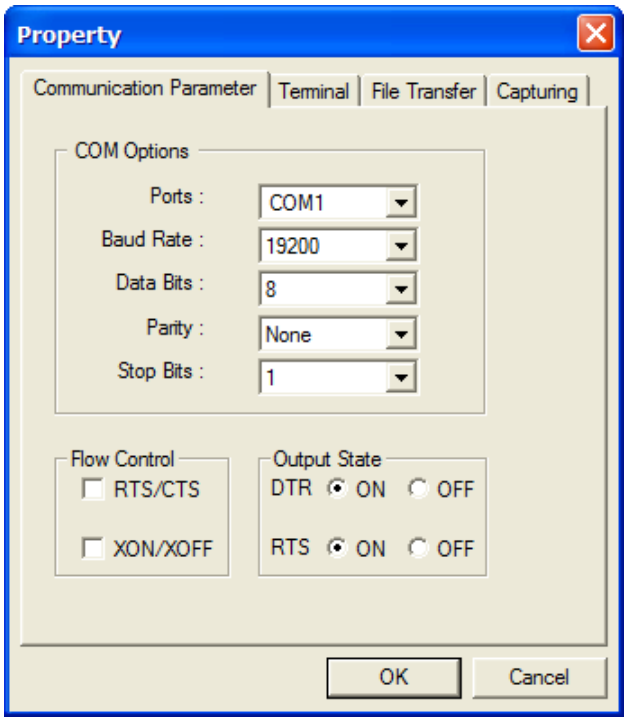
> **ATTENTION**
>
> The serial console port is an RS-232 port.

Before you configure the NPort device server over the serial console, turn off the power and connect the serial cable from the NPort to your computer's serial port.

1. Connect the NPort's serial port 1 directly to your computer's male RS-232 serial port. From the Windows desktop click **Start > Programs > PComm Lite > Terminal Emulator**.
2. When the **PComm Terminal Emulator** window opens, first click on the **Port Manager** menu item and select **Open**, or simply click on the **Open** icon.

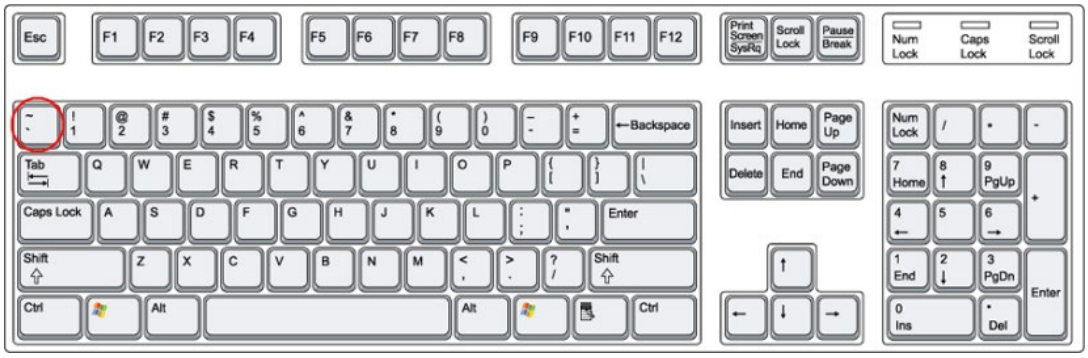


3. The **Property** window opens automatically. From the **Communication Parameter** page, select the appropriate COM port for the connection, COM1 in this example, and 19200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits.

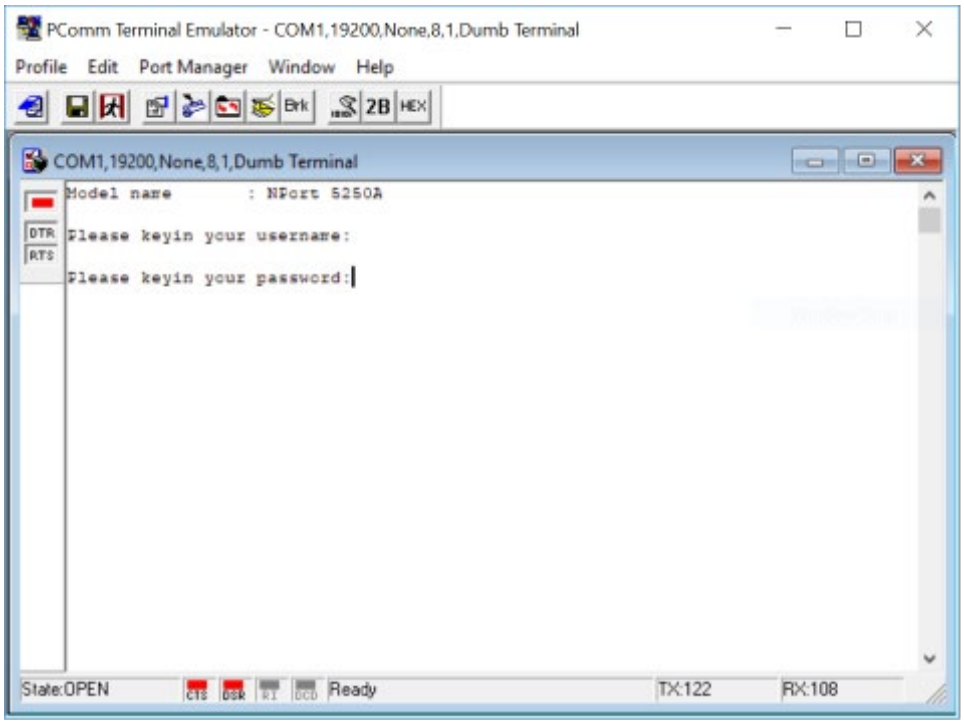


4. From the **Property** window's **Terminal** page, select ANSI or VT100 for **Terminal Type** and then click **OK**.

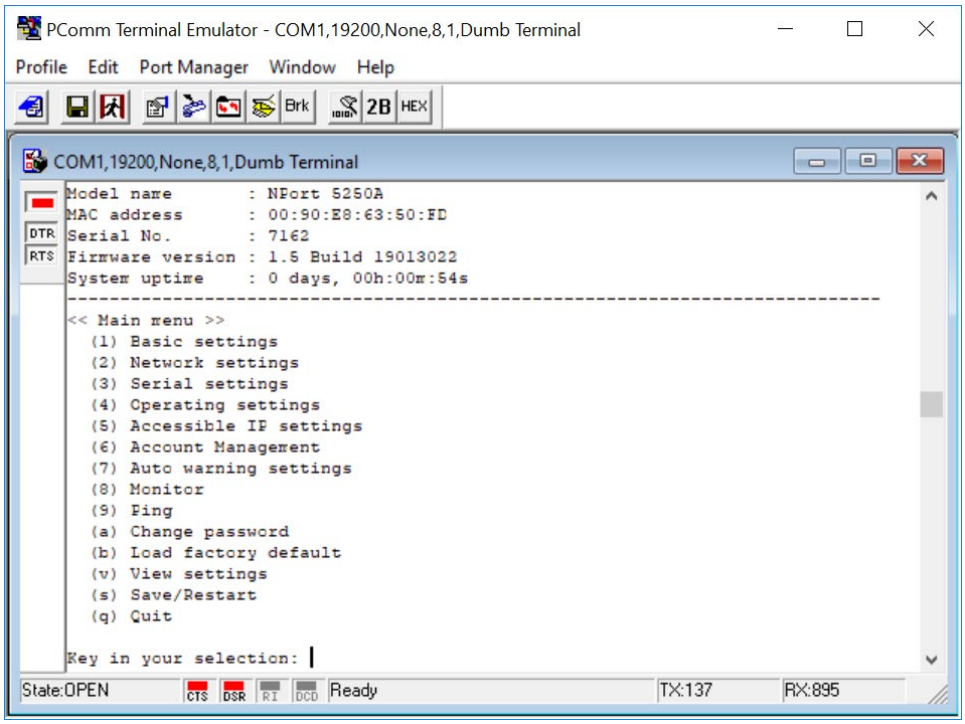
5. If you select **Dumb Terminal** as the terminal type, some of the console functions—especially the **Monitor** function—may not work properly.
6. Press the " ` " key continuously and then power on the NPort.



7. The NPort will automatically switch from data mode to console mode as it receives a continuous string of " ` " characters.
8. The default username is **admin**, and the password is **moxa**.



9. Start configuring the IP address under **Network Settings**. Refer to step 4 in the Telnet Console section for the rest of the IP settings.



Testing Your NPort

After completing installation and configuration, you can do a simple test to ensure that your NPort will communicate successfully. Click on the appropriate link below to view a technical note that explains how to test your NPort one of four common operation modes: Real COM, TCP client, TCP server, and UDP.

- Real COM Mode for NPort
- TCP Client Mode for NPort
- TCP Server Mode for NPort
- UDP Mode for NPort

3. Cybersecurity Considerations

With cyberattacks growing in number and sophistication, network device vendors are adding functions geared towards protecting sensitive business and personal information. Moxa has dedicated itself in this area by developing measure to make sure all the products can and will meet the security standard, so customers will use Moxa's product without too much to worry about. 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 exact settings or commands. The following topics are covered in this chapter:

Updating Firmware

When a customer buys a product from Moxa or reseller, Moxa may have already pushed out a newer version of firmware and that is likely to have enhanced the security features included. We suggest you always update to the latest firmware. Check with Moxa's support website for further details.

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. It is always recommended to turn off services and ports that are not in use to reduce the chances of being attacked.

Turn Off Moxa Service After Installation

Moxa Service is extremely helpful for first-time installation as it helps the device to be discovered in a local area network (LAN). Once the installation is completed, this service should be turned off for safety reasons; however, once it is turned off, a utility such as Moxa's DSU (Device Search Utility) is no longer seeking for the device, and only by the IP and login with username and password will have the access to the product.

Turn On Services That Are Necessary

There are services that were designed some while ago, but then cybersecurity wasn't much of an issue, therefore the design's considerations didn't quite cover cybersecurity. Below is a list of services that are recommended to turn on only when necessary:

HTTP/HTTPS: If the web console is required to access the product, it is recommended to use HTTPS over HTTP

Telnet: Only enable Telnet if a command line is required to manage the product

SNMP: If using Simple Network Management Protocol for remote device monitoring and management, this should be turned on. We strongly advised to change the default community name once enabled and also set SNMP to send a trap if authentication failures happen.

NOTE

Once all the settings are configured according to your needs, remember to save and restart the device so that all the new settings are effective. Remember to export your settings.

NOTE

If all HTTP/HTTPS/Telnet/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. Refer to the user manual on how to reset the device.

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 there are only limited desktop/notebook/mobile devices that would access the product, grant those IPs access.

Account and Password

- There is a default username and password for first-time installation; it is strongly suggested to change the password after installation has been done.
- Use your own passwords for users of the devices. If possible, also change the default name of the account. For example, don't name admin group "admin" before the device is deployed.
- Use strong passwords. The devices support a function to check if the passwords are strong enough. You can enable the function to help you check whether the passwords are strong enough.
- Use account login failure lockout feature to prevent unwelcome access

System Log

System log can contain all kinds of activities that are happening on your NPort, such as Login Fail, IP Changed, Password Changed, Config Changed, etc. Check the log periodically to examine any abnormal behavior.

Testing the Security Environment

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

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

1. Testing tools for cybersecurity environment checks are available. Some may provide limited free use, for example, Nessus. These tools help identify possible security leaks in the environment.
2. The device should be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
3. Control access to the serial console as with any physical access to the device.
4. Avoid using insecure services such as Telnet and TFTP; the best way is to disable them completely.
5. Limit the number of simultaneous web server and Telnet sessions allowed. Periodically, change the passwords.
6. Backup the configuration files periodically and compare the configurations to make sure the devices work properly.
7. Audit the devices periodically to make sure they comply with these recommendations and/or any internal security policies.
8. 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: 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 security level to defend against cyberattacks and do not guarantee that the above information will meet your specific requirements. Furthermore, the above information is provided "as is", and we make no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

4. Choosing the Proper Operation Mode

In this chapter, we describe the NPort device server's various operation modes. The options include an operation mode that uses a driver installed on the host computer, and operation modes that rely on TCP/IP socket programming concepts. After choosing the proper operation mode in this chapter, refer to **Chapter 5** for detailed configuration parameter definitions.

Overview

NPort serial device servers network-enabled traditional RS-232/422/485 devices. A serial device server is a small computer equipped with a CPU, real-time OS, and TCP/IP protocols that can bi-directionally translate data between the serial and Ethernet formats. NPort device servers that are connected to a network that with access to the Internet can be accessed from a computer located anywhere in the world.

Traditional SCADA and data collection systems rely on serial ports (RS-232/422/485) to collect data from various kinds of instruments. Since NPort serial device servers network-enabled instruments equipped with an RS-232/422/485 communication port, your SCADA and data collection system will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

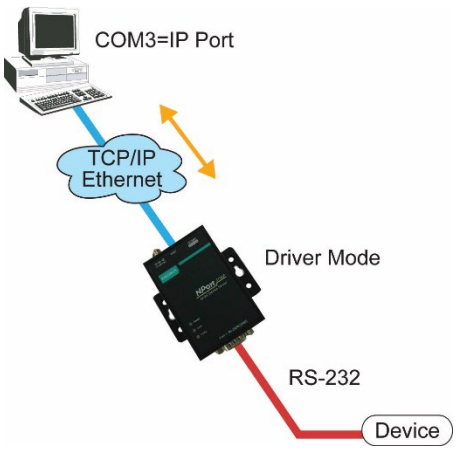
An NPort serial device server is an external IP-based network device that allows you to expand the number of serial ports for a host computer on demand. If your host computer supports the TCP/IP protocol, you won't be limited by the host computer's bus limitation (such as ISA or PCI), or lack of drivers for various operating systems.

Besides providing socket access, the NPort also comes with a Real COM / TTY driver that transmits all serial signals intact. This means that you can continue using your existing COM/TTY-based software, without needing to invest in additional software.

Three different socket modes are available: TCP Server, TCP Client, and UDP Server/Client. The major difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer speedier delivery. UDP also allows data to be unicast to only one IP address, or multicast to groups of IP addresses.

Real COM Mode

The NPort comes equipped with COM drivers that work with Windows systems, and also TTY drivers for Linux systems. The driver establishes a transparent connection between the host and serial device by IP-Port mapping the for NPort's serial port to a local COM/TTY port on the host computer. Real COM Mode also supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device simultaneously.



ATTENTION

The driver used for Real COM Mode is bundled with NPort Administrator. The driver is installed on your computer automatically when you install NPort Administration Suite.

One of the major conveniences of using Real COM Mode is that Real COM Mode allows users to continue using RS-232/422/485 serial communications software that was written for pure serial communications applications. The driver intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card. At the other end of the connection, the NPort accepts the Ethernet frame, unpacks the TCP/IP packet, and then sends it transparently to the appropriate serial device attached to one of the NPort's serial ports.

ATTENTION

Real COM Mode allows several hosts to access the same NPort. The driver that comes with your NPort controls host access to attached serial devices by checking the host's IP address. Refer to the **Accessible IP Settings** section in **Chapter 2** for details.

RFC2217 Mode

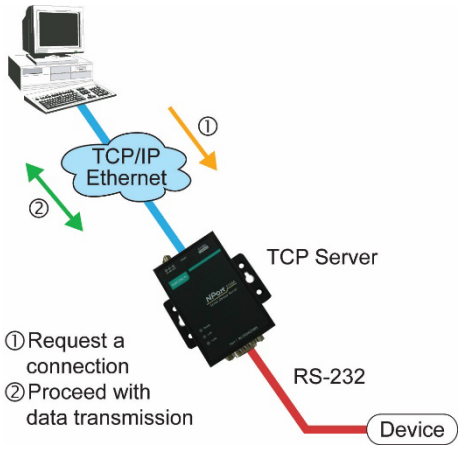
RFC2217 Mode is only supported by the NPort 5000A, NPort 5000AI-M12, NPort IA5000A, NPort 5600, and NPort 5600-8-DT/DTL Series.

RFC 2217 mode is similar to Real COM mode in that a driver is used to establish a transparent connection between a host computer and a serial device by mapping the serial port on the NPort to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third party drivers supporting RFC2217 are widely available on the Internet and can implement Virtual COM mapping to your NPort serial port(s).

TCP Server Mode

In TCP Server Mode, the NPort is configured with a unique IP-Port combination on a TCP/IP network. Here, the NPort waits passively to be contacted by the host computer. After the host computer establishes a connection with the serial device, it can then proceed with data transmission. TCP Server mode also supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device—simultaneously. As illustrated in the figure, data transmission proceeds:

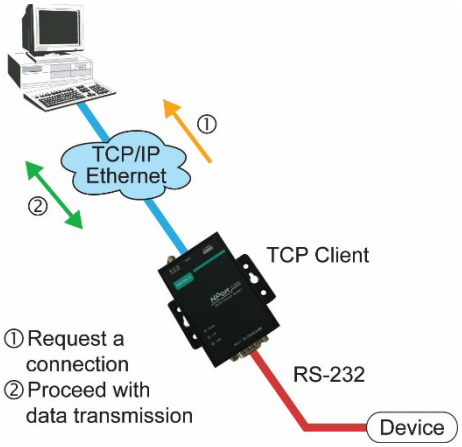
1. The host requests a connection from the NPort configured for TCP Server Mode.
2. Once the connection is established, data can be transmitted in both directions—from the host to the NPort, and from the NPort to the host.



TCP Client Mode

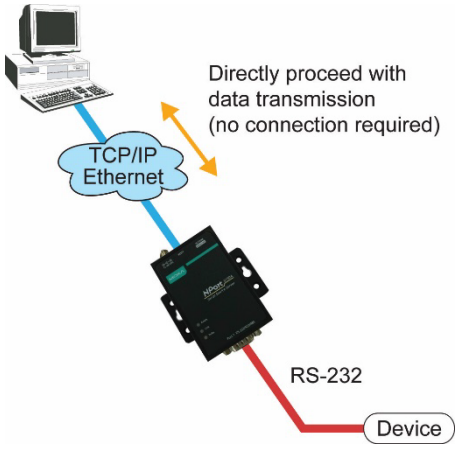
In TCP Client Mode, the NPort can actively establish a TCP connection with a pre-determined host computer when serial data arrives. After the data has been transferred, the NPort can disconnect automatically from the host computer by using the **TCP alive check time** or **Inactivity time** settings. Refer to **Chapter 5** for detailed configuration instructions. As illustrated in the figure, data transmission proceeds:

1. The NPort configured for TCP Client Mode requests a connection from the host.
2. Once the connection is established, data can be transmitted in both directions—from the host to the NPort, and from the NPort to the host.



UDP Mode

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can unicast or multicast data from the serial device to one or multiple host computers, and the serial device can also receive data from one or multiple host computers, making this mode ideal for message display applications.



Pair Connection Mode

Pair Connection Mode employs two NPort units in tandem and can remove the 15-meter distance limitation imposed by the RS-232 interface. One NPort is connected from its RS-232/422/485 port to the COM port of a PC or other type of computer, such as hand-held PDAs that have a serial port, and the serial device is connected to the RS-232/422/485 port of the other NPort. The two NPort units are then connected to each other with a crossover Ethernet cable, both are connected to the same LAN, or in a more advanced setup, they communicate with each other over a WAN (i.e., through one or more routers). Pair Connection Mode transparently transfers both data and modem control signals (although it cannot transmit the DCD signal) between the two NPorts.

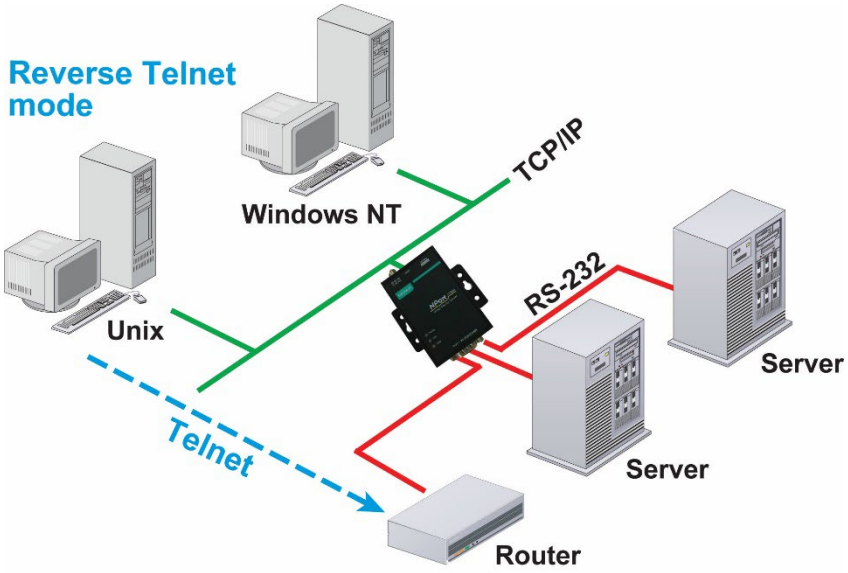
Ethernet Modem Mode

Ethernet Modem Mode is only supported by the NPort IA5000/IA5000A, NPort 5000A, NPort 5000AI-M12, and NPort 5100 Series.

Ethernet Modem Mode is designed for use with legacy operating systems, such as MS-DOS, that do not support TCP/IP Ethernet. By connecting one of NPort's serial ports to the MS-DOS computer's serial port, it is possible to use legacy software originally designed to transmit data via modem, but now transmit the data over the Ethernet.

Reverse Telnet Mode

Console management is commonly used by connecting to Console/AUX or COM ports of routers, switches, and UPS units. Reverse Telnet works the same as TCP Server mode in that only one TCP port is listened to after booting up. The system then waits for a host on the network to start a connection. The difference is that the TCP Server mode does not provide the conversion function provided by Telnet. If the connected devices need to use the CR/LF conversion function when controlling, then users must choose Reverse Telnet mode.



PPP Mode

PPP Mode is only supported by the NPort 5600 Series.

The NPort 5000 provides dial-in access for ISPs and enterprises that need a remote access solution. When a user at a remote site uses a PPP dial-up connection to access the NPort 5600, the NPort 5600 plays the role of a dial-up server, but also ensures that the user has legal access to the network by verifying the user's identity with the NPort 5600 User Table.

Disabled Mode

When the Operation Mode for a particular port is set to **Disabled**, that port will be disabled.

5. Advanced Operation Mode Settings

Your NPort's serial ports can be configured to use one of several operation modes, such as Real COM mode or Reverse Telnet mode. In this chapter, we explain the settings for every parameter of every operation mode.

Overview

A device port's operation mode determines how the port interacts with the network. Depending on your application and device, you may choose between two or more operating modes. For each mode, the default settings should work for most applications. Change these settings only if absolutely necessary for your application. The operation mode and related parameters can be configured through NPort Administrator. The same parameters may also be configured using the web console, Telnet console, or serial console.

List of Parameters

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	
							Connection Management Parameters
✓	✓	✓		✓	✓	✓	TCP alive check time
	✓	✓		✓			Inactivity time
✓	✓	✓					Max connection
✓	✓	✓					Ignore jammed IP
✓	✓						Allow driver control
							Data Packing Parameters
✓	✓	✓	✓			✓	Packing length
✓	✓	✓	✓			✓	Delimiter 1 and 2
✓	✓	✓	✓			✓	Delimiter process
✓	✓	✓	✓			✓	Force transmit
							Other Parameters
	✓			✓	✓		Local TCP port
	✓						Command port
					✓		Destination IP address
		✓	✓				Destination IP address 1 through 4
		✓					Designated local port 1 through 4
			✓				Local listen port
		✓					Connection Control
				✓			Map <CR-LF>

When to Make Adjustments

The default settings for each operation mode work for most applications and rarely need to be changed. However, adjustments may be required for the following situations:

- You may need to control network data packing using specific delimiter characters.
  Adjust **Delimiters 1 and 2 and Delimiter process.**
- Multiple hosts will simultaneously access the attached device.
  Adjust **Max Connection, Ignore Jammed IP, and Allow driver control.**
- Data will be broadcast from the serial device to multiple network destinations.
  Adjust **Destination IP 1 through 4.**
- You are using Pair Connection modes to connect two serial devices over Ethernet.
  Adjust **Local TCP port and Destination IP Address**

Using Pair Connection Modes

For some applications, you may want to configure two serial devices to communicate directly with each other over the network. This can be done with a pair of NPort device servers configured for Pair Connection Master/Slave modes. Configure one device port on one of the NPorts to Pair Connection Master mode, and one device port on the other NPort to Pair Connection Slave mode. It doesn't matter which NPort is the master and which NPort is the slave.

For the device port configured for Pair Connection Slave mode, designate a Local TCP port to be used for communication. For the device port configured for Pair Connection Master mode, enter the slave's IP address and Local TCP port as the **Destination IP**.

Once both device ports have been configured, the attached serial devices will communicate over Ethernet as if they were connected by a serial cable. The two NPorts can be connected by an Ethernet cable, or they can be connected to the same network.

Parameter Summary

Connection Management Parameters

✓ Real COM Mode	✓ TCP Server Mode	✓ TCP Client Mode	UDP Mode	✓ Reverse Telnet Mode	✓ Pair Connection Mode	✓ RFC2217 Mode	PPP Mode	**TCP alive check time**
								Setting Options: 0 to 99 minutes Default: 7 minutes Description: Specifies the time counter to check if the TCP connection is alive. If there is no response from the other end of the connection after the specified time, then the TCP connection will be closed. A setting of 0 means disabled. This is a good practice to free up the device's resources.

	✓	✓		✓			✓	**Inactivity time**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: 0 to 65535 ms Default: 0 Description: Specifies the time limit for keeping the connection open if no data flows to or from the serial device. If there is no activity for the specified time, the connection will be closed. A setting of 0 keeps the connection open even if no data is ever received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. If you wish to use Inactivity time with TCP Client mode, you must set Connection Control to Any Character/Inactivity Time (see Connection Control). When adjusting Inactivity time, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.

✓	✓	✓						**Max connection**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: 1 to 8 (for NPort 5100A/5200A/IA5250A/IA5450A and NPort 5150AI-M12/5250AI-M12/5450AI-M12 Series) Setting Options: 1 to 4 (for other NPort 5000 Series) Default: 1 Description: Specifies the maximum number of simultaneous connections that the port will accept. When adjusting Max connection, make sure that Ignore jammed IP and Allow driver control are also configured correctly.

✓	✓	✓						**Ignore jammed IP**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: Yes or No Default: No Description: This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the device port (see Max connection). **Yes** means that transmission to the other hosts will not be suspended if one IP address becomes unresponsive. **No** means that all transmission will be suspended if one IP address becomes unresponsive and will resume when all hosts have responded. **Yes** is the recommended setting when Max connection is 2 or more.

✓	✓							**Allow driver control**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: Yes or No Default: No Description: Specifies whether the device port will respond to driver control commands when multiple simultaneous connections are enabled (see Max connection).

Data Packing Parameters

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Packing length**
✓	✓	✓	✓			✓		Setting Options: 0 to 1024 Default: 0 Description: Controls data packing by the amount of data received. Serial data accumulates in the device port's buffer until it reaches the specified length. When the specified amount of data has accumulated in the buffer, the data is packed for network transmission. A setting of 0 means that data will not be packed until the buffer is full. 0 is the recommended setting, unless your application specifically needs to limit packet sizes or improve response times.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Delimiter 1 and 2**
✓	✓	✓	✓			✓		Setting Options: Enable, 0 to FF Default: Disable Description: Controls data packing using special delimiter character(s). Serial data accumulates in the device port's buffer until the delimiter character(s) are received, after which the data is packed for network transmission. If only one delimiter character is needed, be sure to enable Delimiter 1 only. If both Delimiter 1 and 2 are enabled, both characters must be received in sequence for data packing to occur. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data is packed according to the Delimiter process parameter. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When the device port buffer is full, the data will be packed for network transmission, regardless of the settings for Delimiter 1, Delimiter 2, and Force transmit.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Delimiter process**
✓	✓	✓	✓			✓		Setting Options: Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter Default: Do Nothing Description: Controls how data is packed when delimiter characters are received. Note that this field has no effect if delimiters are not enabled (see Delimiters 1 and 2). "Do nothing" will pack the accumulated data including delimiters. "Delimiter + 1" will wait for an additional character before packing the accumulated data. "Delimiter + 2" will wait for two additional characters before packing the accumulated data. "Strip Delimiter" will pack the accumulated data but will not include the delimiter characters in the packet.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Force transmit**
✓	✓	✓	✓			✓		Setting Options: 0 to 65535 ms Default: 0 ms Description: Controls data packing by the time that elapses between bits of data. As serial data is received, it accumulates in the device port's buffer. If serial data is not received for the specified amount of time, the data that is currently in the buffer is packed for network transmission. A setting of 0 means that data in the buffer will not be automatically packed when additional data is not received from the device. When using this field, make sure Inactivity time is disabled or set to a larger value. Otherwise, the connection may be closed before the data in the buffer can be transmitted.

Other Parameters

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Local TCP port**
	✓			✓	✓			Setting Options: 1 to 65535 Default: 4001 for port 1, 4002 for port 2, etc. Description: Specifies the TCP port number for communicating with the attached device. Socket applications will need to use this port number to refer to the device. For Pair Connection modes, this field specifies the slave's port number, and the same value must be used for the master's Destination IP parameter.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Command port**
	✓							Setting Options: 1 to 65535 Default: 966 Description: Specifies the TCP port number for Moxa IP-Serial Library commands. You do not need to reference this port number in your application when using the Moxa IP-Serial Library, since the library automatically gets the number from the device server. Only change this setting if there is a port number conflict with another application or device.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Destination IP address**
					✓		✓	Setting Options: N/A Default: none Description: Specifies the IP address for the slave end of a pair connection.

Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	**Destination IP address 1 through 4**
		✓	✓					Setting Options: N/A Default: none Description: Specifies the network host(s) that will access the device. Serial data will be transmitted to every address listed, and network data will be sent to the device on a first-in-first-out basis.

		✓						**Designated local port 1 through 4**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: 1 to 65535 Default: none Description: Specifies the TCP port number that will be used for data transmission with the device port.

			✓					**Local listen port**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: 1 to 65535 Default: 4001 for port 1, 4002 for port 2, etc. Description: Specifies the UDP port number for network communication to the serial device. Socket applications will need to use this port number to refer to the device.

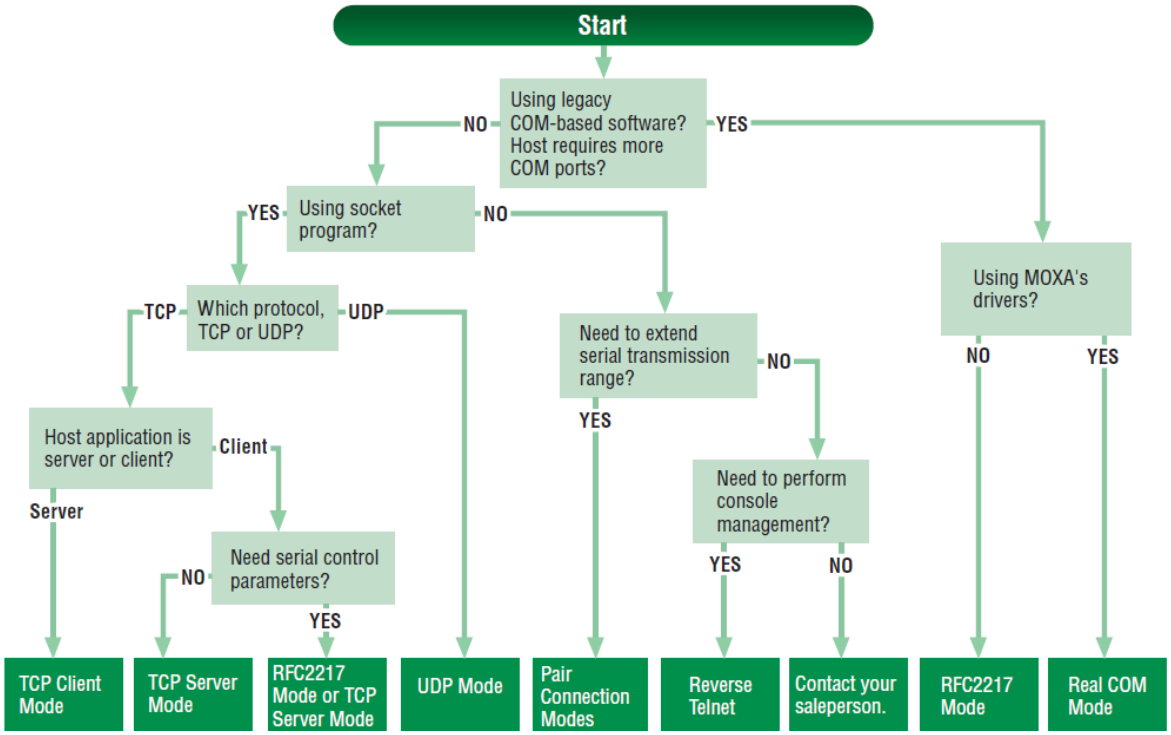
		✓						**Connection Control**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: Startup/None, Any Character/None, Any Character/Inactivity Time, DSR On/DSR Off, DSR On/None, DCD On/DCD Off, DCD On/None Default: Startup/None Description: Specifies how connections to the device are established and closed. For example, "Startup/None" means that as soon as the device server starts up, the TCP connection is opened, and the connection can only be closed manually. "DCD On/DCD Off" means that the TCP connection is opened when the DCD signal is on, and closed when the DCD signal is off. If you want to use the Inactivity Time parameter to close the connection when the serial device is inactive, you must set Connection Control to "Any Character/Inactivity time".

				✓				**Map <CR-LF>**
Real COM Mode	TCP Server Mode	TCP Client Mode	UDP Mode	Reverse Telnet Mode	Pair Connection Mode	RFC2217 Mode	PPP Mode	Setting Options: CR, LF, or CR-LF Default: CR-LF Description: Specifies how the ENTER key is mapped from the Ethernet port through the serial port. For certain terminal applications, the Enter key needs to be translated specifically as a CR character rather than CR-LF.

Operation mode codes in the configuration file are listed below:

0: Pair slave
1: Part master
2: Real COM
7: Disable
8: Reverse Telent
10: TCP server
12: Ethernet Modem mode
13: TCP client
14: UDP
15: PPP
20: RFC2217

How to Choose Proper Operation Mode



Web Console

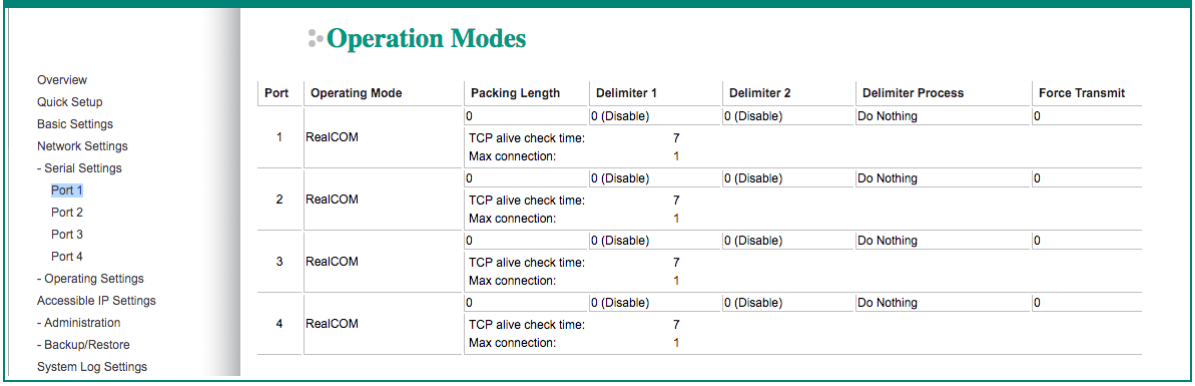
Click **Operating Settings** to display the operating settings for each of the NPort's serial ports.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

Operating Settings

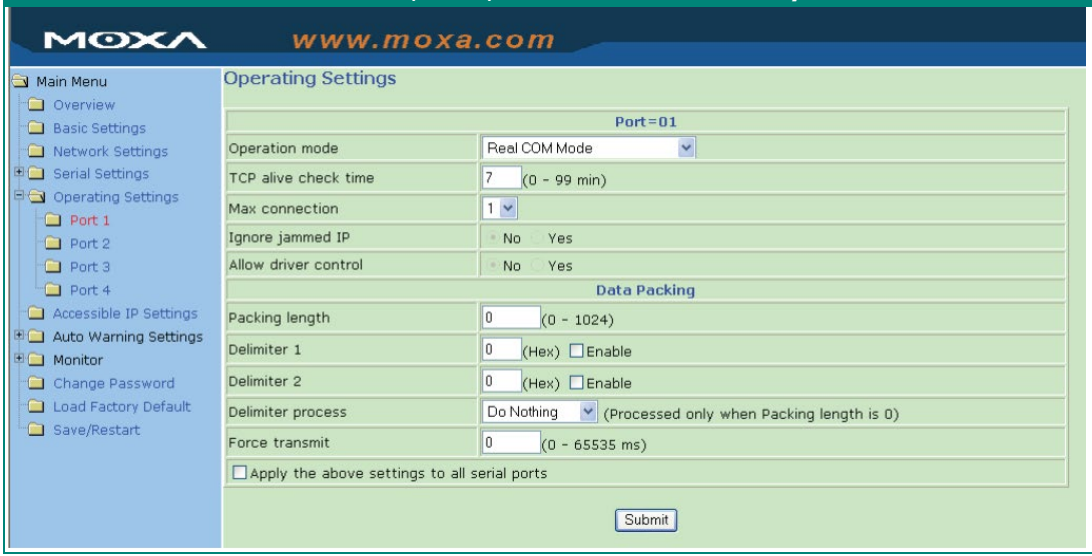
Operating Settings						
Port	Operating mode	Packing length	Delimiter 1	Delimiter 2	Delimiter process	Force transmit
1	Real COM Mode	0	0 (Disable)	0 (Disable)	Do Nothing	0
		TCP alive check time: 7 Max connection: 1				
2	Real COM Mode	0	0 (Disable)	0 (Disable)	Do Nothing	0
		TCP alive check time: 7 Max connection: 1				

Web Interface for the Overall NPort 5000 Series

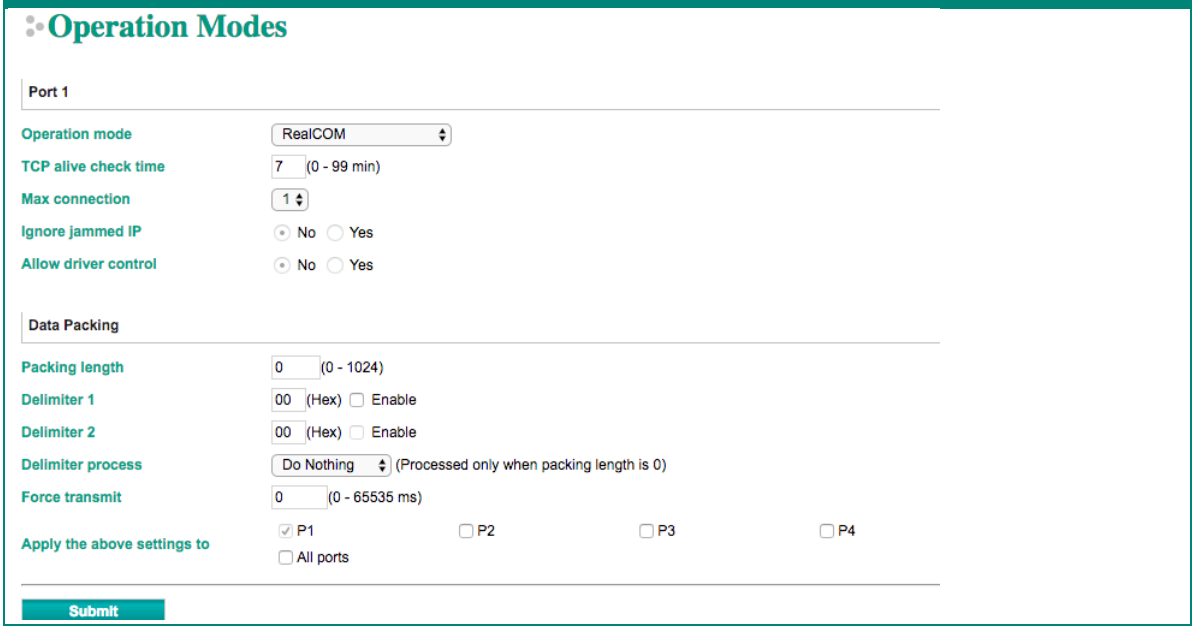


Real COM Mode

Web Interface for the NPort 5100, 5200, and IA5000A Series Only



Web Interface for the Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort automatically closes the TCP connection if there is no TCP activity for the given time. After the connection is closed, the NPort starts listening for another Real COM driver connection.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Max Connection	1 to 8 for NPort 5100A/ 5200A/IA5250A/ IA5450A and NPort 5150AI-M12/ 5250AI-M12/ 5450AI-M12 Series (1 to 4 for other NPort 5000 Series)	1	**Max connection** is set to 2 to 8 when the user needs to receive data from different hosts simultaneously. The factory default only allows 1 connection at a same. When Max Connection is set to 1, the Real COM driver on the specific host has full control. **Max. Connection 1:** Allows only 1 host's Real COM driver to open the specific NPort serial port. **Max Connection 2 to 8:** Allows 2 to 8 host's Real COM drivers to open the specific NPort serial port, at the same time. When multiple hosts' Real COM drivers open the serial port at the same time, the COM driver only provides a pure data tunnel without control ability. This serial port parameter will use the firmware's settings, not the settings of your application program (AP). Application software that is based on the COM driver will receive a driver response of "success" when the software uses any of the Win32 API functions. The firmware will only send the data back to the driver on the host. Data will be sent first-in-first-out when data comes into the NPort from the Ethernet interface.	Required
Ignore jammed IP	No or Yes	No	No: When Max connections > 1, and the serial device is transmitting data, if any of the connected hosts are not responding, it will wait until the data has been transmitted successfully before transmitting the second group of data to all hosts. Yes: If you select Yes for "Ignore jammed IP," the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.	Optional
Packing length	0 to 1024	0	0: The Delimiter Process will be followed, regardless of the length of the data packet. Greater than 0: If the data length (in bytes) matches the configured value, the data will be forced out.	Optional
Delimiter 1	00 to FF	None	Once the NPort receives both delimiters through its serial port, it immediately packs all data currently in its buffer and sends it to the NPort's Ethernet port.	Optional
Delimiter 2	00 to FF	None		Optional
Delimiter process	Do nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter	Do nothing	**[Delimiter + 1] or [Delimiter + 2]:** The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter. **[Strip Delimiter]:** When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted. **[Do nothing]:** The data will be transmitted when the Delimiter is received.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Force Transmit	0 to 65535 ms	0 ms	**0:** Disable the force transmit timeout. **1 to 65535:** Forces the NPort's TCP/IP protocol software to pack serial data received during the specified time into the same data frame. This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the force transmit time interval reaches the time specified under Force Transmit timeout.	Optional

ATTENTION

When Max connection is set to two or more, the NPort will use a "multiconnection application" (i.e., two or more hosts are allowed access to the port simultaneously). When using a multiconnection application, the NPort will use the serial communication parameters set in the console. All of the hosts connected to that port must use the same serial settings. If one host opens the COM port with parameters that differ from the NPort's console setting, data communication may not work properly.

NOTE

Optimal force transmit timeout differs according to your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. Here, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is:

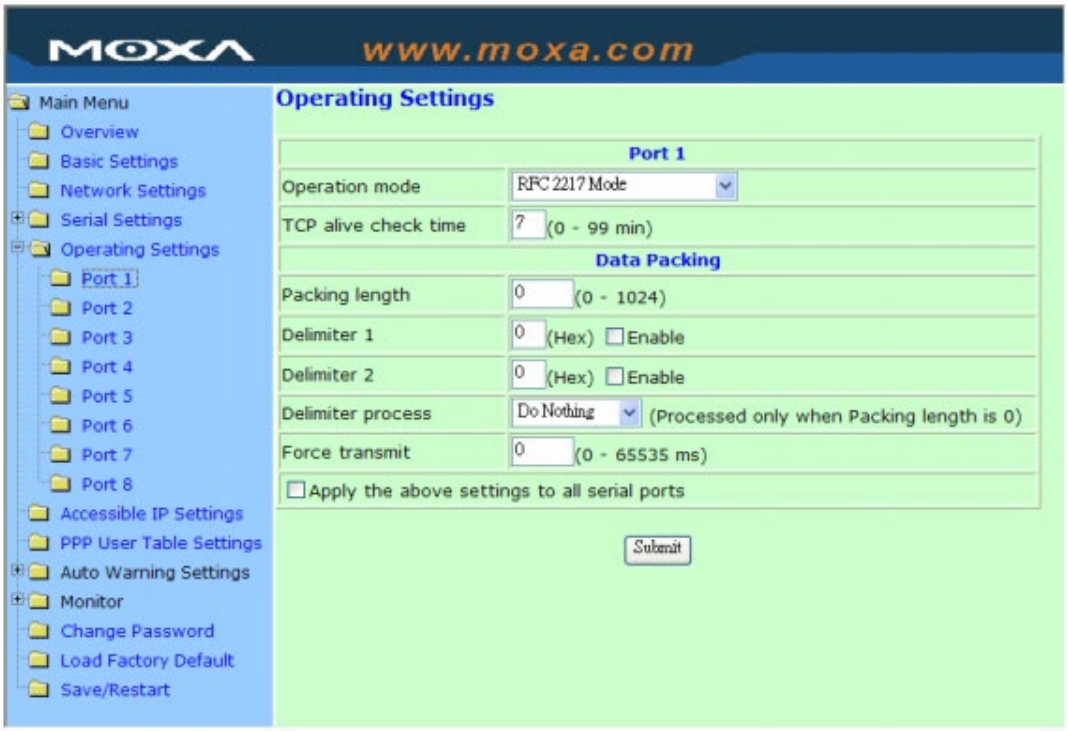
10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

Therefore, set Force Transmit timeout greater than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be greater than 10 ms.

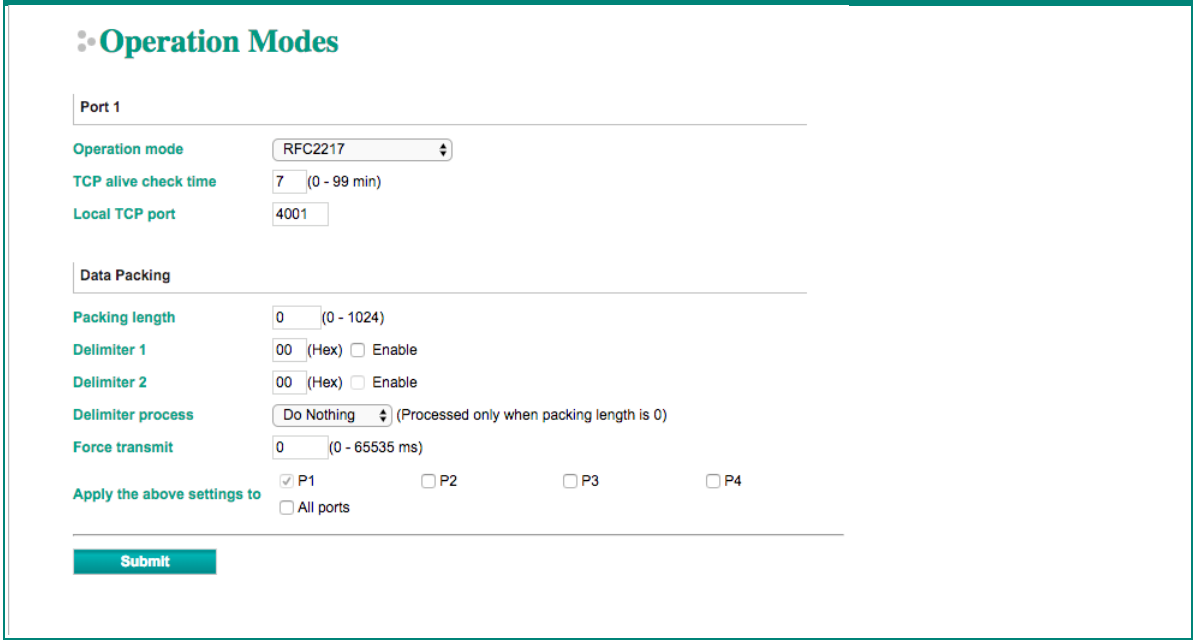
If you want to send the series of characters in a packet, the serial device attached to the NPort should send characters with time delay less than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbyte per port.

RFC2217 Mode

Web Interface for the NPort 5000A and NPort IA5000A Series Only



Web Interface for the Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort automatically closes the TCP connection if there is no TCP activity for the given time. After the connection is closed, the starts listening for another TCP connection.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Local TCP Port	1 to 65535	4001	The TCP port that the NPort uses to listen to connections, and that other devices must use to contact the NPort. To avoid conflicts with well-known TCP ports, the default is set to 4001.	Required
Packing length	0 to 1024	0	0: The Delimiter Process will be followed, regardless of the length of the data packet. Greater than 0: If the data length (in bytes) matches the configured value, the data will be forced out.	Optional
Delimiter 1	00 to FF	None	Once the NPort receives both delimiters through its serial port, it immediately packs all data currently in its buffer and sends it to the NPort's Ethernet port.	Optional
Delimiter 2	00 to FF	None		Optional
Delimiter process	Do nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter	Do nothing	**[Delimiter + 1] or [Delimiter + 2]:** The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter. **[Strip Delimiter]:** When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted. **[Do nothing]:** The data will be transmitted when the Delimiter is received.	Optional
Force Transmit	0 to 65535 ms	0 ms	**0:** Disable the force transmit timeout. **1 to 65535:** Forces the NPort's TCP/IP protocol software to pack serial data received during the specified time into the same data frame. This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the force transmit time interval reaches the time specified under Force Transmit timeout.	Optional

NOTE

Optimal force transmit timeout differs according to your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. Here, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is:

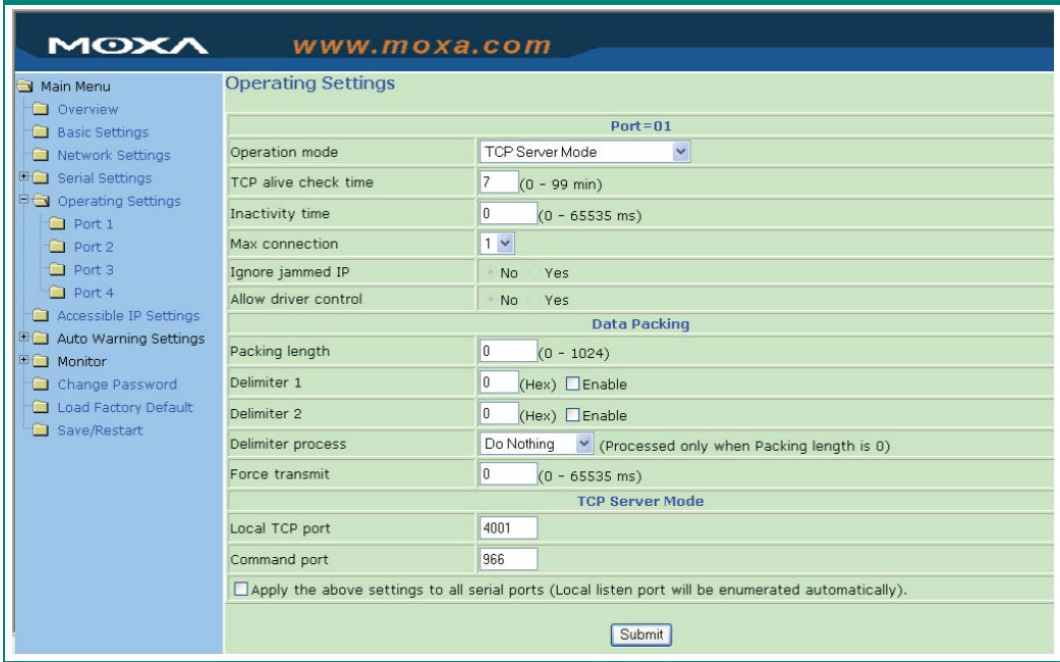
10 (bits) / 1200 (bits/s) * 1000 (ms/s) = 8.3 ms.

Therefore, set Force Transmit timeout to be larger than 8.3 ms. Force Transmit timeout is specified in milliseconds and must be larger than 10 ms.

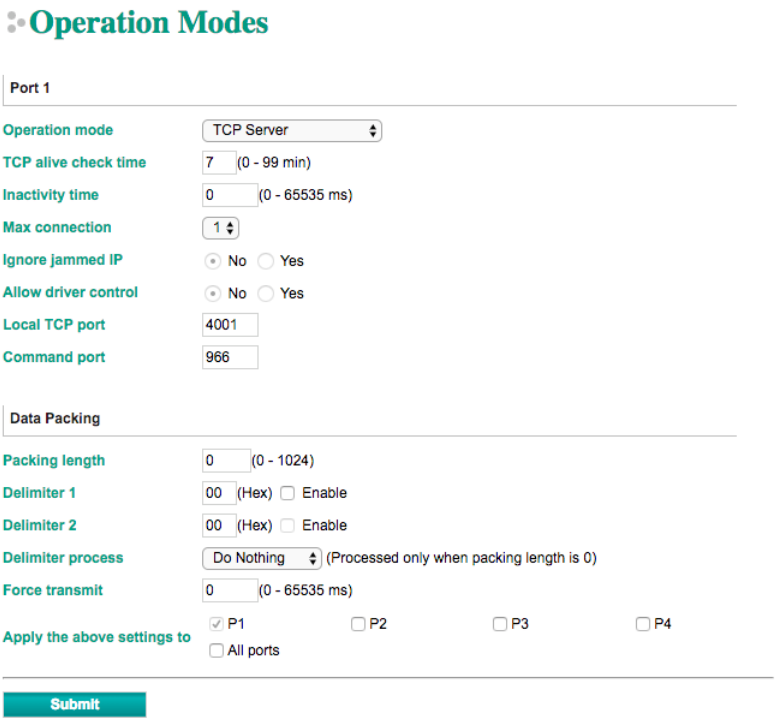
If you want to send the series of characters in a packet, the serial device attached to the NPort should send characters with time delay less than Force Transmit timeout between characters and the total length of data must be smaller than or equal to the NPort's internal buffer size. The serial communication buffer size of the NPort is 1 Kbyte per port.

TCP Server Mode

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort automatically closes the TCP connection if there is no TCP activity for the given time. After the connection is closed, the NPort starts listening for another Real COM driver connection.	Optional
Inactivity Time	0 to 65535 ms	0 ms	**0 ms:** TCP connection is not closed because of an idle serial line. **0-65535 ms:** The NPort automatically closes the TCP connection if there is no serial data activity for the given time. After the connection is closed, the NPort starts listening for another TCP connection. This parameter determines when the TCP connection is in Closed or Listen status. The connection is closed if there is no incoming or outgoing data through the serial port during the specific Inactivity time. If the inactivity time is set to 0, the current TCP connection is maintained until there is a connection close request. Although inactivity time is disabled, the NPort will check the connection status between the NPort and remote host by sending "keep alive" packets periodically. If the remote host does not respond to the packet, it assumes that the connection was closed down unintentionally. The NPort will then force the existing TCP connection to close.	Optional
Max Connection	1 to 8 for NPort 5100A/ 5200A/IA5250A/ IA5450A and NPort 5150AI-M12/ 5250AI-M12/ 5450AI-M12 Series (1 to 4 for other NPort 5000 Series)	1	**Max connection** is set to 2 to 8 when the user needs to receive data from different hosts simultaneously. The factory default only allows 1 connection at a same. When Max Connection is set to 1, the Real COM driver on the specific host has full control. **Max. Connection 1:** Allows only 1 host's Real COM driver to open the specific NPort serial port. **Max Connection 2 to 8:** Allows 2 to 8 host's Real COM drivers to open the specific NPort serial port simultaneously. When multiple hosts' Real COM drivers open the serial port at the same time, the COM driver only provides a pure data tunnel without controlling ability. This serial port parameter will use firmware settings, not the settings of your application program (AP). Application software that is based on the COM driver will receive a driver's response of "success" when the software uses any of the Win32 API functions. The firmware will only send the data back to the driver on the host. Data will be sent first-in-first-out when data comes into the NPort from the Ethernet interface.	Required

Parameter	Setting	Factory Default	Description	Necessity
Ignore jammed IP	No or Yes	No	No: When Max connections > 1, and the serial device is transmitting data, if any of the connected hosts are not responding, it will wait until the data has been transmitted successfully before transmitting the second group of data to all hosts. Yes: If you select Yes for "Ignore jammed IP," the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.	Optional
Allow Driver Control	No or Yes	No	If "max connection" is greater than 1, the NPort will ignore driver control commands from all connected hosts. However, if you set "Allow driver control" to Yes, control commands will be accepted. Note that since the NPort may get configuration changes from multiple hosts, the most recent command received will take precedence.	Optional
Packing length	0 to 1024	0	0: The Delimiter Process will be followed, regardless of the length of the data packet. Greater than 0: If the data length (in bytes) matches the configured value, the data will be forced out.	Optional
Delimiter 1	00 to FF	None	Once the NPort receives both delimiters through its serial port, it immediately packs all data currently in its buffer and sends it to the NPort's Ethernet port.	Optional
Delimiter 2	00 to FF	None		Optional
Delimiter process	Do nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter	Do nothing	**[Delimiter + 1] or [Delimiter + 2]:** The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter. **[Strip Delimiter]:** When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted. **[Do nothing]:** The data will be transmitted when the Delimiter is received.	Optional
Force Transmit	0 to 65535 ms	0 ms	**0:** Disable the force transmit timeout. **1 to 65535:** Forces the NPort's TCP/IP protocol software to pack serial data received during the specified time into the same data frame. This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the force transmit time interval reaches the time specified under Force Transmit timeout.	Optional
Local TCP port	1 to 65535	4001	The TCP port that the NPort uses to listen to connections, and that other devices must use to contact the NPort. To avoid conflicts with well-known TCP ports, the default is set to 4001.	Required
Command port	1 to 65535	966	The command port is a listen TCP port for IP-Serial Lib commands from the host. In order to prevent a TCP port conflict with other applications, the user can adjust the command port to another port if needed.	Optional

ATTENTION

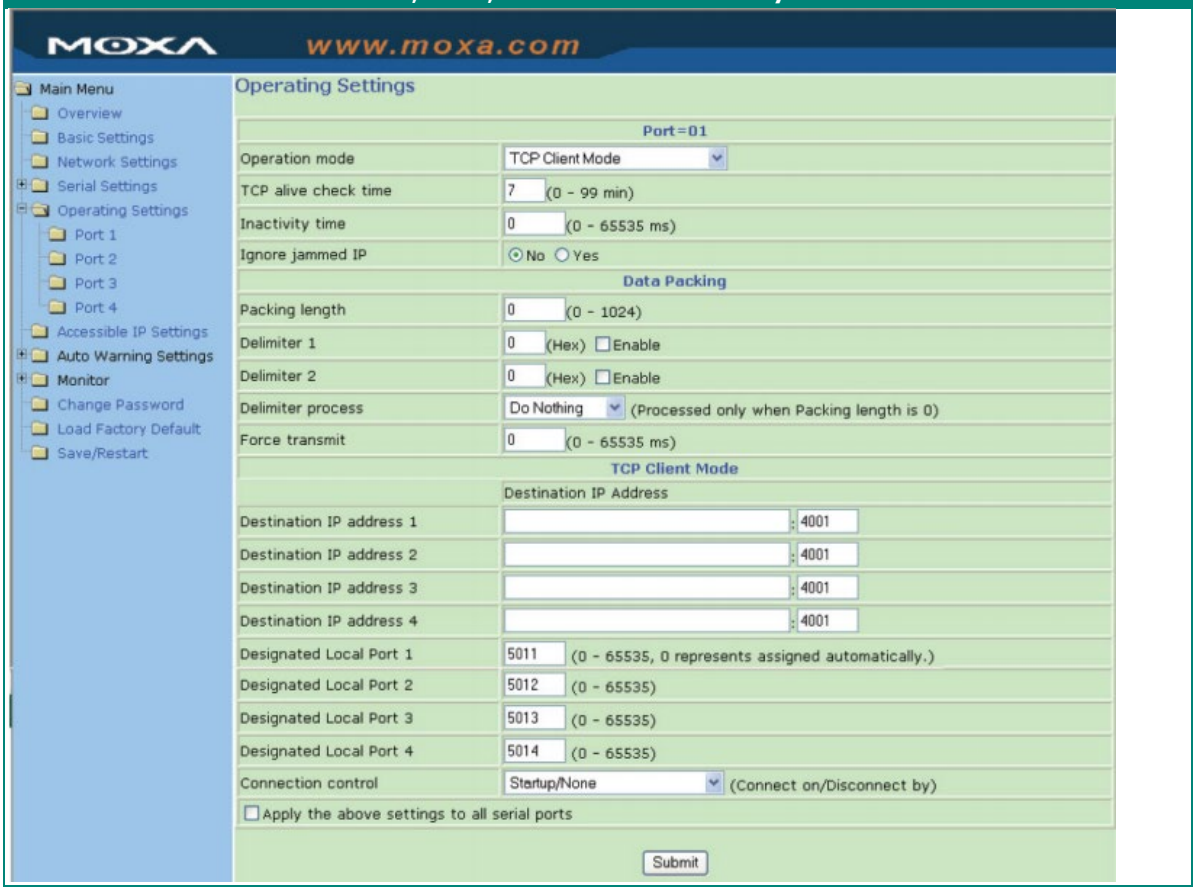
The Inactivity time should at least be set larger than that of Force transmit timeout. To prevent the unintended loss of data because of the session being disconnected, it is highly recommended that this value is set large enough, so that the intended data transfer is completed.

ATTENTION

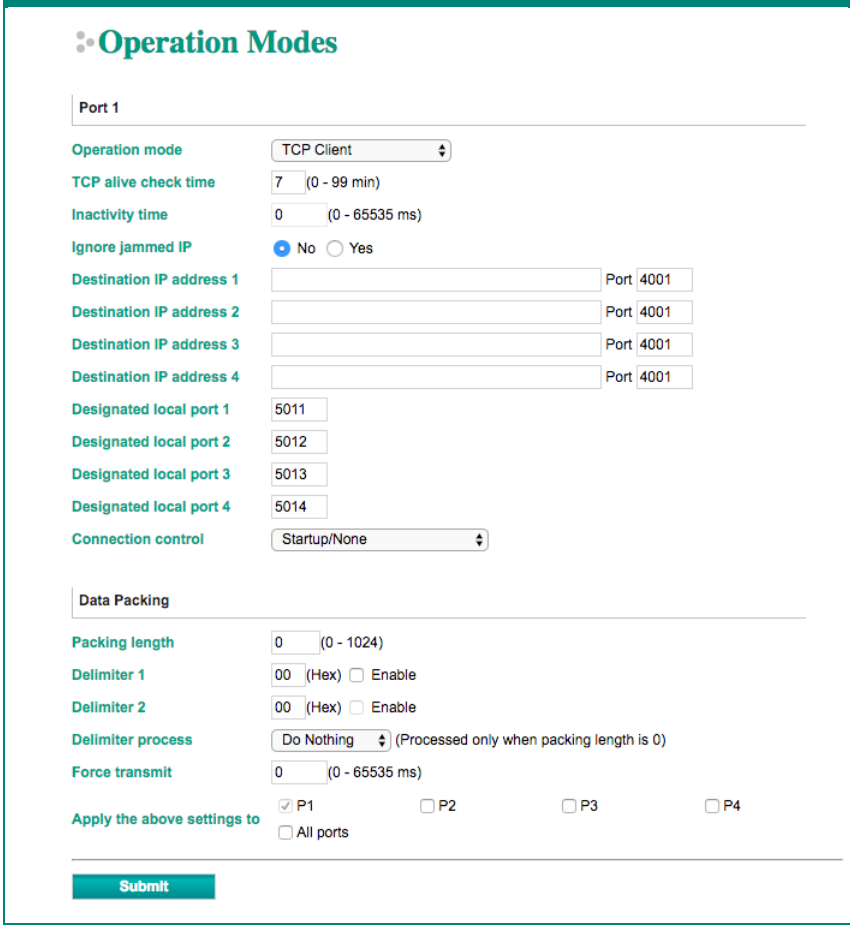
Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips the clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

TCP Client Mode

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort automatically closes TCP connection if there is no TCP activity for the given time. After the connection is closed, the NPort starts listening for another Real COM driver connection.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Inactivity Time	0 to 65535 ms	0 ms	0 ms: TCP connection is not closed because of an idle serial line. 0-65535 ms: The NPort automatically closes the TCP connection if there is no serial data activity for the given time. After the connection is closed, the NPort starts listening for another TCP connection. This parameter determines when the TCP connection is in Closed or Listen status. The connection is closed if there is no incoming or outgoing data through the serial port during the specific Inactivity time. If the inactivity time is set to 0, the current TCP connection is maintained until there is connection close request. Although inactivity time is disabled, the NPort will check the connection status between the NPort and remote host by sending "keep alive" packets periodically. If the remote host does not respond to the packet, it assumes that the connection was closed down unintentionally. The NPort will then force the existing TCP connection to close.	Optional
Ignore jammed IP	Yes or No	No	No: When Max connections > 1, and the serial device is transmitting data, if any of the connected hosts are not responding, it will wait until the data has been transmitted successfully before transmitting the second group of data to all hosts. Yes: If you select Yes for "Ignore jammed IP," the host that is not responding will be ignored, but the data will still be transmitted to the other hosts.	Optional
Allow Driver Control	Yes or No	No	If "max connection" is greater than 1, the NPort will ignore driver control commands from all connected hosts. However, if you set "Allow driver control" to Yes, control commands will be accepted. Note that since the NPort may get configuration changes from multiple hosts, the most recent command received will take precedence.	Optional
Packing length	0 to 1024	0	0: The Delimiter Process will be followed, regardless of the length of the data packet. Greater than 0: If the data length (in bytes) matches the configured value, the data will be forced out.	Optional
Delimiter 1	00 to FF	None	Once the NPort receives both delimiters through its serial port, it immediately packs all data currently in its buffer and sends it to the NPort's Ethernet port.	Optional
Delimiter 2	00 to FF	None		Optional
Delimiter process	Do nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter	Do nothing	**[Delimiter + 1] or [Delimiter + 2]:** The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter. **[Strip Delimiter]:** When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted. **[Do nothing]:** The data will be transmitted when the Delimiter is received.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Force Transmit	0 to 65535 ms	0 ms	**0:** Disable the force transmit timeout. **1 to 65535:** Forces the NPort's TCP/IP protocol software to pack serial data received during the specified time into the same data frame. This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the force transmit time interval reaches the time specified under Force Transmit timeout.	Optional
Destination IP address 1 *Destination IP address 2/3/4*	IP address or Domain Name (E.g., 192.168.1.1)	None	Allows the NPort to connect actively to the remote host (up to 4 hosts) whose IP address is set by this parameter. The "Destination IP address" parameter can use either IP address or Domain Name. For some applications, the user may need to send the data actively to the remote destination domain name.	Required
Designated Local Port 1/2/3/4	TCP Port No.	5011 (Port 1) 5012 (Port 2) 5013 (Port 3) 5014 (Port 4)	N/A	Required
Connection control	Startup/None, Any Character/ None, Any Character/ Inactivity Time, DSR ON/ DSR OFF, DSR ON/None, DCD ON/ DCD OFF, DCD ON/None	Startup/None	The meaning of each of the above settings is given in the table below. Both the Connect condition and Disconnect condition are given.	Required

Connect/Disconnect	Description
Startup/None (default)	A TCP connection will be established on startup and will remain active indefinitely.
Any Character/None	A TCP connection will be established when any character is received from the serial interface and will remain active indefinitely.
Any Character/ Inactivity Time	A TCP connection will be established when any character is received from the serial interface and will be disconnected when the Inactivity timeout is reached.
DSR On/DSR Off	A TCP connection will be established when a DSR "On" signal is received and will be disconnected when a DSR "Off" signal is received.
DSR On/None	A TCP connection will be established when a DSR "On" signal is received and will remain active indefinitely.
DCD On/DCD Off	A TCP connection will be established when a DCD "On" signal is received and will be disconnected when a DCD "Off" signal is received.
DCD On/None	A TCP connection will be established when a DCD "On" signal is received and will remain active indefinitely.

ATTENTION

The Inactivity time should at least be set larger than that of Force transmit timeout. To prevent the unintended loss of data because of the session being disconnected, it is highly recommended that this value is set large enough, so that the intended data transfer is completed.

Inactivity time is ONLY active when "TCP connect on" is set to "Any character."

NOTE

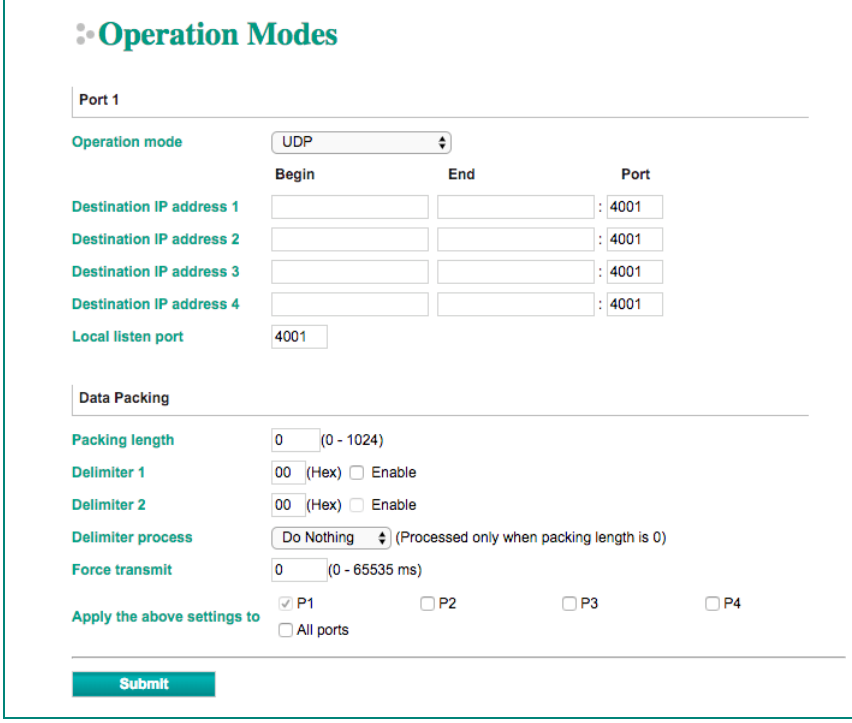
Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips the clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

ATTENTION

Up to four connections can be established between the NPort and hosts. The connection speed or throughput may be low if one of the four connections is slow since the slow connection will slow down the other three connections.

UDP Mode

Web Interface for the Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
Packing length	0 to 1024	0	0: The Delimiter Process will be followed, regardless of the length of the data packet. Greater than 0: If the data length (in bytes) matches the configured value, the data will be forced out.	Optional
Delimiter 1	00 to FF	None	Once the NPort receives both delimiters through its serial port, it immediately packs all data currently in its buffer and sends it to the NPort's Ethernet port.	Optional
Delimiter 2	00 to FF	None		Optional

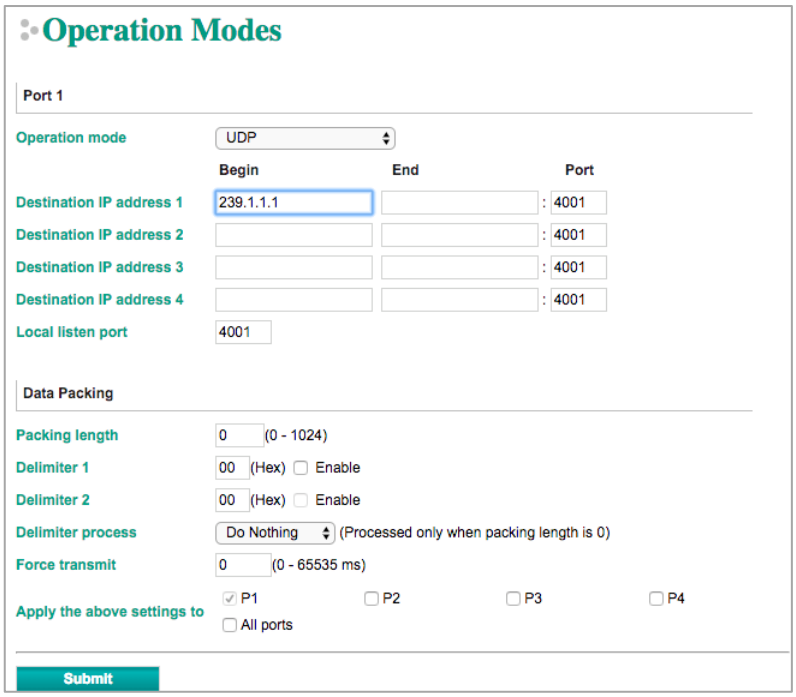
Parameter	Setting	Factory Default	Description	Necessity
Delimiter process	Do nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter	Do nothing	**[Delimiter + 1] or [Delimiter + 2]:** The data will be transmitted when an additional byte (for Delimiter +1), or an additional 2 bytes (for Delimiter +2) of data is received after receiving the Delimiter. **[Strip Delimiter]:** When the Delimiter is received, the Delimiter is deleted (i.e., stripped), and the remaining data is transmitted. **[Do nothing]:** The data will be transmitted when the Delimiter is received.	Optional
Force Transmit	0 to 65535 ms	0 ms	**0:** Disable the force transmit timeout. **1 to 65535:** Forces the NPort's TCP/IP protocol software to pack serial data received during the specified time into the same data frame. This parameter defines the time interval during which the NPort fetches the serial data from its internal buffer. If data is incoming through the serial port, the NPort stores the data in the internal buffer. The NPort transmits data stored in the buffer via TCP/IP, but only if the internal buffer is full or if the force transmit time interval reaches the time specified under Force Transmit timeout.	Optional
Destination IP address 1	IP address range E.g., Begin: 192.168.1.1 End: 192.168.1.10	Begin: Empty End: Empty Port: 4001	N/A	Required
Destination IP address 2/3/4			N/A	Optional
Local listen port	1 to 65535	4001	The UDP port that the NPort listens to, and that other devices must use to contact the NPort. To avoid conflicts with well-known UDP ports, the default is set to 4001.	Required

NOTE

Delimiter 2 is optional. If left blank, then Delimiter 1 alone trips the clearing of the buffer. If the size of the serial data received is greater than 1 KB, the NPort will automatically pack the data and send it to the Ethernet. However, to use the delimiter function, you must at least enable Delimiter 1. If Delimiter 1 is left blank and Delimiter 2 is enabled, the delimiter function will not work properly.

UDP Multicast

A multicast is a packet sent by one host to multiple hosts. In multicast mode, each host that belongs to a specific multicast group will receive multicast packets for that group. For a host to be configured as a multicast receiver over the Internet, the must inform the routers on its LAN. The Internet Group Management Protocol (IGMP) is used to communicate group membership information between hosts and routers on a LAN. The NPort 5000 Series supports IGMP version 2. The NPort 5100, NPort 5200, IA5000 Series do not support IGMP function.



Type the IP address (e.g., 239.1.1.1) assigned to the multicast group in the **Begin** column. The NPort will automatically add the Group, and receive all packets from this group as required by the multicast function.

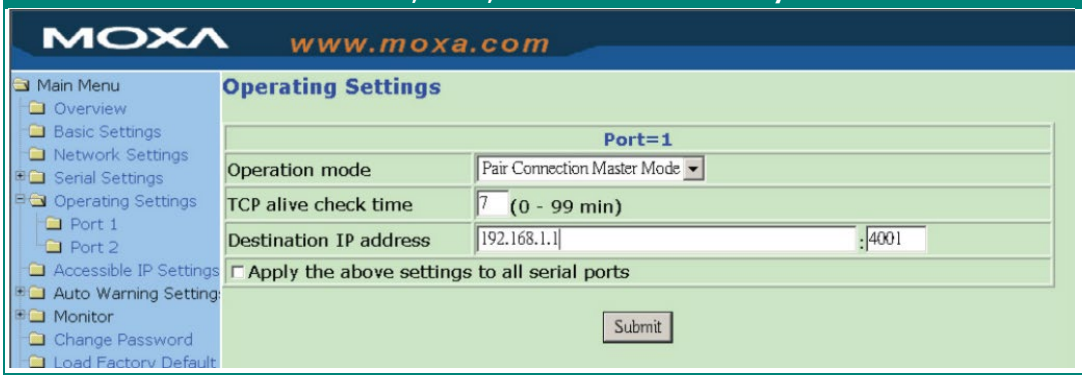
Pair Connection Mode

Pair Connection Mode employs two NPort device servers in tandem, and can be used to remove the 15-meter distance limitation imposed by the RS-232 interface. One NPort is connected from its RS-232 port to the COM port of a PC or other type of computer, such as a hand-held PDA, and the serial device is connected to the RS-232 port of the other NPort. The two NPort device servers are then connected to each other with a crossover Ethernet cable, both are connected to the same LAN, or in a more advanced setup, they communicate with each other over a WAN (i.e., through one or more routers). Pair Connection Mode transparently transfers both data and modem control signals (although it cannot transmit the DCD signal) between the two NPort device servers.

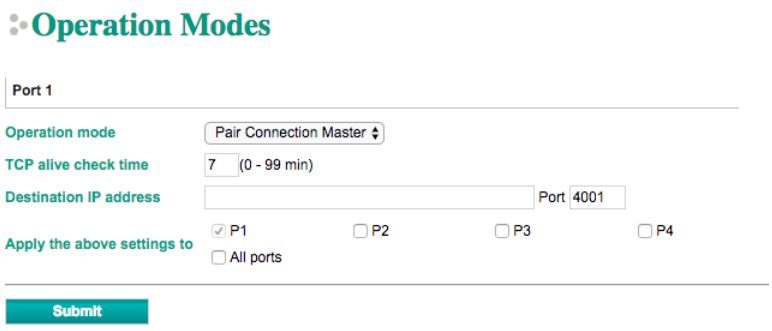
Pair Connection Master Mode

When using Pair Connection Mode, you must select **Pair Connection Master Mode** for the Operation Mode of one of the NPort device servers. In effect, this NPort will act as a TCP client.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series



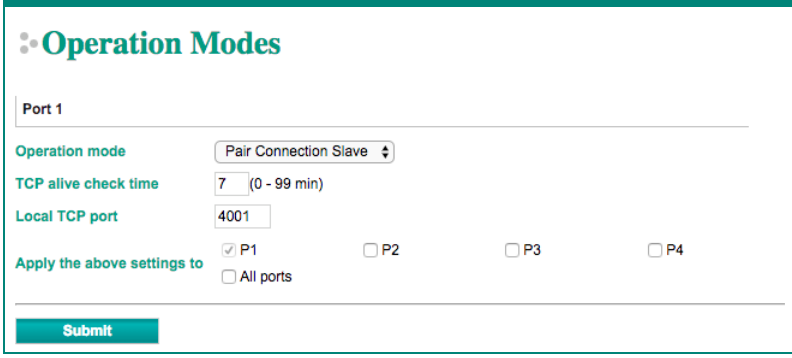
Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort closes the TCP connection automatically if there is no TCP activity for the given time.	Required
Destination IP address	IP address or Domain Name (E.g., 192.168.1.1)	blank	The Pair Connection "Master" will contact the network host that has this IP address. Data will be transmitted through the port No. (4001 by default). Note that you must configure the same TCP port No. for the device server acting as the Pair Connection "Slave."	Optional
	TCP Port	4001		Required

Pair Connection Slave Mode

When using Pair Connection Mode, you must select **Pair Connection Slave Mode** for the Operation Mode of one of the NPort device servers. In effect, this NPort will act as a TCP server.

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

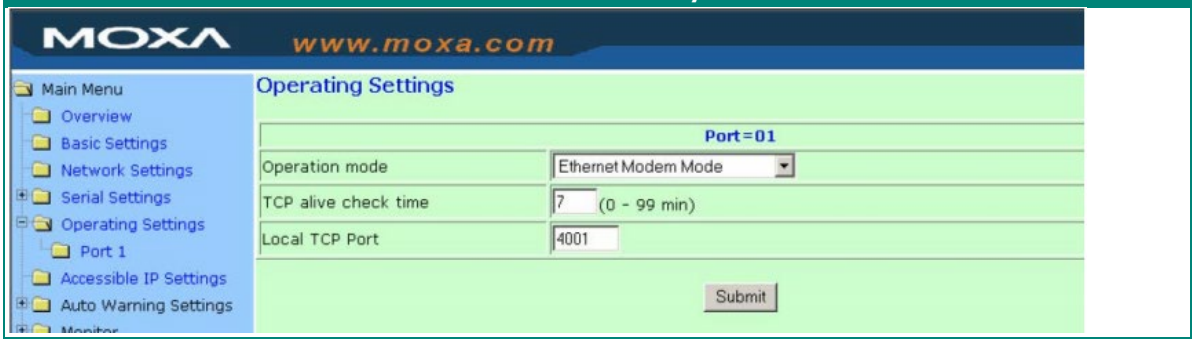
Web Interface for the Overall NPort 5000 Series



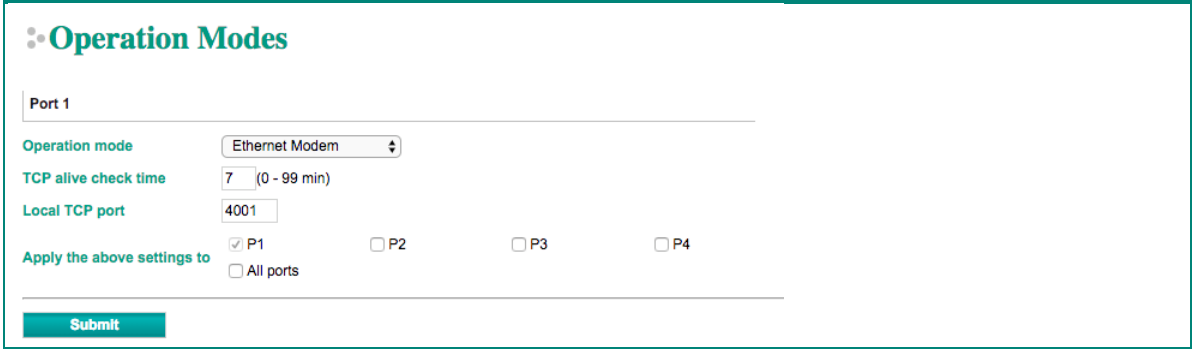
Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort closes the TCP connection automatically if there is no TCP activity for the given time.	Required
Local TCP port	TCP port No. (e.g., 4001)	4001	This Port No. must be the same port No. that you set up for the Pair Connection "Master" device server.	Required

Ethernet Modem Mode (for the NPort IA5000/IA5000A, NPort 5000A, NPort 5000AI-M12, NPort 5100 Series only)

Web Interface for the NPort 5100 and IA5000 Series Only



Web Interface for the NPort IA5000A, 5000A, and 5000AI-M12 Series Only



Dial-in

The NPort listens for a TCP/IP connection request from the remote Ethernet modem or host. The NPort's response depends on the ATS0 value, as outlined below.

ATS0=0 (default):

The NPort will temporarily accept the TCP connection and then send the **RING** signal out through the serial port. The serial controller must reply with "ATA" within 2.5 seconds to accept the connection request, after which the NPort enters data mode. If no "ATA" command is received, the NPort will disconnect after sending three "RING" signals.

ATS0≥0:

The NPort will accept the TCP connection immediately and then send the **CONNECT <baud>** command to the serial port, in which <baud> represents the baudrate of the NPort's serial port. After that, the NPort immediately enters data mode.

Dial-out

The NPort accepts the AT command **ATD <IP>:<TCP port>** from the serial port and then requests a TCP connection from the remote Ethernet Modem or PC. This is where <IP> is the IP address of the remote Ethernet modem or PC, and <TCP port> is the TCP port number of the remote Ethernet modem or PC. Once the remote unit accepts this TCP connection, the NPort will send out the **CONNECT <baud>** signal via the serial port and then enter data mode.

Disconnection Request from the Local Site

When the NPort is in data mode, the user can drive the DTR signal to OFF, or send **+++** from the local serial port to the NPort. The NPort will enter command mode and return **NO CARRIER** via the serial port, and then input **ATH** to shut down the TCP connection after 1 second.

NOTE

The "+++" command cannot be divided. The "+" character can be changed in register S2, and the guard time, which prefixes and suffixes the "+++" in order to protect the raw data, can be changed in register S12.

Disconnection Request from the Remote Site

After the TCP connection has been shut down by the remote Ethernet modem or PC, the NPort will send the **NO CARRIER** signal via the serial port and then return to command mode.

AT Commands

The NPort supports the following common AT commands used with a typical modem:

No.	AT command	Description	Remarks
1	ATA	Answer manually	
2	ATD <IP>:<Port>	Dial up the IP address: Port No.	
3	ATE	ATE0=Echo OFF ATE1=Echo ON (default)	
4	ATH	ATH0=On-hook (default) ATH1=Off-hook	
5	ATI, ATI0, ATI1, ATI2	Modem version	reply "OK" only
6	ATL	Speaker volume option	reply "OK" only
7	ATM	Speaker control option	reply "OK" only
8	ATO	Online command	
9	ATP, ATT	Set Pulse/Tone Dialing mode	reply "OK" only
10	ATQ0, ATQ1	Quiet command (default=ATQ0)	
11	ATSr=n	Change the contents of S register	See "S registers"
12	ATSr?	Read the contents of S register	See "S registers"
13	ATV	Result code type ATV0 for digit code ATV1 for text code 0=OK 1=connect (default) 2=ring 3=No carrier 4=error	
14	ATZ	Reset (disconnect, enter command mode and restore the flash settings)	
15	AT&C	Serial port DCD control AT&C0=DCD always on AT&C1=DTE detects connection by DCD on/off (default)	
16	AT&D	Serial port DTR control AT&D0=recognize DTE always ready AT&D1, AT&D2=reply DTE when DTR On (default)	
17	AT&F	Restore manufacturer's settings	
18	AT&G	Select guard time	reply "OK" only
19	AT&R	Serial port RTS option command	reply "OK" only
20	AT&S	Serial port DSR control	reply "OK" only
21	AT&V	View settings	
22	AT&W	Write current settings to flash for next boot up	

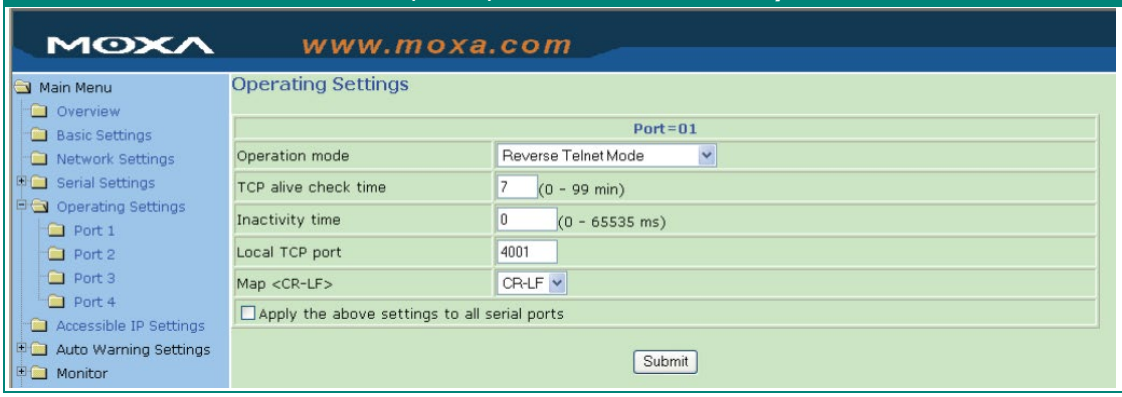
S Registers

No.	S Register	Description & default value	Remarks
1	S0	Ring to auto-answer (default=0)	
2	S1	Ring counter (always=0)	no action applied
3	S2	Escape code character (default=43 ASCII "+")	
4	S3	Return character (default=13 ASCII)	
5	S4	Line feed character (default=10 ASCII)	
6	S5	Backspace character (default= 8 ASCII)	
7	S6	Wait time for dial tone (always=2, unit=sec)	no action applied
8	S7	Wait time for carrier (default=3, unit=sec)	
9	S8	Pause time for dial delay (always=2, unit=sec)	no action applied
10	S9	Carrier detect response time (always=6, unit 1/10 sec)	no action applied
11	S10	Delay for hang up after carrier (always=14, unit 1/10 sec)	no action applied
12	S11	DTMF duration and spacing (always=100 ms)	no action applied
13	S12	Escape code guard time (default=50, unit 1/50 sec) to control the idle time for "+++"	

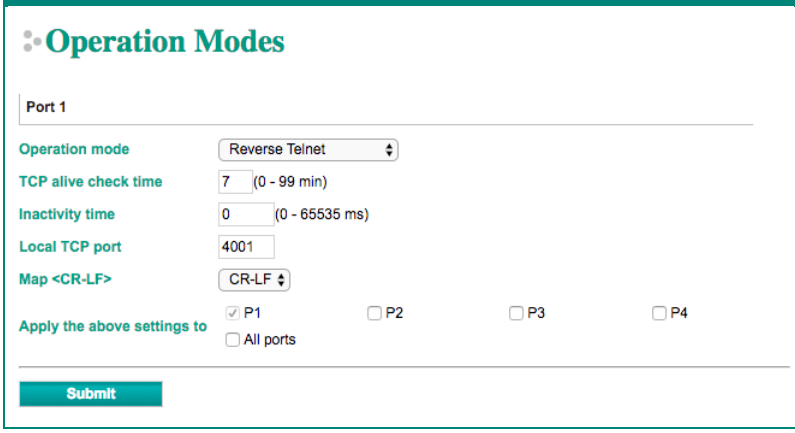
Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	7 min.	**0 min.:** TCP connection is not closed because of an idle TCP connection. **1 to 99 min.:** The NPort closes the TCP connection automatically if there is no TCP activity for the given time.	Required
Local TCP port	1 to 65535	4001	The TCP port that other devices must use to contact this device. To avoid conflicts with standard TCP ports, the default is set to 4001.	Required

Reverse Telnet Mode

Web Interface for the NPort 5100, 5200, and IA5000 Series Only

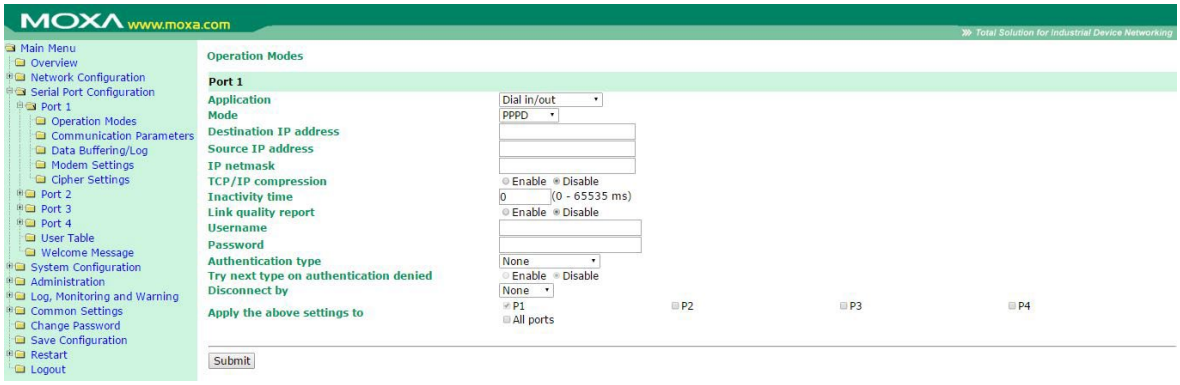


Web Interface for the Overall NPort 5000 Series



Parameter	Setting	Factory Default	Description	Necessity
TCP Alive Check Time	0 to 99 min.	0 min.	Specifies the time slice for checking if the TCP connection is alive. If no response is received, the NPort will disconnect the original connection.	Optional
Inactivity time	0 to 65535 ms	0	Idle time setting for auto-disconnection. 0 min. means it will never disconnect.	Optional
Local TCP port	1 to 65535	4001	Each of the NPort's serial ports is mapped to a TCP port. To avoid conflicts with TCP ports, set port numbers to 4001 for port1, 4002 for port 2, etc. (like the default values).	Optional
Map <CR-LF>	CR, LF, or CR-LF	CR-LF	If data received through the NPort's Ethernet port is sent using the "enter" command, the data will be transmitted out the serial port with an added: 1. "carriage return + line feed" if you select the <CR-LF> option (i.e., the cursor will jump to the next line, and return to the first character of the line) 2. "carriage return" if you select the <CR> option (i.e., the cursor will return to the first character of the line) 3. "line feed" if you select the <LF> option. (i.e., the cursor will jump to the next line, but not move horizontally)	Optional

PPPD Mode



PPPD (PPP on demand) is used for dial-in services since it provides PPP services only when receiving a request from a remote PC.

Destination IP address: This is the IP address of the remote dial-in/ dial-out server.

Source IP address: The Source IP address is IP address assigned to this serial port.

IP netmask: The IP netmask defines the netmask, also known as the subnet mask, for the PPP connection

TCP/IP compression (default=Disable): The setting of this field depends on whether the remote user's application requests compression.

Inactivity time (default=0 ms): This field specifies the idle time setting for auto-disconnection. A setting of 0 ms will cause the port to remain connected even if idle.

Link quality report (default=Disable): Setting this field to **Enable** allows the NPort 5000 to disconnect a connection if the link noise exceeds a certain threshold.

Username: This is the dial-out user ID account.

Password: This is the dial-out user password.

Authentication type (default=None): This field allows you to configure the method used, if any, to verify a user's ID and authorization.

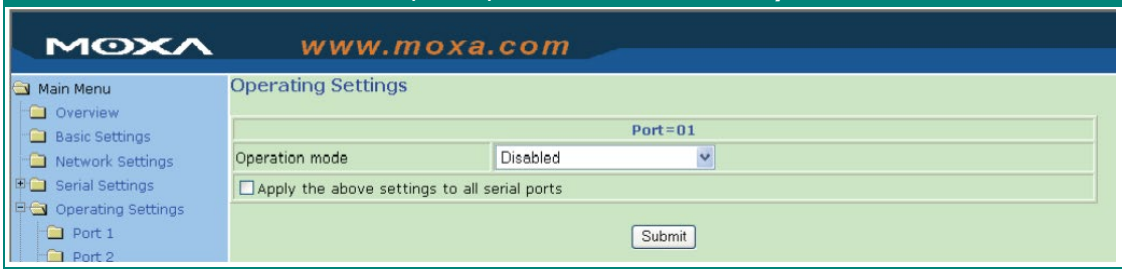
Option	Description
Local	Verify the ID against the NPort 5000 User Table.
RADIUS	Verify the ID against the external RADIUS server.
RADIUS-Local	Radius authentication is tried first, switching to Local if unsuccessful.
Local-RADIUS	Authentication is performed locally first, switching to Radius if unsuccessful
TACACS+	Verify the ID against the external TACACS+ server.
TACACS+-Local	TACACS+ authentication is tried first, switching to Local if unsuccessful.
Local-TACACS+	Authentication is performed locally first, switching to Radius if unsuccessful
None	Authentication is not required.

Try next type of authentication denied (default=Disable): The field enables or disables the system to try next type on first authentication denied.

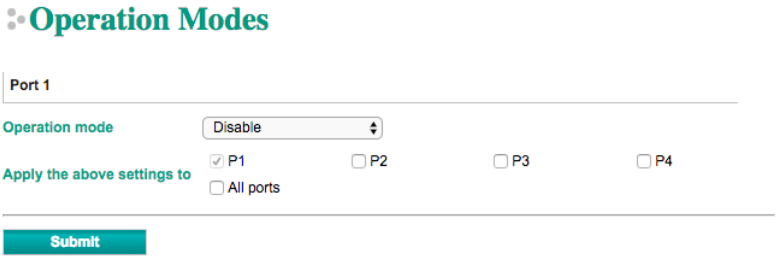
Disconnect by (default=None): If this field is set as **DCD-off**, the connection will be disconnected when the DCD signal is off. If this field is set as **DSR-off**, the connection will be disconnected when the DSR signal is off.

Disabled Mode

Web Interface for the NPort 5100, 5200, and IA5000 Series Only



Web Interface for the Overall NPort 5000 Series



When Operation mode is set to Disabled, that port will be disabled. Select the **Apply the above settings to all serial ports** checkbox to apply this setting to the other ports.

6. Installing Windows Driver

NPort **Real COM** driver can be installed by installing NPort Administrator Suite or NPort Windows Driver Manager is intended for use with NPort 5000 serial ports that are set to **Real COM** mode. The software manages the installation of drivers that allow you to map unused COM ports on your PC to serial ports on the NPort 5000. When the drivers are installed and configured, devices that are attached to serial ports on the NPort 5000 will be treated as if they were attached to your PC's own COM ports.

For how to configure NPort by NPort Administrator Suite or how to use Windows Driver Manager for COM mapping, refer to **Chapter 7. Windows Utilities for NPort**.

7. Windows Utilities for NPort 5000 Models

Device Search Utility (DSU)

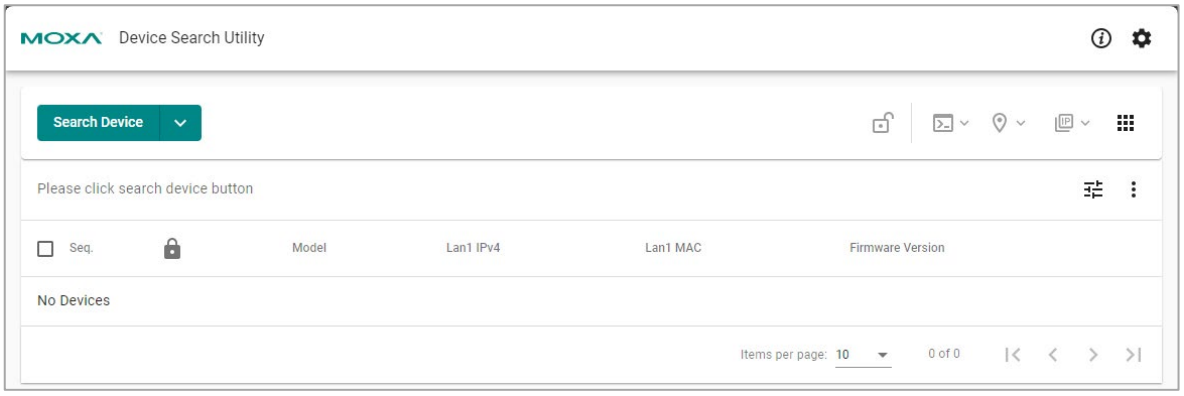
Installing Device Search Utility

Double-click the **Device Search Utility** installer, which you download from the Moxa website and follow the installation steps to complete the setup.

Configuring by Device Search Utility v3.x

Find the Device

The default IP address of each NPort 6000-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

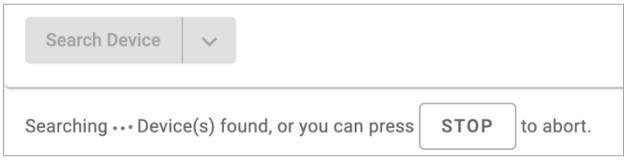
NOTE

For detailed instruction of how to use **DSU**, 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.

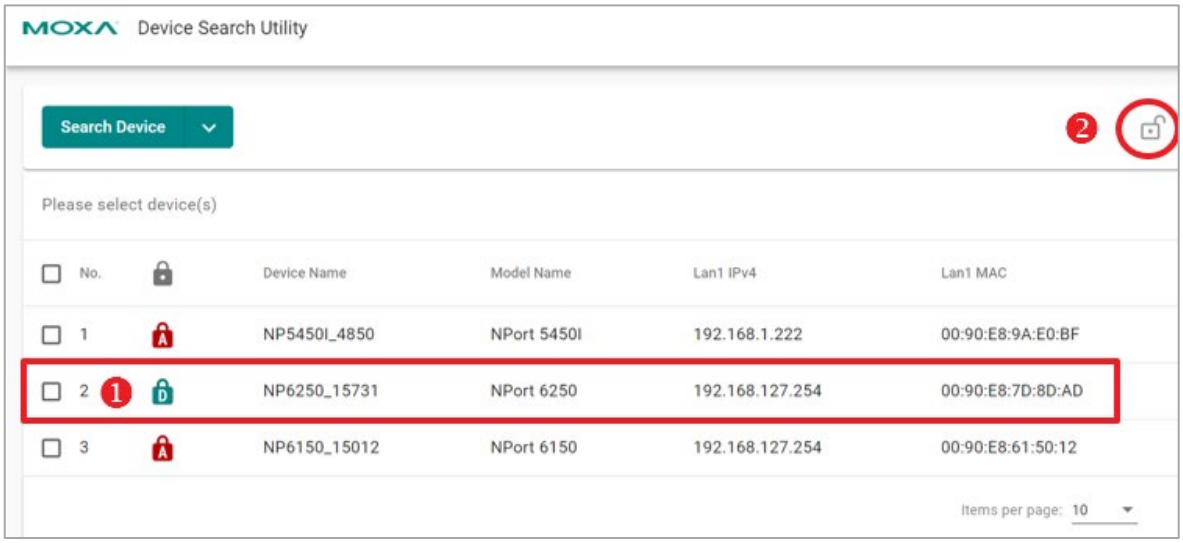


It's possible to stop the search at any stage of the process. A **STOP** button appears on top of the table; click it to halt the search and keep the already searched devices on the list.

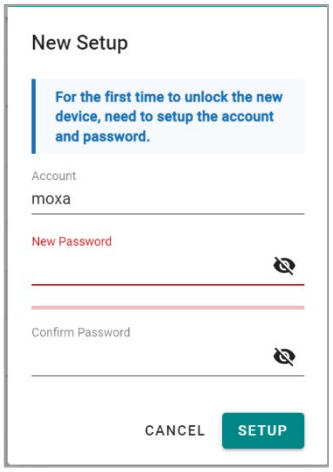
The default search time is 10 seconds. DSU will continue searching until time runs out. If your device(s) does not appear, you may change the search timeout limit in **Preferences > Device Search > Timeout limit for device searching**, to give the network a bit more time to respond.

First-time login with Device Search Utility

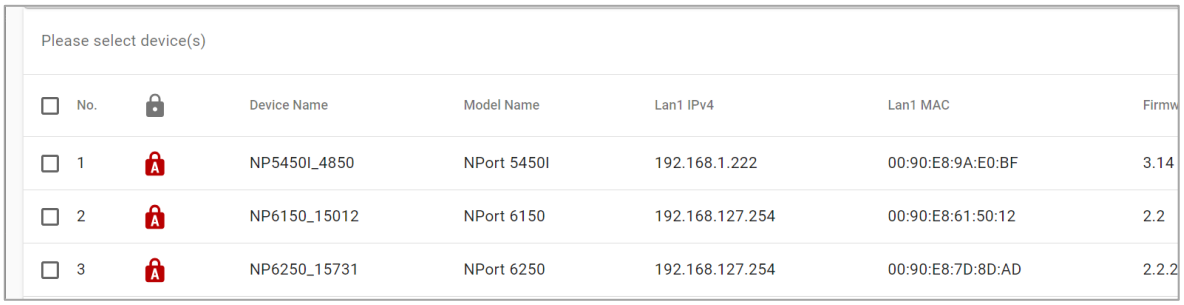
To address cybersecurity concerns, the NPort device server found through DSU will prompt for an account name and password during the first login.



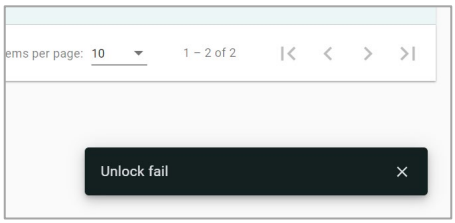
Select the target device and click the unlock button . The login window will remind you to set up the account name and password, and it will show the password minimum requirements as tips below the password field.



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:



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.



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
D	Default	The device has not completed the first-time login process, which requires setting the first account name and password.
B	Basic	The device only has password protection; the login requires inputting the password only.
A	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

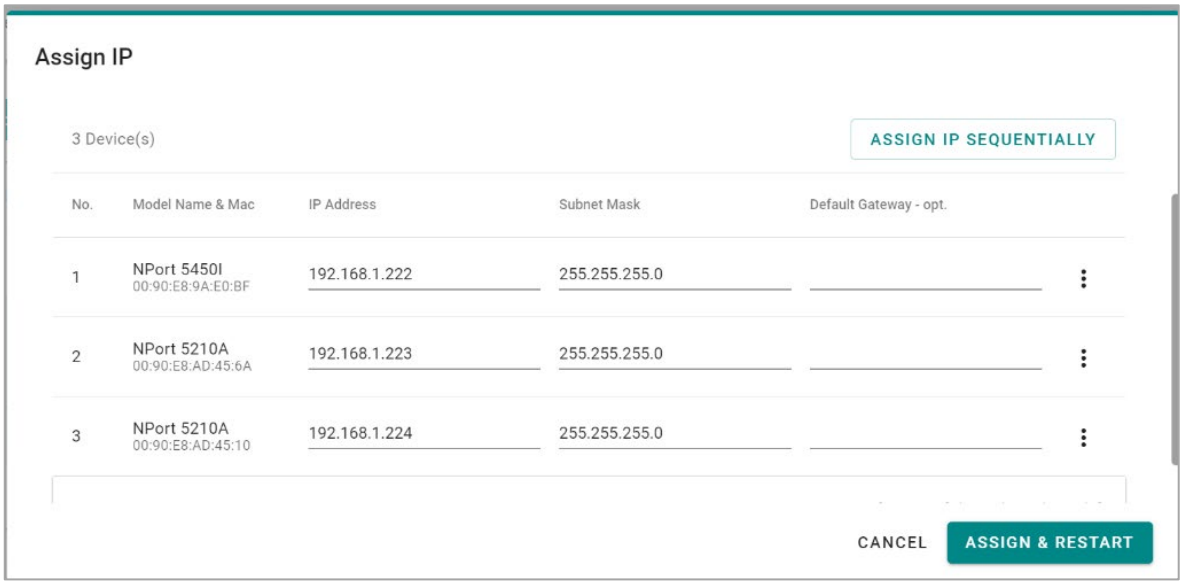
If your device does not support certain options, they will be disabled.

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 on the list.



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

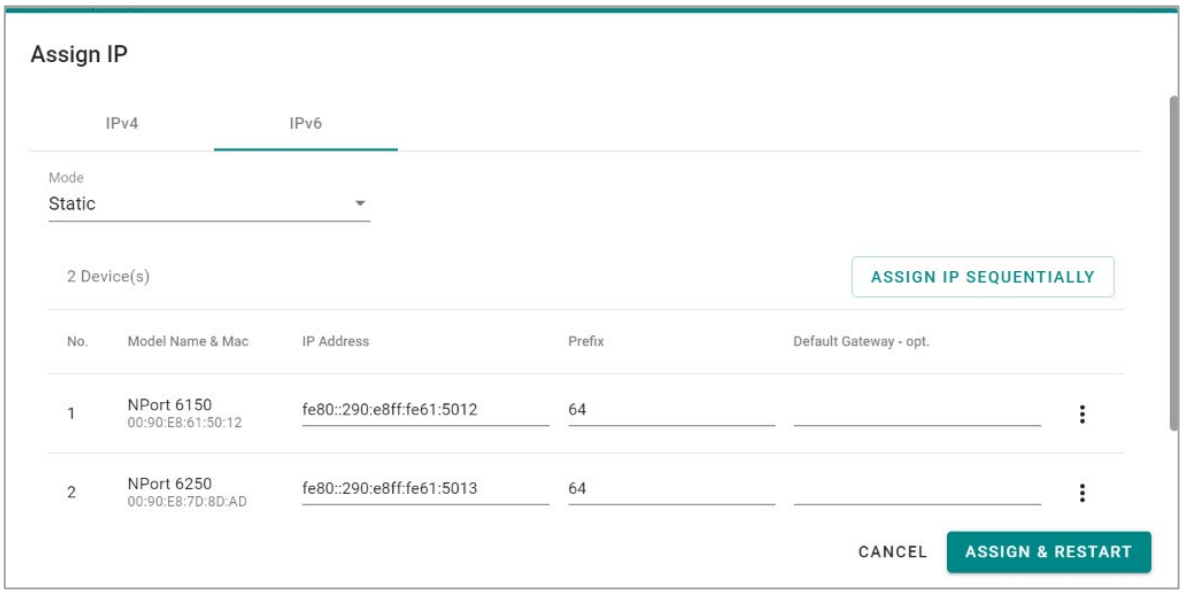
This is a quick way to copy and paste Netmask or gateway values to all the selected devices. Edit **Subnet Mask** and **Default Gateway – Opt** of any device first, and find the options in the menu icon at the end of the list and apply:

Assign IPv6

Mode: Static or DHCP

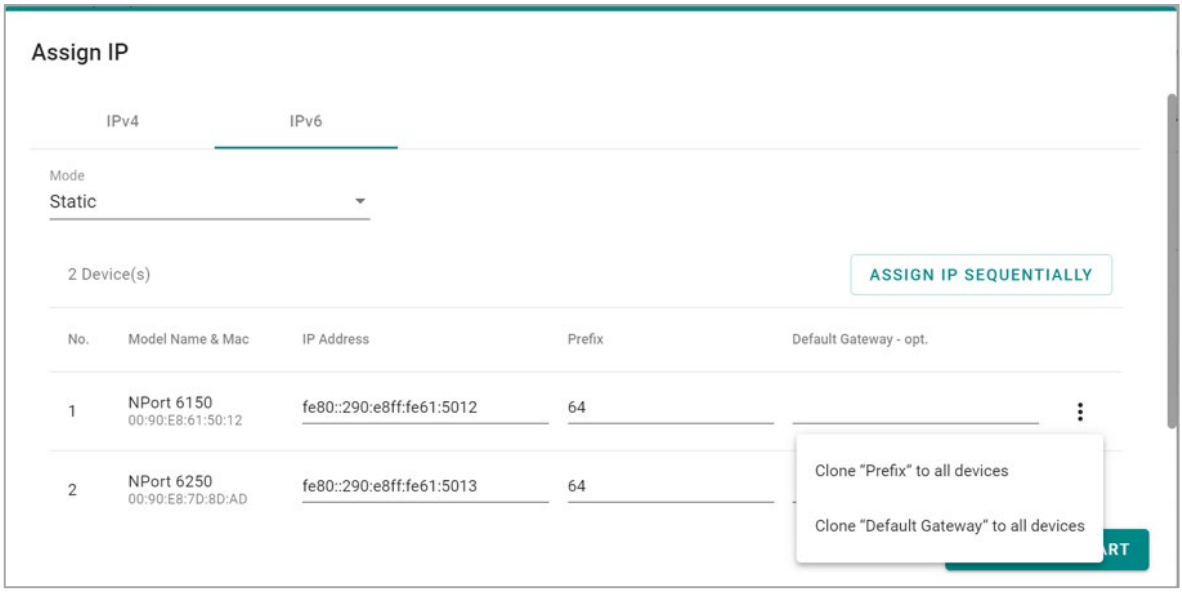
Click on the field of **IP Address, Prefix, Default Gateway – opt**, to manually key in the values.

If you have selected multiple devices and 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 .



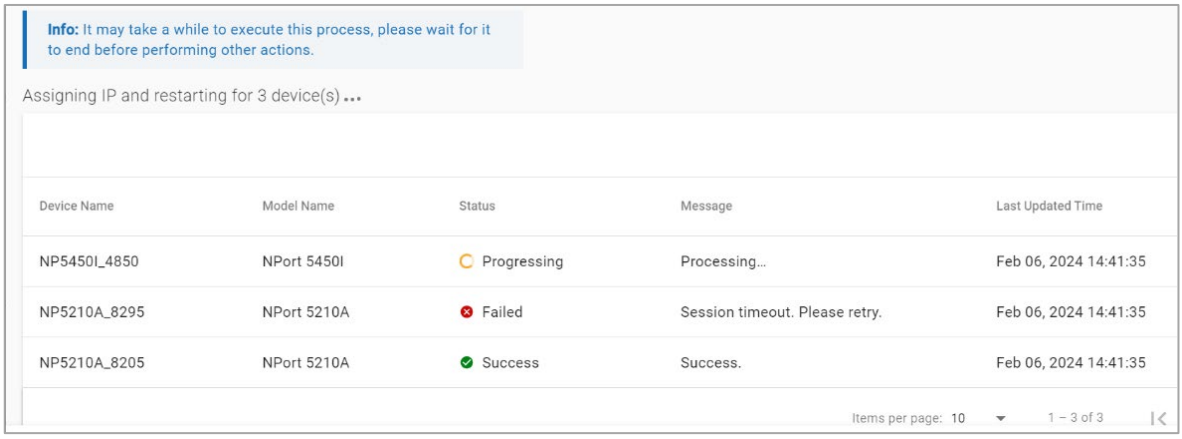
Clone "Network Mask"/"Default Gateway" to all devices

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

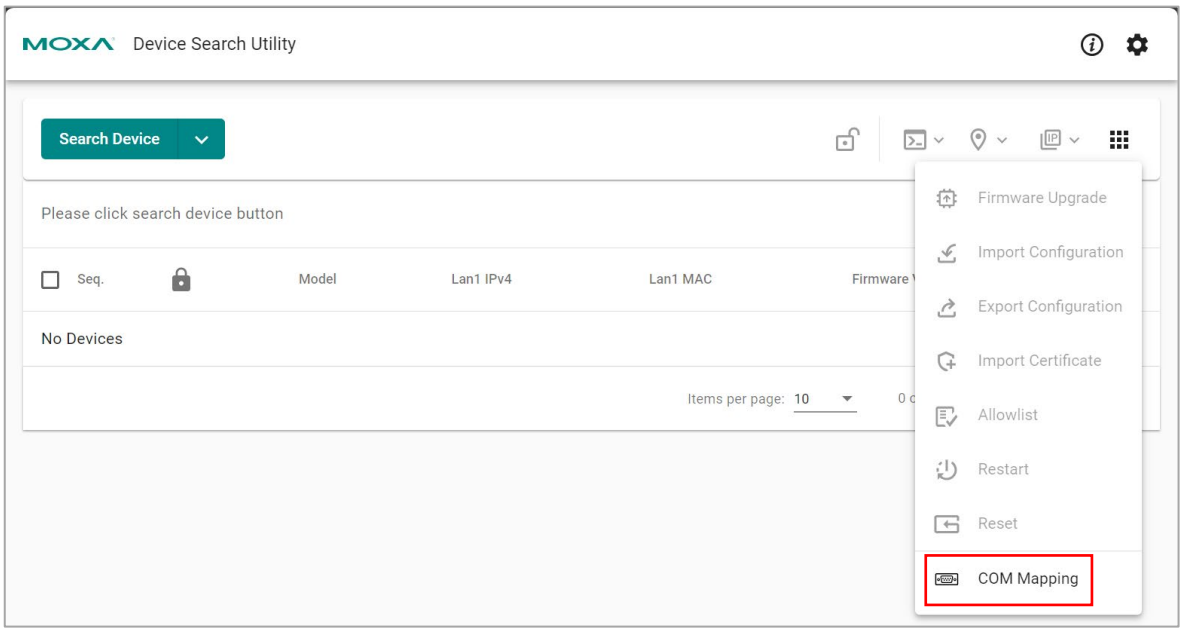


Apply the changes

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.



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. Refer to the Configuring by NPort Windows Driver Manager section under Chapter 7, "Windows Utilities for NPort 5000 Models," for more information.

Console

When you want to configure more detail settings, click the **Console** button to connect to the HTTPS console of the NPort 6000-G2 Series.

For how to use web console for configuration, refer to Configuration by Web Console section under the Chapter 2. Getting Started.

Locate

Unlock the device before you can use the **Locate** function.

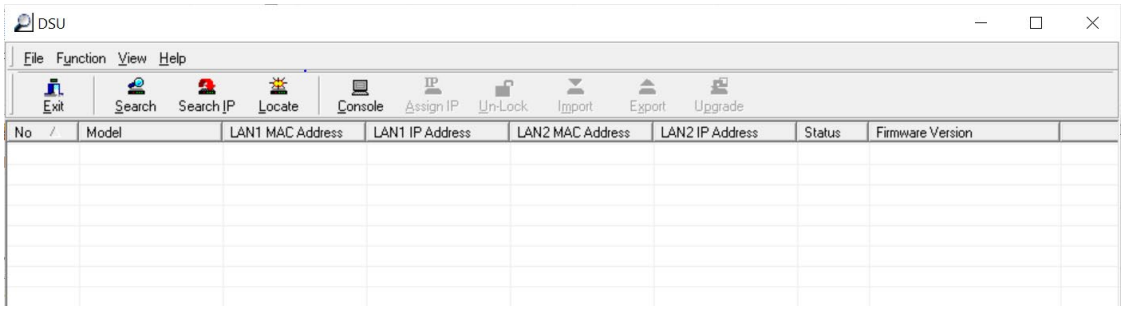
This is to locate the device by triggering the buzzer to help you find the target device server easily. Clicking the button would show all options of **Locate**. If your device does not support certain options, they will be disabled:

- Locate (IPv4)
- Locate (IPv6)

Configuring by Device Search Utility v2.7

Search

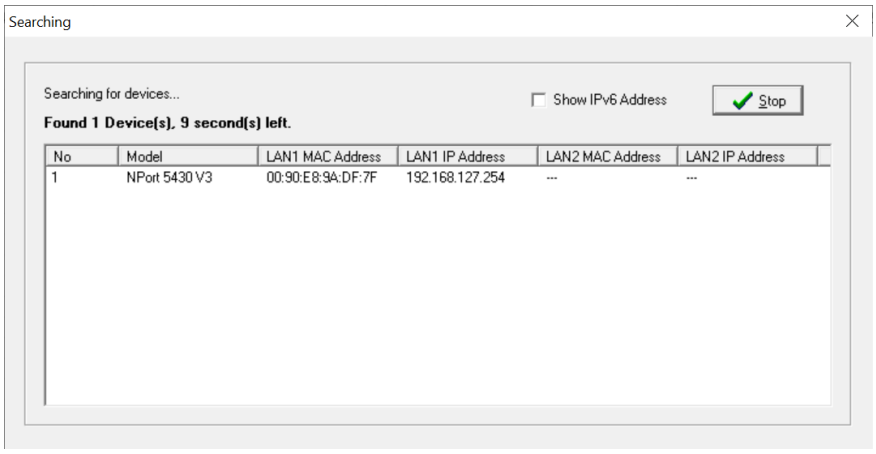
Before configuring the NPort, you will need to find it on the network first. The Broadcast Search function is used to locate all NPort 5000 servers that are connected to the same LAN as your computer.



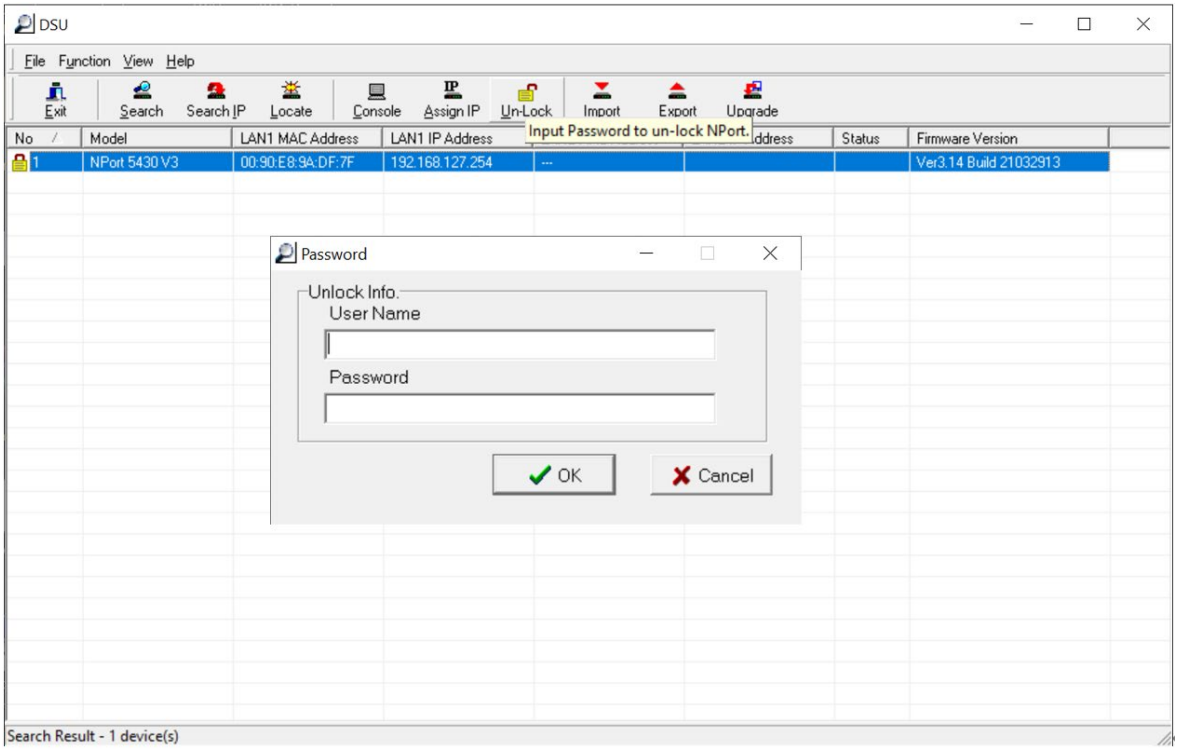
Exit	Quit DSU
Search	Broadcast search for devices
Search IP	Search device by specific IP
Locate	Locate the device by beeping it
Console	Access the device through consoles
Assign IP	Assign IP to a device
Un-Lock	Unlock the device before anything else
Import	Import configuration file to a device
Export	Export configuration file from a device
Upgrade	Upgrade firmware of a device

In DSU, click **Search** to search your LAN for NPort device servers, or right-click to find **Search** function. Since the Broadcast Search function searches for MAC address and not IP address, all NPort 5000 servers connected to the LAN will be located, regardless of whether they are part of the same subnet as the host.

When your unit appears in the search results, you may click **Stop** to end the search or wait a few more moments for the search to complete.



When the search is completed, all NPort 5000 serial device servers that are located are displayed in the DSU window. Select the device you wish to access and press the **Unlock** button to input the username and password for the device.

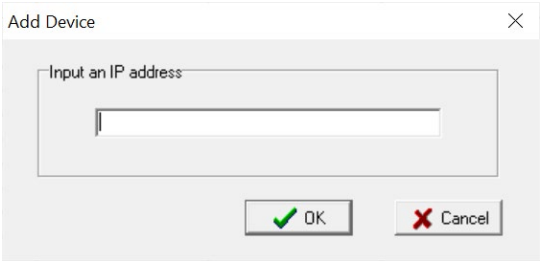


Note

1. The username and password are mandatory for the NPort 5000 installed with firmware v1.14 and above.
2. There will be session timeout after unlocking the NPort for 5 minutes. You will need to unlock the device again before further operation.

Search IP

You may also search for the NPort by specific IP address. Click **Search IP** in the toolbar and enter the IP address of the NPort.

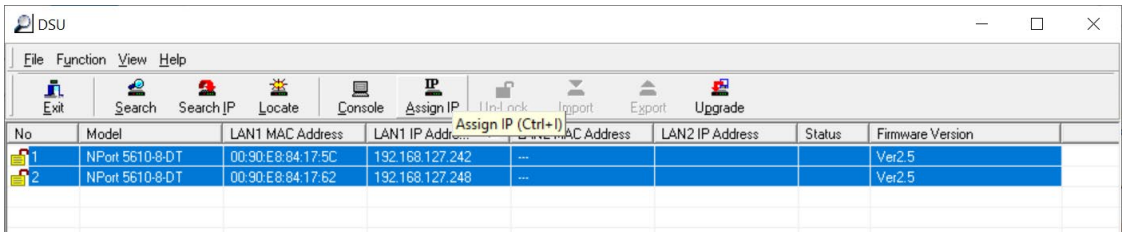


Assign IP

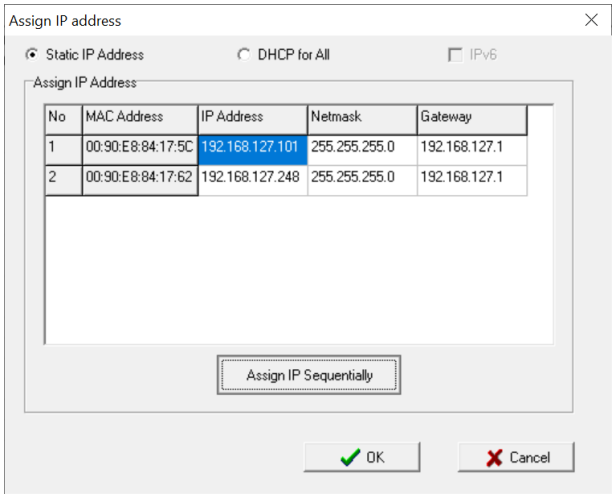
After locating a NPort, you may change its IP address if required.

1. Select the NPort that you would like to change to IP. You may perform the action to multiple units of the same model at once by holding CTRL and click the NPorts that you wish to change the IP.

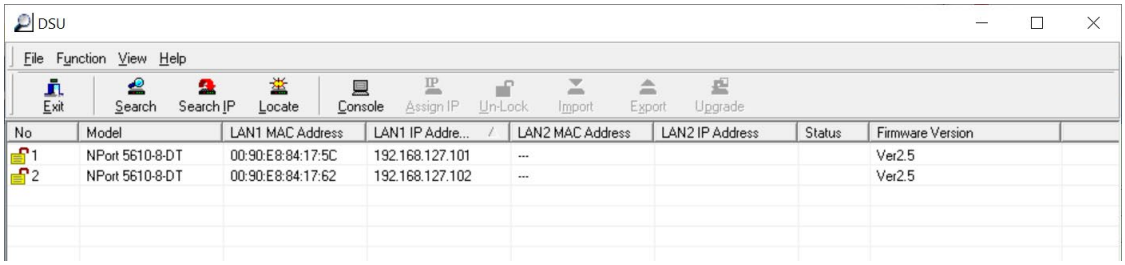
   Click **Assign IP** in the toolbar.



2. In most cases, the NPort requires a fixed IP address, select **Static IP address**. If you are not sure of your network environment, consult your network administrator.

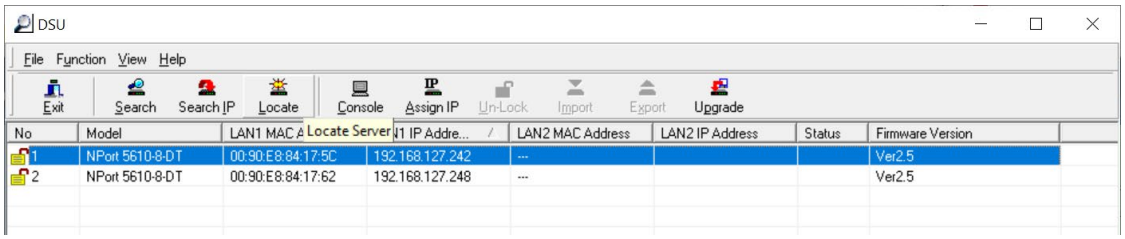


3. Click on the IP Address box to input the IP address manually. Do the same action to the **Netmask** cell as well. If multiple units of the same model are selected, click **Assign IP Sequentially** so it will assign IP in sequence, starting from the IP address of the first device.

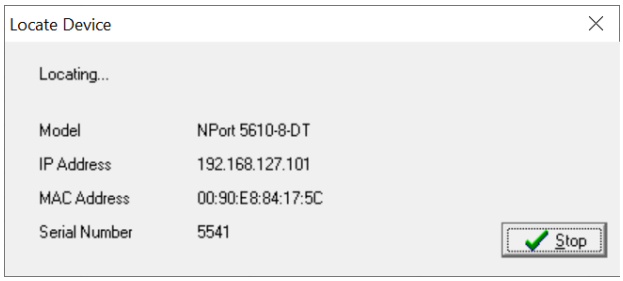


Locate

Locate provides a way of finding the NPort's whereabout when in need. Select the NPort that you are trying to find then click **Locate** in the toolbar.

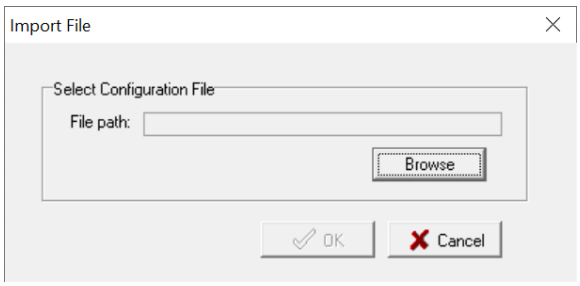


If the NPort is equipped with a buzzer, after **Locate** is triggered, the NPort's buzzer will beep continuously until it is turned off.



Import Configuration

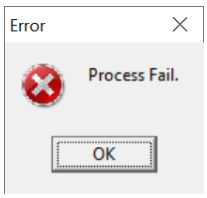
The Import Configuration function is used to import an NPort configuration from a file into one or more of the same NPort model. To import a configuration, first select the target device, click **Import** in the toolbar, and then click on the **Browse** button to locate the configuration file and press **OK**.



NOTE

You can import the same configuration to multiple units of the same model.

For the overall NPort 5000 Series with a security enhanced firmware version, importing configuration decryption will be based on the pre-shared key defined in the NPort. If the pre-shared key does not match, you will see an error dialogue box on the screen.



You will then need to change the pre-shared key in **Console > Backup/Restore > Pre-shared Key** to match the encryption password of the configuration file before you can import.

For firmware versions supporting encrypted configuration files, refer to the table below.

Model Name	Firmware version supporting encrypted configuration files.
NPort 5000 Series	
NPort 5110	Firmware v2.6 and up with NPort Administration Suite v1.22 and up
NPort 5130, NPort 5150	Firmware v3.6 and up with NPort Administration Suite v1.22 and up
NPort 5200 Series	Firmware v2.8 and up with NPort Administration Suite v1.22 and up
NPort 5400 Series	Firmware v3.11 and up with NPort Administration Suite v1.22 and up
NPort 5600-8-DT Series	Firmware v2.4 and up with NPort Administration Suite v1.22 and up
NPort 5600-8-DTL Series	Firmware v1.3 and up with NPort Administration Suite v1.22 and up
NPort 5600 Series	Firmware v3.7 and up with NPort Administration Suite v1.22 and up
NPort 5000A/IA5000A Series	
NPort 5100A Series	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort 5200A Series	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort 5x50AI-M12 Series	Firmware v1.2 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort IA5150A, NPort IA5250A	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort IA5450A	Firmware v1.4 and up (Support with both web console and NPort Administration Suite v1.22 or above)

NOTE

1. You can simultaneously import the same configuration file into multiple NPort units of the same model. To select multiple NPort units, hold down the **Ctrl** key when selecting an additional NPort, or hold down the **Shift** key to select a block of NPort units.
2. If you have an encrypted configuration file, you will need to use the Device Search Utility V2.4 or above to import an encrypted configuration file.

NOTE

If you do not remember the password of the encrypted configuration file, there is no alternative way to decrypt the file.

Export Configuration

The Export Configuration function is a handy tool that can produce a text file that contains the current configuration of a particular NPort.

If you are using the NPort 5100 Series, NPort 5200 Series, or NPort IA5000 Series

For the overall NPort 5000 Series with security enhanced firmware version, export configuration encryption will be based on the Pre-shared key defined in the NPort (default is empty password, and you may configure the password in **Console > Backup/Restore > Pre-shared Key**. So when you are exporting the configuration file, you are only required to select the output file location. You may refer to page 96 for the security firmware version for your NPort.

Upgrade Firmware

From time to time, Moxa would roll up new firmware for feature/security enhancement, patches, etc. It may be necessary to visit the NPort product website frequently to check for new firmware. You may also register to Moxa's website and follow the product updates so that you will be notified automatically for any recent activity. Check for **G. How to Become a Registered User of Moxa Website**.

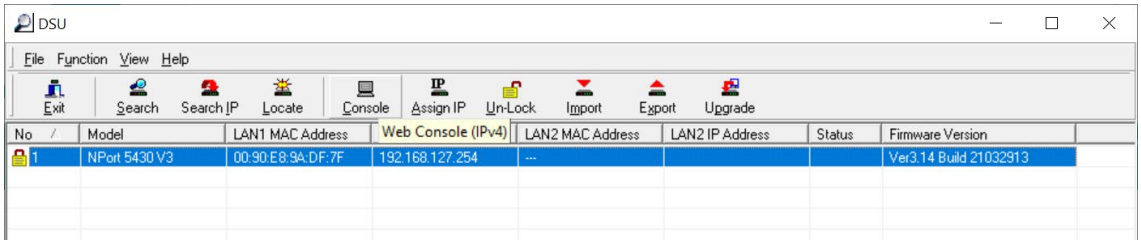
1. Unlock the NPort you wish to upgrade, then click **Upgrade** function in the toolbar to start the process.
2. In the file picker, choose the firmware file for your NPort.
3. You will see the progress.

NOTE

You can simultaneously upgrade the firmware of multiple NPort units that are of the same model. To select multiple NPort units, hold down the Ctrl key when selecting an additional NPort, or hold down the Shift key to select a block of NPort units.

Web Console

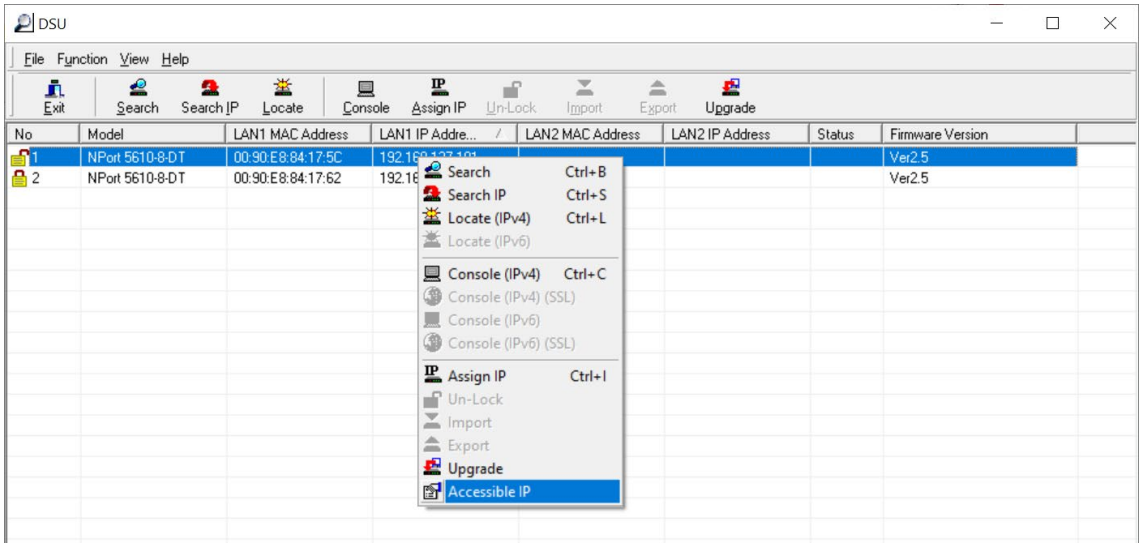
To change further settings NPort, click on the **Console** icon in the toolbar to launch the web console. This will take you to the web console where you can make all configuration changes.

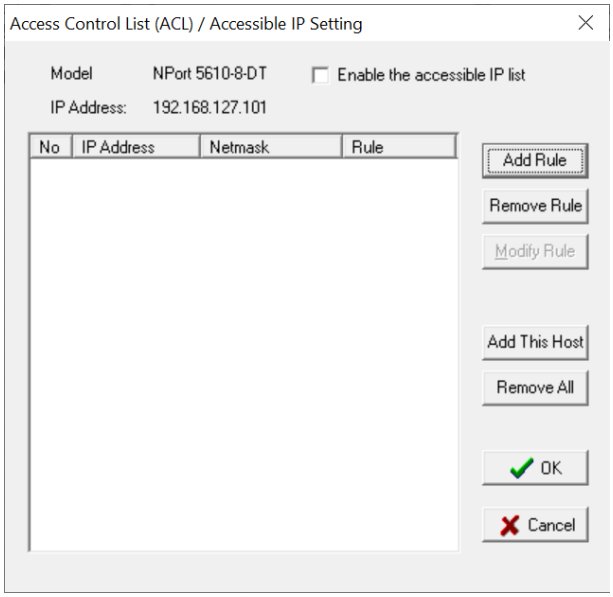


Refer to **Chapter 2, Configuration by Web Console**, for information on how to use the web console.

Accessible IP

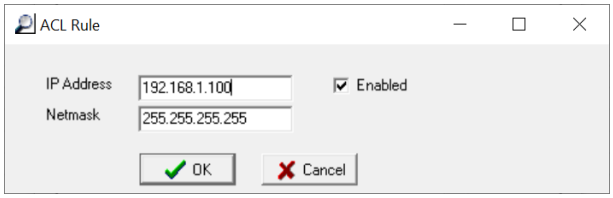
Accessible IP provides restriction of only listed IP can access the NPort. Select the specific NPort that you wish to set the access control and then right click and pick **Accessible IP**.





Enable the accessible IP list: Turn on or off the Accessible IP function.

Add Rule: To add an IP address that will be allowed to access the NPort.



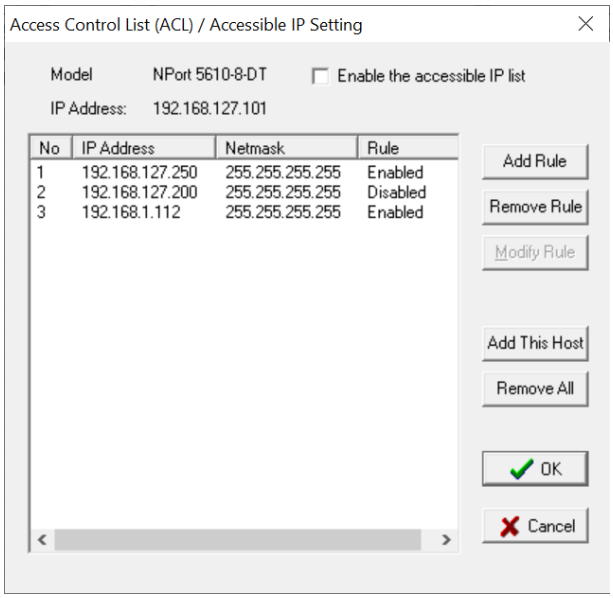
Enabled: To enable or disable this specific rule for the IP address

Remove Rule: To remove an established rule from the accessible IP list

Modify Rule: To adjust any established rule.

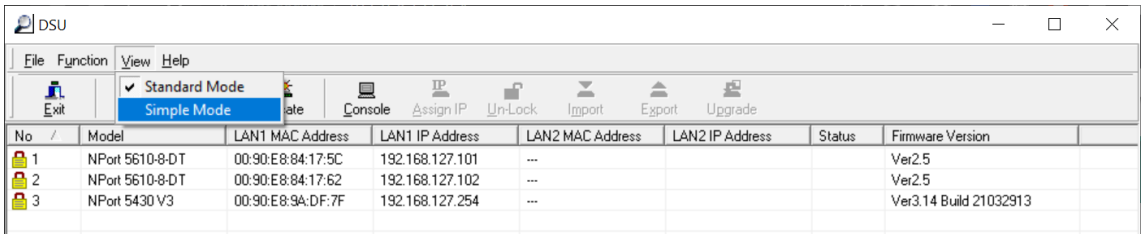
Add This Host: To add all your computer's available IP to the list.

Remove All: To remove all added IP addresses from the list.

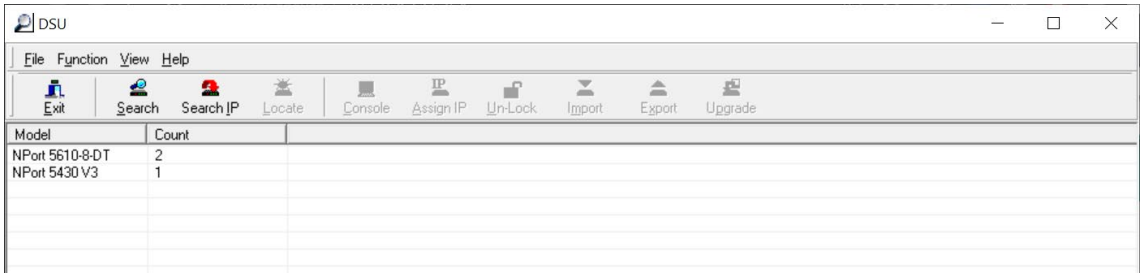


Standard Mode View/Simple Mode View

Simple Mode view summarizes how many NPorts and other Moxa devices are supported by **DSU**.

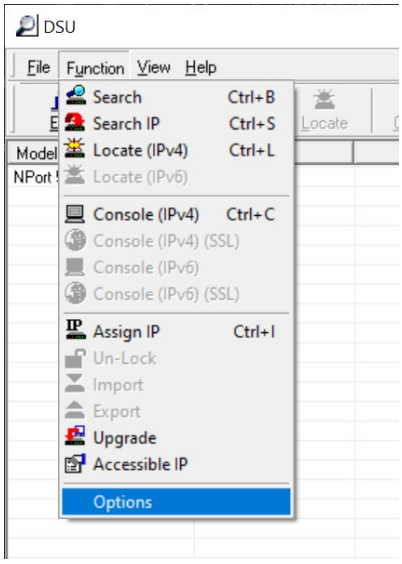


The list is defaulted and sorted by the model's name; you may sort by other fields by clicking the header.

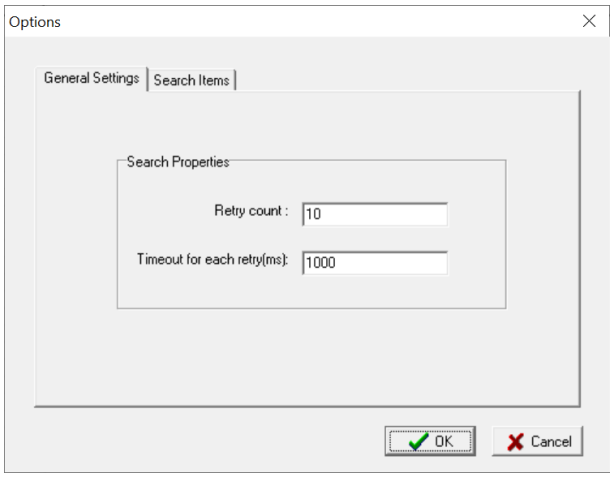


Other Options

There are few other options available for your to change to make **DSU** works better for your needs.

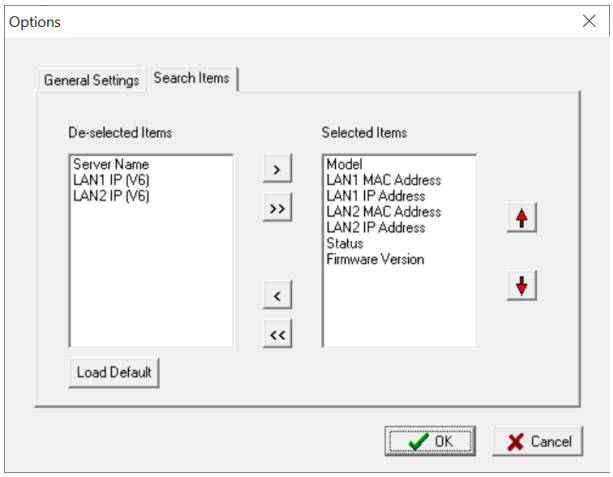


General Settings - Search Properties



Retry count: How many times does **DSU** retry to search for the devices in the LAN, 10 is the default. If your networking is slower to respond, you may increase the count.

Timeout for each retry (ms): The time interval between each retry. If your network environment has concerns for busy data traffic, you may increase the timer.



Search items: You may add or remove fields from the search result table to help with a better overview. Select the item in either pane and click the right or left arrow to switch side. Double arrows will move everything over. Items in **Selected Items** pane will be shown on the table header row, and the up and down red arrows are to adjust the display sequence.

Configuration by NPort Administrator Suite

ATTENTION

Before installing and configuring the NPort Administration suite, make sure your user privilege is set as system administrator.

NPort Administrator Suite is an integrated software suite that bundles NPort Administrator and the IP Serial Library, providing everything you need to manage, monitor, and change your NPort from a remote location.

With NPort Administrator, you can easily install and configure your NPort device server over the network. Five different functions are provided to ease the installation process: Configuration, Monitor, Porting Monitor, COM Mapping, and IP Address Report.

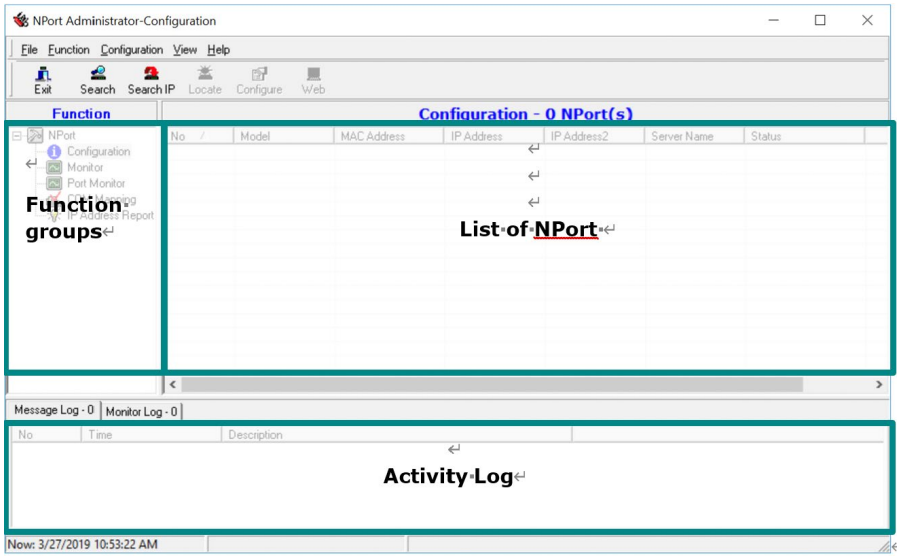
You may also use the other interface, like web console, Moxa CLI tool, serial console, or Telnet, to configure the device server. Refer to the specific section for additional information on using these consoles.

Installing NPort Administrator

Download and run the setup program from Moxa's support website. Run NPort Administrator when the installation has been completed.

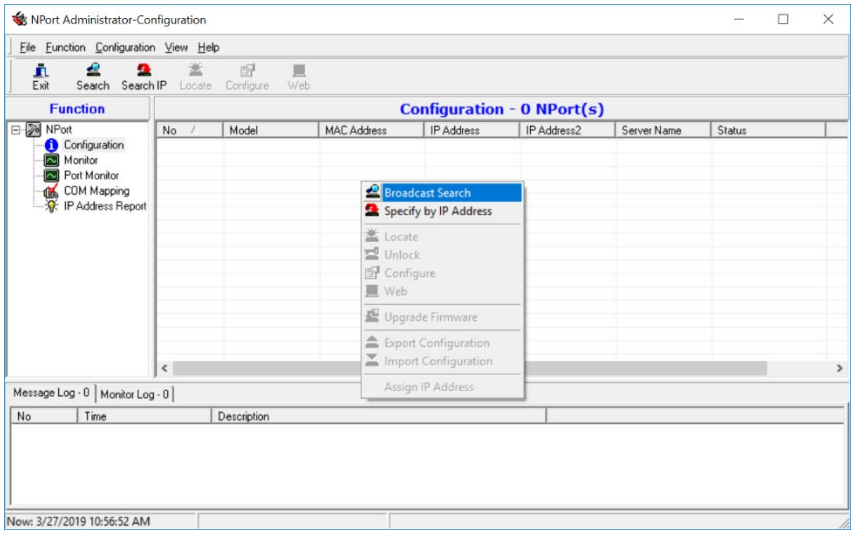
The Administrator-Configuration window is divided into four parts.

- The top section contains the function list and online help area. (Windows NT does not support this .chm file format.)
- The five Administrator function groups are listed in the left section.
- A list of NPort serial device servers, each of which can be selected to process user requirements, is displayed in the right section.
- The activity log, which displays messages that record the user's processing history, is shown in the bottom section.

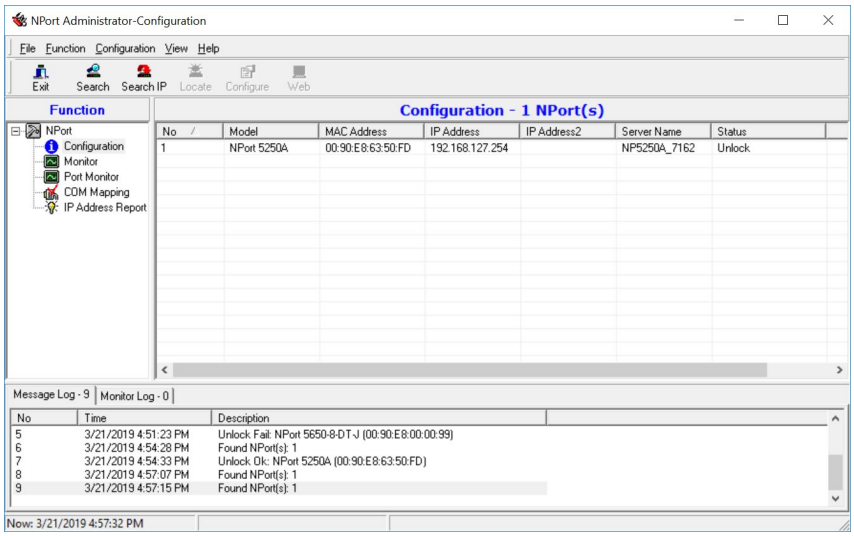


Searching for Device Servers Over a LAN

The **Search** function is used to locate all NPort 5000 device servers that are connected to the same LAN as your computer. Since the Search function broadcast searches by MAC address and not IP address, all NPorts connected to the LAN will be located, regardless of whether they are part of the same subnet as the host.



In NPort Administrator, click **Search** to search your LAN for NPort device servers, or right-click to find **Search** function. When your unit appears in the search results, you may click **Stop** to end the search or wait a few more moments for the search to complete.



You may also search the NPort by specific IP address. Right-click and select **Search by IP address** and enter the IP address of the NPort.

The **Configuration** screen will list the NPort device servers that were found on the LAN. If your unit cannot be found, you may need to check your network environment. Check all cables and verify that your PC and device server are on the same LAN. If you still have problems, try connecting the device server directly to your PC.

Unlock Your NPort

Before configuring the NPort, you will need to unlock the NPort first. Right-click the unit on the Configuration screen and select **Unlock** on the pop-up menu. Before configuring the NPort, you will need to unlock it first. Right-click the unit on the Configuration screen and select **Unlock** on the pop-up menu.

The default login is:

Username: **admin**
Password: **moxa**

NOTE

The NPort 5100/5200/IA5000 Series only requires a password.

Default password: **moxa**

The meanings of the six "Status" states are given below (note that the term Fixed is borrowed from the standard fixed IP address networking terminology):

Lock

The NPort is password protected, "Broadcast Search" was used to locate it, and the password has not yet been entered from within the current Administrator session.

Unlock

The NPort is password protected. "Broadcast Search" was used to locate it, and the password has been entered from within the current Administrator session. Henceforth, during this Administrator session, activating various utilities for this NPort will not require re-entering the server password.

Blank

The NPort is not password protected, and "Broadcast Search" was used to locate it.

Fixed

The NPort is not password protected, and "Search by IP address" was used to locate it.

Lock Fixed

The NPort is password protected, "Specify by IP address" was used to locate it, and the password has not yet been entered from within the current Administrator session.

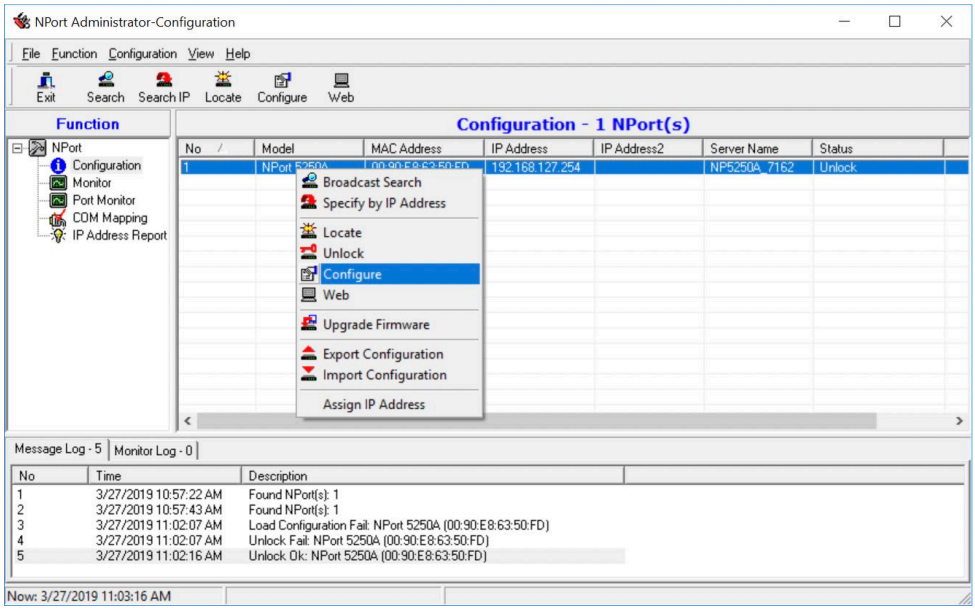
Unlock Fixed

The NPort is password protected, "Specify by IP address" was used to locate it, and the password has been entered from within the current Administrator session. Henceforth, during this Administrator session, activating various utilities for this NPort will not require re-entering the server password.

Configure

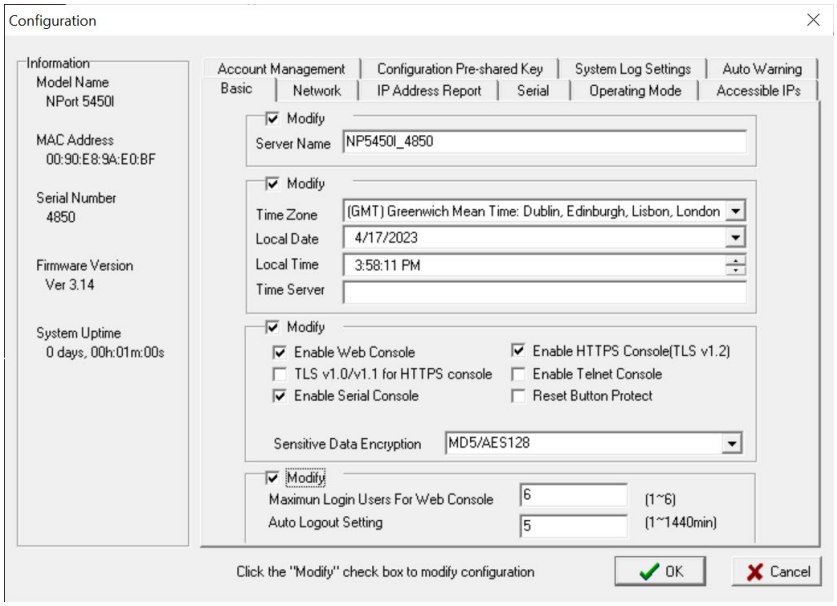
When NPort is in an unlocked state, right-click your unit in the Configuration screen and select **Configure** in the pop-up menu.

The progress bar shows that Administrator is retrieving configuration information from the specific NPort.



The progress bar would appear, showing that Administrator is retrieving configuration information from the specific NPort.

Basic



In **Basic**, you can give your NPort an alias name, set the time zone, date, and time. Also you can define how your NPort can be accessed, refer to 3. Cybersecurity Considerations for security suggestions from Moxa.

NOTE

The NPort 5100/5100A does not support **Time Setting** and **Sensitive Data Encryption**.

Parameter	Setting	Factory Default	Description	Necessity
Server name	1 to 39 characters	NP[model name]_[Serial No.]	This option is useful for specifying the location or application of different NPorts.	Optional
Time zone	User selectable time zone Not available in NPort 5100/5100A/5200/5200A Series	GMT (Greenwich Mean Time)	N/A	Required
Local time	User adjustable time (1900/1/1-2037/12/31) Not available in NPort 5100/5100A Series	GMT (Greenwich Mean Time)	Click the **Modify** button to open the Modify time settings window to input the correct local time.	Required
Time server	IP or Domain address (only available in 2/4/8/16 ports models) E.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov	None	NPorts use SNTP (RFC-1769) for auto time calibration. Input the correct **Time server** IP address or domain name. Once the NPort is configured with the correct Time server address, the NPort will request time information from the Time server every 10 minutes.	Optional
Daylight saving	Setting 1: "Start Date: Month, Week, Day, Hour"	None	The NPort can offset the system time to the values you have set in these settings. (This feature only applies to the NPort 5000AI-M12 Series.)	
	Setting 2: "End Date: Month, Week, Day, Hour"			
	Setting 3: "Offset: hours"			
http console	Enable or Disable	Disable	The options that are disabled by default—http Console, Telnet	Required
https console	Enable or Disable	Enable		Required

Parameter	Setting	Factory Default	Description	Necessity
TLS v1.0/v1.1 for HTTPS console	Enable or Disable	Disable	Console, and Serial Console—are for security reasons. In some cases, disable one or most of these console utilities as an extra precaution to prevent unauthorized users from accessing your NPort. Refer to **Chapter 3** "Cybersecurity Considerations" for detailed suggestions.	Required
Telnet console	Enable or Disable	Disable		Required
Serial Consoles	Enable or Disable	Enable		Required
Moxa Service	Enable or Disable	Enable		Required
Beep Service	Enable or Disable	Enable	Beeper Service is to provide audio notification and warning according to the different situations. (This feature only applies to the NPort 5000AI-M12 Series.)	Optional
Reset button protection	No or Yes	No	Select the **Yes** option to allow limited use of the reset button. In this case, the reset button can be used for only 60 seconds; 60 s. after booting up, the Reset Button will be disabled automatically.	Required
LCM read-only protection	Writeable/Read-only	Writeable	The NPort 5000 front panel, known as the LCM (Liquid Crystal Module), may be configured for read-only or writeable access. Read-only access allows settings to be viewed but not changed. Writeable access allows users in the Administration group to change the setting. This setting is only available for the model that has a font panel.	Optional

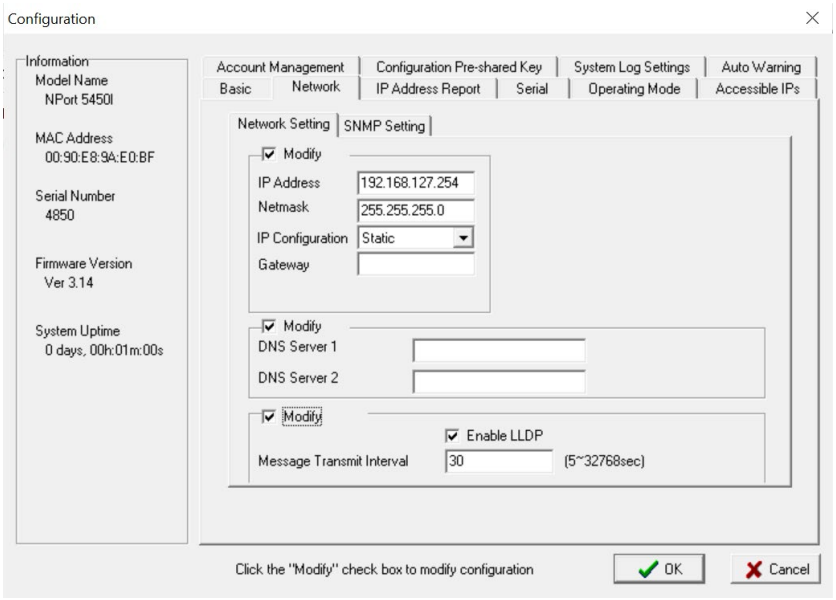
WARNING

If you disable all the console and services, there is no alternative way to access the NPort device servers neither locally nor remotely. The only way to gain control is to reset to factory default settings.

Network

You must assign a valid and unique IP address to the NPort before it will work in your network environment, otherwise, the NPort will not have a valid connection to the network. Your network system administrator should provide you with an IP address and related settings for your network. Select the **Modify** checkbox for items for editing.

You can choose from four possible **IP configuration** modes—Static, DHCP, DHCP/BOOTP, and BOOTP—located under the web console screen's IP configuration dropdown box.



Method	Function Definition
Static	The user must define the IP address, Netmask, and Gateway.
DHCP	The DHCP Server assigns the IP address, Netmask, Gateway, DNS, and Time Server
DHCP/BOOTP	The DHCP Server assigns the IP address, Netmask, Gateway, DNS, and Time Server, or the BOOTP Server assigns the IP address (if the DHCP Server does not respond).
BOOTP	The BOOTP Server assigns the IP address.

Network Settings

Parameter	Setting	Factory Default	Description	Necessity
IP Address	E.g., 192.168.1.1	192.168.127.254	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.	Required
Netmask	E.g., 255.255.255.0	255.255.255.0	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 will use the subnet mask to check whether 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, a connection is established directly from the NPort. Otherwise, the connection is established through the given default gateway.	Required

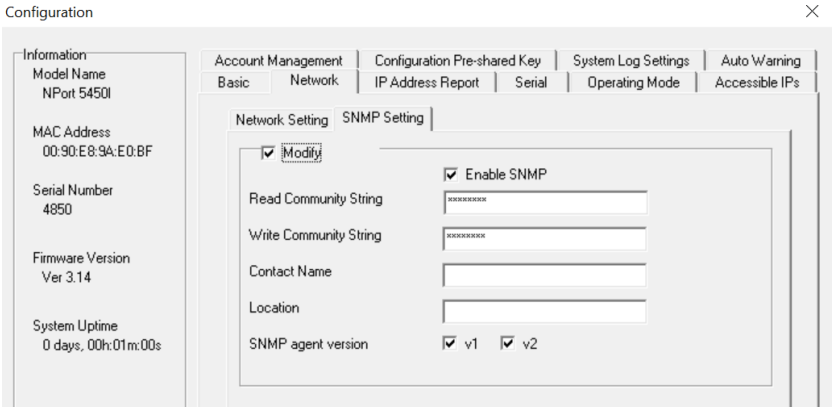
Parameter	Setting	Factory Default	Description	Necessity
Gateway	E.g., 192.168.1.1	None	A gateway is a network gateway that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort needs to know the IP address of the default gateway computer to communicate with the hosts outside the local network environment. For correct gateway IP address information, consult with your network administrator.	Optional
IP Configuration	Static DHCP DHCP/BOOTP BOOTP	Static	N/A	Required
Multi-LAN mode (for the NPort IA5000A Series only)	Switch Redundant LAN Dual IP	Switch	Dual LAN can be used as a redundant connection or dual IP. The scenario for redundancy is the NPort will automatically switch to working connection in case the other one loses connectivity (because of failed network component in the NPort, port at the switch/router stop working, etc.). As for dual IP scenario, each port will have its own IP address, but both will have the same MAC address, as it is convenient to connect the NPort to different network.	Optional
DNS server 1/ DNS server 2	E.g., 192.168.1.1	None	To use the NPort's DNS feature, you need to configure the DNS server. Doing so allows the NPort to use a host's domain name to access the host. The NPort provides DNS server 1 and DNS server 2 configuration items to configure the IP address of the DNS server. DNS Server 2 is included for use when DNS server 1 is unavailable. The NPort plays the role of DNS client, in the sense that the NPort will actively query the DNS server for the IP address associated with a particular domain name.	Optional
LLDP Settings	Enable or Disable	Enable	Not available for the NPort 5600DT Rev 1.5 or earlier	Optional

WARNING

In Dynamic IP environments, the firmware will retry three times every 30 seconds until network settings are assigned by the DHCP or BOOTP server. The Timeout for each try increases from 1 second, to 3 seconds, to 5 seconds.

If the DHCP/BOOTP Server is unavailable, the firmware will use the default IP address (192.168.127.254), Netmask, and Gateway for IP settings.

SNMP Settings



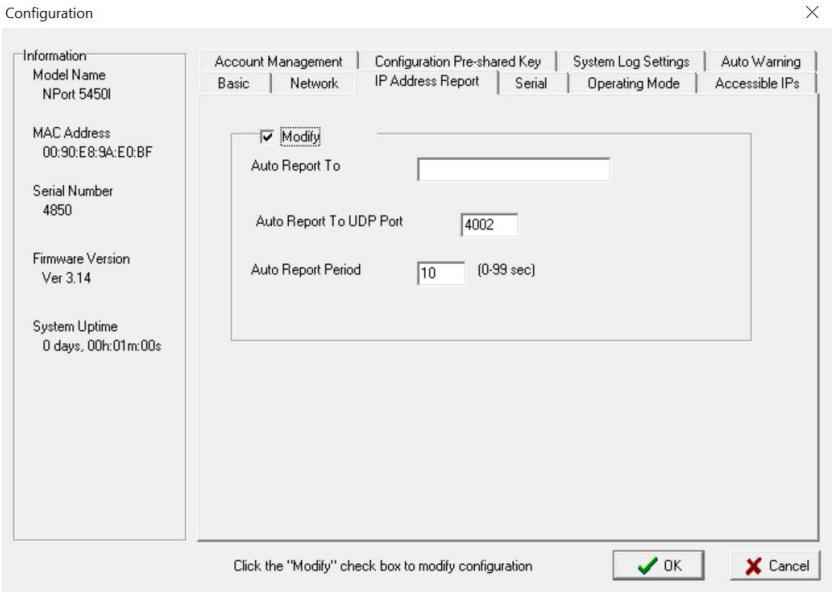
Parameter	Setting	Factory Default	Description	Necessity
Community Name	1 to 31 characters (e.g., Moxa)	Public	A community name is a plain-text password mechanism that is used to weakly authenticate queries to agents of managed network devices.	Optional
Contact	1 to 31 characters (e.g., Support, 886-89191230 #300)	None	The SNMP contact information usually includes an emergency contact name and telephone or pager number.	Optional
Location	1 to 39 characters (E.g., floor 1, office 2)	None	Specify the location string for SNMP agents, such as the NPort. This string is usually set to the street address where the NPort is physically located.	Optional
SNMP Agent Version V1, V2, V3	V1, V2, V3 (V3 is available on 4/8/16 ports model)	V1, V2 checked for 1/2-port models. V1, V2, V3 checked for 4/8/16-port models..	The NPort 5000 1- and 2-port model supports SNMP V1 and V2, where the 4/8/16-port model supports V1, V2 and V3. Select the version according to your environmental needs. Note that the 4/8/16-port model only supports standard MIB such as RFC1213/1317, which supports Set server name, contact, location, whereas the 1/2-port model only supports Get, but not Set.	Optional
The following fields allow you to define usernames, passwords, and authentication parameters for two levels of access: read-only and read/write. The name of the field will show which level of access it refers to. For example, Read-only authentication mode allows you to configure the authentication mode for read-only access, whereas Read/write authentication mode allows you to configure the authentication mode for read/write access. For each level of access, you may configure the following:				
Read-only username	1 to 31 characters	None	Use this optional field to identify the username for the specified level of access.	Optional
Read-only authentication mode	MD5, SHA	Disable	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication	Optional
Read-only password	1 to 31 characters		Use this field to set the password for read only of access.	Optional
Read-only privacy mode	DEC, CBC	Disable	Use this field to enable or disable DES_CBC data encryption for the specified level of access.	Optional
Read-only privacy	1 to 31 characters	None	Use this field to define the encryption key for the specified level of access.	Optional
Read/write username	1 to 31 characters	None	Use this optional field to identify the username for the specified level of access.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Read/write authentication mode	MD5, SHA	Disable	Use this field to select MD5 or SHA as the method of password encryption for the specified level of access, or to disable authentication	Optional
Read/write only password	1 to 31 characters		Use this field to set the password for read/write access.	Optional
Read/write only privacy mode	DEC, CBC	Disable	Use this field to enable or disable DES_CBC data encryption for the specified level of access.	Optional
Read/write only privacy	1 to 31 characters	None	Use this field to define the encryption key for the specified level of access	Optional

IP Address Report

When NPort products are used in a dynamic IP environment, users must spend more time on IP management tasks. For example, if the NPort works as a server (TCP or UDP), then the host, which acts as a client, must know the IP address of the server. If the DHCP server assigns a new IP address to the NPort, the host must have some way of determining the NPort's new IP address.

NPort products help by reporting their IP address periodically to the IP location server, in case the dynamic IP has changed. The parameters shown below are used to configure the Auto IP report function. There are two ways to develop an "Auto IP report Server" to receive NPort's Auto IP report.



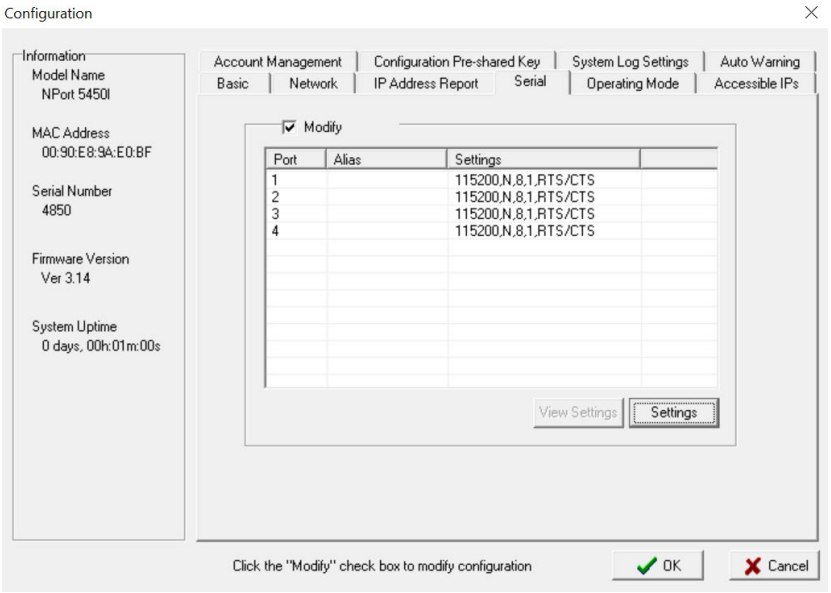
1. Use Device Server Administrator's **IP Address Report** function.
2. **Auto IP report protocol**, which can receive the Auto IP report automatically regularly, is also available to help you develop your own software. Refer to **Appendix E** for details about the **Auto IP report protocol**.

Parameter	Setting	Factory Default	Description	Necessity
Auto report to IP	E.g., 192.168.1.1 or URL	None	Reports generated by the Auto report function will be automatically sent to this IP address. In the multiple-LAN model version, two IPs can be set for Auto report. The report will be sent to each IP when generated.	Optional
Auto report to UDP port	E.g., 4001	4002	In the multiple-LAN model version, two IPs can be set for Auto report. Report will be sent to each IP when generated.	Optional

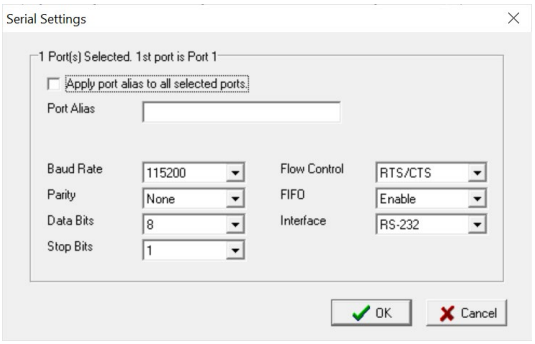
Parameter	Setting	Factory Default	Description	Necessity
Auto report period	Time interval (in seconds)	10	NA	Optional

Serial

The **Serial** tab is where you set the serial communication parameters for each device port. Settings include baudrate, parity, and flow control. Each device port can be configured independently.



Click **Modify** and select the port(s) that you would like to edit settings then click **Settings** for editing.



Parameter	Setting	Factory Default	Description	Necessity
Port Alias	1 to 15 characters (E.g., PLC-No.1)	None	Port Alias is specially designed to allow easy identification of the serial devices that are connected to the NPort's serial port.	Optional

Parameter	Setting	Factory Default	Description	Necessity
Baud rate	Support standard baudrates (bps): 50/ 75/ 110/ 134/ 150/ 300/ 600/ 1200 1800/ 2400/ 4800/ 7200/ 9600/ 19200/ 38400/ 57600/ 115200/ 230.4k/ 460.8k/ 921.6k * The NPort 5110/5210/ 5230/5232I Series, and IA 5000 Series are as low as 110 bps, and up to 230.4 kbps	115200 bps	The rate of data transmission to and from the attached serial device.	Required
Data bits	5, 6, 7, 8	8	When data bits is set to 5 bits, the stop bits setting will automatically change to 1.5 bits.	Required
Stop bits	1, 1.5, 2	1	The size of the stop character.	Required
Parity	None, Even, Odd, Space, Mark	None	Even and Odd parity provides rudimentary error-checking; Space and Mark parity are rarely used.	Required
Flow control	None, RTS/CTS, DTR/DSR, Xon/Xoff	RTS/CTS	The method used to suspend and resume data transmission to ensure that data is not lost. If you can use it, **RTS/CTS (hardware)** flow control is recommended.	Required
FIFO	Enable, Disable	Enable	Controls whether the device port's built-in 128-byte FIFO buffer is used. When enabled, the FIFO helps reduce data loss regardless of direction.	Required
*Interface**	RS-232 RS-422 2-wire RS-485 4-wire RS-485	RS-232	The serial interface that will be used. The options that are available depend on the specific model of the device server.	Required

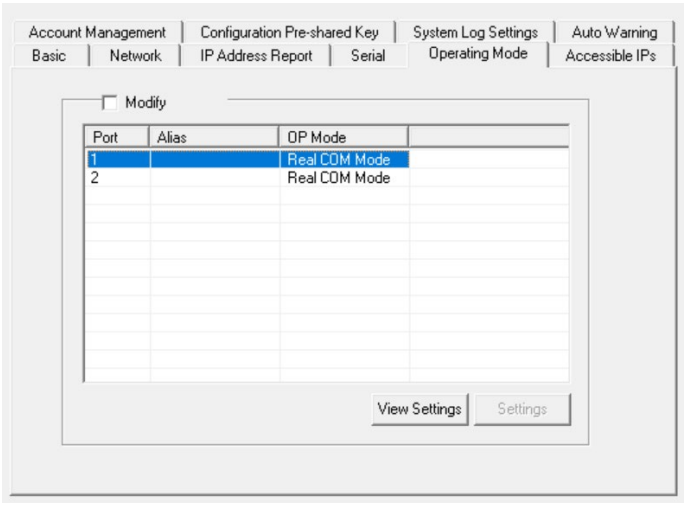
*Supported interfaces vary by model. Refer to the datasheet of your NPort device to see which serial interface it supports.

Operation Mode

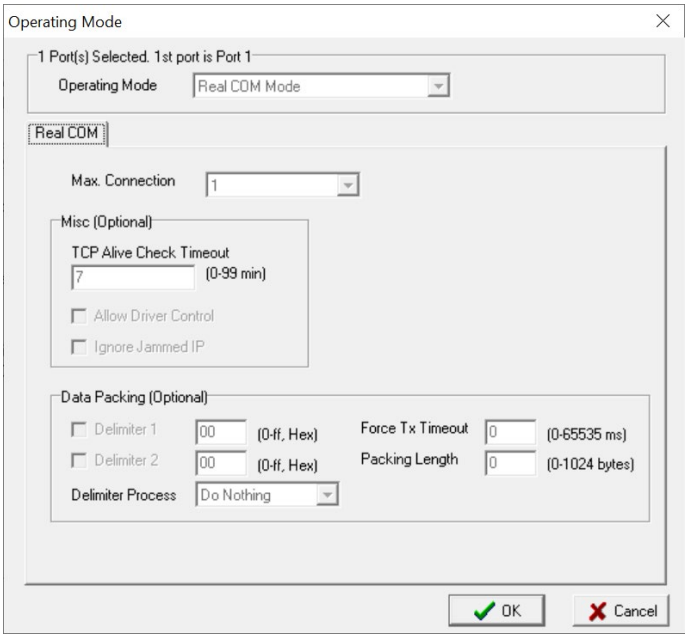
This section covers configuration of a device port's operation mode. The operation mode determines how the device port will interact with the network. Which operation mode you select will depend on your specific application. Refer to the chart at the end of this section for guidance on selecting the most appropriate operation mode. For additional information on each operation mode, refer to **Chapter 4** and **Chapter 5**.

Adjusting Operation Mode Settings

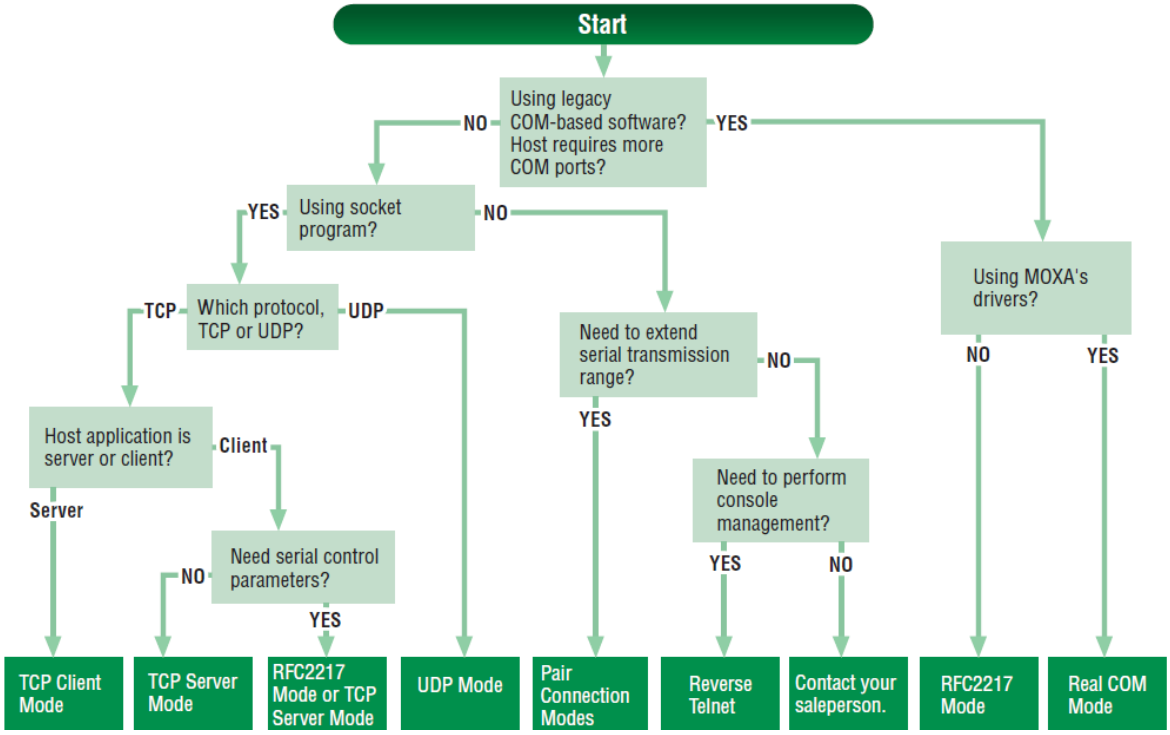
The operation mode parameters for each device port can be configured through NPort Administrator. Open your device server's configuration window using the same method you used to adjust the network parameters. On the **Operating Mode** screen, select the **Modify** checkbox and then select the device port you wish to configure. Click **Settings** to configure the selected device port.



Set the operating mode and associated parameters as needed. Refer to **Chapter 4** and **Chapter 5** for additional information on operating modes and advanced settings. When you are ready to restart the device server with the new settings, click **OK**.

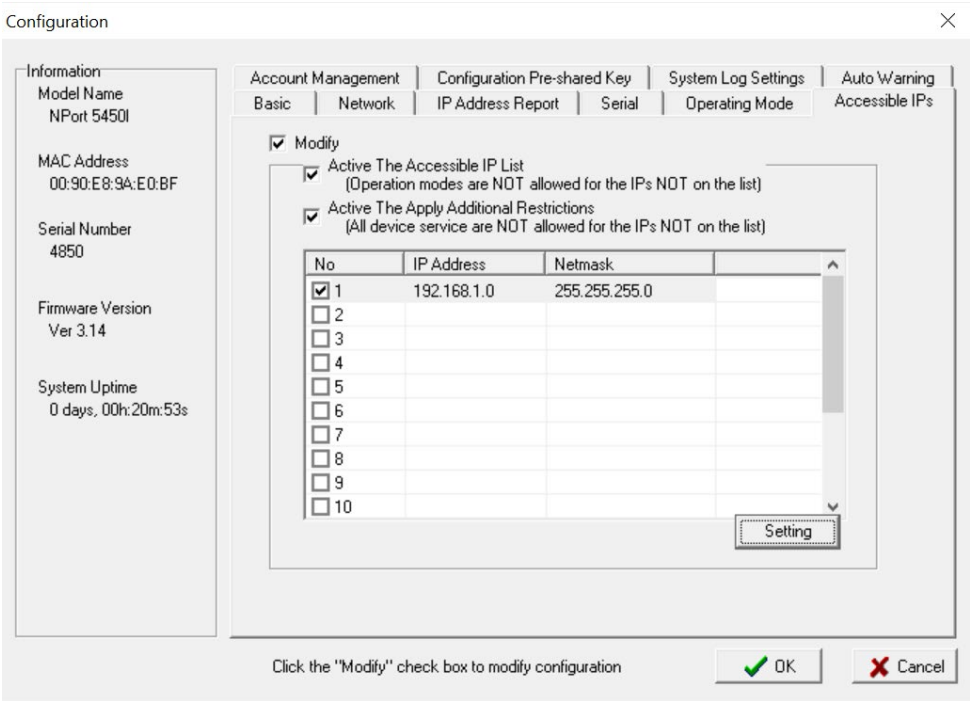


How to Choose Proper Operation Mode



Accessible IP Settings

Accessible IP Settings allow you to add or block remote host IP addresses to prevent unauthorized access. Access to the NPort is controlled by an IP address. That is, if a host's IP address is in the accessible IP table, then the host will be allowed to access the NPort. Three setting types are described below:



- **Activate the Accessible IP list**

  Operation modes are NOT allowed for IPs NOT on the list. IPs that are not on the list will not be granted when communicating with NPort via Operation Mode.

- **Apply additional restrictions**

  All device services are NOT allowed for IPs NOT on the list. Services will not be granted for IPs that are not on the list. Note that all IPs will still have access if the IP list is empty, even though the function is enabled.

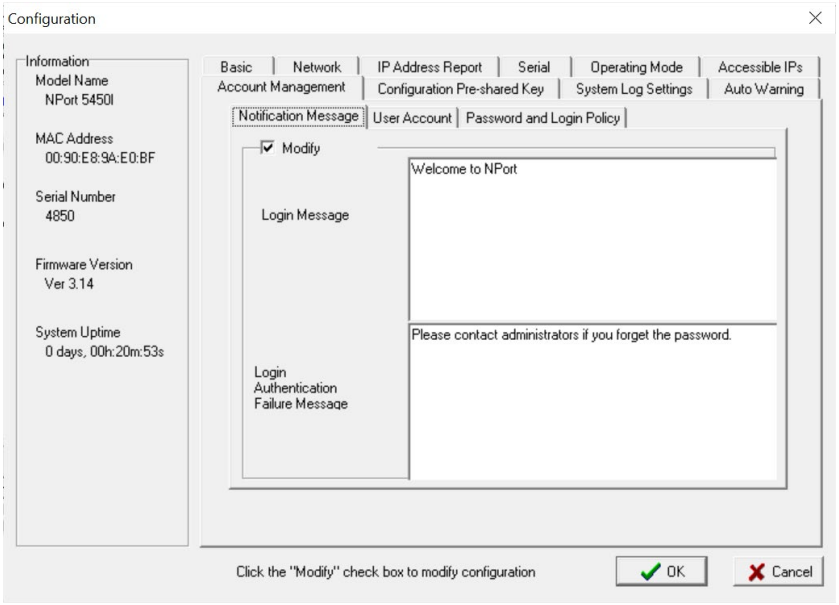
  Tip: For exact IP identification, the netmask needs to be 255.255.255.255.

- **Only one host with a specific IP address can access the NPort**
  Enter "[IP address]/255.255.255.255" (e.g., "192.168.1.1/255.255.255.255").
- **Hosts on a specific subnet can access the NPort**
  Enter "[IP address]/255.255.255.0" (e.g., "192.168.1.0/255.255.255.0").
- **Any host can access the NPort**
  Disable this function. Refer to the following table for more details about the configuration.

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

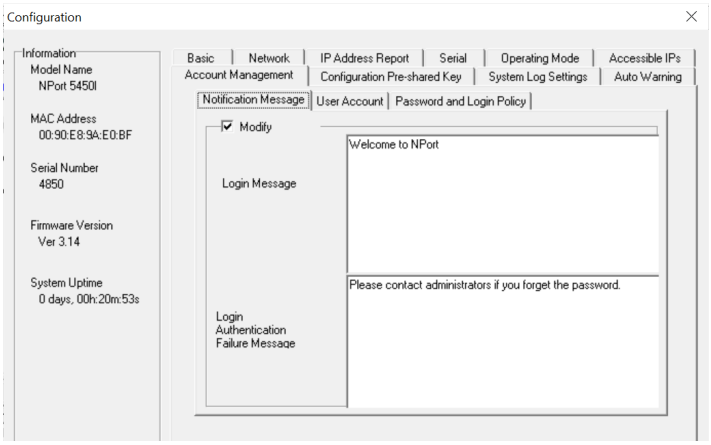
Account Management

The Account Management setting provides administrators the authority to add/delete/modify a user account, grant access to the device users for specified function groups, and manage password and login policy to ensure device is used by a proper set of people.

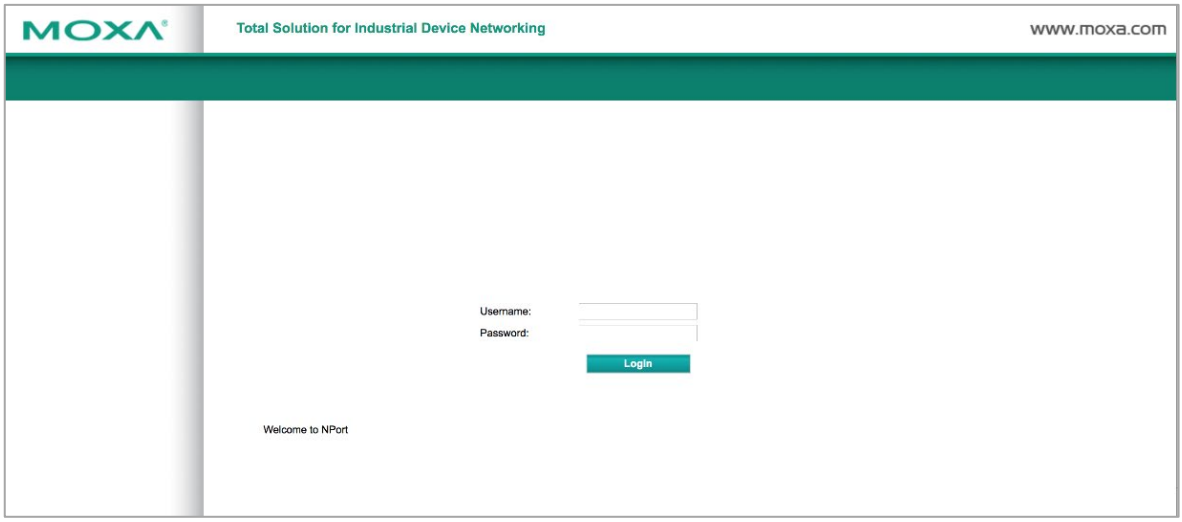


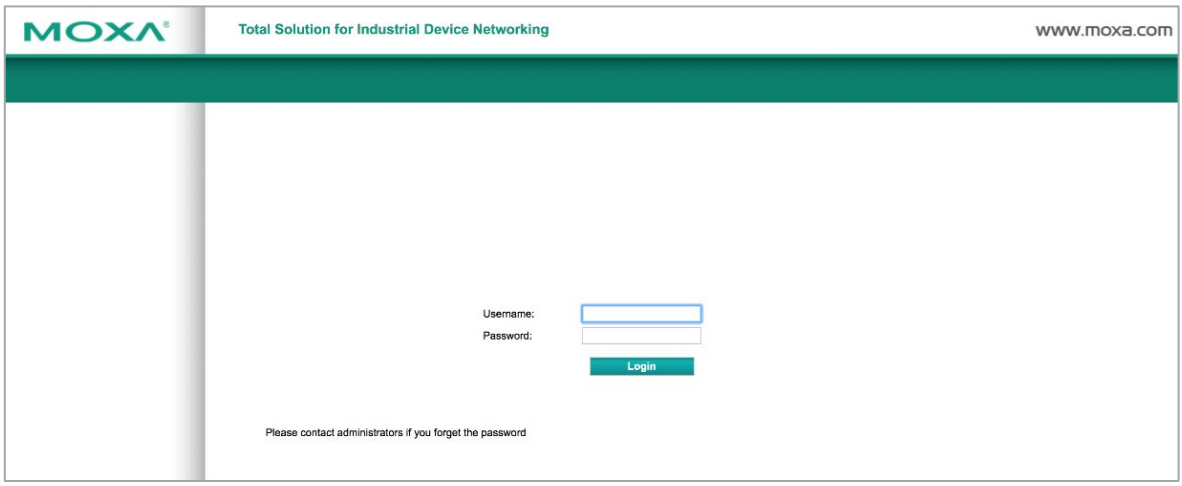
Notification Message

As an administrator, you may customize your **Login Message** and the **Login Authentication Failure Message** to notify users with information you would like to provide.



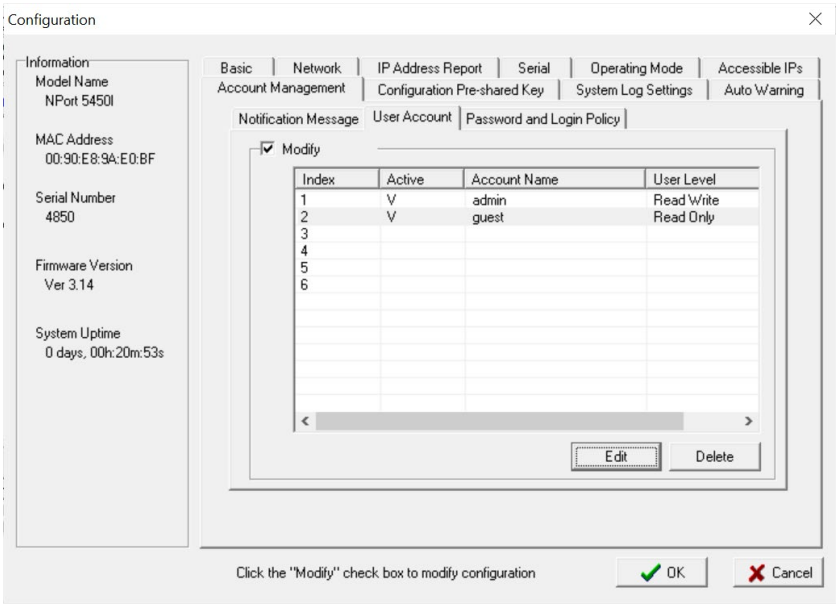
The message will appear on the login page at the time of a successful login or login failure. Examples are below.



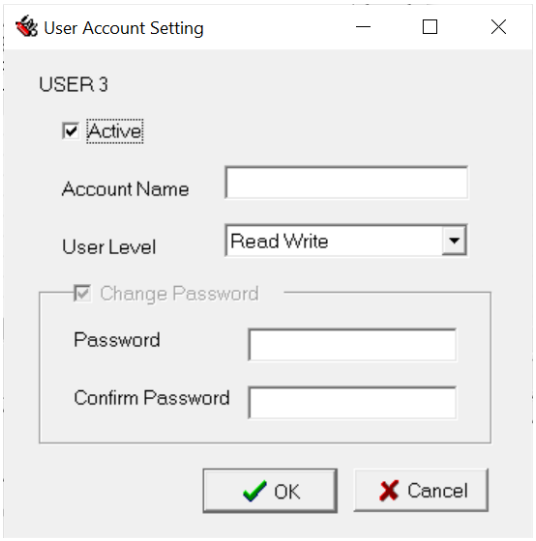


User Account

In the NPort 5000 Series, the main function groups are highly correlated with the **User Level** set by the administrator(s). Administrators are allowed to add user accounts to the NPort 5000 device by clicking the **Add** button on the **User Account** page. You may also click on the current user to **Edit** or Delete the selected account.

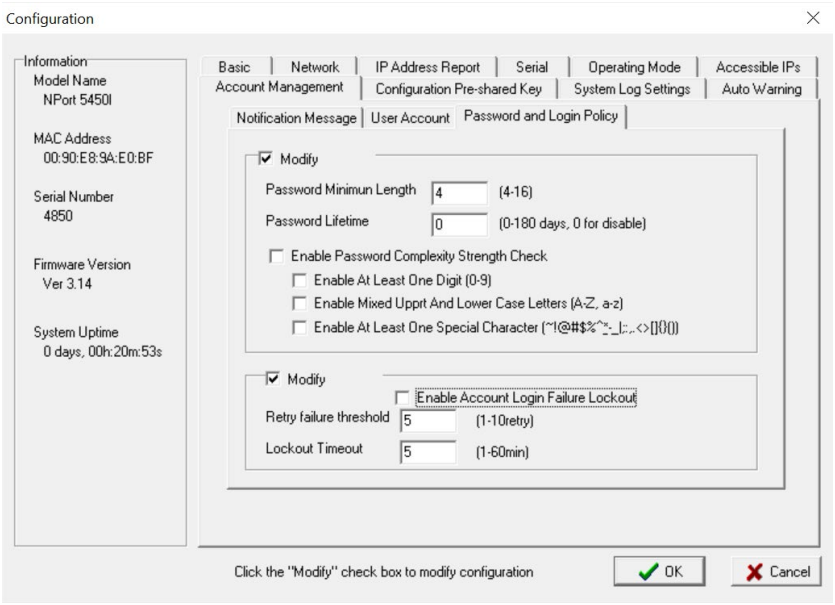


The **Add Account (Edit Account)** page will show up for you to enter (modify) account information and assign password to this user. Also, the Administrator(s) may assign proper **User Level** to this user to limit his/her privileges of using the NPort 5000.



Password and Login Policy

A user with an administrator role is authorized to determine the password and login policy of the NPort 5000 device.



Account Password Policy

Parameter	Setting	Default	Description
Password minimum length	4-16 characters	4	Define the minimum length of the login password
Password complexity strength check:	Enable/Disable	Disable	Enable password complexity strength check will enforce the password combination setting
• At least one digit (0-9)	Enable/Disable	Disable	The password must contain at least one number (0-9) when enabling this parameter
• Mixed upper and lower case letters (A to Z, a to z)	Enable/Disable	Disable	The password must contain an upper and a lowercase letter when enabling this parameter
• At least one special characters (~!@#$%^&*-_|;:,.<>[]{}())	Enable/Disable	Disable	The password must contain at least one special character when enabling this parameter
Password lifetime	0-180 days (0 for disable)	90 days	A password lifetime can be specified, and a system notification message will show up to remind users to change the password if the option is enabled.

Account Login Failure Lockout

Parameter	Setting	Default	Description
Account Login Failure Lockout	Enable/Disable	Disable	An account login failure lockout rule can be defined and enforced when enabled.
• Retry failure threshold	1-10 retry	5 if enabled	Number of retries can be determined prior to the lockout
• Lockout time	1-60 minute(s)	5 if enabled	Lockout duration can be specified to determine time until the next retry.

Configuration Pre-shared Key

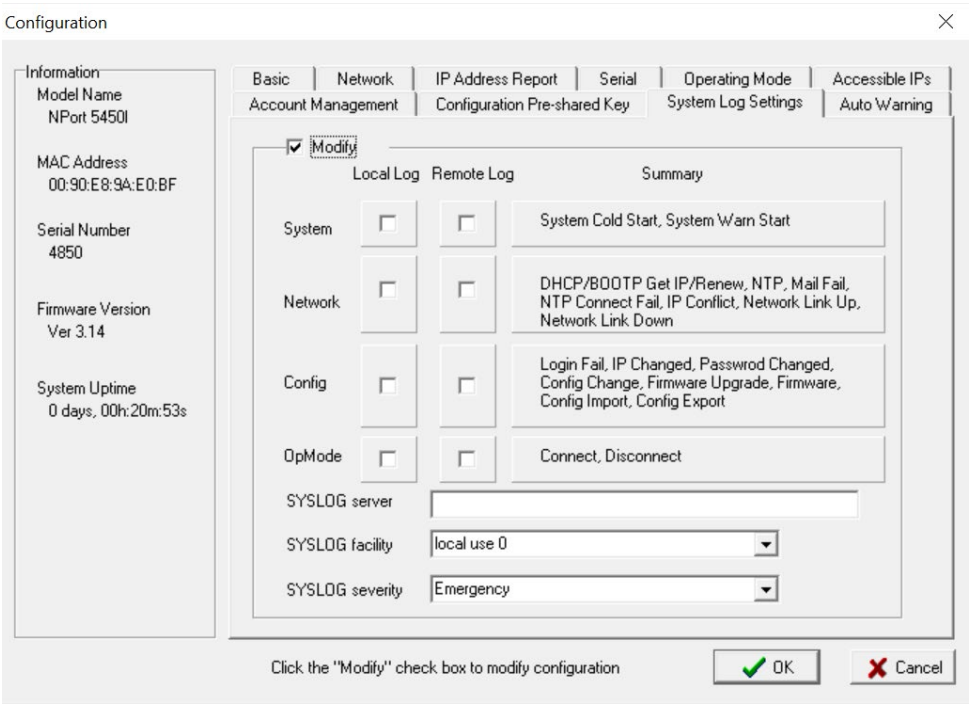
For the overall NPort 5000 Series with a security enhanced firmware version, importing configuration decryption will be based on the pre-shared key defined in the NPort. If the pre-shared key does not match, you will see an error dialogue box on the screen.

System Log Settings

System Log Settings allow NPort users to customize network events that are logged by the NPort 5000. Events are grouped into four categories, known as event groups, and the user selects which groups to log as Local Log (on the NPort 5000). The actual system events that would be logged for each system group are listed under the column "Summary". For example, if **System** was enabled, then System Cold Start events and System Warm Start events would be logged.

NOTE

- The NPort 5100, NPort 5200, and NPort IA5000 Series don't support this function.
- Remote Log does not apply to the NPort 5000 Series.



Local Log	Keep the log in the flash of NPort 5000 up to 512 items.

System

System Cold Start	NPort 5000 cold start.
System Warm Start	NPort 5000 warm start.

Network

DHCP/BOOTP/PPPoE Get IP/Renew	IP of the NPort 5000 is refreshed.
NTP	Time synchronization successful.
NTP Connect Fail	The NPort 5000 failed to connect to the NTP Server.
Mail Fail	Failed to deliver the email.
IP Conflict	There is an IP conflict on the local network.
Network Link Down	LAN 1 Link is down.

Config

Login Fail	
IP Changed	Static IP address was changed.
Password Changed	Administrator Password was changed.
Config Changed	The NPort 5000's configuration was changed.
Firmware Upgrade	Firmware was upgraded.
SSL Certificate Import	SSL Certificate was imported.
Config Import	Config was imported.
Config Export	Config was exported.

OpMode

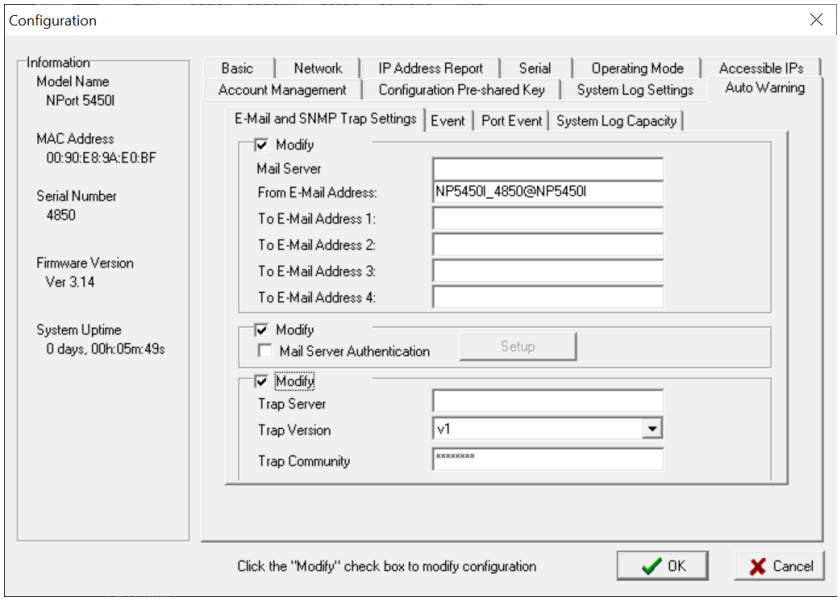
Connect	Op Mode is in use
Disconnect	Op Mode switched from in use to disconnect.
Authentication Fail	The Authentication failed in terminal; reverse terminal; or dial in/out operation modes
Restart	Serial port restarted.

Auto Warning Settings

The NPort device server can automatically warn administrators of certain system, network, and configuration events. Depending on the event, different options for automatic notification are available. These options are configured in the Auto Warning Settings.

Email and SNMP trap

The Email and SNMP trap parameters are used to configure how email and SNMP traps are sent when an automatic warning is issued by the NPort device server.



Mail Server

Parameter	Setting	Factory Default	Description	Necessity
Mail server	IP or Domain Name	None	This optional field is for the IP address or domain name of your network mail server, if applicable. A mail server is required for the NPort to send email warnings about administrative events.	Optional
Username	1 to 15 characters	None	This optional field is used if your mail server requires it.	Optional
Password	1 to 15 characters	None	This optional field is used if your mail server requires it.	Optional
From email address	1 to 63 characters	None	This optional field sets the "from" email address that will show up in an automatic warning email.	Optional
Email address 1/2/3/4	1 to 63 characters	None	These optional fields set the "destination" email address for automatic email warnings.	Optional

SNMP Trap Server

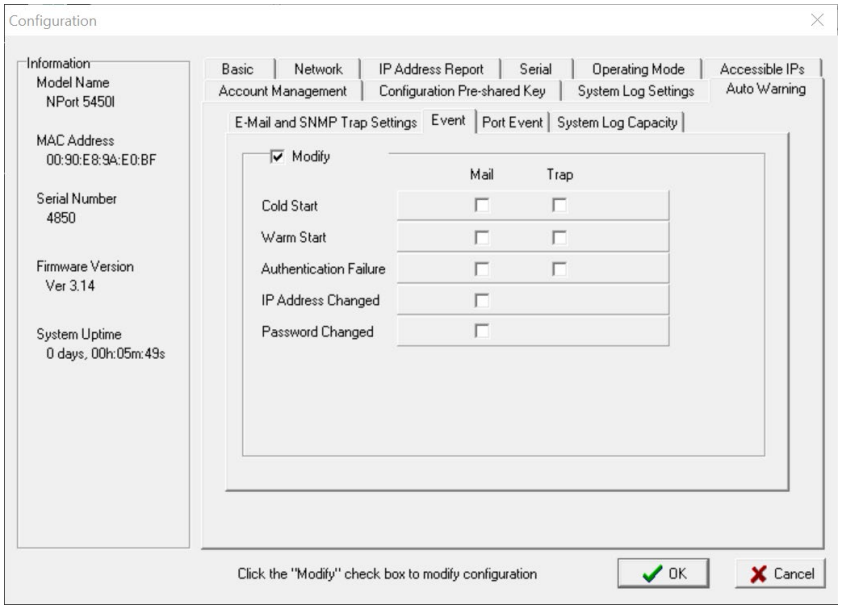
Parameter	Setting	Factory Default	Description	Necessity
SNMP trap server IP or domain name	IP address or Domain Name	None	Selecting the version based on your environmental needs. We strongly suggest to that you change the community name from the default **public** to another name; it is for security prevention reasons.	Optional

ATTENTION

Consult your network administrator or ISP for the proper mail server settings. The **Auto warning** function may not work properly if it is not configured correctly. NPort SMTP AUTH supports LOGIN, PLAIN, CRAM-MD5 (RFC 2554).

Event

The Email and SNMP trap parameters are used to configure how email and SNMP traps are sent when an automatic warning is issued by the NPort device server.



The Event Type parameters are used to configure which events will generate an automatic warning from the NPort device server, and how that warning will be issued. For each listed event, certain automatic warning options are available. If Mail is selected, an email will be sent. If Trap is selected, an SNMP trap will be sent. The **Relay Output** option is available for the NPort IA5000/IA5000A Series.

Cold start

Refers to starting the system from power off (contrast this with warm start). When performing a cold start, the NPort will automatically issue an auto warning message by email or send an SNMP trap after booting up.

Warm start

A warm start refers to restarting the computer without turning the power off. When performing a warm start, the NPort will automatically send an email, or send an SNMP trap after rebooting.

Authentication failure

An authentication failure event is triggered when the user inputs an incorrect password from the Console or Administrator. When an authentication failure occurs, the NPort will immediately send an email or SNMP trap.

IP address changed

An IP address changed event is triggered when the user has changed the NPort's IP address. When the IP address changes, the NPort will send an email with the new IP address before the NPort reboots. If the NPort cannot send an email message to the mail server within 15 seconds, the NPort will reboot anyway, and abort the email auto warning.

Password changed

A password changed event is triggered when the user has changed the NPort's password. When the password changes, the NPort will send an email with the password changed notice before the NPort reboots. If the NPort cannot send an email message to the mail server within 15 seconds, the NPort will reboot anyway, and abort the email auto warning.

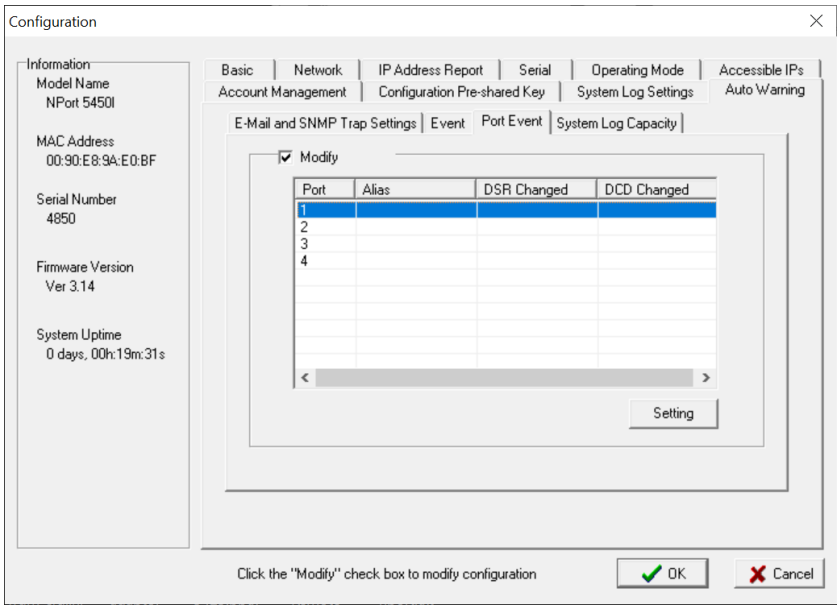
Power failure (this event type only applies to NPort IA5000/IA5000A Series)

The NPort IA5000/IA5000A Series has two DC power inputs for redundancy. Different approaches are used to warn engineers automatically, including by email and by relay output. The relay output will be canceled after the power recovers, or by selecting "acknowledge event" using the web console or Telnet. When the Relay Output is sending a warning, the Ready LED will flash red until the warning event ceases.

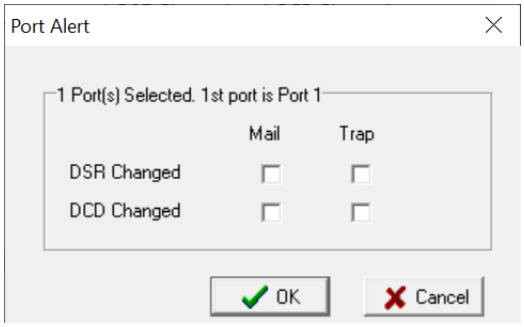
Port Event

Port event helps you with monitoring the serial communication status and changes. Here we provide two events of monitoring: **DCD changed** and **DSR changed**.

First, click **Modify** select the serial port you would like to monitor and click **Settings** below:



Port Alert option appears:



DCD changed

A DCD (Data Carrier Detect) signal change shows that the modem connection status has changed. For example, a DCD change too high shows that the local modem and remote modem are connected. A DCD signal change to low shows that the connection line is down. When the DCD changes, the NPort will immediately send an email, send an SNMP trap, or trigger the relay output*.

DSR changed

A DSR (Data Set Ready) signal change shows that the data communication equipment's power is off. For example, a DSR change to high indicates that the DCE is powered ON. A DSR signal changes to low indicates that the DCE is powered off. When the DSR changes, the NPort will immediately send an email, send an SNMP trap, or trigger the relay output*.

*Relay output is only supported by the NPort IA5000/IA5000A Series.

NOTE

Relay Output is only available for the NPort IA5000/IA5000A Series. Users can connect to **Monitor > Relay Output** from the web console to check which event is causing the warning. The relay output will be canceled if the abnormal state is restored, or if **Acknowledge Event** is selected from the web or Telnet console. When the Relay Output is issuing a warning, the Ready LED will flash red until the warning event ceases.

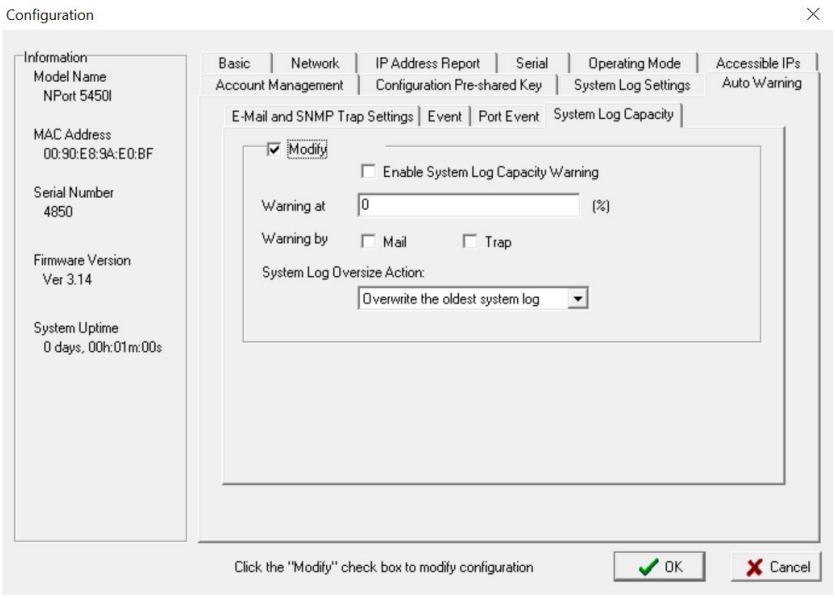
Parameter	Setting	Factory Default	Description	Necessity
Mail	Enable, Disable	Disable	This feature helps the administrator manage how the NPort sends email to pre-defined email boxes when the enabled events (Cold start, Warm start, Authentication failure, etc.) occur. To configure this feature, click the **Event Type Mail** checkbox.	Optional
Trap	Enable, Disable	Disable	This feature helps the administrator manage how the NPort IA5000A sends an SNMP Trap to a pre-defined SNMP Trap server when the enabled events (Cold start, Warm start, Authentication failure, etc.) occur. To configure this feature, click the **Event Type Trap** checkbox.	Optional

ATTENTION

DCD and **DSR** signal changes only apply to the RS-232 interface.

System Log Capacity

You can decide how to store your log data and if you need to be informed when the storing capacity is nearing a certain percentage and how if log data can be overwritten or kept if the storage is full.

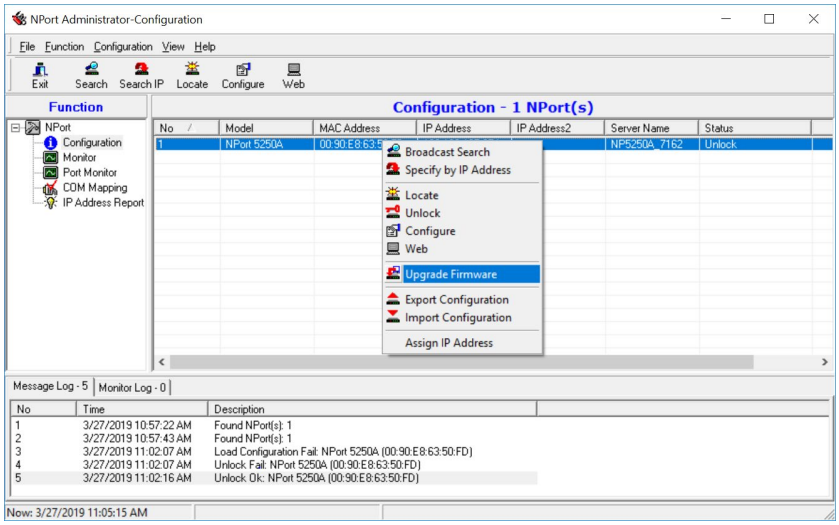


Upgrading the Firmware

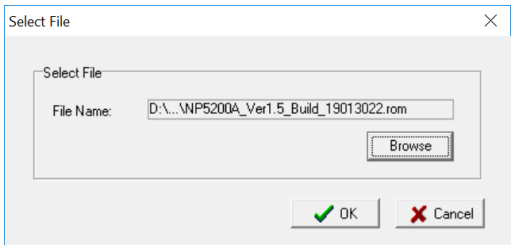
From time to time, Moxa would roll up new firmware for feature/security enhancement, patches, etc. It may be necessary to visit the NPort product website frequently to check for the latest firmware. You may also register for Moxa's website and follow the product updates so that you will be notified automatically about any recent activity. Check for **G. How to Become a Registered User of Moxa Website.**

Follow these steps to upgrade the firmware of an NPort.

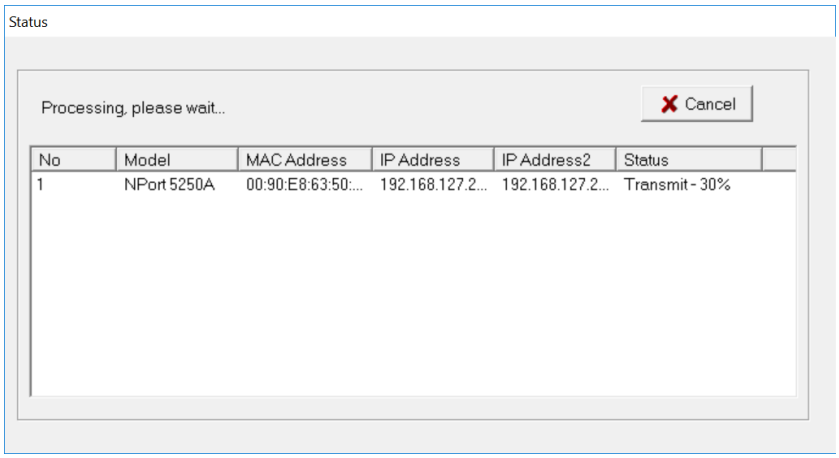
1. Unlock the NPort you wish to configure. Right click a specific NPort and select the **Upgrade Firmware** function to upgrade the firmware.



2. Select the correct firmware file to load.



3. Wait while the Upgrade Firmware action is processed.



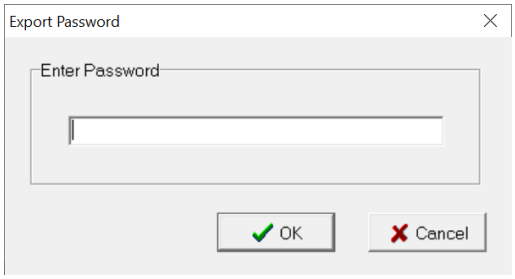
NOTE

You can simultaneously upgrade the firmware of multiple NPort units that are of the same model. To select multiple NPort units, hold down the Ctrl key when selecting an additional NPort, or hold down the Shift key to select a block of NPort units.

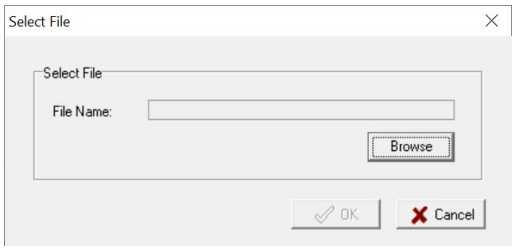
Export Configuration

The Export Configuration function is a handy tool that can produce a text file that contains the current configuration of a particular NPort.

If you are using the NPort 5100 Series, NPort 5200 Series, or NPort IA5000 Series and Administration Suite v1.22 or above, to export the configuration of an NPort, right-click the targeted NPort, select **Export Configuration**. An Export Password window will pop up for the user to assign a password for the exported configuration file. The exported configuration file will be encrypted for security. You will need the same password you use for the exported file to import the same file back into the NPort.



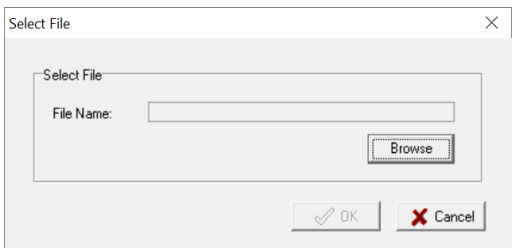
After assigning the export password, click the **Browse** button to set the file name and path, and then click **OK**.



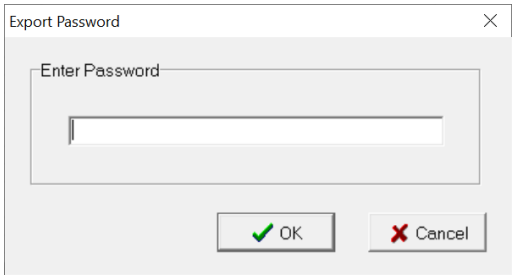
For the overall NPort 5000 Series with security enhanced firmware version, export configuration encryption will be based on the Pre-shared key defined in the NPort (default is empty password, and you may configure the password in **Configuration > Configuration Pre-shared Key**. So, when you are exporting the configuration file, you are only required to select the output file location. You may refer to page 96 for the security firmware version of your NPort.

Import Configuration

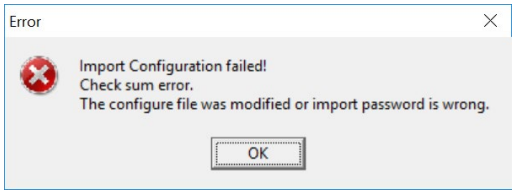
The Import Configuration function is used to import an NPort configuration from a file into one or more of the same NPort model. To import a configuration, first select the target servers, right-click, and then select **Import Configuration**. Click on the **Browse** button to locate the configuration file and press **OK**.



For the NPort 5100 Series, NPort 5200 Series, or NPort IA5000 Series and with NPort Administration Suite v1.22 or above, an **Import Password** window will pop up, and you will need to enter the password that is unique to the configuration file (which is assigned when exporting the configuration file) to successfully import the configuration file.



For the overall NPort 5000 Series with a security enhanced firmware version, importing configuration decryption will be based on the pre-shared key defined in the NPort. If the pre-shared key does not match, you will see an error dialogue box on the screen.

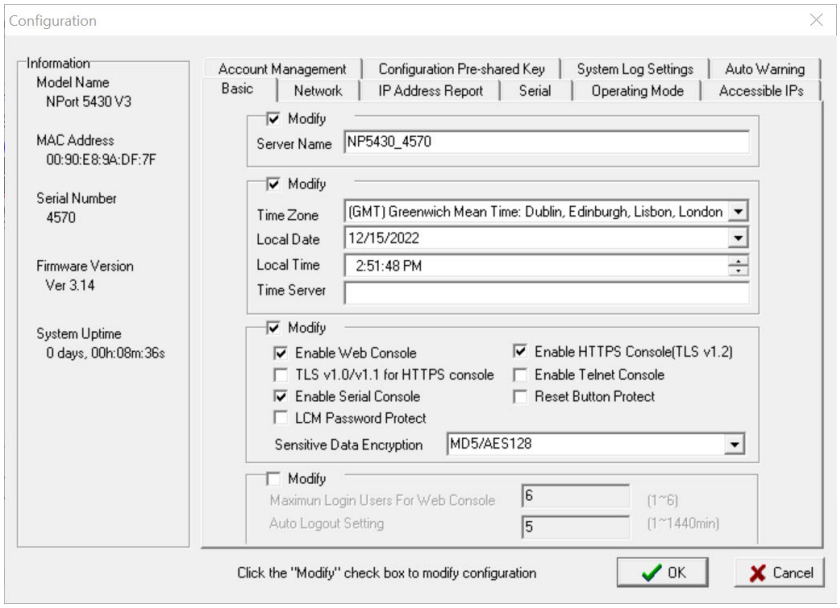


You will then need to change the pre-shared key in **Configuration** to match the encryption password of the configuration file before you can import.

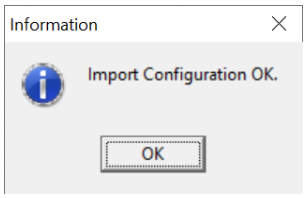
ATTENTION

If you do not remember the password of the encrypted configuration file, there is no alternative way to decrypt the file.

You will be able to confirm the import content before downloading the file.



Press **OK** to start downloading the configuration file. A window will pop up to show that import was successful.



For firmware versions supporting encrypted configuration files, refer to the table below.

Model Name	Firmware version supporting encrypted configuration files.
NPort 5000 Series	
NPort 5400 Series	Firmware v3.11 and up with NPort Administration Suite v1.22 and up
NPort 5600-8-DT Series	Firmware v2.4 and up with NPort Administration Suite v1.22 and up
NPort 5600-8-DTL Series	Firmware v1.3 and up with NPort Administration Suite v1.22 and up
NPort 5600 Series	Firmware v3.7 and up with NPort Administration Suite v1.22 and up
NPort 5000A/IA5000A Series	
NPort 5100A Series	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort 5200A Series	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort 5x50AI-M12 Series	Firmware v1.2 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort IA5150A, NPort IA5250A	Firmware v1.3 and up (Support with both web console and NPort Administration Suite v1.22 or above)
NPort IA5450A	Firmware v1.4 and up (Support with both web console and NPort Administration Suite v1.22 or above)

NOTE

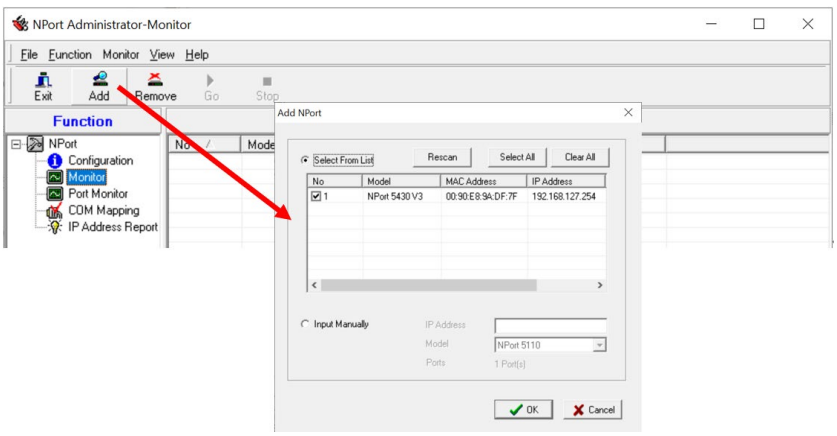
1. You can simultaneously import the same configuration file into multiple NPort units of the same model. To select multiple NPort units, hold down the **Ctrl** key when selecting an additional NPort, or hold down the **Shift** key to select a block of NPort units.
2. If you have an encrypted configuration file, you will need to use the NPort Administration Suite V1.22 or above to import an encrypted configuration file. On the other hand, if your configuration file is non-encrypted, it will also be accepted by the NPort Administration Suite V1.22 or above. (i.e., the NPort Administration Suite will not ask you to key in the **Import Password**.

Monitor

Use the following method to start the Monitor function.

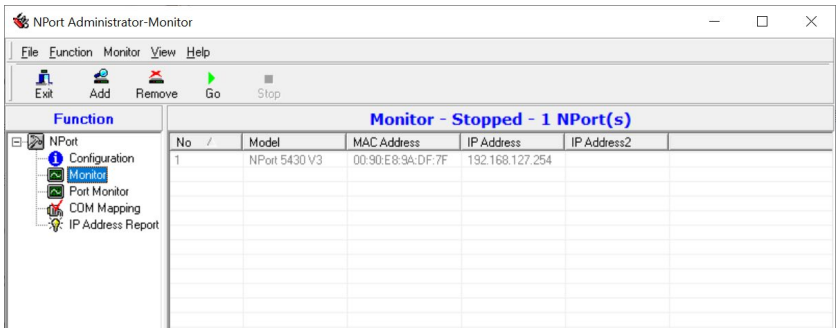
Monitor > Add Target

1. Click **Monitor > Add Target** and select your targets from the list, and then click **OK**.

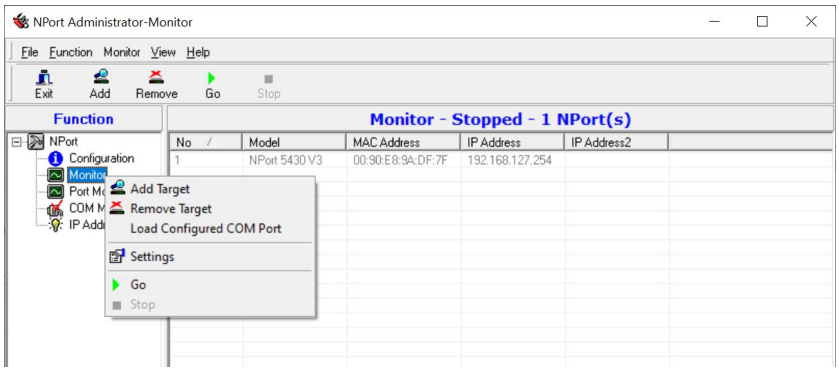


Once the Monitor Function Is Running:

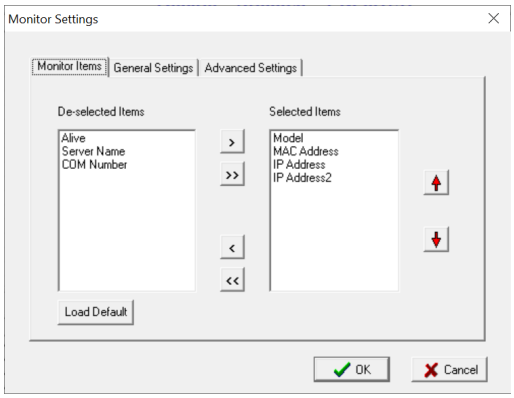
2. The added NPort will appear on the Monitor screen.



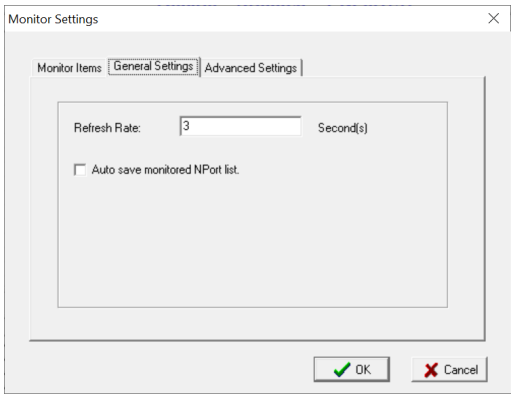
3. Right-click the panel and select **Settings**.



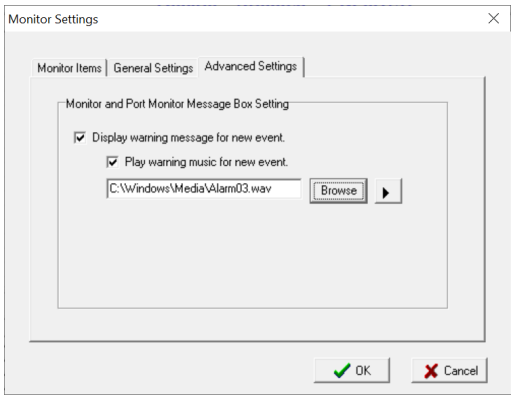
4. Select or deselect **Monitor Items**. Use the single arrowhead buttons to move highlighted items from one box to the other. Use the double arrowhead buttons to move all items from one box to the other.



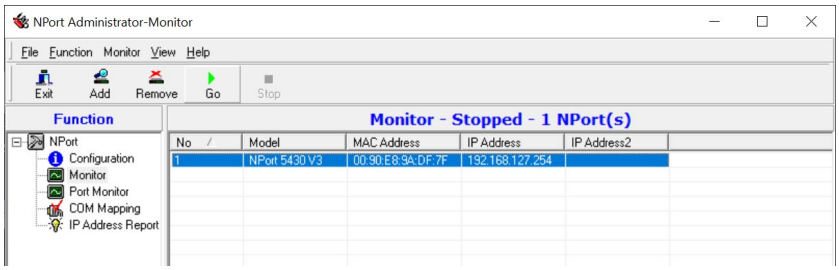
5. Select a **Refresh Rate** (the default is 3 seconds) on the General Settings page.



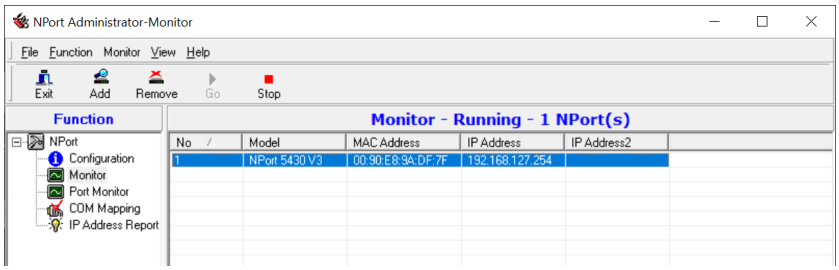
6. On the **Advanced Settings** page, select **Display warning message for new event** and/or **Play warning music for new event**. In the second case, you must enter the path to the WAV file you want to be played. "New event" means that one of the NPort units in the monitor is "Alive" or "Not Alive," or has lost connection with the Monitor program.



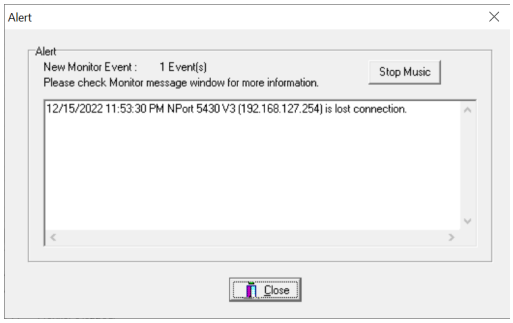
7. Right-click in the NPort list section and select **Go** to monitor the NPort.



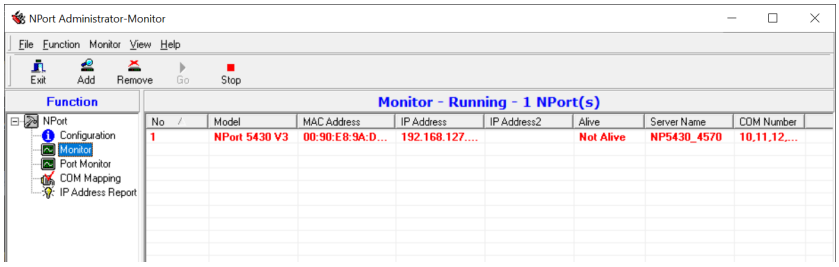
8. For this example, the NPort shown in the list will be monitored.



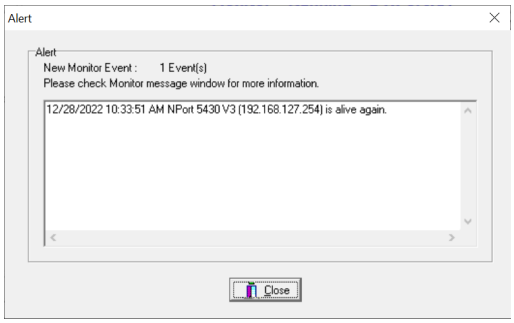
9. When one of the NPort units loses connection with the Monitor program, a warning alert will display automatically. The warning music will be played at the same time.



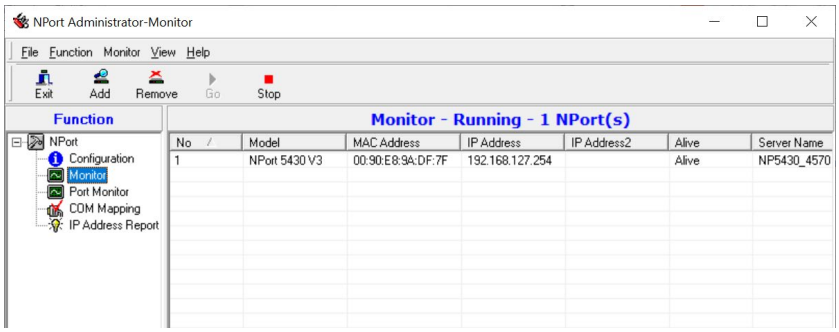
10. In the Monitor screen, you can see that the NPort units that are "Not Alive" are shown in red.



11. If the NPort reconnects, a warning will remind the user that the NPort is now "Alive."

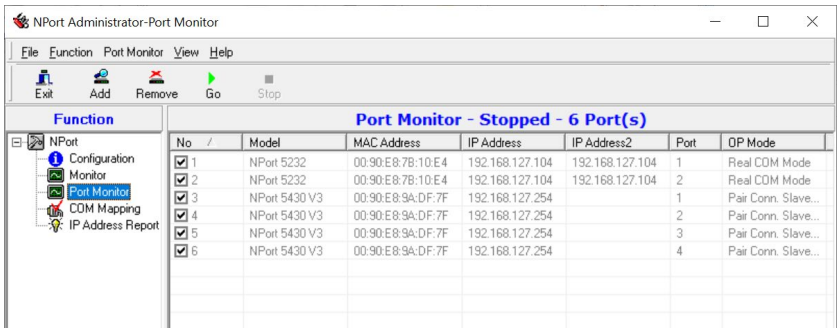


12. The NPort units that were reconnected, and are now “Alive,” will be shown in black.

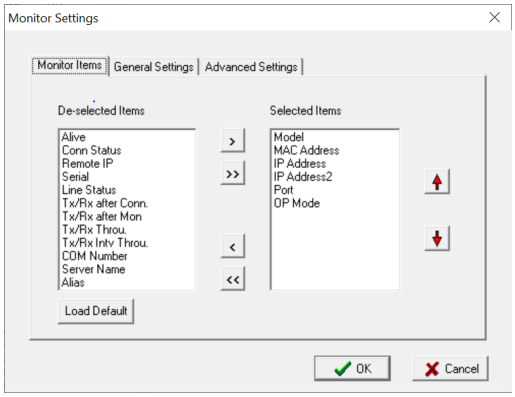


Port Monitor

The process described here is the same as in the previous “Monitor” section. The only difference is that you can select more items under Port Monitor than under Monitor.



Right-click on Port Monitor and select or deselect **Monitor Items**. Use the single arrowhead buttons to move highlighted items from one box to the other or the double arrowhead buttons to move all items in one box to the other.



COM Mapping

This section covers how to map the COM ports on a Windows PC to NPort device ports. The mapping will allow Windows software to access serial devices over the network as if they were local COM devices, providing instant device networking without software migration. COM mapping is supported in Real COM and RFC2217 modes only.

NPort Administration Suite comes with Windows Real COM drivers. After you install the NPort Administration Suite, there are two ways to set up the NPort's serial port as your host's remote COM port.

The first way is with On-line COM Mapping. On-line COM Mapping will make sure that the NPort is connected correctly to the network and then install the driver on the host computer.

The second way is with Off-line COM Installation, without first connecting the NPort to the network. Off-line COM Mapping can decrease the system integrator's effort by solving different field problems. Via offline installation, users can first process software installation for the host, and then install the NPort to different fields.

The following instructions are for device ports operating in Real COM mode. For device ports operating in RFC2217 mode, follow the instructions for your particular driver. Real COM mode also supports TTY port mapping of Linux and UNIX systems.

Use the following procedure to map COM ports:

On-line COM Mapping:

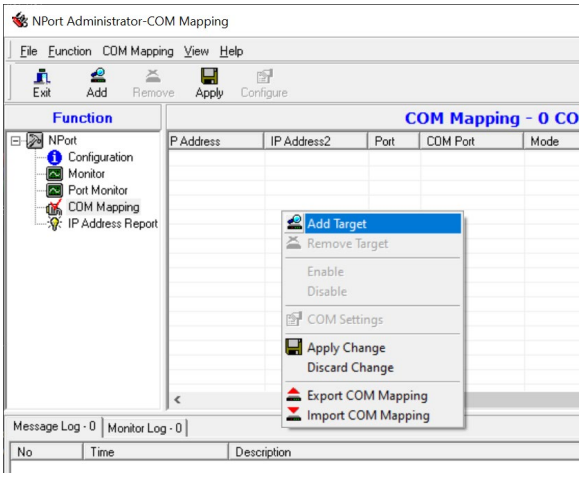
Connect the NPort to the network > Set the NPort's IP address > Map COMs to your host > Apply Change.

Off-line COM Mapping:

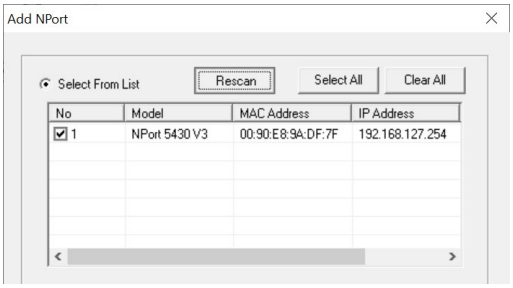
Map COMs to your host > Apply Change > Connect the NPort to the network > Configure the NPort's IP address.

Online COM Mapping

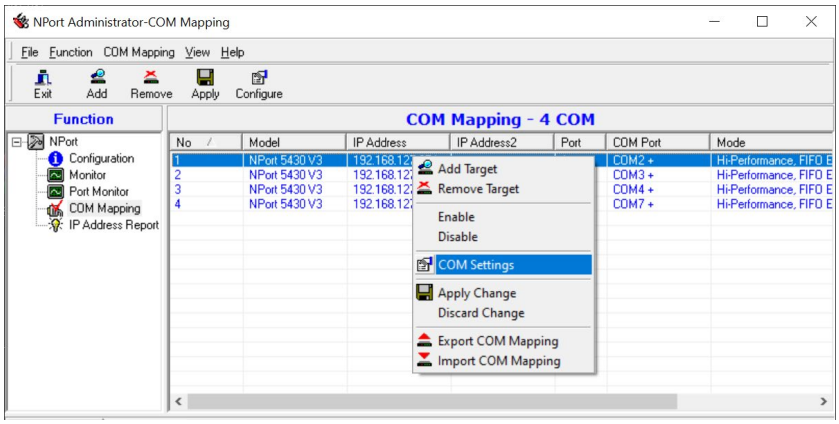
1. Select the **COM Mapping** function group and right-click **Add Target**.



2. Add the target to which you would like to map COM ports, select the NPort to which you would like to map COM ports.

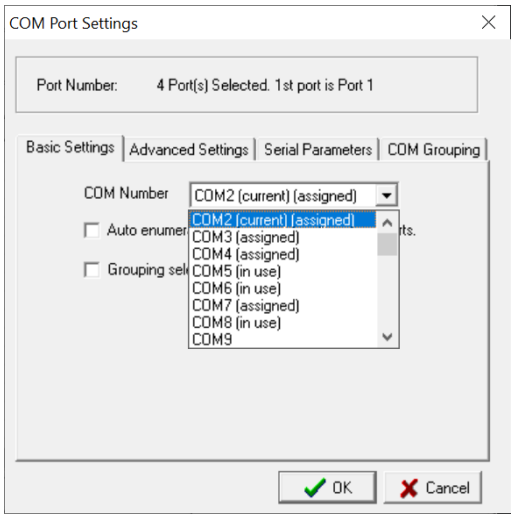


3. COM ports and their mappings will appear in blue until they are "**Apply**". Next, select **COM Settings** to change COM No., default setting, etc.

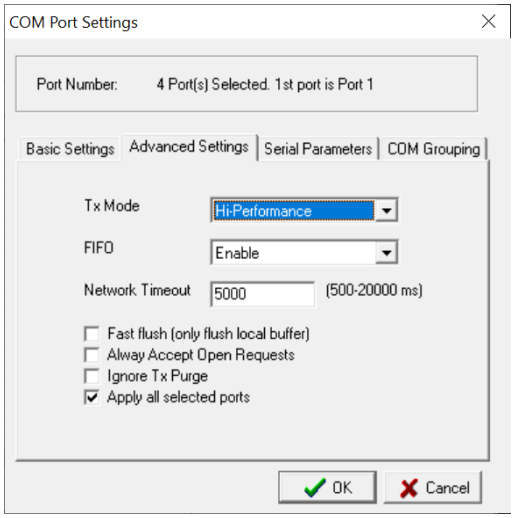


4. Select the **COM Number**.

   COM ports that are "In use" or "Assigned" will also be stated in this drop-down list. If you select multiple serial ports or multiple NPort units, remember to check the **Auto Enumerating COM number for selected ports** function to use the COM No. you select as the first COM No.



Advanced Settings



Tx Mode: Hi-performance mode is the default for Tx mode. In Hi-Performance mode, the driver immediately issues a "Tx Empty" response to the program after sending data to the NPort. Under **Classical Mode**, the driver sends the "Tx Empty" response until all Tx data has been sent out from the NPort and a confirmation is received from the NPort. Classical mode is recommended if you want to ensure that all data is sent out before further processing, however, this mode will cause lower throughput.

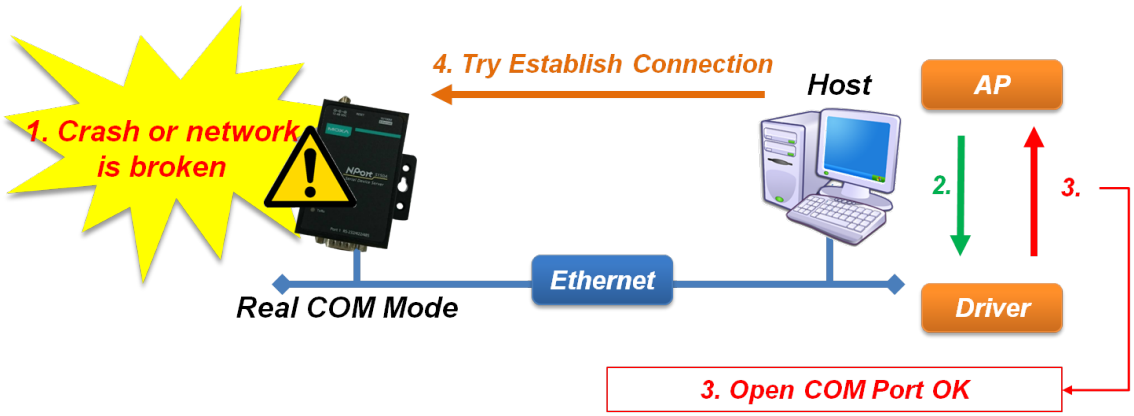
FIFO: Enable/Disable Tx/Rx. If disabled, the NPort will send one byte each time the Tx FIFO becomes empty; and a Rx interrupt will be generated for each incoming byte. This will cause a faster response and lower throughput. If you want to use XON/XOFF flow control, we recommend setting FIFO to Disable.

Network Timeout: Specifies when an open, close, or serial parameter change operation will time out.

Fast Flush (only flush local buffer)

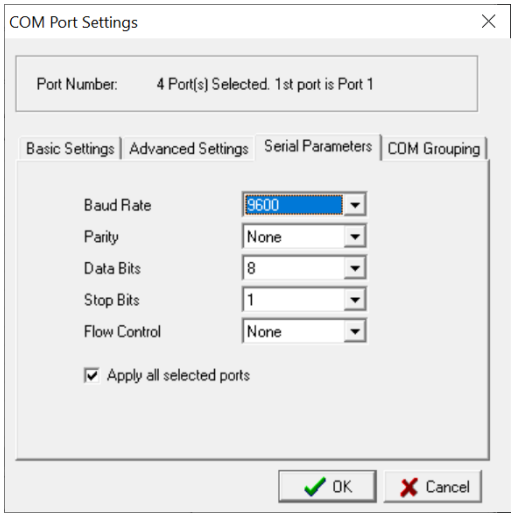
- We have added one optional Fast Flush function to Moxa's new NPort Real COM driver. **NPort Administrator Suite for NPort** adds it after version 1.2.
- For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. With our design, after the program uses this Purge Comm() function, the NPort driver will keep querying the NPort's firmware several times to make sure there is really no data queued in the NPort firmware buffer, rather than just flushing the local buffer. This kind of design is used because of some special considerations. However, it might take more time (on the order of several hundred milliseconds) than a native COM1, because it needs to work via Ethernet. That's why the native COM ports on the motherboard can work fast with this function call, but the NPort requires much more time. To accommodate other applications that require a faster response time, the new NPort driver implements a new "Fast Flush" option. Note that, by default, this function is disabled.
- To begin with, make sure there are some "PurgeComm()" functions being used in your application program. In this kind of situation, you might find that your NPort exhibits a much poorer operation performance than when using the native COM1 port. Once you have enabled the "Fast Flush" function, you can check to see if there has been an improvement in performance.
- By default, the optional "Fast Flush" function is disabled. If you would like to enable this function, from the "NPort Administrator," double click the COM ports that are mapped to the NPort, and then select the "Fast Flush" checkbox. You should find that when "Fast Flush" is enabled, the NPort driver will work faster with "PurgeComm()."

Always Accept Open Requests: Even the driver cannot establish the connection to NPort, user's software still can open the mapped COM port just like an onboard COM port.

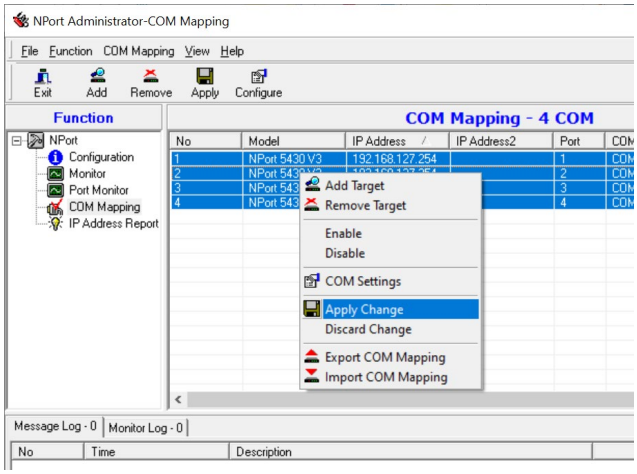


Ignore TX Purge: The application can use Win32 API PurgeComm to clear the output buffer and end outstanding overlapped write operations. Select **Ignore TX Purge** if you do not want the output buffer to be purged.

5. The Serial Parameter settings shown here are the default settings when the NPort is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.

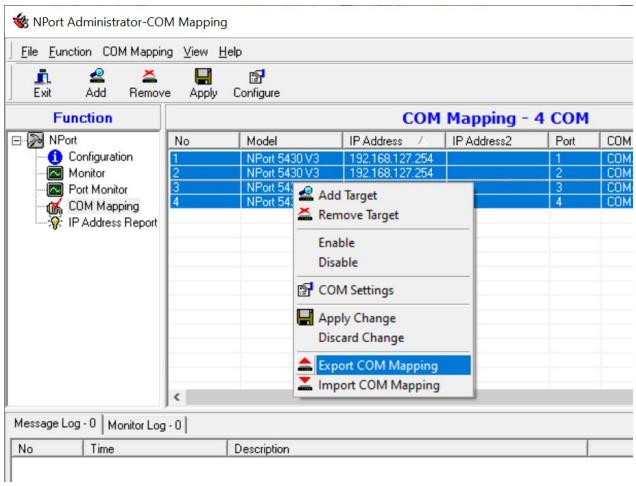


6. After setting the COM Mapping, remember to select **Apply Change** to save the information in the host system registry. The host computer cannot use the COM port until after **Apply Change** is selected.



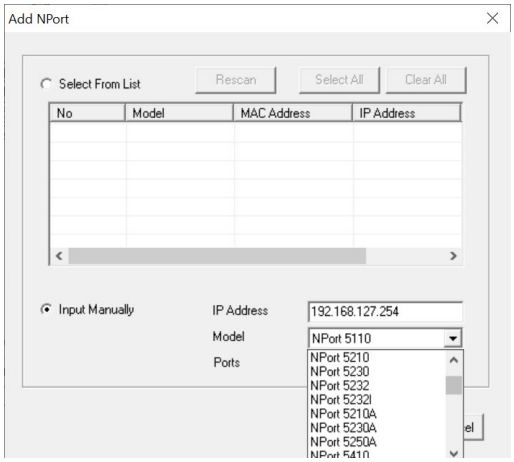
Or, select **Discard Change** to if you wish NOT to save the COM Mapping information to the host.

7. To save the configuration to a text file, select **Export COM Mapping**. You will then be able to import this configuration file to another host and use the same COM Mapping settings in the other host.

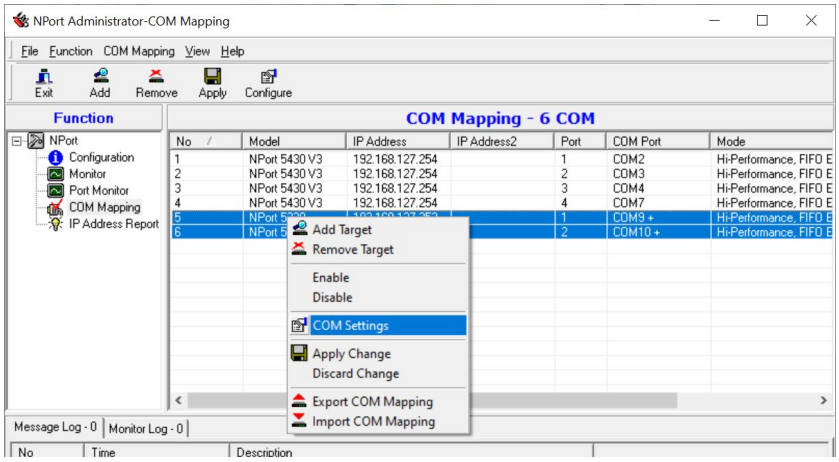


Offline COM Mapping

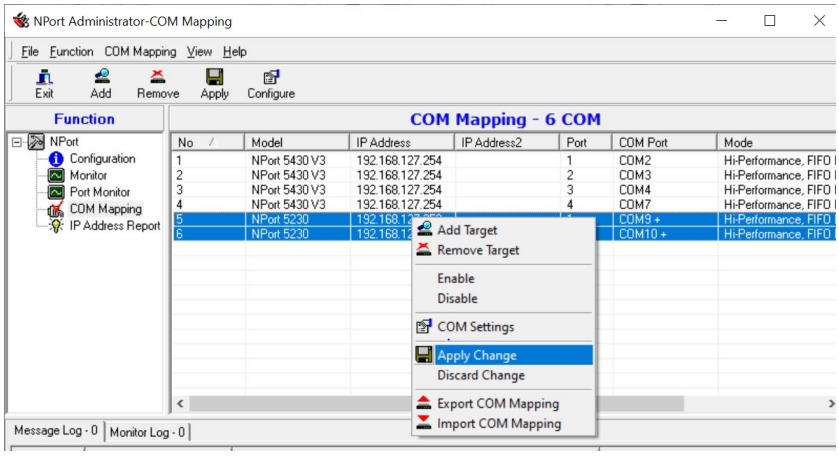
1. Add a target by inputting the IP address and selecting the Model Name without physically connecting the NPort to the network.



2. Change the port settings as needed.



3. Right-click in the NPort list section and select **Apply Change**.



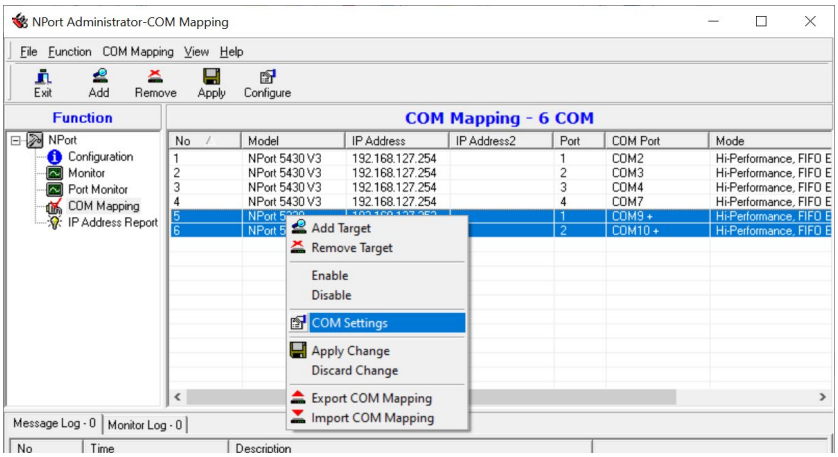
COM Grouping

The **COM Grouping** function simulates the multidrop behavior of serial communication over an Ethernet network. COM Grouping allows you to create a COM Group and redirect data from it to several physical COM ports on NPort device servers. With COM Grouping, you can control multiple physical serial ports simultaneously by operating only one COM port.

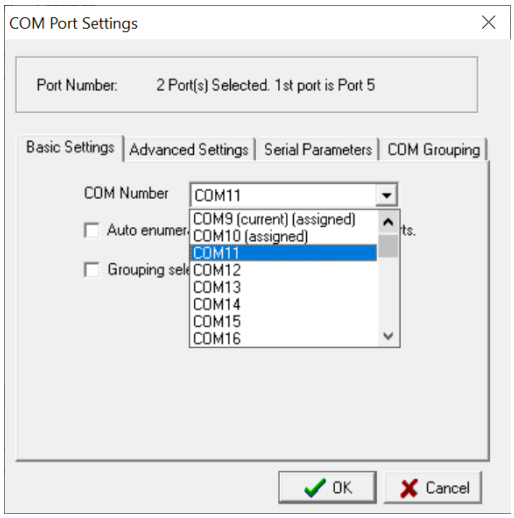
Creating a COM Group

Follow the steps below to add multiple COM ports into one group:

1. Select serial port(s) for the group that you are going to create, and right-click to select **COM Settings**.

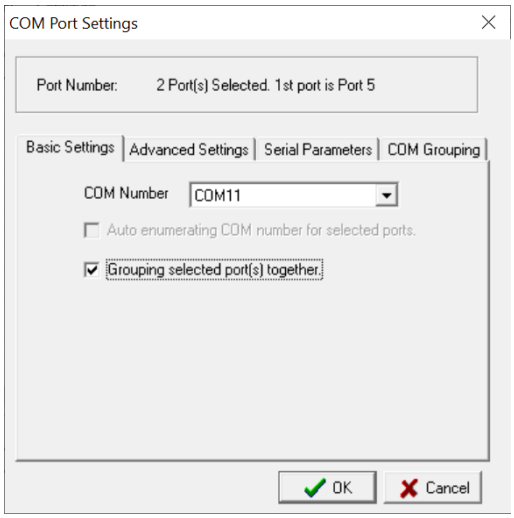


2. Select a COM number for this COM group. You may select one port already assigned to a member of the COM Group. However, once the COM Group is configured, all the original COM number(s) within the group will be released simultaneously.

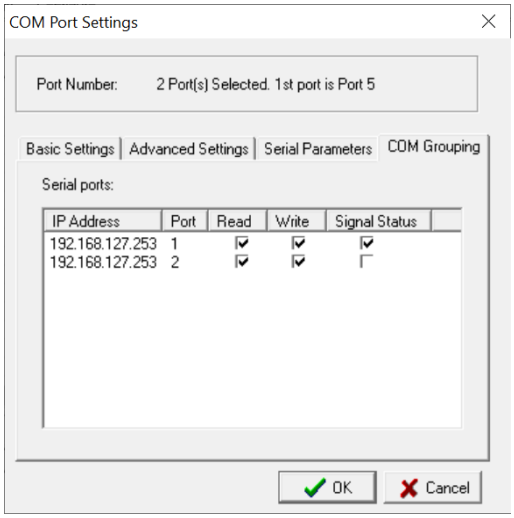


> **ATTENTION**
>
> The COM Grouping function only supports Windows NT, 2000, and later. The maximum number of ports for each group is 32.

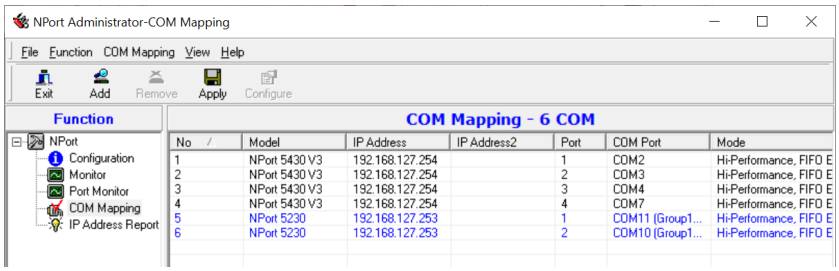
3. Select the **Grouping selected port(s) together** checkbox.



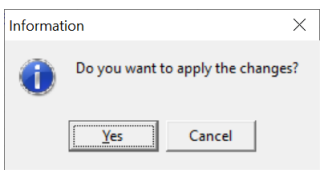
4. On the **COM Grouping** page, you can set "Read" and "Write" permissions for every serial port. It is necessary to set **Signal Status** to control the data transmission with specified control signals (e.g., DTR/RTS). You can assign one serial port which signals will be considered by the COM Group.



5. Click **OK**, and confirm the serial ports that were assigned. The COM Port column shows that your selected ports are labeled as part of a "Group." You will be able to view the serial ports that were assigned to and removed from the Group. Click **Apply** to apply the settings.



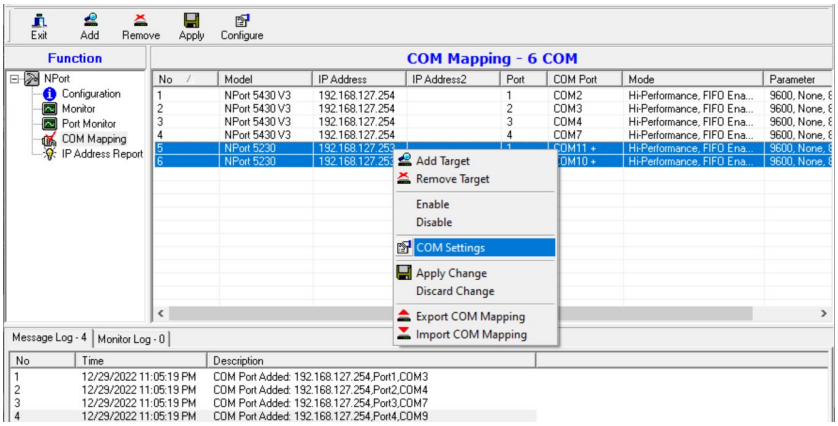
6. Finally, click **Yes** to confirm.



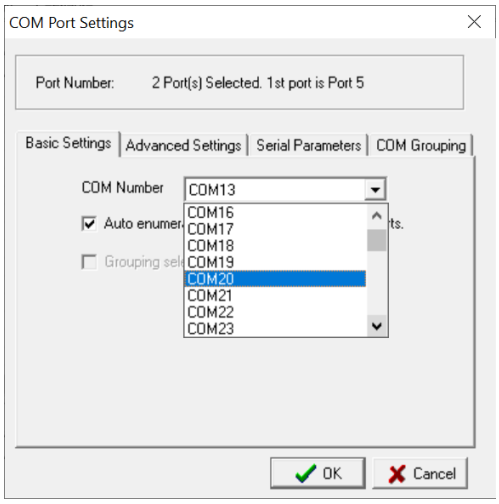
Deleting a COM Group

Follow the steps below to delete a COM Group and then auto-assign COM numbers for each port in the Group:

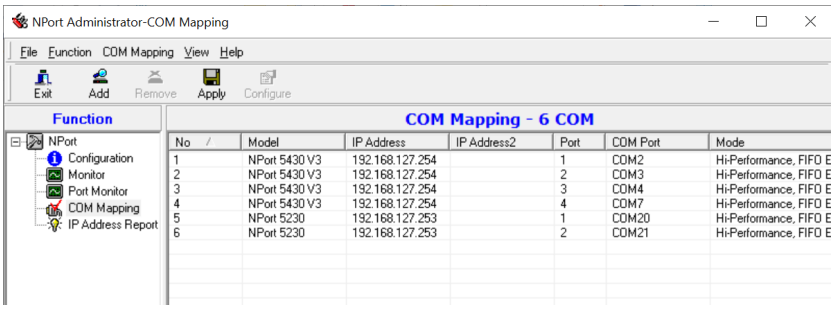
1. Select all serial ports in the Group you are deleting and then right-click to select **COM Settings**.



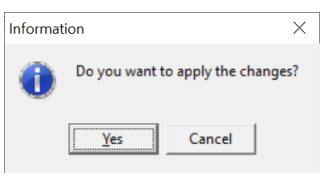
2. Uncheck Grouping selected port(s) together first then select a COM number for this COM group and check the **Auto enumerating COM number for selected ports** to use the COM number you select as the first starting COM number, and then click **OK**.



3. You can view the serial ports that were assigned to and removed from the Group. Click **Apply** to apply the settings.



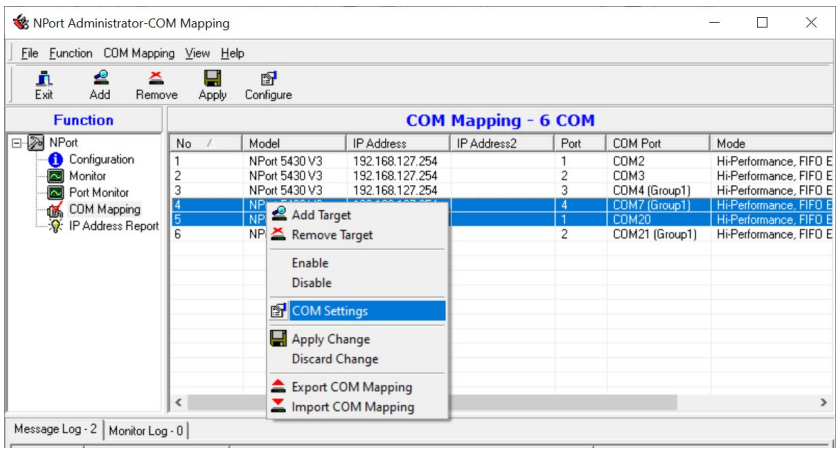
4. Finally, click **Yes** to confirm.



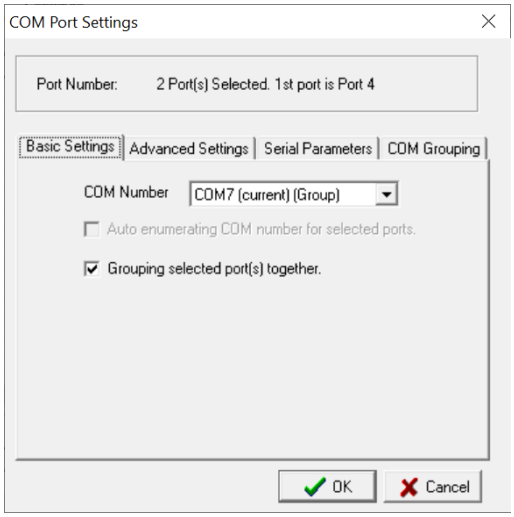
Adding an Additional Port to a COM Group

Follow the steps below to add a serial port into an existing COM Group:

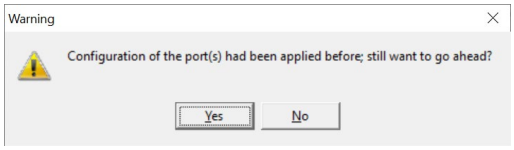
1. Select the serial port and the COM Group that you wish to bind and right-click to select **COM Settings**.



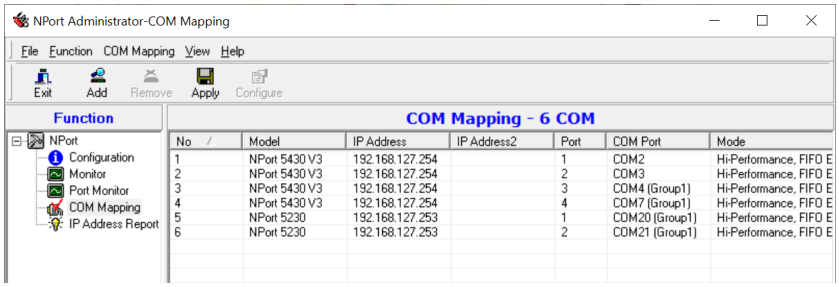
2. Make sure **Grouping selected port(s) together** is checked and then click **OK**.



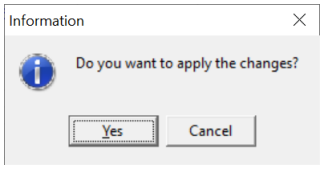
3. Confirmation for the changes, click **Yes** to apply the settings.



4. You can view the serial ports that were assigned to and removed from the Group. Click **Apply** to apply the settings.



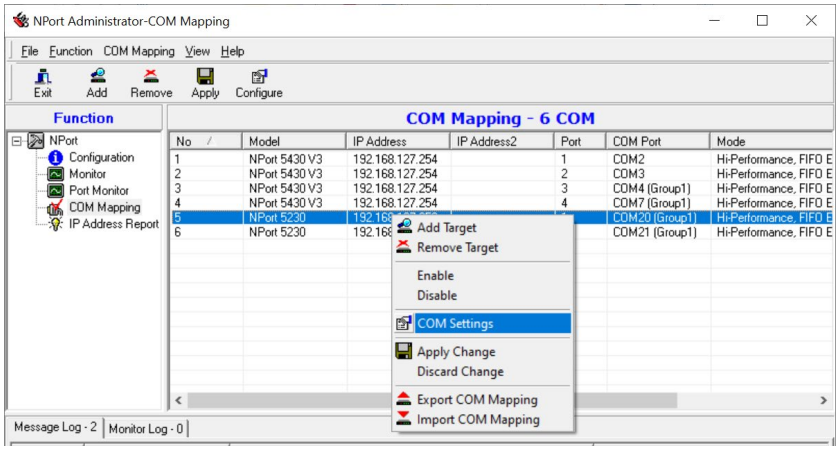
5. Finally, click **Yes** to confirm.



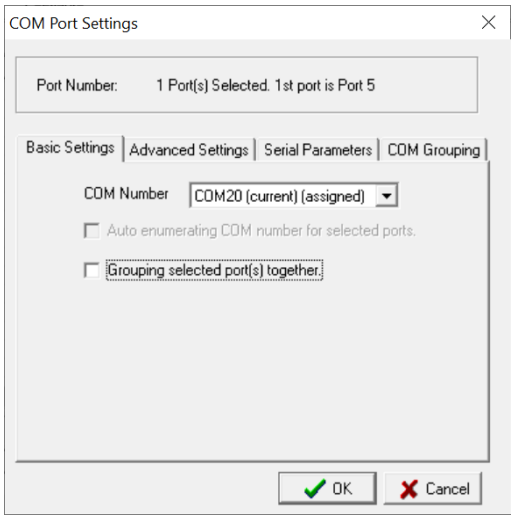
Removing a Port from a COM Group

Follow the steps below to remove a serial port from a COM Group:

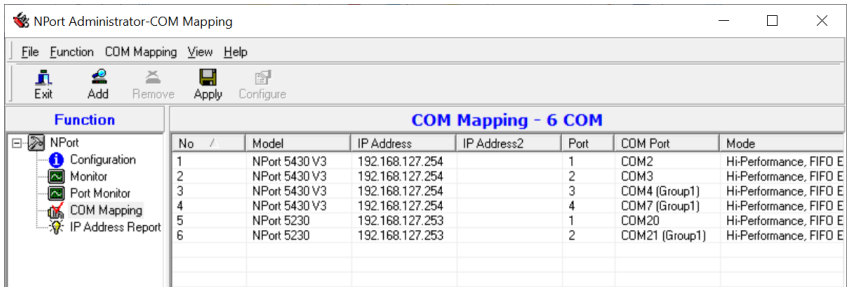
1. Select a serial port in the Group and right-click to select **COM Settings**.



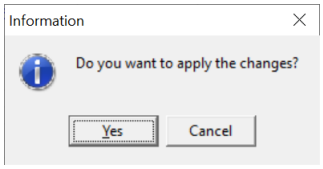
2. Select a COM number that is not in use or assigned to a group and click **OK**.



3. You can view the serial ports that were assigned to and removed from the group. Click **Apply** to apply the settings.



4. Finally, click **Yes** to confirm.



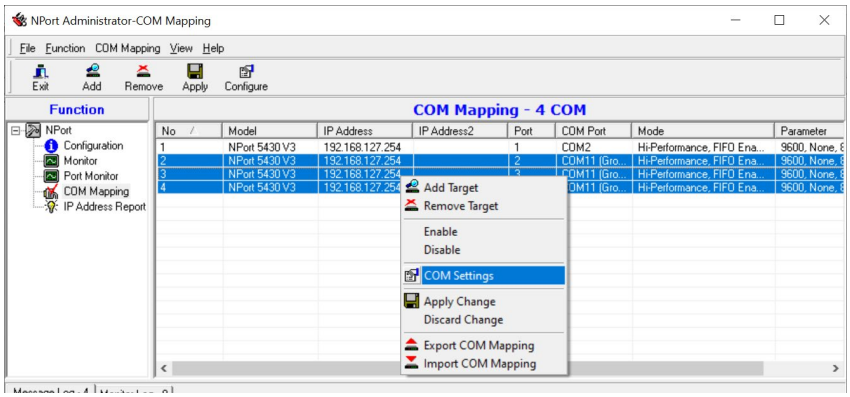
Modify Ports in a COM Group

For version v4.0 and after, to change COM number of a specific serial port in a COM group, you need to ungroup the COM group and then proceed with COM port re-assignment as explained in **On-line COM Mapping** and **Off-line COM Mapping** section.

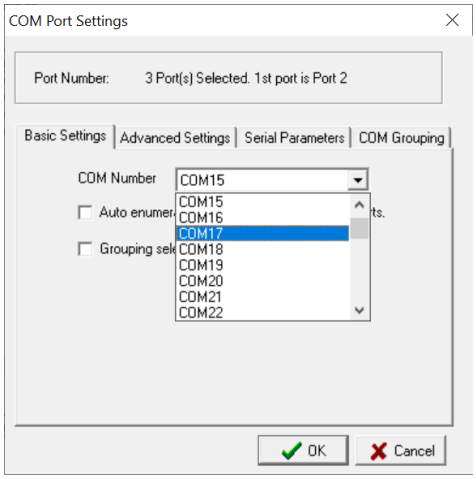
For version before v4.0, the following subsections we examine three ways in which the serial ports in a COM group can be changed:

Changing the COM Number of a COM Group

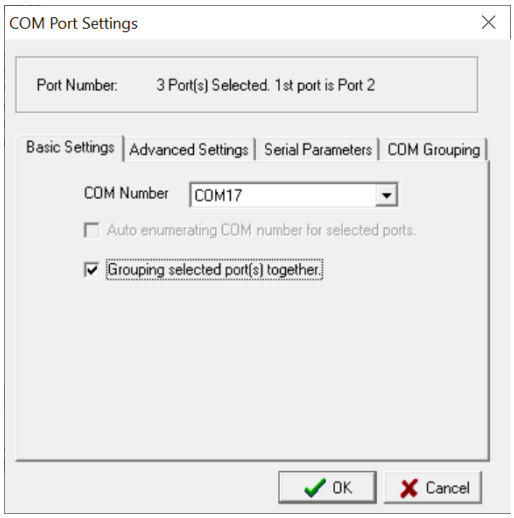
1. Select all serial ports in the group and right-click to select **COM Settings**.



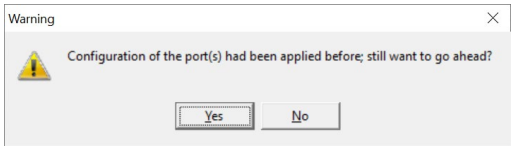
2. Select a COM number that is not in use or assigned to a group.



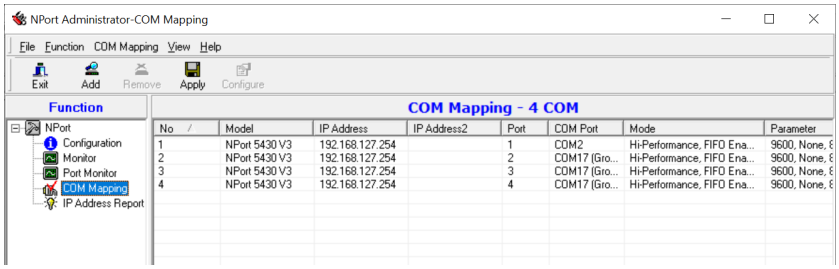
3. Select the **Grouping selected port(s) together** checkbox and then click **OK**.



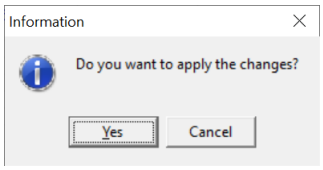
4. Confirmation dialogue would appear, click **Yes**.



5. You can view the serial ports that were assigned to and removed from the group.
6. Click **Apply** to apply the settings.

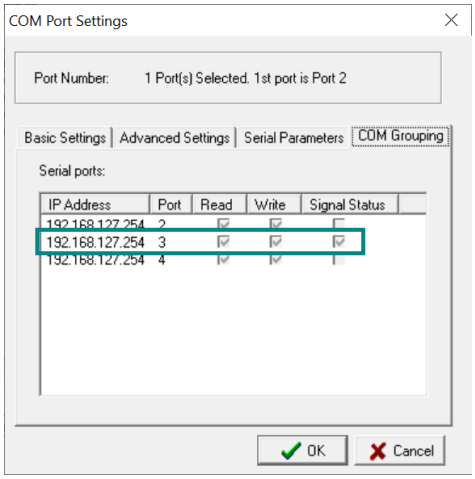


7. Finally, click **Yes** to confirm.

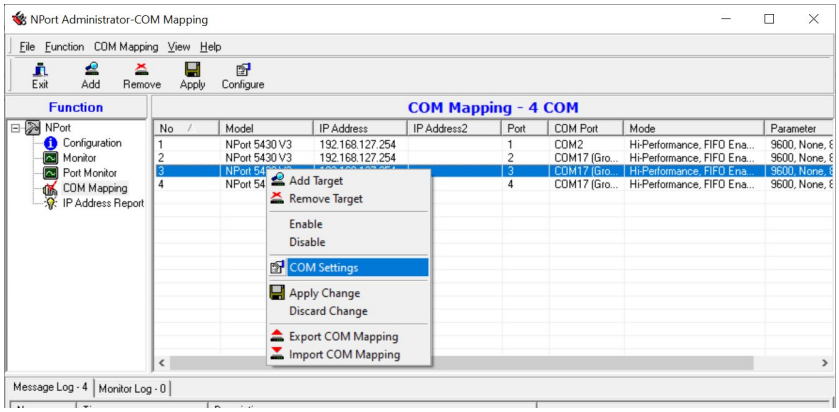


Changing Advanced Settings and Serial Parameters of the COM Group

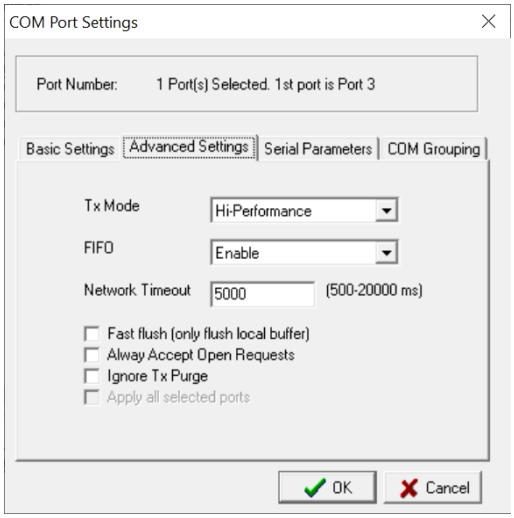
1. Click any COM port in **COM Group** and right-click **COM Settings** to check the port specified on the **COM Grouping** page as the signal port.

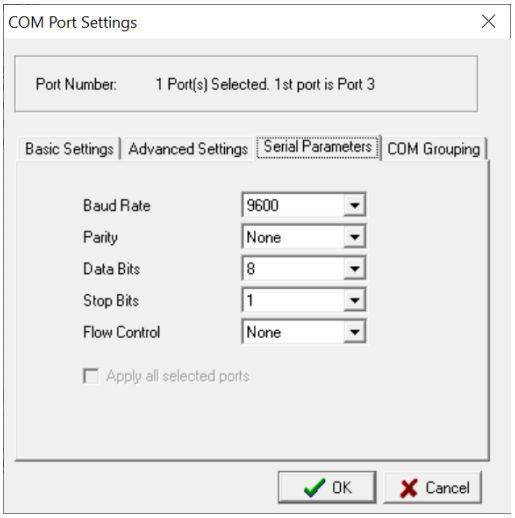


2. Select the ”Signal Status” controlled port and then right-click and select **COM Settings**.



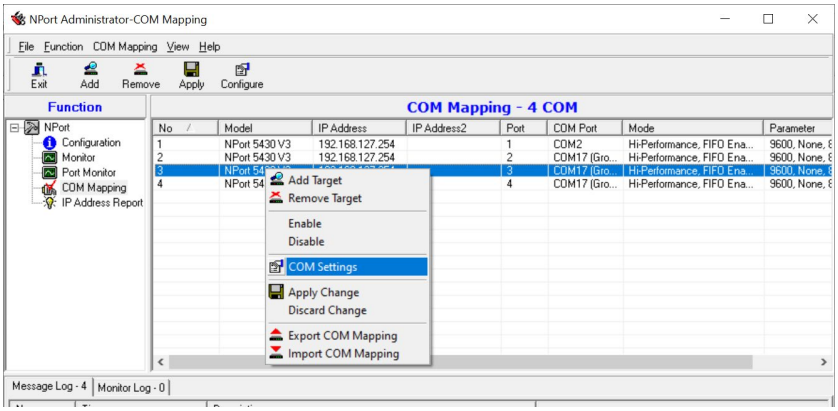
3. The **Advanced Settings** and **Serial Parameters** pages will be available for modification.



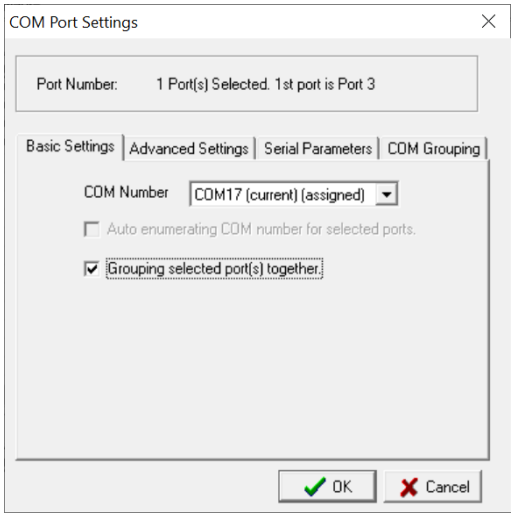


Changing the Serial Port Specified as a Signal Port for the COM Group

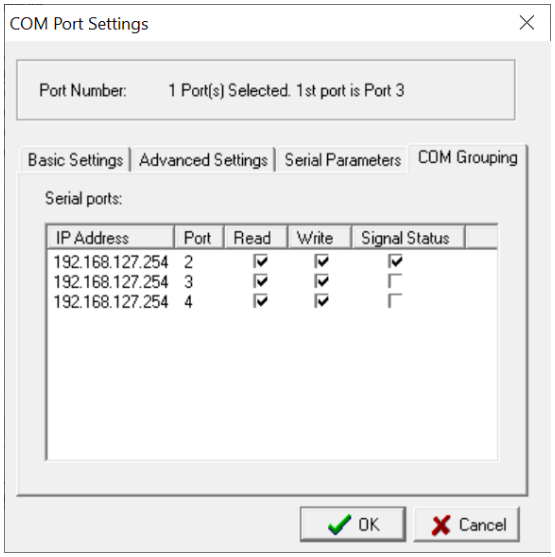
1. Select a serial port in the group and then right-click and select **COM Settings**.



2. Check the **Grouping selected port(s) together** checkbox.



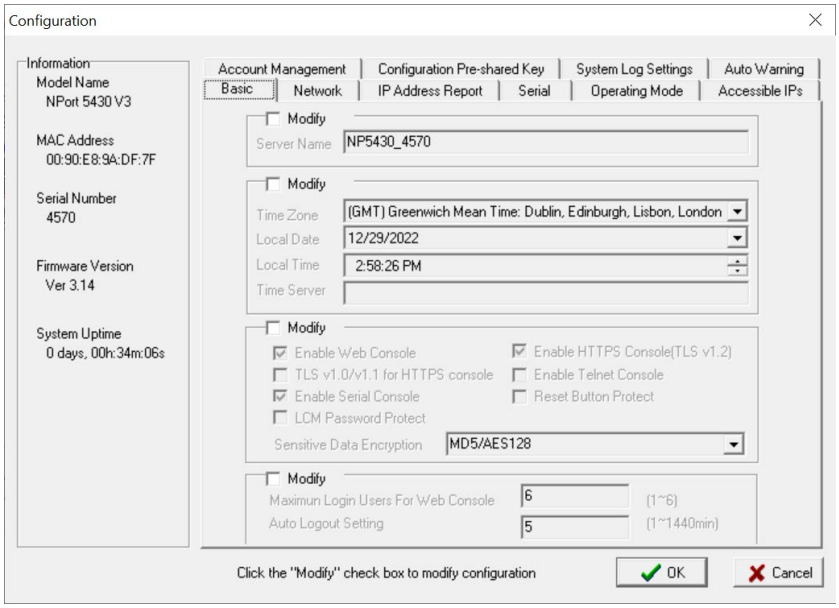
3. On **COM Grouping** page, you can specify one serial port whose signals will be considered by the COM group and change the Read/Write status for each serial port.



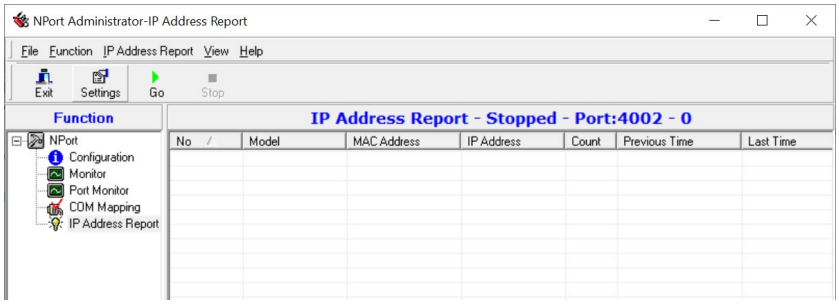
IP Address Report

When the NPort is used in a dynamic IP environment, users must spend more time on IP management tasks. NPort serial device servers help by periodically reporting their IP address to the IP location server, in case, the dynamic IP has changed.

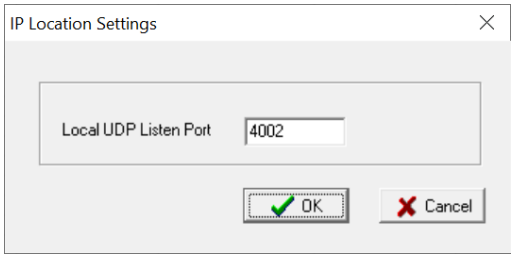
1. Configure the NPort with Dynamic IP settings (DHCP, BOOTP, or DHCP/BOOTP). Assign the remote Auto IP report server's IP address and UDP port.



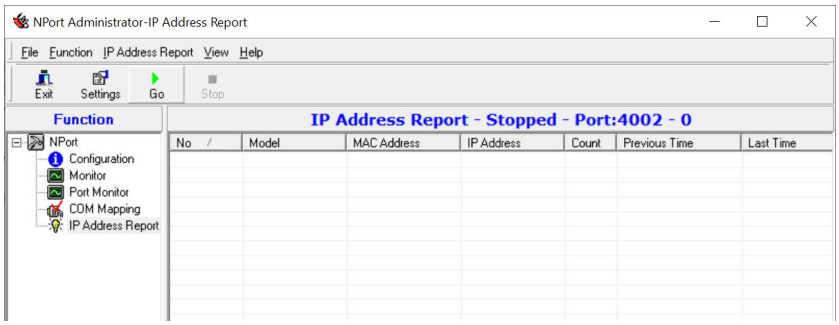
2. In **Administrator function groups** pane, select the **IP Address Report**, and click the **Settings** on the toolbar or right-click to select **Settings**.



3. Configure the Local Listen Port to be the same as the NPort's "Auto report to UDP port" setting.



4. Click **Go** on the toolbar or right-click to receive the Auto IP address report from the NPort.



NOTE

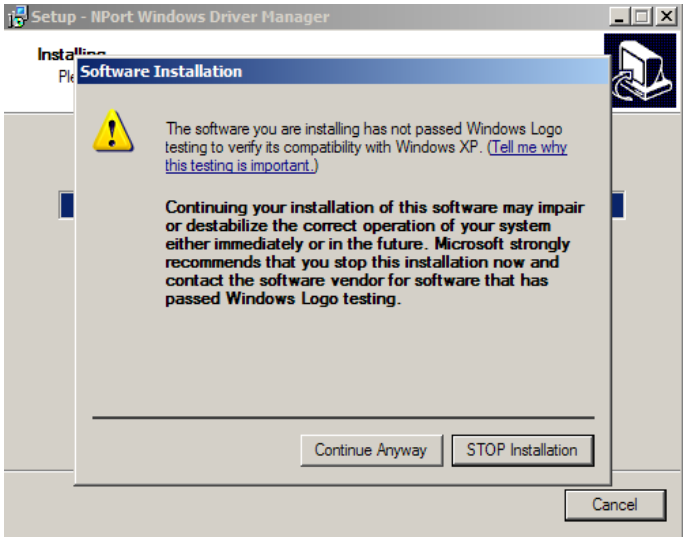
You can simultaneously change the configurations of multiple NPort units that are of the same model. To select multiple NPort units, hold down the Ctrl key when selecting additional NPort units, or hold down the Shift key to select a group of NPort units.

Configuring by NPort Windows Driver Manager

NPort Windows Driver Manager is intended for use with NPort 5000 serial ports that are set to Real COM mode. The software manages the installation of drivers that allow you to map unused COM ports on your PC to serial ports on the NPort 5000. When the drivers are installed and configured, devices that are attached to serial ports on the NPort 5000 will be treated as if they were attached to your PC's own COM ports.

Double-click on the **NPort Windows Driver Manager** icon when you download it from the Moxa website to follow the installation steps to complete the setup.

On Windows XP, the installer will display a message that the software has not passed Windows Logo testing. This is shown:



Click **Continue Anyway** to finish the installation.

Using NPort Windows Driver Manager

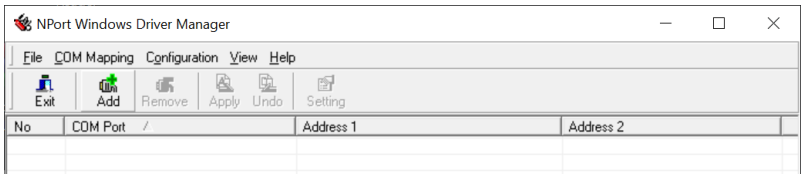
NOTE

You will need to install the latest of Visual Studio in order to run COM mapping.

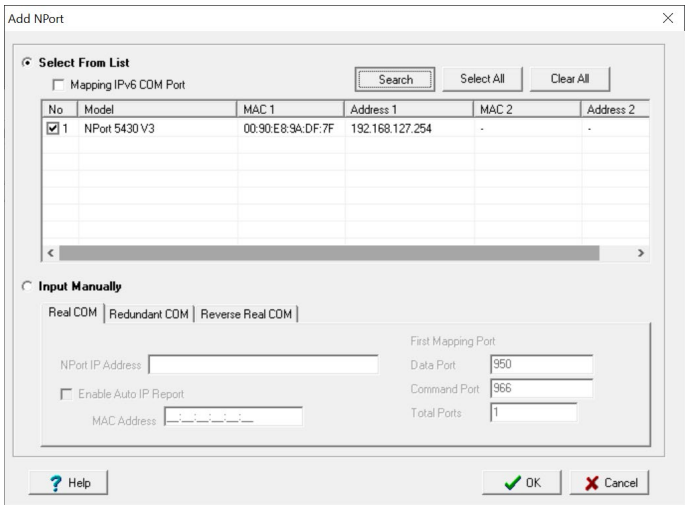
Real COM Mode

After you install NPort Windows Driver Manager, you can set up the NPort 5000's serial ports as remote COM ports for your PC host. Make sure that the serial port(s) on your NPort 5000 are set to Real COM mode when mapping COM ports with the NPort Windows Driver Manager.

1. Launch the **NPort Windows Driver Manager**
2. Click the **Add** icon



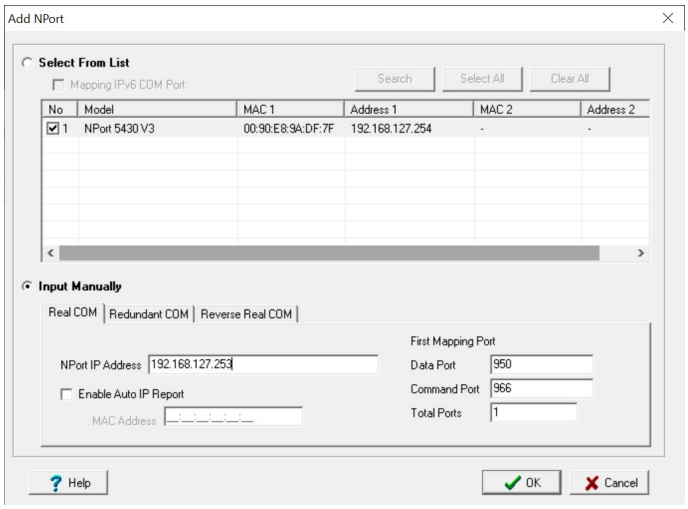
3. Click **Search** to search for NPort device servers. From the list that is generated, select the server to which you will map COM ports, and then click **OK**. The default IPv4 address will be changed to the IPv6 address when **Mapping IPv6 COM Port** is checked.



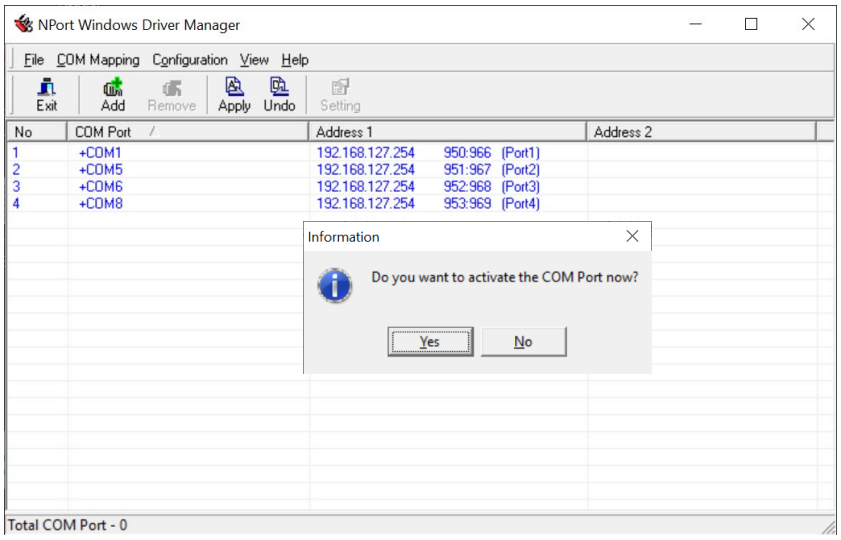
NOTE

Only the NPort 6000 models support IPV6.

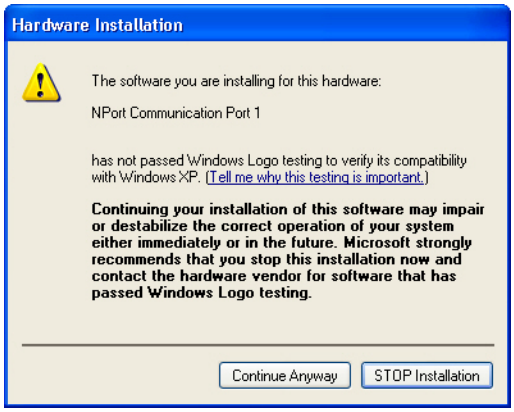
4. Alternatively, you can select **Input Manually** and then manually enter the NPort IP Address, 1st Data Port, 1st Command Port, and Total Ports to which COM ports will be mapped. Click **OK** to proceed to the next step. Note that the Add NPort page supports FQDN (Fully Qualified Domain Name), in which case the IP address will be filled in automatically.



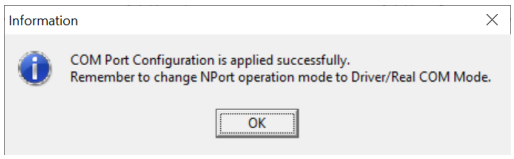
5. COM ports and their mappings will appear in blue until they are activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not use the COM port until the COM ports are activated. Click **Yes** to activate the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

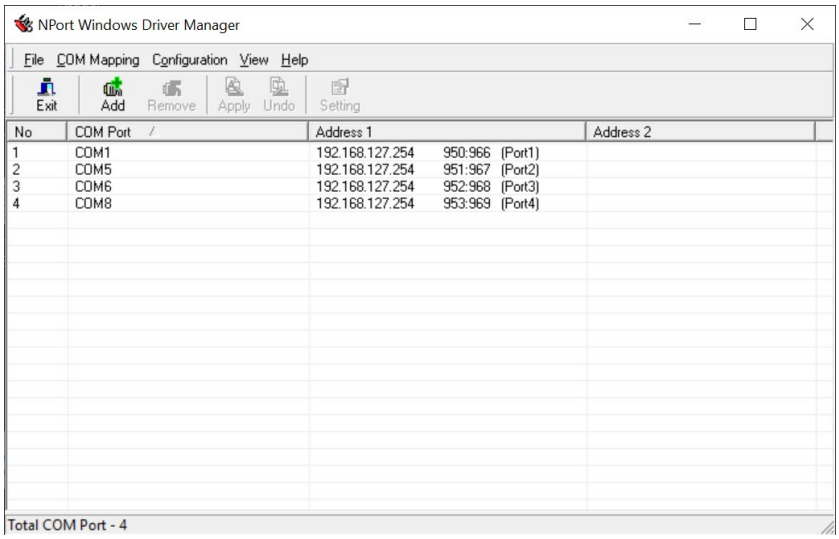


6. In Windows XP, a message is displayed during activation of each port, showing that the software has not passed Windows Logo certification. Click **Continue Anyway** to proceed.



7. A confirmation dialogue would show upon activation is success, and all ports that have been activated will change to black.

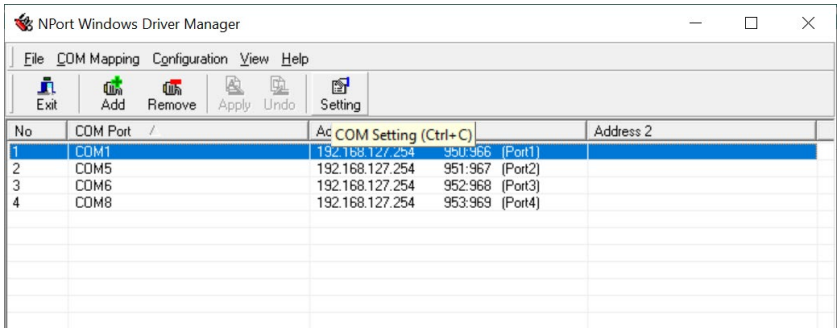




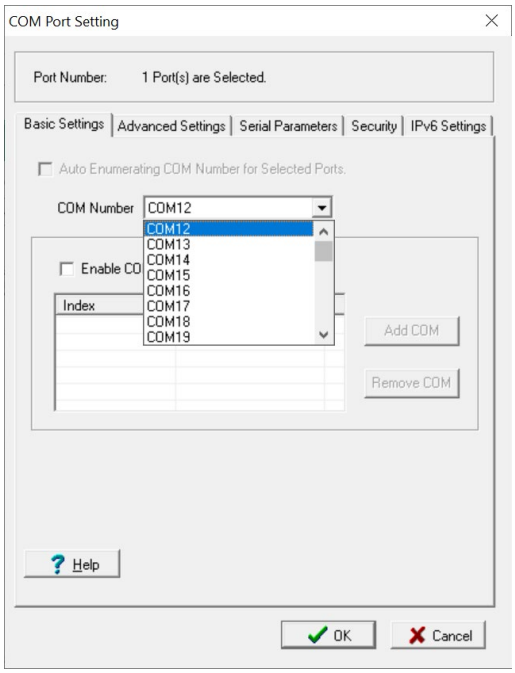
> **NOTE**
>
> The **Redundant COM Mode** and **Reverse Real COM Mode** are available for the NPort 6000 models only.

Configure the mapped COM ports

For Real COM Mode, to reconfigure the settings for a particular serial port on the NPort 5000, select the row corresponding to the desired port and then click the **Setting** icon.



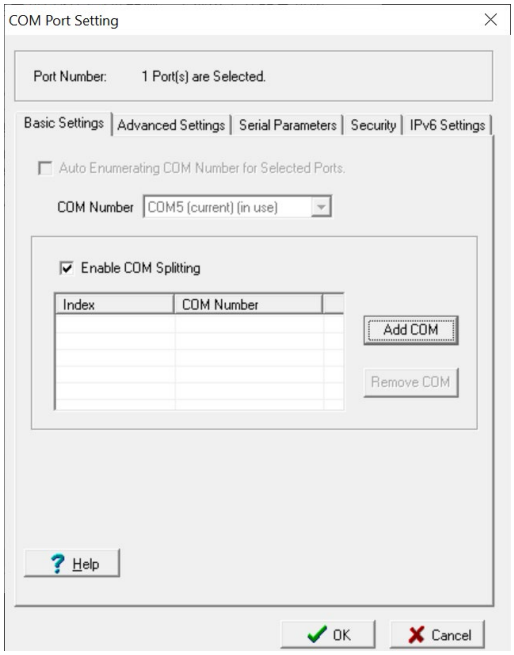
On the **Basic Setting** window, use the **COM Number** drop-down list to select a COM number to be assigned to the NPort 5000's serial port that is being configured. When you have selected multiple ports, you may select the **Auto Enumerating COM Number for Selected Ports** option to automatically assign available COM numbers in sequence to selected serial ports. Note that ports that are "in use" will be labeled accordingly.



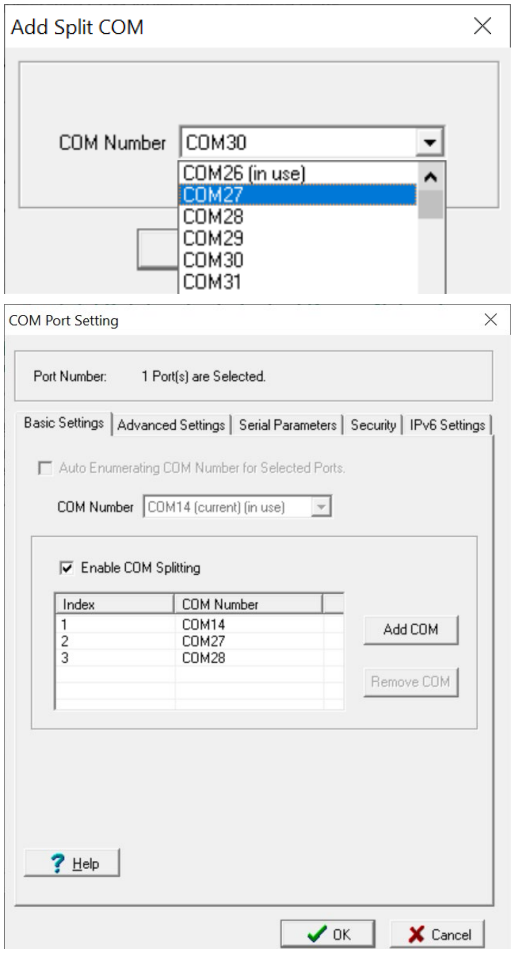
COM Splitting

The "COM Splitting" allows you to redirect data from the same serial port to several virtual COM ports on your computer. Remember, you need to adjust **Max Connection** in your NPort. For example, if you split to two COM ports, **Max Connection** needs to be adjusted to 2. Refer to the **Max Connection** introduction in the User Manual regarding configuration and number limitation.

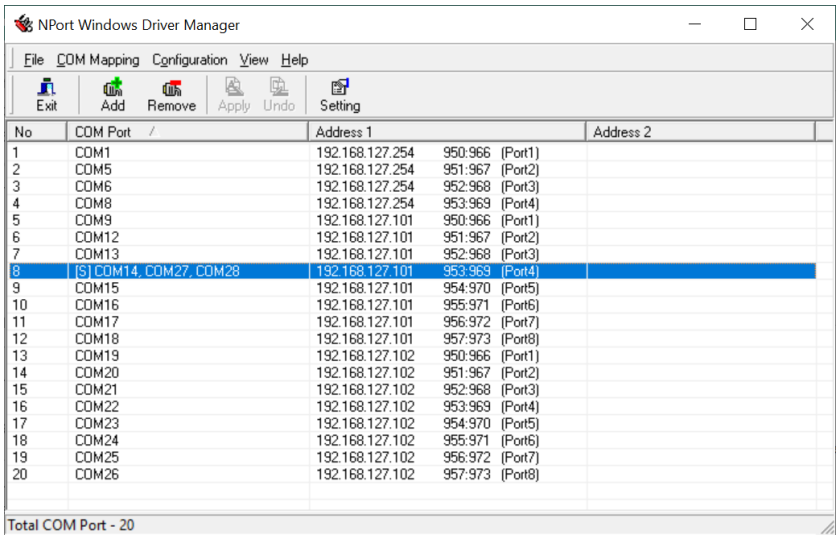
1. **Enabled COM Splitting**



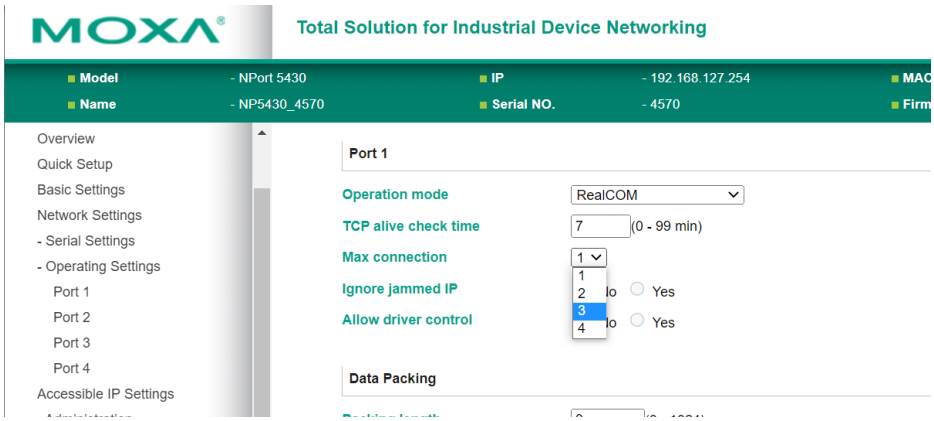
2. **Add COM** to select target COM ports for splitting; the COM port must be available.



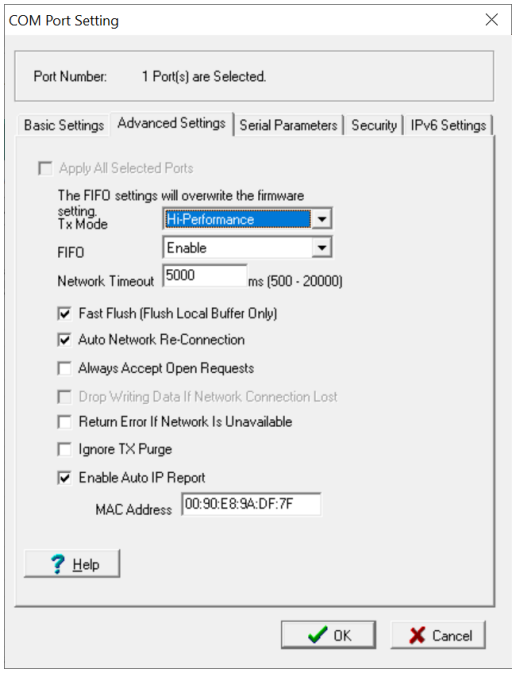
3. After pressing OK, check if the COM ports you just selected are grouped together. Click Apply to save the change.



4. Adjust Max Connection number in the NPort's Operating Settings to match the unit's number in the COM Split Group



Click the **Advanced Setting** tab to change Tx Mode, FIFO, and Flash Flush.



Tx Mode

Hi-Performance is the default for Tx mode. After the driver sends data to the NPort 5000, the driver immediately issues a "Tx Empty" response to the program. Under **Classical** mode, the driver will not send the "Tx Empty" response until after confirmation is received from the NPort 5000's serial port. This causes lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO

If FIFO is **Disabled**, the NPort 5000 will transmit one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will cause a faster response and lower throughput.

Network Timeout

Use this option to prevent blocking if 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. After a program uses this PurgeComm() function, the NPort driver continues to query the NPort's firmware several times to make sure no data is queued in the NPort's firmware buffer, rather than just flushing the local buffer. This design is used to satisfy some special considerations. However, it may take more time (about several hundred milliseconds) than a native COM1 because of the additional time spent communicating across the Ethernet. Therefore, PurgeComm() works significantly faster with native COM ports on the PC than with mapped COM ports on the NPort 5000. In order to accommodate other applications that require a faster response time, the new NPort driver implements a new Fast Flush option. By default, this function is enabled.

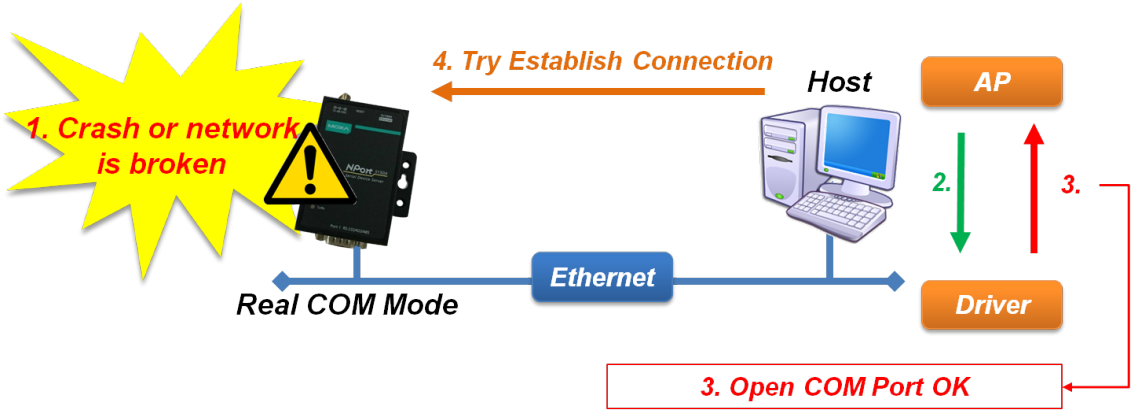
If you have disabled Fast Flush and find that COM ports mapped to the NPort 5000 perform markedly slower than when using a native COM port, try to verify if "PurgeComm()" functions are used in your application. If so, try enabling the Fast Flush function and see if there is a significant improvement in performance.

Auto Network Re-Connection

With this option enabled, the driver will repeatedly attempt to re-establish the TCP connection if the NPort 5000 does not respond to background "check-alive" packets.

Always Accept Open Requests

When the driver cannot establish a connection with the NPort, the user's software can still open the mapped COM port, just like an onboard COM port.



Return Error If Network Is Unavailable

If this option is disabled, the driver will not return any errors even when a connection cannot be established to the NPort 5000. With this option enabled, calling the Win32 Comm function will cause the error return code "STATUS_NETWORK_UNREACHABLE" when a connection cannot be established to the NPort 5000. This usually means that your host's network connection is down, perhaps because of a cable being disconnected. However, if you can reach other network devices, maybe the NPort 5000 is not powered on or is disconnected. Note that **Auto Network Re-Connection** must be enabled to use this function.

Drop Writing Data If Network Connection Lost

When enabled, the NPort driver will drop the writing data if the network connection between Windows and NPort device is lost. In other words, the writing data will not be sent out after the network reconnects.

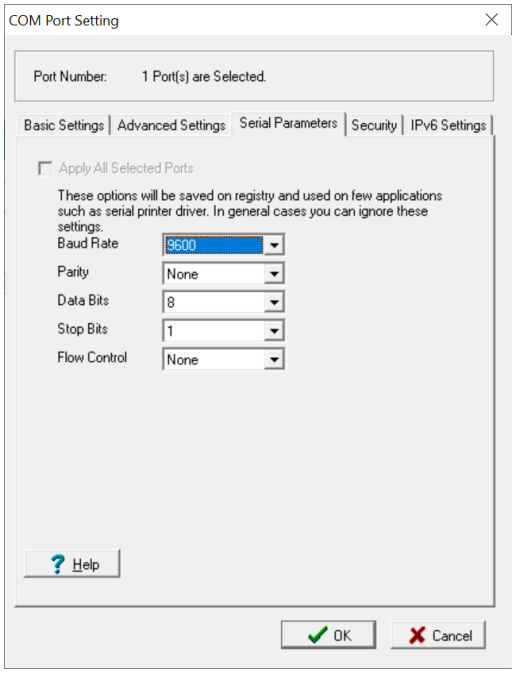
Ignore TX Purge

Applications can use the Win32 API PurgeComm to clear the output buffer. Outstanding overlapping write operations will be terminated. Select the **Ignore TX Purge** checkbox to ignore the effect on output data.

NOTE

Starting Windows Driver Manager v1.19 supports Moxa OnCell Series; the **Enable Auto IP Report** function in the Advance setting only supports OnCell products.

The **Serial Parameters** window in the following figure shows the default settings when the NPort 5000 is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



Security (NPort 6000 and 6000-G2 models)

Enable Data Encryption

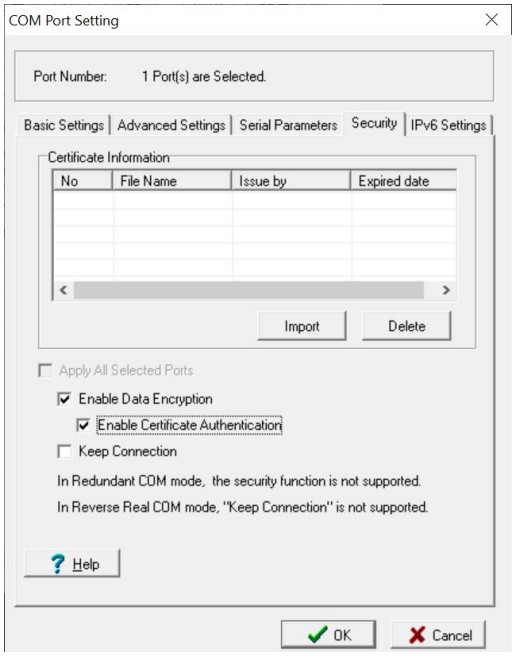
Enable the SSL encryption for data transmission of the COM port. In Redundant COM mode, the security function is not supported.

- Enable Certification Authentication:

  "Enable Certification Authentication" is a security enhancement that provides you a mechanism to check if the Certificate Authority (CA) has certified an imported certificate.

Keep Connection

If your COM port, with data encryption enabled, will be opened/closed frequently, and the NPort is used by only one host, it is recommended to enable this option for quicker operations. A COM port with encryption enabled will take a short time(300 to 500 ms) while opening because of the SSL protocol. By enabling these options, the COM port connection (SSL) will always be kept connected. Here, opening/closing the COM port will be quicker. In Reverse Real COM mode, the "Keep Connection" is not supported.



IPv6 Settings (NPort 6000 and 6000-G2 models)

Interface Index

The Interface Index is for Link-Local address mapping only. Ignore the setting if the mapping address is not a Link-Local(e.g., fe80: 0/64) one. If the COM port is mapped with a link local address, the interface index must be assigned for routing issues. This setting is used to tell the windows system which interface the data should be routed to.

NOTE

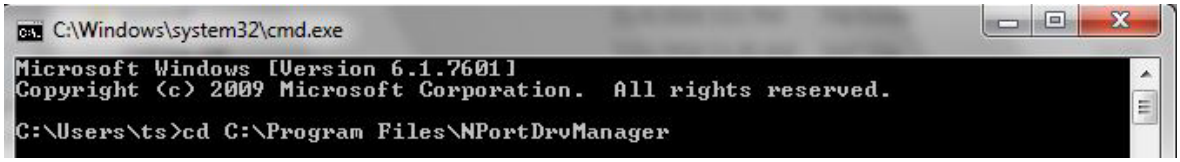
Security and **IPv6 Settings** are supporting NPort 6000 and 6000-G2 models only.

Command-line Installation/Removal

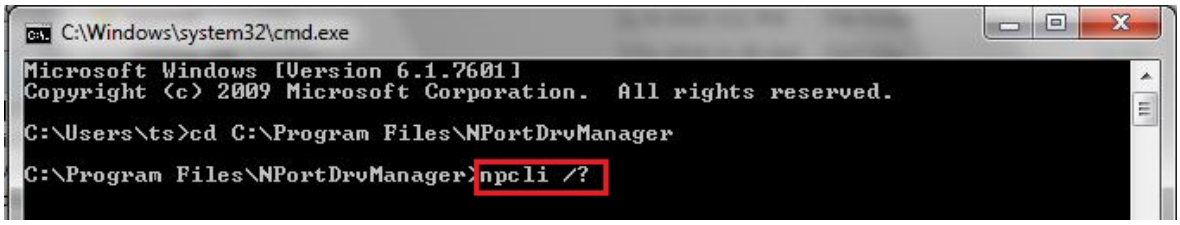
For NPort Windows Driver Manager v1.19 and above, it comes with command-line script tool – ***npcli.exe*** for installation, removal of the driver and capability of configuring NPort driver functions.

After successfully installing NPort Windows Driver Manager v1.19 (or above), the default file path is ***C:\Program Files\NPortDrvManager*** as shown below. The main files that support the NPort command-line tool are ***npcli.exe*** and ***GIdMap.dat***. You may move these two files to your preferred location.

Once NPort Windows Driver Manager v1.19 (or later) is installed, call out ***cmd*** screen on your computer. Change the directory to the location where these two files are installed.



Type ***npcli /?*** to get detailed information of what command lines are supported and the function descriptions.



The usage instructions will show up as below for user's reference:

```
--------------------------------------------------------------------------------
NPort Command-line Interface Ver2.0 Build 16052400
--------------------------------------------------------------------------------
NPort Command-line Interface allows user to manage Real COM port in command
mode.
  It offers these features.
    - Install, remove, or upgrade NPort Driver Manager without entering user
interface.
    - Assign or manage Real COM port with serial parameters.
    - Search NPorts and change some network configurations.

--------------------------------------------------------------------------------
-------
  1. NPort Driver Manager installation and management
     User may copy npcli.exe to a repository to use following commands.

     Usage: npcli /driver [[/install | /upgrade] PATH_NAME] | [/uninstall]

  Parameters are described below:
     /driver       This command is related to driver.
  /install      Install specified driver to host.
  /uninstall    Uninstall current installed driver from host.
  /upgrade      Upgrade specified driver without modify the mapped ports.
  PATH_NAME     Specify the installer file of NPort Driver Manager to install
                or upgrade.

     Examples:
      Install a specified NPort Driver Manager.
       >npcli /driver /install
D:\Users\drvmgr_setup_Ver1.19.0_Build_15122492.exe

      Remove NPort Driver Manager from system.
       >npcli /driver /uninstall

--------------------------------------------------------------------------------
-------
  2. Real COM port management
     These features require the NPort Driver Manager installed. User may change
the port
     settings without using NPort Driver Manager utility.

     Usage:
       - npcli /driver /add IP_ADDR /port PORT_NO /com COM_NO [/txmode [hiperf |
          classical]] [/fifo [enable | disable]] [/flush [fast | normal]]
       - npcli /driver /remove /com [COM_NO | all]
       - npcli /driver /list
       - npcli /driver /set /com [COM_NO] /ip [IP_ADDR]
```

```
  Parameters are described below:
     /driver       This command is related to driver.
  /add          Add a RealCOM with a valid IP address (IP_ADDR).
  /port         Specify the NPort port number (PORT_NO) to add.
     /com          Specify the COM number to add/set or remove (COM_NO).
  /txmode       Set the TX mode as hi-performance (hiperf) or classical. The
                default is hiperf.
  /fifo         Set the FIFO as enable or disable. The default is enable.
  /flush        Set to enable fast flush(fast) or disable fast flush(normal).
                The default is fast.
  /remove       Remove specified COM number (COM_NO) or all RealCOM ports.
     /list         Show the current Real COM ports
     /set          Change the parameter of specified (COM_NO)
     /ip           Specify the IP address (IP_ADDR) to change.

     Examples:
      Create a Real COM port COM3 for Port1 of NPort(192.168.127.254).
       >npcli /driver /add 192.168.127.254 /port 1 /com 3

      Create a Real COM port COM4 on the same NPort with FIFO disable.
       >npcli /driver /add 192.168.127.254 /port 2 /com 4 /fifo disable

      List current Real COM ports
       >npcli /driver /list
       COM3   192.168.127.254   950     966     Port1
       COM4   192.168.127.254   951     967     Port2

      Change IP address to 192.168.0.112 for Read COM port COM4
       >npcli /driver /set /com 4 /ip 192.168.0.112

      Remove COM3 from system
       >npcli /driver /remove /com 3

      Remove all COM ports from system
       >npcli /driver /remove /com all

-------------------------------------------------------------------------------
-------
  3. NPort device configuration
     User may copy npcli.exe and GIdMap.dat together to a repository to use
following
     commands.

     Usage:
       - npcli /devicd /search
       - npcli /device /set ID /network [/ip IP_ADDR] [/mask SUBNET]
          [/gateway IP_ADDR] [/username NAME] [/password CIPHER]
       - npcli /device /apply ID [/username NAME] [/password CIPHER]

  Parameters are described below:
     /device       This command is related to NPort.
  /search       Search the NPort and store the list to the memory.
  /set          Specify the ID to set. Users must specify one of the searched
                NPorts for further operations. The default is 1.
  /port         Specify the NPort port number (PORT_NO) to set.
  /username     Specify the login username (NAME) if the NPort has one.
  /password     Specify the password (CIPHER) if the NPort has one.
  /network      Set to change the network settings.
```

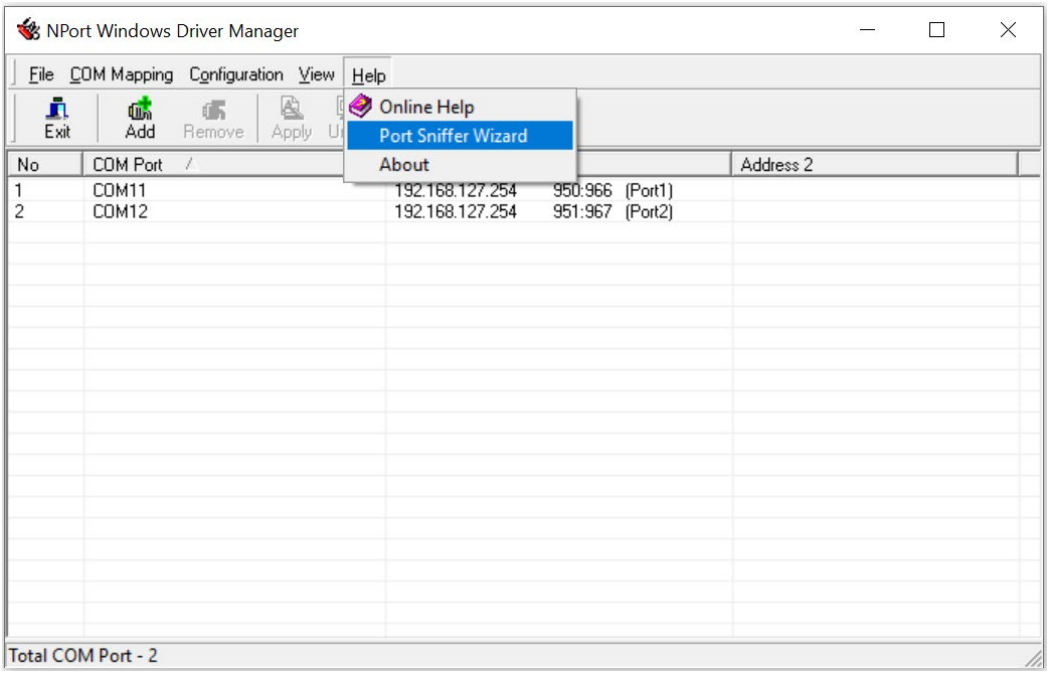
```
  /ip            Change the IP address (IP_ADDR) of NPort.
  /mask          Change the subnet mask (SUBNET) of NPort.
  /gateway       Change the IP address (IP_ADDR) of gateway.
  /apply         Specify the ID to save changes and restart the NPort.

     Examples:
      Search NPorts in LAN. Following example shows 2 NPorts are found. The
first
      column is unique IDs which will be used for other commands.
       >npcli /device /search
       1       192.168.0.112   0090e84843e3    NPort 6650-32
       2       192.168.0.162   0090e8f673e1    NPort 6610-16

      Change the IP of NPort 6610-16 from 192.168.0.162 to 192.168.0.188. For
some
      NPorts the username and password is required to access the configuration.
       >npcli /device /set 2 /network /ip 192.168.0.188 /username admin
/password moxa

      Apply above setting to that NPort.
       >npcli /device /apply 2 /username admin /password moxa

-------------------------------------------------------------------------------
-------
Note:
  Npcli.exe requires an administrator privilege to change device settings.
  It support only IPv4 and it must be run under Windows XP and later versions.
```

Port Sniffer Wizard

A port sniffer is a utility that monitors and captures all serial ports activity on a system. It has advanced filtering and search capabilities that make it a powerful tool for exploring the way Windows works, seeing how applications use ports, or tracking down problems in system or application configurations.

How to Use a Port Sniffer

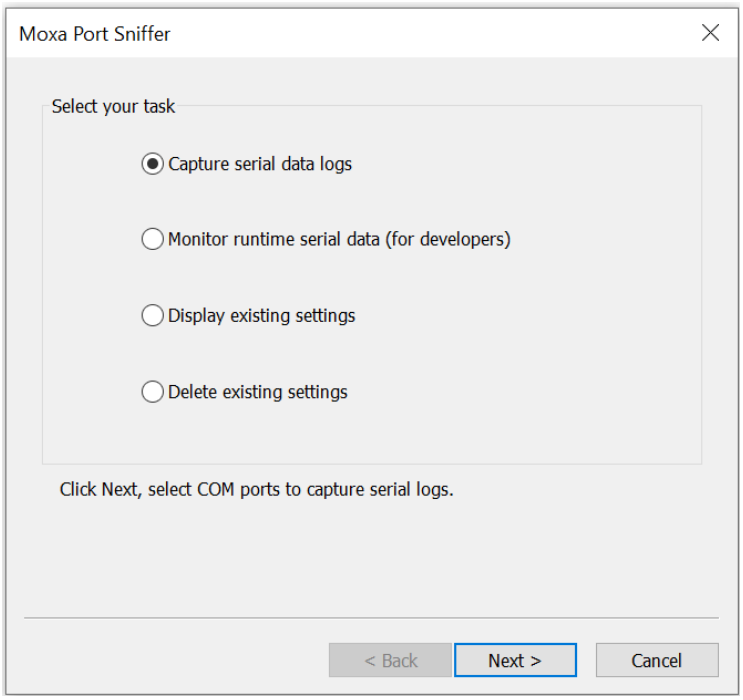
Click **Port Sniffer Wizard** in the drop-down menu under Help.



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 them back to Moxa. We can help you check the problems. Select this function to export log files.

NOTE

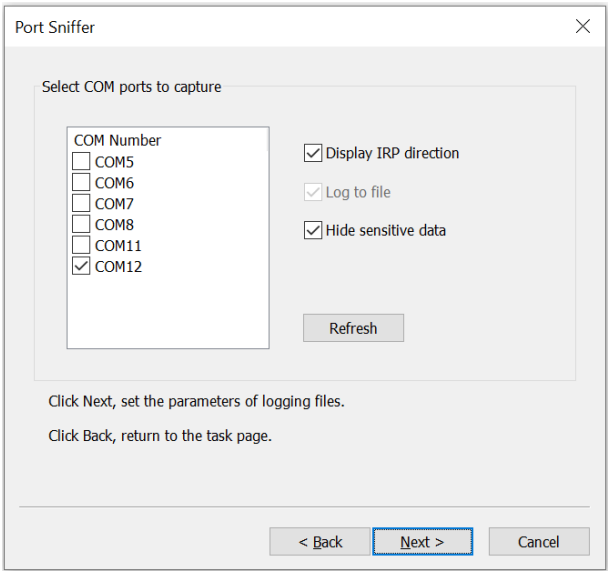
Enabling capture serial data log function may cause slight latency.

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 the 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. This is specifically used for sensitive data.

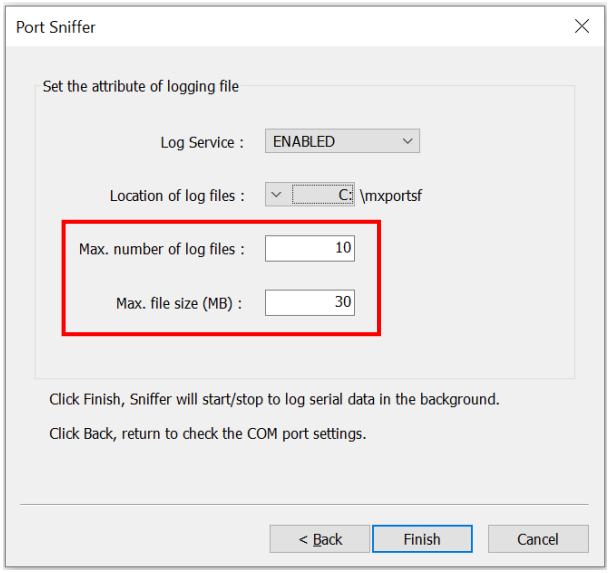


Step 2: Set the parameters of logging files

- Enabled log service.

> **NOTE**
>
> Disable 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).



- Click finish and check log files at the locations you set.

Monitor Runtime Serial Data (for developers)

In comparison with the “Capture serial data logs” function, the “Monitor runtime serial data” function presents the status in real-time.

> **NOTE**
>
> Usually used by developers or serial driver programmers to troubleshoot.

> **NOTE**
>
> Download some debug tools like "DebugView" from a third party to view the real-time status.

Step 3: COM port setting

- Select one or more COM ports to monitor the serial log in runtime.
- Turn on the function you need.
  - Display IRP direction

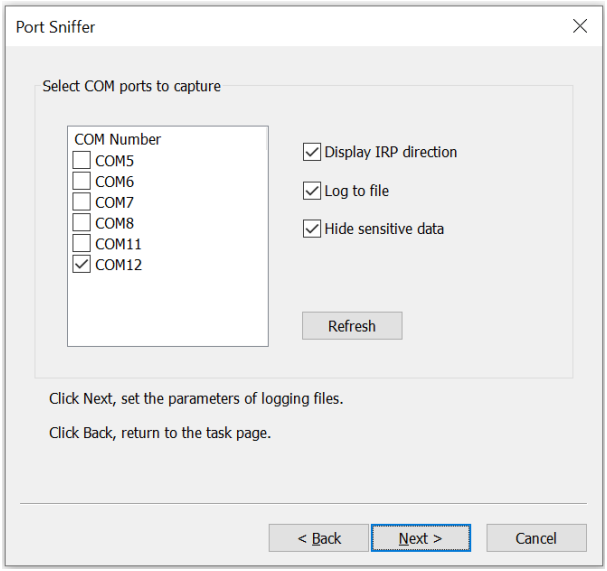
    IRP will inform users whether an error occurs when issuing a command or returning a response.
  - Log to file

    Export log files simultaneously.

> **NOTE**
>
> Export log files simultaneously will cause latency.

  - Hide sensitive data

    The system will hide the data. This is specifically used for sensitive data.

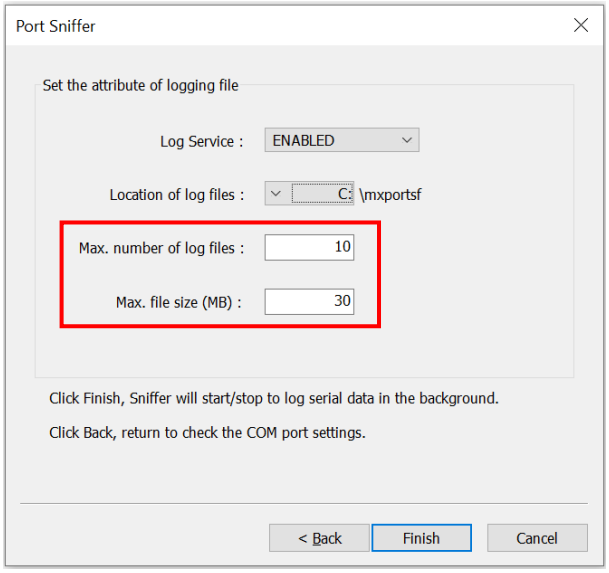


Step 4: Set the parameters for logging files

NOTE

Skip step 2 if you disable 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).

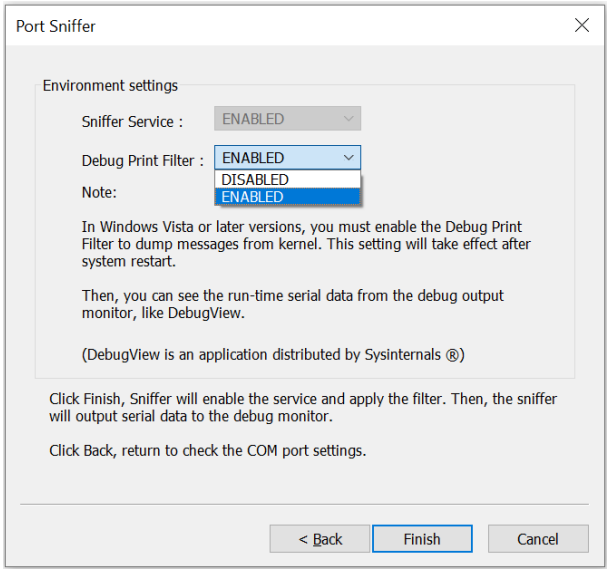


Step 5: Set the environment settings.

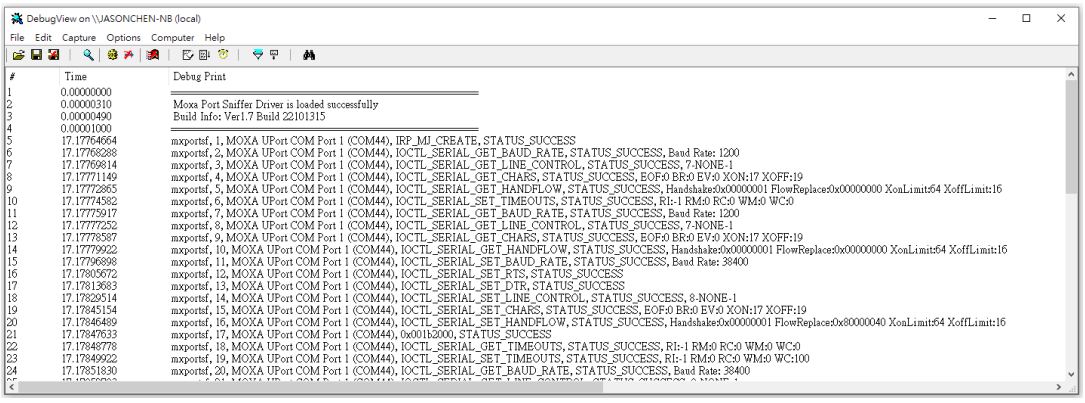
- Enable the Debug Print Filter to dump messages from the kernel. The setting will take effect after the system restarts.

> **NOTE**
>
> Disable the Debug Print Filter will not output the serial data on the monitor.

> **NOTE**
>
> You can see the runtime serial data from the debug output monitor.

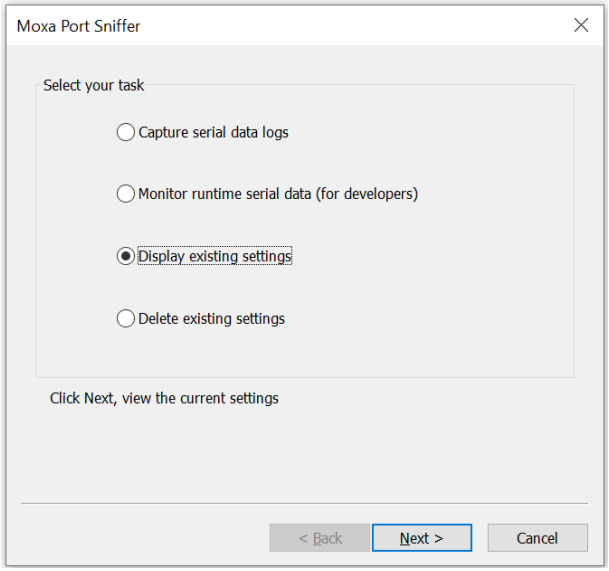


- Click **Finish** and open "DebugView" to Monitor runtime serial data.

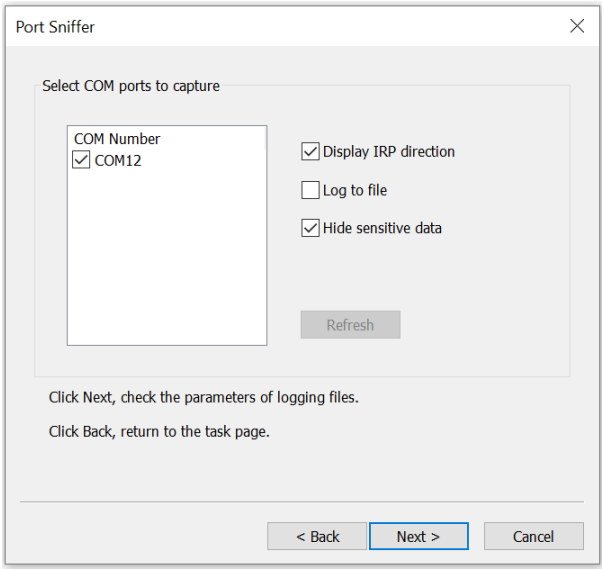


Display existing settings

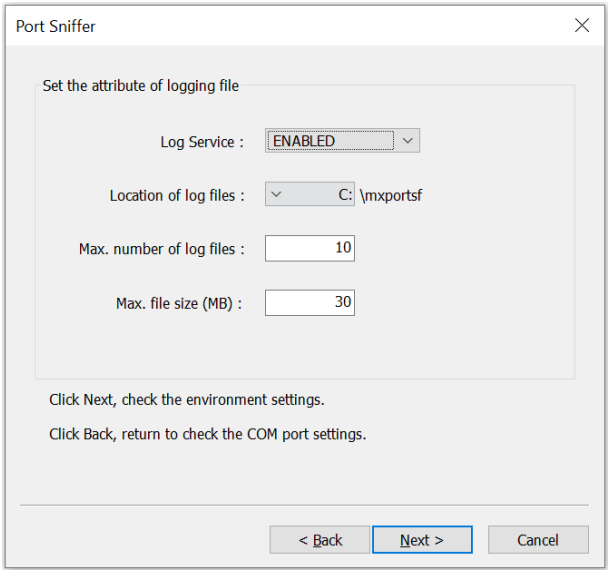
Step 1: Click **Display existing settings** to view the current setting.



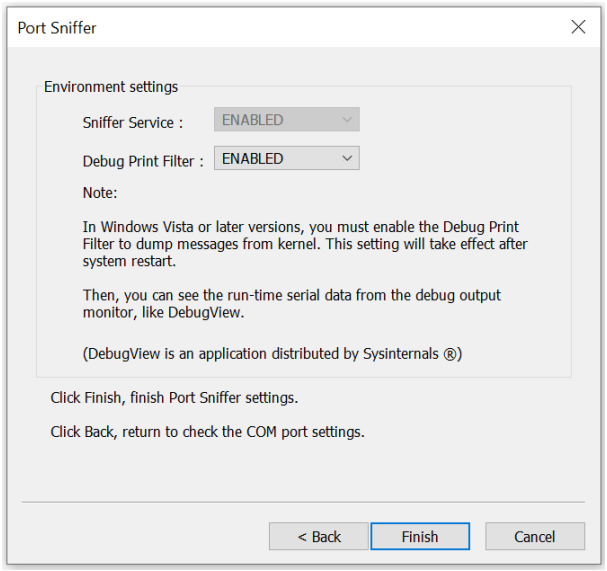
Step 2: Check the COM port settings.



Step 3: Check the parameters of logging files.



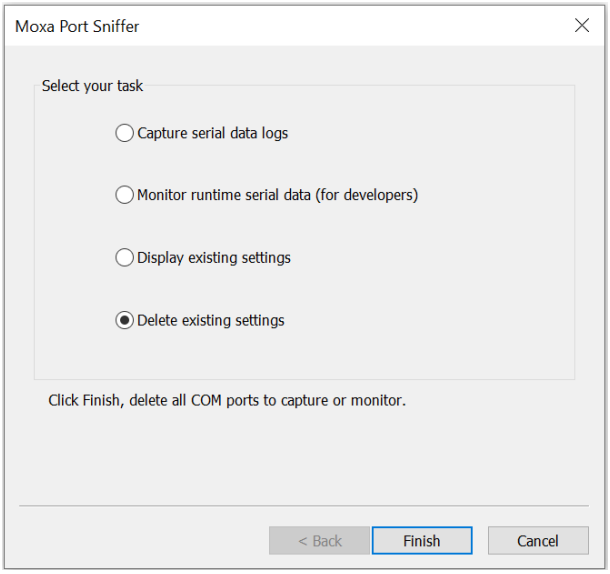
Step 4: Check the environment settings.



Step 5: Click **Finish** to finish the port sniffer settings.

Delete existing settings

Step 1: Select **Delete existing settings**.



Step 2: Click **Finish** to delete existing settings.

8. Installing Linux Real TTY Driver

Basic Procedures

To map an NPort 5000 serial port to a Linux host's tty port, follow these instructions:

1. Set up the NPort 5000. After verifying that the IP configuration works and you can access the NPort 5000 (by using ping, telnet, etc.), configure the desired serial port on the NPort 5000 to Real COM mode.
2. Install the Linux Real tty driver files on the host
3. Map the NPort serial port to the host's tty port

Hardware Setup

Before proceeding with the software installation, make sure you have completed the hardware installation. Note that the default IP address for the NPort 5000 is 192.168.127.254.

NOTE

After installing the hardware, you must configure the operating mode of the serial port on your NPort 5000 to Real COM mode.

Installing Linux Real TTY Driver Files

NOTE

The newest information, refer to readme.txt on Linux Real TTY Driver

1. Obtain the driver file from Moxa's website, at http://www.moxa.com. You may find it in the **Resource** section under your product page.
2. Log in to the console 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 be able to 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)

At this point, you will be ready to map the NPort serial port to the system tty port.

Mapping TTY Ports

Make sure that you set the operation mode of the desired NPort 5000 serial port to Real COM mode. After 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 mxaddsvr is as follows:

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

The mxaddsvr command performs the following actions:

1. Changes npreal2d.cf.
2. Creates tty ports in directory /dev with major & minor number configured in npreal2d.cf.
3. Restarts the driver.

Mapping tty ports automatically

To map tty ports automatically, you may execute mxaddsvr with just the IP address and the number of ports, as in the following example:

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

In this example, 16 tty ports will be added, all with IP 192.168.3.4, with data ports from 950 to 965 and command ports from 966 to 981.

Mapping tty ports manually

To map tty ports manually, you may execute mxaddsvr and manually specify the data and command ports, as in the following example:

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

In this example, 16 tty ports will be added, all with IP 192.168.3.4, with data ports from 4001 to 4016 and command ports from 966 to 981.

Removing Mapped TTY Ports

After 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. Modify 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. You will need to 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:

1. Unload the driver.
2. Delete all files and directories in /usr/lib/npreal2
3. Delete directory /usr/lib/npreal2
4. Modify the system initializing script file.

9. Installing Linux Arm Driver

Introduction

This section is intended for programmers who are porting the NPort Real TTY driver to a specified Arm-based platform. The following knowledge is recommended before reading the instructions in this guide.

- Linux kernel programming
- Arm platform compiler
- The Yocto Project documentation
- Moxa UC-Series Manual
- Raspberry Pi Manual

Instructions in this section use examples of porting on the Moxa UC-Series Arm platform and Raspberry Pi. You can apply the experience of porting Real TTY driver to other platforms.

The Real TTY driver fully supports all modern-day Linux distributions running on x86 environments, and the driver core is also compatible with the Arm platform. This document will guide you on how to port the Real TTY driver core.

However, some platform-dependent services, such as installer, are not available. You may refer to the platform's documentation to fulfill the requirements.

Porting to the Moxa UC-Series—Arm-based Computer

Build Binaries on a General Arm Platform

If your platform is powerful and comprises the necessary development tools, the driver can be built on the platform directly. You can refer to README.TXT of Real TTY Driver to understand the requirement.

The step of building this driver in an Arm environment is the same as in x86 and x64 environments.

```
# ./mxinst
```

Cross-compiler and the Real TTY Driver

> **NOTE**
>
> To cross-compile on a x86 or x64 Linux host, the target ARM environment's kernel source package and cross compiler toolchain must be installed first.

After installing and configuring the kernel source package and toolchain, you need to compile all of the source code with the kernel source package and toolchain.

In this example, we install the cross-compiler for the Moxa UC-Series ARM-based computer. You can refer to the product's manual for further detail.

1. Download the cross-compiler toolchain and the kernel source package webpage under the product page.

   ```
   $ git clone https://github.com/Moxa-Linux/am335x-linux-4.4
   ```

2. Download the toolchain from the product's webpage. The toolchain, which is used by the UC Series, is arm-linux-gnueabihf. It is a script that will install the related packages. Execute the script and follow the steps to install the Linux cross-compiler tools. You will need the root privilege to install the toolchain and the kernel source.

   ```
   # sh arm-linux-gnueabihf_6.3_Build_amd64_<build_date>.sh
   ```

   If the script shows the notification message: "Please export these environment variables before using toolchain", enter the following script command:

   ```
   # export PATH=$PATH:/usr/local/arm-linux-gnueabihf-6.3/usr/bin
   ```

3. The kernel source, which is used by the UC Series, is am335x-linux-4.4. You need to configure these files before cross-compiling.

   Move the kernel source to /moxa/kernel and configure the kernel source.

   ```
   # mv am335x-linuc-4.4 /moxa/kernel
   # cd /moxa/kernel
   # make uc3100_defconfig ← Replace the UC 3100 with the UC Series that is being used.
   # make modules_prepare
   ```

After the abovementioned steps, follow the processes as set out in Section “Moxa cross-compiling interactive script,” and Section “Manually build the Real TTY driver with a cross-compiler,” to cross-compile Moxa's driver for the UC-Series platforms.

The NPort Real TTY driver, which includes the driver module, service daemons, and tools, needs to be compiled. The files are listed as follows:

- npreal2.ko: Real TTY kernel extension
- npreal2d: Daemon of Real COM communication
- npreal2d_redund: Daemon of Redundant COM mode only for the NPort CN2500/CN2600 Series.
- mxloadsvr: Daemons reloading tool.
- mxaddsvr: Port-mapping tool.
- mxdelsvr: Port-unmapping tool.
- mxsetsec: Secure mode setting tool.
- mxcfmat: Internal-use only tool.
- mxmknod: Internal-use only tool.
- mxrmnod: Internal-use only tool.
- npreal2d.cf: Configuration template.

If it is preferred to build these binaries with automatic script, refer to the section “Moxa cross-compiling interactive script.” If you find the build script troublesome, or you prefer to build these binaries manually, refer to the section “Manually build the Real TTY driver with a cross-compiler.”

If you have generated the necessary binaries, refer to Section “Deploy cross-compiled binary to target” to deploy to the target platform.

Moxa cross-compiling Interactive Script

To simplify the processes above, Moxa has provided an interactive script, "mxcc", to cross-compile these drivers. You may execute ./mxcc in the Real TTY driver source directory to cross-compile the Moxa driver.

The steps are as follows:

```
# ./mxcc
Enter target device architecture (ARCH) [arm]:
Enter cross-compiler (CROSS_COMPILE) [arm-linux-gnueabihf-]:
Enter target device kernel source directory [/moxa/kernel/]:
If you wish to use secure communication with the NPort 6000 Series device, choose
[Y] to enable the SSL function.
Note: This function supports Real COM with secure mode in the NPort 6000 Series
only.
Do you want to enable secure mode? [Y/N]: N
The polling mode allows you to open the tty port as nonblocking even if the NPort
is not connected.
Do you want to set the driver to polling mode? [Y/N]: N

****************************************************************
Moxa NPort Server Real TTY Driver Series driver cross-compiling finished.
When cross compiling is successful, the driver is outputted to output folder.
****************************************************************
```

The binaries will now be generated and placed in the output directory under the source code folder.

Manually Build the Real TTY Driver With a Cross-compiler

To cross-compile npreal2 driver, users can find "Makefile" in the driver source folder, then run it.

```
# make -C KDIR=<KERNEL_SOURCE> M=<DRIVER_SOURCE> ARCH=<ARCH>
CROSS_COMPILE=<CROSS_COMPILE>  KVER_MAJOR=<KERNEL_MAJOR>
KVER_MINOR=<KERNEL_MINOR> modules
```

<KERNEL_SOURCE>: The directory of target kernel source.

<DRIVER_SOURCE>: The directory of the Real TTY driver source.

<ARCH>: The target Arm environment device's CPU architecture. For example, arm, arm64.

<CROSS_COMPILE>: The cross-compile toolchain path. If the toolchain is arm-linux-gnueabihf, and the path of toolchain exists in your PATH environment variable, enter "arm-linux-gnueabihf-" here.

<KERNEL_MAJOR>: The target Arm system kernel source's kernel major version. You can use the command "make kernelversion" to get the kernel source's major version.

For example:

```
# make kernelversion
4.4.0
|
+--- kernel major version
```

<KERNEL_MINOR>: The target Arm system kernel source's kernel minor version. You can use the command "make kernelversion" to get the kernel source's minor version.

For example:

```
$ make kernelversion
4.4.0

|
+--- kernel minor version
```

The “make” command would be similar to the following example:

```
# make -C KDIR=/moxa/kernel M=/home/user/moxa/source ARCH=arm CROSS_COMPILE=arm-linux-gnueabihf- KVER_MAJOR=4 KVER_MINOR=4 modules
```

After using the "make" command to cross-compile the drivers, the driver file "npreal2.ko" can be found in the source code directory.

To cross-compile the daemons and tools, find "Makefile" in the driver source folder, then run it.

```
# make <TARGET> CROSS_COMPILE=<CROSS_COMPILE> CC=<C_COMPILE> CFLAGS=<C_FLAGS>
```

<TARGET>: Set one of npreal2d, preal2d_redund, and tools.

<CROSS_COMPILE>: The cross-compile toolchain path. If the toolchain is “arm-linux-gnueabihf”, and the path of toolchain exists in your PATH environment variable, enter "arm-linux-gnueabihf-" here.

<C_COMPILE>: The C compiler offered by the cross-compiler toolchain. It is "gcc" if the toolchain is "arm-linux-gnueabihf-".

<C_FLAGS>: Specify the preprocessor definitions of Real TTY driver here.

NOTE

"-DNO_INIT" must be included or else the cross-compiler may return error messages.

See the definitions:

- "-DNO_INIT": Disable the startup service.
- "-DOFFLINE_POLLING": Allow tty not to be blocked if the NPort is offline.

e.g.: To build TARGET=npreal2d with a polling feature, use the following command:

```
# make npreal2d CROSS_COMPILE="arm-linux-gnueabihf-" CC=gcc CFLAGS="-DNO_INIT -DOFFLINE_POLLING"
```

After using the "make" command to cross compile the daemons and tools, the binaries can be found in the source code directory.

(Optional) Build a secure mode connection to the NPort 6000 Series

When it is required to use a secure mode connection to the NPort 6000 Series, the npreal2d daemon should be built manually because it needs an extra OpenSSL library. This section introduces the secure mode npreal2d building besides the OpenSSL library demonstration. OpenSSL is maintained by www.openssl.org.

Most of the Linux distributions have package management tools, such as apt-get or yum, which help you install OpenSSL library and development tools. In an Arm platform, it has to be built from the source code. You may refer to OpenSSL's user guide to generate the library first. The instructions may vary amongst different OpenSSL versions, cross-compilers, or building hosts.

The demonstration here illustrates the process that Moxa has built for the library for Real TTY driver and for the Moxa's lab testing.

1. Create the folders below for OpenSSL products:

   ```
   $ cd ~
   $ mkdir openssl-lib
   $ cd openssl-lib
   $ mkdir openssl-arm
   $ mkdir ssl-arm
   ```

2. Check out the OpenSSL source code. We used a stable branch named OpenSSL-fips-2_0_9. The command below will download the OpenSSL-fips-2_0_9 source code in the openssl folder.

   $ git clone https://github.com/openssl/openssl.git -b OpenSSL-fips-2_0_9

3. The OpenSSL needs to be configured before executing the "make" command.

NOTE

The <openssl-arm> and <ssl-arm> are the folders that were created in the previous instruction. The cross-compiler toolchain "arm-linux-gnueabihf-" is used for the Moxa UC-serial computer.

```
$ cd openssl
$ setarch i386 ./config no-asm no-shared enable-ssl3 enable-ssl3-method
enable-tls1_3 --prefix=<openssl-arm> --openssldir=<ssl-arm> --cross-compile-
prefix=arm-linux-gnueabihf-
```

4. Next, make and install the OpenSSL:

```
$ make
$ make install_sw
```

Finally, the headers and libraries will be constructed in the following hierarchy:

```
openssl-arm
├── bin
├── include
└── lib
    ├── engines
    ├── libcrypto.a
    ├── libssl.a
    └── pkgconfig
```

The following command is to build npreal2d with secure mode:

```
$ arm-linux-gnueabihf-gcc -c ${CFLAGS} -DNO_INIT -DSSL_ON -DOPENSSL_NO_KRB5
npreal2d.c -I/home/user/openssl-lib/openssl-arm/include
```

If polling mode is preferred, change "${CFLAGS}" to "-DOFFLINE_POLLING".

```
$ arm-linux-gnueabihf-gcc npreal2d.o -o npreal2d -lssl -lcrypto -ldl -lpthread -
L/home/user/openssl-lib/openssl-arm/lib/ -I/home/user/openssl-lib/openssl-
arm/include
```

The npreal2d binary will be generated.

NOTE

Only the npreal2d requires OpenSSL library; other binaries should follow the section "Manually build the Real TTY driver with a cross-compiler".

NOTE

The secure mode is supported only if the NPort 6000 enables it. Refer to the NPort 6000 Series User Manual to configure secure mode in the NPort 6000.

Deploy Cross-compiled Binary to Target

You should find the following binaries under the output or source code directory:

- npreal2.ko
- npreal2d
- npreal2d_redund
- mxloadsvr
- mxaddsvr
- mxdelsvr
- mxsetsec

A few necessary tools are available in the source code directory:

- mxcfmat
- mxmknod
- mxrmnod
- npreal2d.cf

Follow the steps below to deploy to the target Arm platform.

1. Copy the npreal2.ko to the path /lib/modules/`uname -r`/kernel/drivers/char on the Arm platform.
2. Create a folder /usr/lib/npreal2/driver. Copy all the above files to that folder, except npreal2.ko.
3. Boot into the Arm platform and load the driver.
   ```
   # modprobe npreal2
   ```
4. Change the directory to "/usr/lib/npreal2/driver" and run "mxaddsvr, mxdelsvr, or mxsetsec", the same as running them on x86 Linux.
5. The module can be unloaded by the following command:
   ```
   # modprobe -r npreal2
   ```

Porting to Raspberry Pi OS

Raspberry Pi OS images are prebuilt by www.raspberrypi.org. You can install the image and start up the system. The process to build the Real TTY driver is the same as with x86 Linux. Refer to README.txt to check the system requirements.

You may use the rpi-source to install the kernel source packages for a more convenient option. Refer to the official website https://github.com/notro/rpi-source/wiki for more information.

rpi-source is a third-party package offering an integrated kernel resource for building a driver. The Real TTY is tested with this package to see if it works well. However, the requirements may vary for different Raspberry Pi OS versions. Read the manual of the rpi-source to understand the know-how and the limitations.

Porting to the Yocto Project on Raspberry Pi

Prerequisite

You are expected to be familiar with the Yocto Project. Refer to https://docs.yoctoproject.org for the Yocto Project documentation for further understanding. Also, it is encouraged to follow the procedures in this guide unless you have sufficient knowledge about the Real TTY driver, the Yocto Project, and Raspberry Pi.

The dunfell branch (3.1.9) is referred to throughout in this section. Base it on this version before reading the instructions in the Yocto Project documentation. You are required to build the Yocto image successfully with the "Yocto Project Quick Build" document.

In the Yocto Project, you can select the platform you want to build. This guide installs Raspberry Pi BSP Layer as a demonstration in the following steps:

1. Suppose the Yocto Project is installed in the /home/user/poky folder. Checkout the source code of the Raspberry Pi BSP Layer.

   ```
   $ cd /home/user/poky
   $ git clone https://git.yoctoproject.org/cgit/cgit.cgi/meta-raspberrypi -b dunfell
   ```

2. A meta-raspberrypi folder will be checked out now. Use the following instructions to set up Raspberry Pi BSP:

   ```
   $ source oe-init-build-env
   ```

3. Use a text editor to add the following content to the configuration file './conf/local.conf'.
4. Add the type 'rpi-sdimg' optionally if SD card is preferred

   IMAGE_FSTYPES="tar.bz2 ext3 rpi-sdimg"

5. Change the machine name of your target

   # Use raspberrypi2 for Pi 2 board

   # Use raspberrypi3 for Pi 3 board

   Use raspberrypi3-64 for 64-bit Pi 3 board

   MACHINE ?= "raspberrypi3"

6. Use the text editor to add the following content to the configuration file './conf/bblayers.conf'
7. Add this line '/home/user/poky/meta-raspberrypi' to BBLAYERS

   BBLAYERS ?= " \

   /home/user/poky/meta \

   /home/user/poky/meta-poky \

   /home/user/poky/meta-yocto-bsp \

   /home/user/poky/meta-raspberrypi \

   "

8. Build the target core-image-base by following this command and the Raspberry Pi image will be generated:

   ```
   $ bitbake core-image-base
   ```

Once the above image runs on Raspberry Pi, go to the next section.

Create a Moxa Layer for the Yocto Project

Introduction

Moxa RealTTY driver is packaged as a layer for Yocto. You can add or remove the driver by modifying the BBLAYERS attribute in the bblayers.conf file.

The following sections describe how to create the meta-moxa layer for the dunfell branch (3.1.9). Note that the process may vary if your target uses a different branch. Refer to Yocto's manual for complete information.

An example is also available in the examples folder in the RealTTY driver.

You may follow the subsequent procedures to create the same meta-moxa layer.

Create an empty Moxa Layer

Use the following commands to create an empty layer, named meta-moxa.

1. Start the environment first. Suppose the project is installed in /home/user/poky.

   ```
   $ cd /home/user/poky
   $ source oe-init-build-env
   ```

2. The above commands changed the directory to the built directory. Now, we change the directory back to the Yocto root directory.

   ```
   $ cd /home/user/poky
   ```

3. Create meta-moxa:

   A message appears reminding you to add the layer later.

   ```
   $ bitbake-layers create-layer meta-moxa
   Note: Starting bitbake server.
   Add your new layer with "bitbake-layers add-layer meta-moxa."
   ```

The meta-moxa directory will be created in /home/user/poky:

```
$ tree meta-moxa
```

```
meta-moxa
├── conf
│   └── layer.conf
├── COPYING.MIT
├── README
└── recipes-example
    └── example
        └── example_0.1.bb
```

The "recipes-example" folder is not necessary; it may be deleted at anytime.

Create a recipe for the Real TTY kernel

Use the following commands to create a recipe for installing Real TTY kernel to the target platform.

1. Create a directory recipes-kernel in meta-moxa:

```
$ cd /home/user/poky
$ mkdir meta-moxa/recipes-kernel
```

2. The simplest way is to copy and modify from a hello example, which is available in the Yocto source code:

```
$ cp -r ./meta-skeleton/recipes-kernel/hello-mod ./meta-
moxa/recipes-kernel
```

   The content of meta-moxa now is listed below:

```
$ tree meta-moxa
meta-moxa/
├── conf
│   └── layer.conf
├── COPYING.MIT
├── README
└── recipes-kernel
    └── hello-mod
        ├── files
        │   ├── COPYING
        │   ├── hello.c
        │   └── Makefile
        └── hello-mod_0.1.bb
```

3. Delete the unnecessary files in hello-mod. Rename the hello-mod.

```
$ cd ./meta-moxa/recipes-kernel
$ rm ./hello-mod/files/COPYING
$ rm ./hello-mod/files/hello.c
$ mv ./hello-mod/hello-mod_0.1.bb ./hello-mod/realtty-kernel_0.1.bb
$ mv ./hello-mod realtty-kernel
```

4. Extract the Real TTY source code in /moxa. Copy the following files into hello-mod:

```
$ cp /moxa/COPYING-GPL.TXT ./realtty-kernel/files/
$ cp /moxa/npreal2.c ./realtty-kernel/files/
$ cp /moxa/npreal2.h ./realtty-kernel/files/
$ cp /moxa/np_ver.h ./realtty-kernel/files/
```

5. The content of the recipes-kernel now is listed below:

```
$ tree ./
./
└── realtty-kernel
    ├── files
    │   ├── COPYING-GPL.TXT
    │   ├── Makefile
    │   ├── npreal2.c
    │   ├── npreal2.h
    │   └── np_ver.h
    └── realtty-kernel_0.1.bb
```

6. Modify the content of the file "./realtty-kernel/files/Makefile" as follows:

   ```
   obj-m := npreal2.o
   SRC := $(shell pwd)

   all:
   $(MAKE) -C $(KERNEL_SRC) M=$(SRC)

   modules_install:
   $(MAKE) -C $(KERNEL_SRC) M=$(SRC) modules_install

   clean:
   rm -f *.o *~ core .depend .*.cmd *.ko *.mod.c
   rm -f Module.markers Module.symvers modules.order
   rm -rf .tmp_versions Modules.symvers
   ```

7. Modify the content of the file './realtty-kernel/realtty-kernel_0.1.bb' as follows:

   ```
   DESCRIPTION = "Linux kernel module for NPort"
   LICENSE = "GPLv3"
   LIC_FILES_CHKSUM = "file://COPYING-GPL.TXT;md5=3c34afdc3adf82d2448f12715a255122"

   inherit module

   SRC_URI = " \
   file://Makefile \
   file://npreal2.h \
   file://np_ver.h \
   file://npreal2.c \
   file://COPYING-GPL.TXT \
   "

   S = "${WORKDIR}"

   # The inherit of module.bbclass will automatically name module packages with the prefix"kernel-module-" as required by the OpenEmbedded Core-build environment.

   RPROVIDES_${PN} += "kernel-module-npreal2"
   ```

Create a recipe for the Real TTY utilities

Similar to creating a realtty-kernel recipe, create a recipe for facilitating the NPort management.

1. Create directory below in meta-moxa:

   ```
   $ cd /home/user/poky
   $ mkdir -p ./meta-moxa/recipes-utility/realtty-tools/files
   ```

2. Copy the Moxa driver which can be downloaded from the Moxa product web page directly. The driver's name format is npreal2_vM.N_BUILD-DATE.tgz.

   ```
   $ cp /home/user/download/npreal2_vM.N_BUILD_DATE.tgz ./meta-moxa/recipes-utility/realtty-tools/files/
   ```

3. Create a bb file ./meta-moxa/recipes-utility/realtty-tools/realtty-tools.bb, which has the following content:

   ```
   DESCRIPTION = "Service utilities for NPort"
   LICENSE = "GPLv3"
   LIC_FILES_CHKSUM = "file://moxa//COPYING-GPL.TXT;md5=3c34afdc3adf82d2448f12715a255122"

   # OpenSSL is required for secured mode
   DEPENDS = "openssl"

   # Specify the compressed driver file for SRC_URI
   SRC_URI = "file://npreal2_vM.N_BUILD-DATE.tgz"

   S = "${WORKDIR}"

   # Specify the destination of RealTTY driver
   DEST_DIR = "${D}${libdir}/npreal2/driver"

   FILES_${PN} += "${libdir}/npreal2/driver/*"

   # If it is required to connect the NPort with the SSL secure mode (secure mode is available in the NPort 6000 Series only), unremark the following line:
   #SSL_MODE = "yes"

   do_compile () {
   ${CC} -o mxaddsvr ${S}/moxa/mxaddsvr.c ${S}/moxa/misc.c
   ${CC} -o mxdelsvr ${S}/moxa/mxdelsvr.c ${S}/moxa/misc.c
   ```

```
${CC} -o mxcfmat ${S}/moxa/mxcfmat.c
${CC} -o mxloadsvr -DNO_INIT ${S}/moxa/mxloadsvr.c ${S}/moxa/misc.c
${CC} -o mxsetsec -DNO_INIT ${S}/moxa/mxsetsec.c ${S}/moxa/misc.c
if [ ${SSL_MODE} = "yes" ], then
${CC} -o npreal2d_redund -lssl -lpthread -DSSL_ON -DOPENSSL_NO_KRB5 ${S}/moxa/redund_main.c
${S}/moxa/redund.c
${CC} -o npreal2d -lssl -DSSL_ON -DOPENSSL_NO_KRB5 ${S}/moxa/npreal2d.c
or else
${CC} -o npreal2d_redund -lpthread ${S}/moxa/redund_main.c ${S}/moxa/redund.c
${CC} -o npreal2d ${S}/moxa/npreal2d.c
fi
}
do_install () {
install -m 0755 -d ${DEST_DIR}
install -m 0755 ${S}/mxaddsvr ${DEST_DIR}
install -m 0755 ${S}/mxdelsvr ${DEST_DIR}
install -m 0755 ${S}/mxcfmat ${DEST_DIR}
install -m 0755 ${S}/mxloadsvr ${DEST_DIR}
install -m 0755 ${S}/mxsetsec ${DEST_DIR}
install -m 0755 ${S}/moxa/mxmknod ${DEST_DIR}
install -m 0755 ${S}/moxa/mxrmnod ${DEST_DIR}
install -m 0755 ${S}/npreal2d ${DEST_DIR}
install -m 0755 ${S}/npreal2d_redund ${DEST_DIR}
install -m 0755 ${S}/moxa/npreal2d.cf ${DEST_DIR}
}
# Ignore GNU_HASH (did not pass LDFLAGS)
INSANE_SKIP_${PN} = "ldflags"
```

NOTE

The file name of SRC_URI must be the same as it was copied in the last step.

4. The content of meta-moxa is listed as below:

```
$ tree meta-moxa
```

```
meta-moxa
├── conf
│   └── layer.conf
├── COPYING.MIT
├── README
├── recipes-kernel
│   └── realtty-kernel
│       ├── files
│       │   ├── COPYING-GPL.TXT
│       │   ├── Makefile
│       │   ├── npreal2.c
│       │   ├── npreal2.h
│       │   └── np_ver.h
│       └── realtty-kernel_0.1.bb
└── recipes-utility
    └── realtty-tools
        ├── files
        │   └── npreal2_vM.N_BUILD-DATE.tgz
        └── realtty-tools.bb
```

Install a Moxa Layer Into the Yocto Project

1. Install the Moxa layer and Real TTY recipes into the Yocto Project.

   ```
   $ cd /home/user/poky
   $ source oe-init-build-env
   ```

2. Use a text editor to add the following content to the configuration file:

   './conf/bblayers.conf':

3. Add this line "/home/user/poky/meta-moxa' to BBLAYERS

   BBLAYERS ?= " \
   /home/user/poky/meta \
   /home/user/poky/meta-poky \
   /home/user/poky/meta-yocto-bsp \
   /home/user/poky/meta-raspberrypi \
   /home/user/poky/meta-moxa \
   "

4. Use a text editor to add the following content to the configuration file:

   './conf/local.conf':

   IMAGE_INSTALL_append += " realtty-tools realtty-kernel"

Deploy the Yocto Image in Raspberry Pi

Build the image with the Real TTY driver:

```
$ cd /home/user/poky
$ source oe-init-build-env
$ bitbake core-image-base
```

An SD-card format image (.rpi-sdimg) is generated under /home/user/poky/build/tmp/deploy/images/raspberrypi3. It is suggested to use the Raspberry Pi official tool 'rpi-imager' to burn the image into the SD-card and then boot it into the Linux kernel in Raspberry Pi.

Start the Real TTY Driver in Raspberry Pi

After logging into the system, start the Real TTY driver

root@raspberrypi3:~# modprobe npreal2
[39.906812] npreal2: loading out-of-tree module taints kernel.
[39.913379] Moxa Async/NPort server family Real TTY driver ttymajor 33 calloutmajor 38 verbose 1 (Ver5.1)

For example, we illustrate how to add a 4-port NPort with the IP address: 192.168.127.254

root@raspberrypi3:~# cd /usr/lib/npreal2/driver
root@raspberrypi3:/usr/lib/npreal2/driver# ./mxaddsvr 192.168.127.254 4
Adding Server...

ttyr00, cur00
ttyr01, cur01
ttyr02, cur02
ttyr03, cur03
Added Real Com IP : 192.168.127.254

Now the device node /dev/ttyr00 ~ /dev/ttyr03 is created for tty port use.

Set the Default tty Mapping to the Real TTY Configuration

You may use the Real TTY configuration file, npreal2d.cf that we set up in 4.5, as the default settings when deploying to a new Raspberry Pi image.

1. Copy and replace npreal2d.cf in the NPort Real TTY driver folder

   '/moxa' extracted in the build system.
2. tar -zxvf new_npreal2_driver.tgz /moxa
3. Go back to "Create a recipe for the Real TTY utilities", change the name of npreal2_vM.N_BUILD_DATE.tgz with the file name in step 2.)
4. Rebuild the image.

Troubleshooting

If the following error is encountered during the building of the image,

ERROR: Task (/home/user/poky/meta/recipes-devtools/binutils/binutils_2.34.bb:do_compile) failed with exit code '1'

It is suggested to compile binutils first, then compile the entire image:

```
$ bitbake binutils -c do_compile
$ bitbake core-image-base
```

10. Installing macOS Driver

Basic Procedures

To map an NPort 5000 serial port to a Mac host's tty port, follow these instructions:

1. Set up the NPort 5000. Verify the IP configuration works by using ping, telnet, etc.
2. Install the Mac driver files on the host.
3. Search or manually input the IP address of the NPort to set up virtual COM port.

Hardware Setup

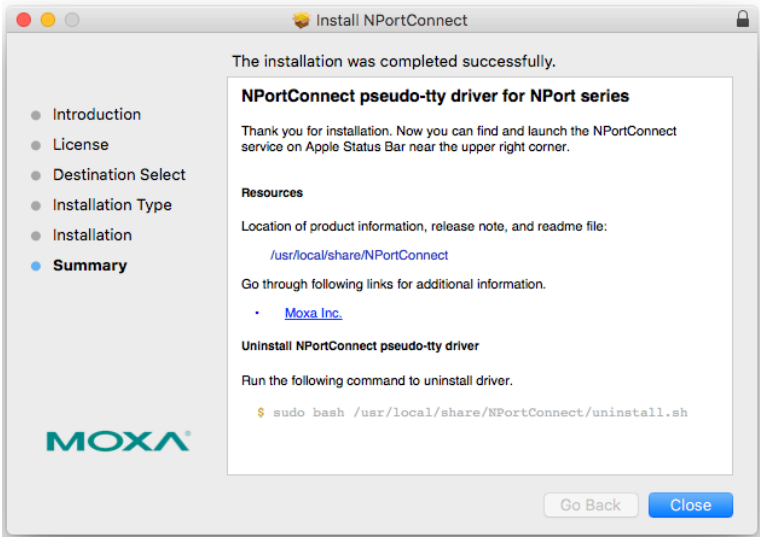
Before proceeding with the software installation, make sure you have completed the hardware installation. Note the default IP address for the NPort 5000 is 192.168.127.254.

Installing macOS TTY Driver Files

NOTE

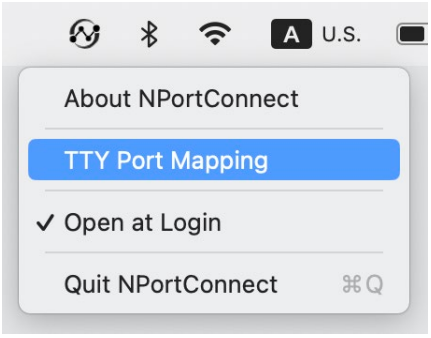
For the newest information, refer to readme.txt on Mac TTY Driver. Resources location of product information, release note, and readme file: /usr/local/share/NPortConnect

1. Obtain the driver file from Moxa's website, at http://www.moxa.com. You may find it in the Resource section under your product page.
2. Execute the installer package 'moxa-macOS-tty-drivers-for-macOS-xx.xx-or-later-vx.x.pkg'.
3. Follow the instruction of each step and complete the installation.
4. Press **Continue** in the **Destination Select** window.
5. In the final step, you may find the location of driver's document and also instruction of driver uninstall.

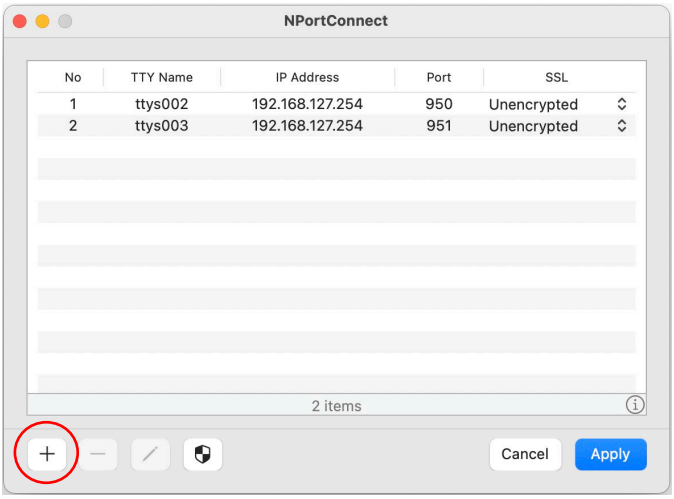


Mapping macOS TTY port

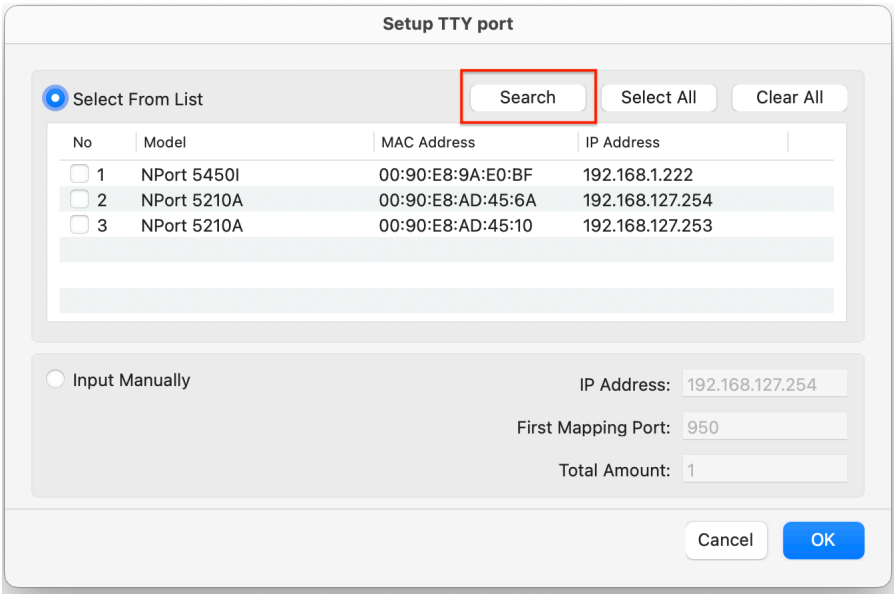
1. In the menu bar, a NPortConnect icon should appear after the installation is completed. Click on the icon and choose **TTY Port Mapping** to start COM port mapping.



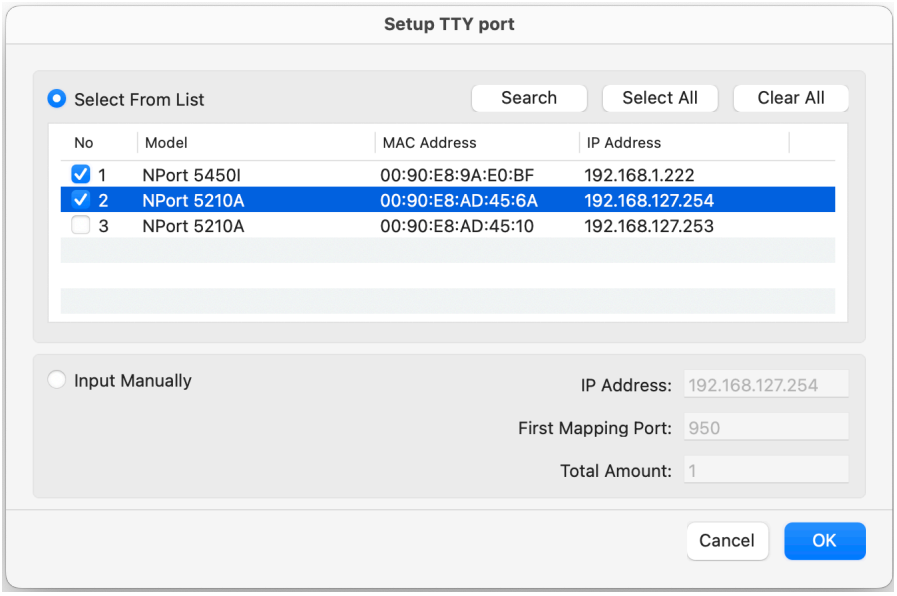
2. Click the **NPortConnect** icon and select **NPort Mapping** for the port mapping function.
3. Click **+** to enter the tty port setup.



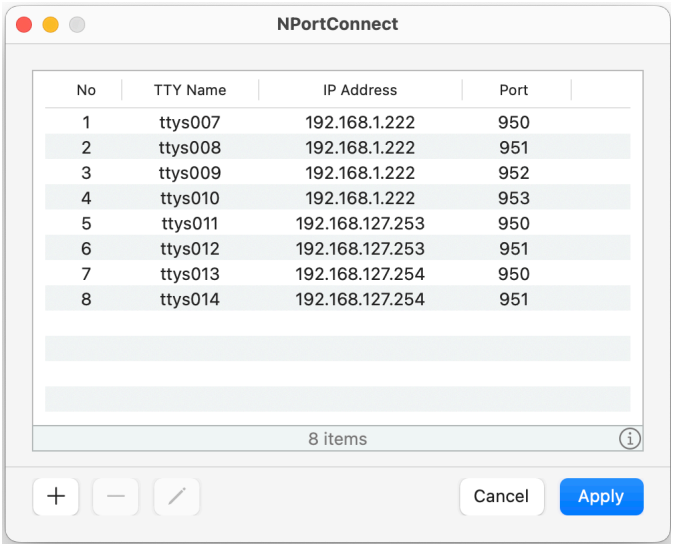
4. Click **Search** to find the NPort that is already setup in the **Hardware Setup** procedure. The **Search** function is broadcast search to locate all the NPort units that are connected to the same LAN as your Mac. Since the Broadcast Search function searches by MAC address and not IP address, all NPort units connected to the LAN will be located, regardless of whether they are part of the same subnet as the host. Or, you can input the IP address manually to find the specific NPort. Once the search is completed, all the NPort found would appear on the list.



5. Select the models that are for the tty port mapping and click **OK**.



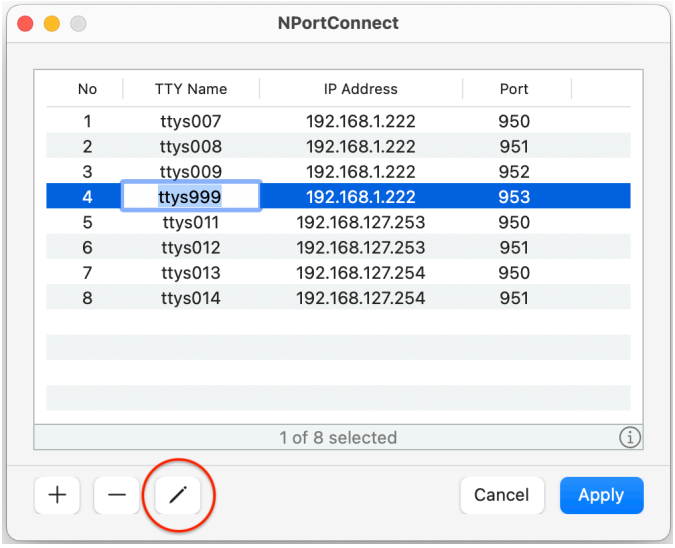
6. NPortConnect would auto assign the tty name and corresponding port number to the IP address of the selected NPort. One port is for data exchange, another port is for sending commands.



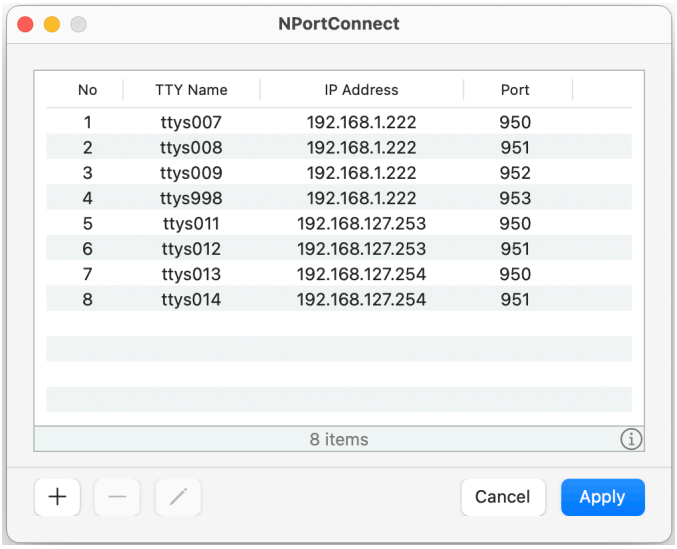
NOTE

It is suggested to rename the assigned tty port, e.g., tty.serial_nport00x or similar, for easier serial communication application integration.

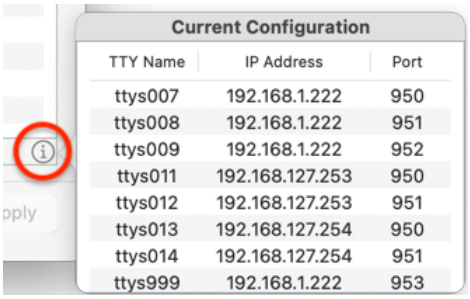
7. The tty name, IP address and port number are editable, or you can click the edit button to edit. Note that these changed values are only for mapping configuration and would not change the values in the NPort settings.



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



9. In each editing interface, there is an info icon at the bottom of the list. A mouse-over would show the original value of each tty port, in case of miss-editing something and you want to refer the original value.

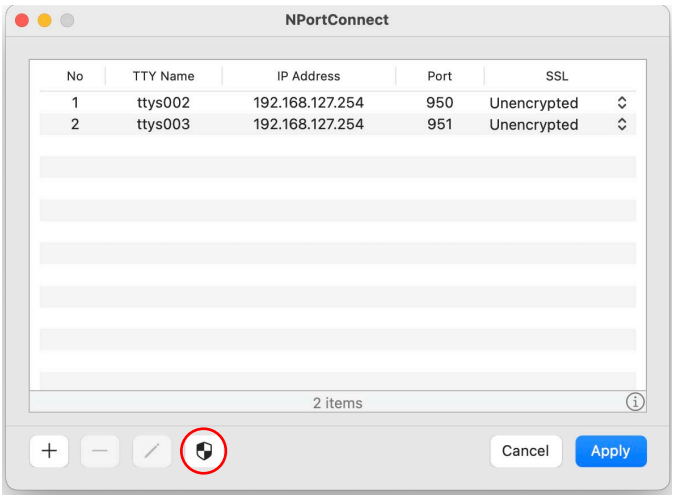


Secured Communication (For NPort 6000-G2 and NPort 6000 models only)

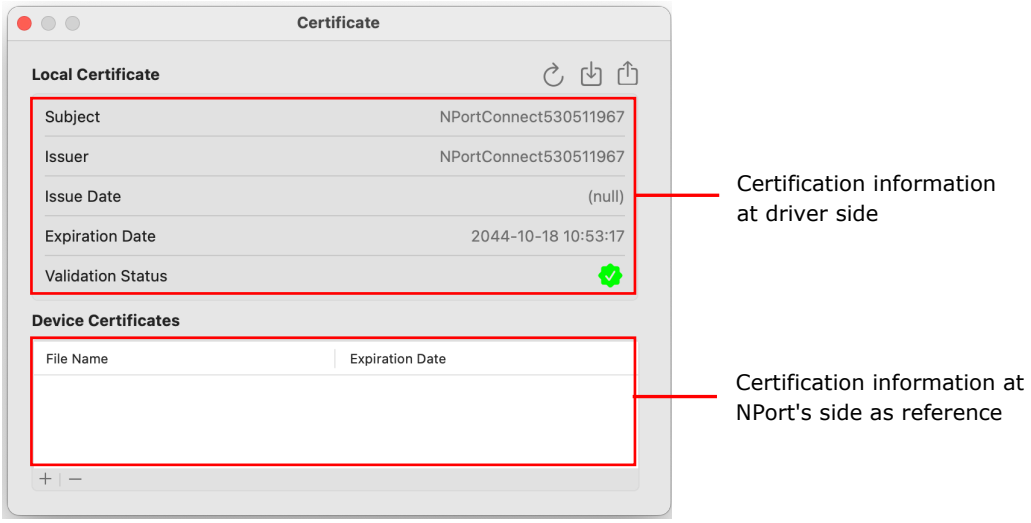
NPort 6000-G2 models and NPort 6000 models provide secured communication for data transmission.

Import Local Certificate

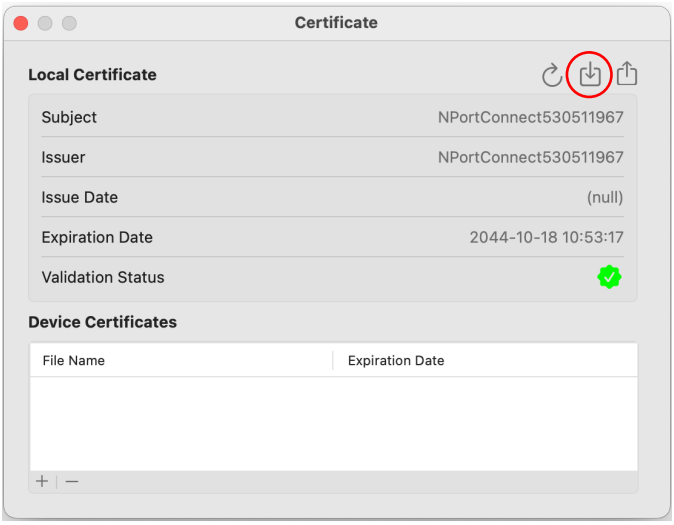
1. Click **Security** icon



Certificate pane would appear:



2. Click **Import Private Key and Certificate**

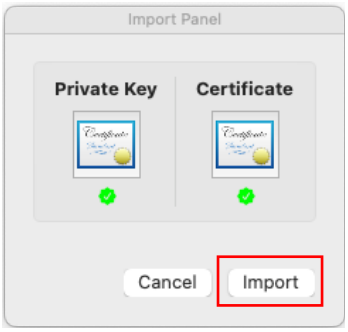


Certificate import window, click either Private Key '+' or Certificate '+' to import your key or certificate.

NOTE

If you file contains both private key and certificate, NPortConnect would help to import to each file holder.

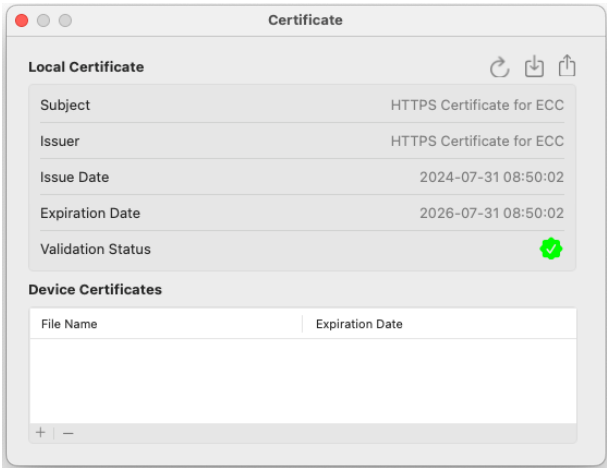
If a private key or certificate is imported successfully, the red cross icon would change to green tick icon.



Or else, it would remain red cross icon.

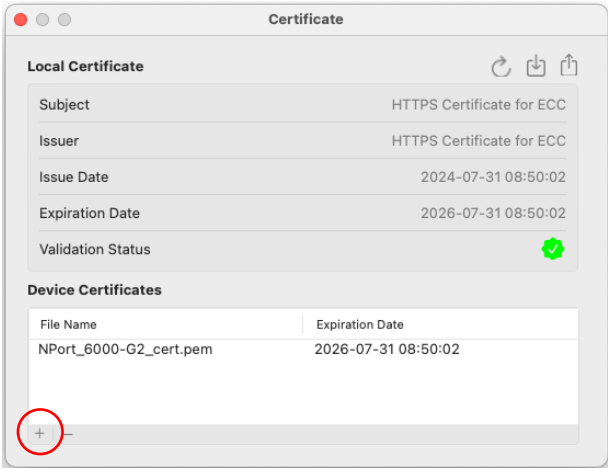
Click **Import** button once everything is imported.

In Certificate pane you should be able to see the **Subject** and **Issuer**, **Issue** and **Expiraration Date** are updated.



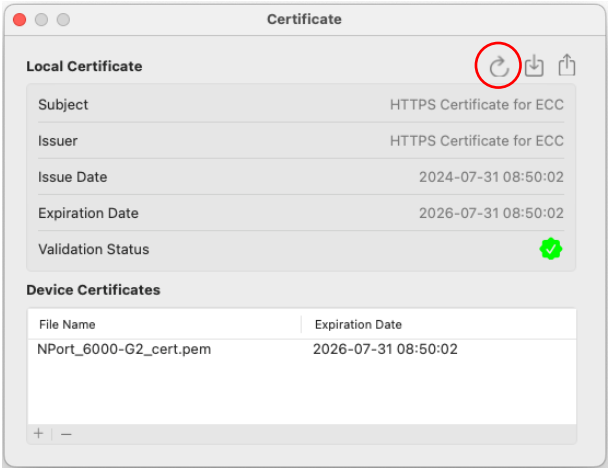
Device Certificate

The **Device Certificate** is to help to display the certificate used in NPort, so you would know which certificate to import for the driver.



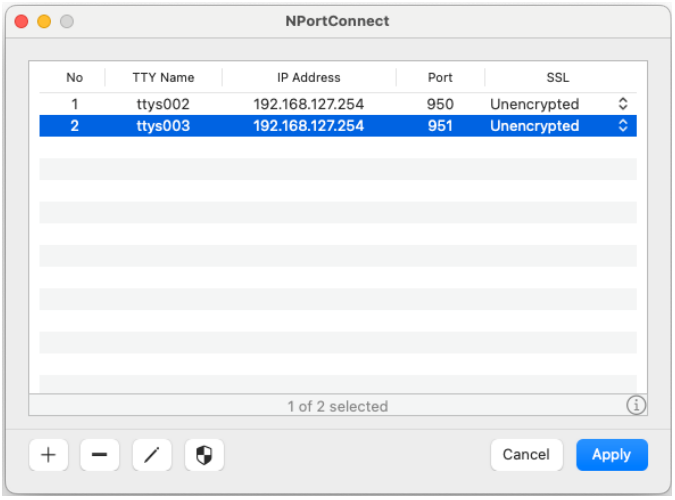
Regenerate Local Certificate

If you wish to cancel the key or certificate that imported, or change the local certificate to another set, click **Regenerate Local Certificate**.



Selecting Proper Encryption Methodology

In the main window, you would need to specify which encryption methodology for your communication with NPort.



Encrypted & Authenticate: NPort 6000-G2 and NPort 6000 models only

Unencrypted: For all models

Uninstalling the Driver

Run the following command to uninstall the driver:

```
$ sudo bash /Library/NPortConnect/uninstall.sh
```

11. Installing WinCE Driver

NPort CE Driver Manager for Windows CE applies to the **NPort 5000 and NPort IA5000 Series** only.

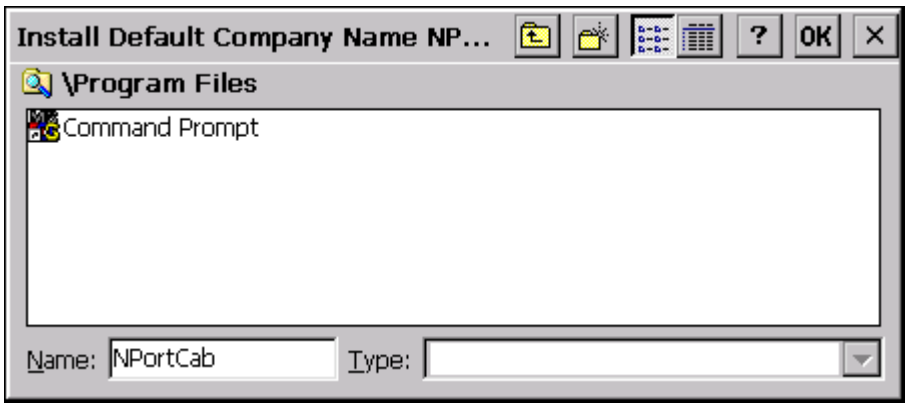
Overview

ATTENTION

Before installing and configuring the NPort Administration suite, make sure your user privilege is set as system administrator.

Installing NPort CE Driver Manager

1. Copy "NPortCab.cab" to Windows CE and install driver by double clicking on it.
2. Click on "OK" to complete the installation when the following screen appears.

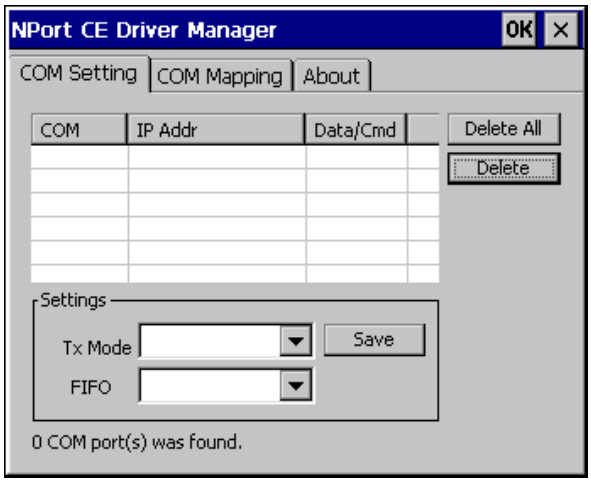


3. Driver installation is now complete and the "NPortCab.cab" icon disappears from the screen. This is normal when installing drivers in Windows CE.

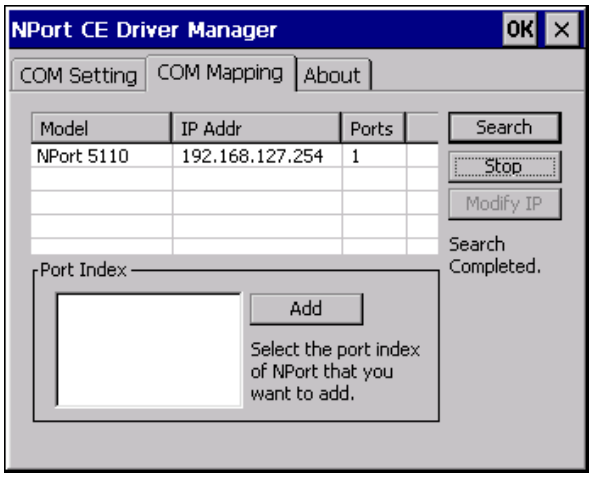
Using NPort CE Driver Manager

After you install NPort CE Driver Manager, you can set up the NPort's serial ports as remote COM ports for your Windows CE. Make sure that the serial port(s) on your NPort are set to Real COM mode when mapping COM ports with NPort CE Driver Manager.

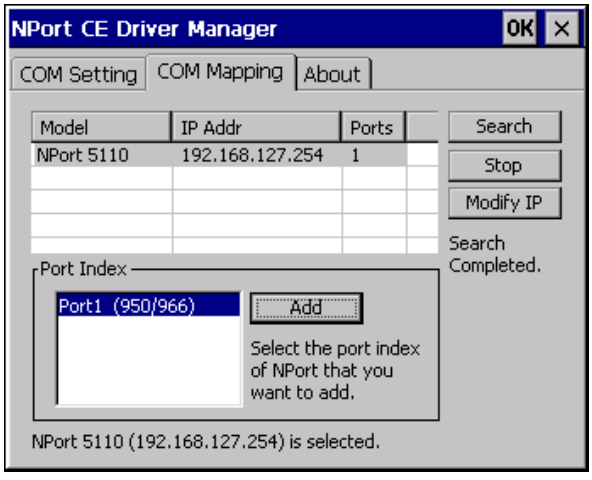
1. Go to **Start > Programs > NPort CE Driver Manager**.



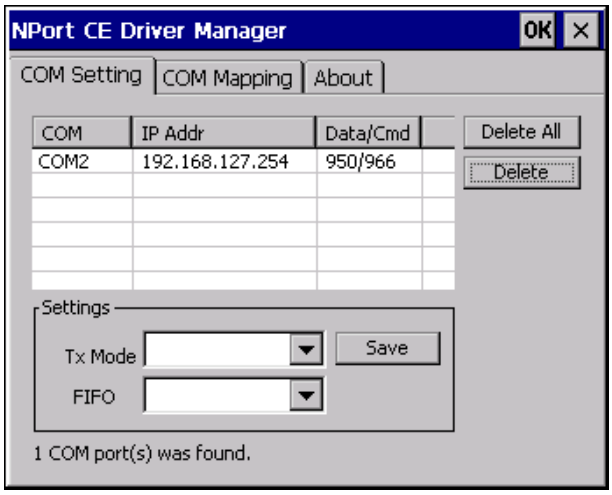
2. Click on the **COM Mapping** page and then the "Search" button to scan for NPort servers



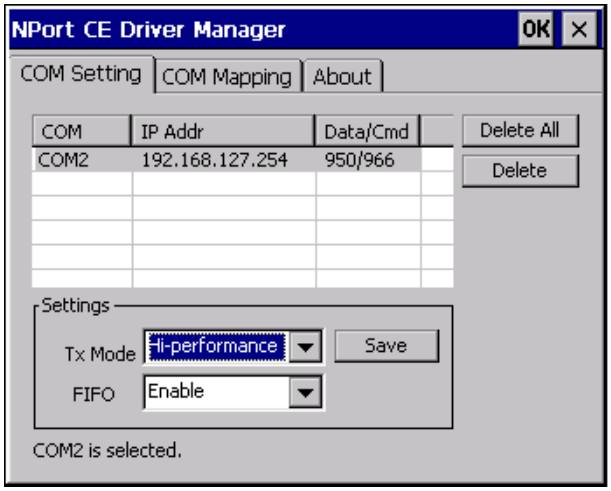
3. All NPort servers that were located will appear in the NPort CE Driver Manager window. Click on the server which COM ports you would like to map to and then select the port index. Note that multiple selections are allowed.
4. Select the port(s) at the Port Index and then click on the "Add" button to map to the COM port(s).



5. Return to the **COM Setting** page. You should be able to see the newly mapped COM port(s).



6. To configure the settings for a particular COM port, select the row of the desired port, and then change the setting in the "Settings" panel, as shown below.



Tx Mode

"Hi-Performance" is the default for Tx mode. After the driver sends data to the NPort server, the driver immediately issues a "Tx Empty" response to the program. Under "Classical mode," the driver will not send the "Tx Empty" response until after confirmation is received from the NPort server's serial port. This causes lower throughput. Classical mode is recommended if you want to ensure that all data is sent out before further processing.

FIFO

If FIFO is disabled, the NPort server will transmit one byte each time the Tx FIFO becomes empty, and an Rx interrupt will be generated for each incoming byte. This will cause a faster response and lower throughput.

12. IP Serial LIB

Overview

What is IP Serial Library?

IP Serial Library is a Windows library with frequently used serial command sets and subroutines. IP Serial Library reduces the complexity and poor efficiency of serial communication over TCP/IP. For example, Telnet can only transfer data, but it cannot monitor or configure the serial line's parameters.

Why Use IP Serial Library?

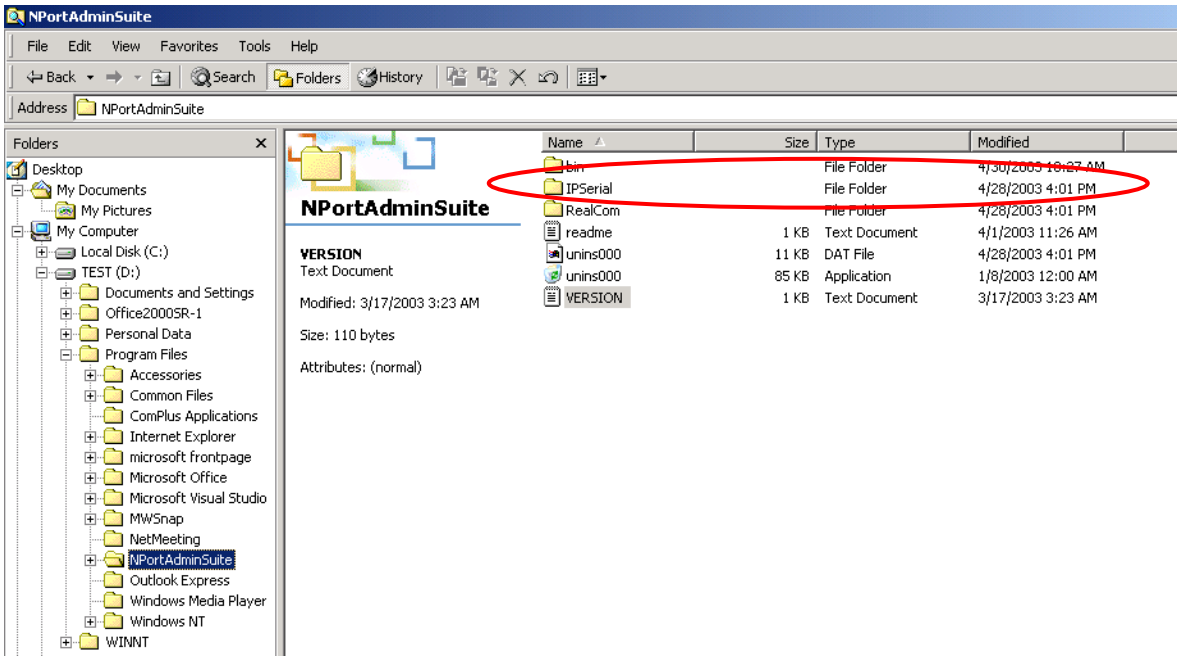
For programmers familiar with serial communication, IP Serial Library provides well-designed function calls that have the same style as Moxa's PComm Library.

IP Serial Library is amazingly simple and easy to understand. By including it in your VB, C, or Delphi programming environment, you can program your own TCP/IP application with the ability to control serial communication parameters.

The NPort serial device server uses 2 TCP ports for communication between the NPort and host computer's Real COM driver. The NPort uses a data port and command port to provide pure data transfer without decoding and encoding. Compared to using only one TCP port to control serial communication (such as RFC 2217), IP Serial Library uses a command port to communicate with the NPort from the user's program. IP Serial Library not only runs with excellent efficiency, but also runs with no decode or encode problems.

How to Install IP Serial Library

IP Serial Lib comes with the NPort Administration Suite. Refer to the IPSerial directory for more detail about the function definitions.



IP Serial LIB Function Groups

Server Control	Port Control	Input/Output Data	Port Status Inquiry	Miscellaneous
nsio_init	nsio_open	nsio_read	nsio_lstatus	nsio_break
nsio_end	nsio_close	nsio_SetReadTimeouts	nsio_data_status	nsio_break_on
nsio_resetserver	nsio_ioctl	nsio_write		nsio_break_off
nsio_checkalive	nsio_flowctrl	nsio_SetWriteTimeouts		nsio_breakcount
	nsio_DTR			
	nsio_RTS			
	nsio_lctrl			
	nsio_baud			
	nsio_resetport			

Example Program

```
char NPort 5100A-Nip="192.168.1.10";
char buffer[255];                          /*data buffer, 255 chars */
int port = 1;                              /*1st port */
int portid;                                /* port handle */
nsio_init();                               /*initial IP Serial Library */
portid = nsio_open(NPort 5100Aip, port);   /*1st port, NPort 5100A
nsio_ioctl(portid, B9600, (BIT_8 | STOP_1 | IP=192.168.1.10 */
P_NONE) );                                 /*set 9600, N81 */
sleep(1000);                               /* wait for 1000 ms for data */
nsio_read(port, buffer, 200);              /* read 200 bytes from port 1 */
nsio_close(portid);                        /* close this serial port */
nsio_end();                                /* close IP Serial Library */
```

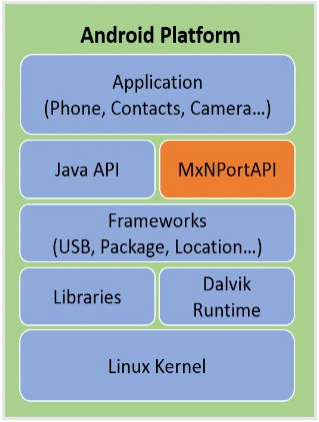
13. Android API Instructions

Overview

If you want to remote control your serial devices on an Android platform, then the MxNPortAPI is a simple application programming tool you can use. The MxNPortAPI helps programmers develop an Android application to access the device server by TCP/IP.

The MxNPortAPI provides frequently used serial command sets like port control, input/output, etc., and the style of developed Android application is similar to Moxa Driver Manager. For more details of the provided functions, refer to the "MxNPortAPI Function Groups" section.

This MxNPortAPI is layered between the Android application and the Android network manager framework. This Android library is compatible with Java 1.7, Android 3.1 (Honeycomb - API version 12), and later versions.

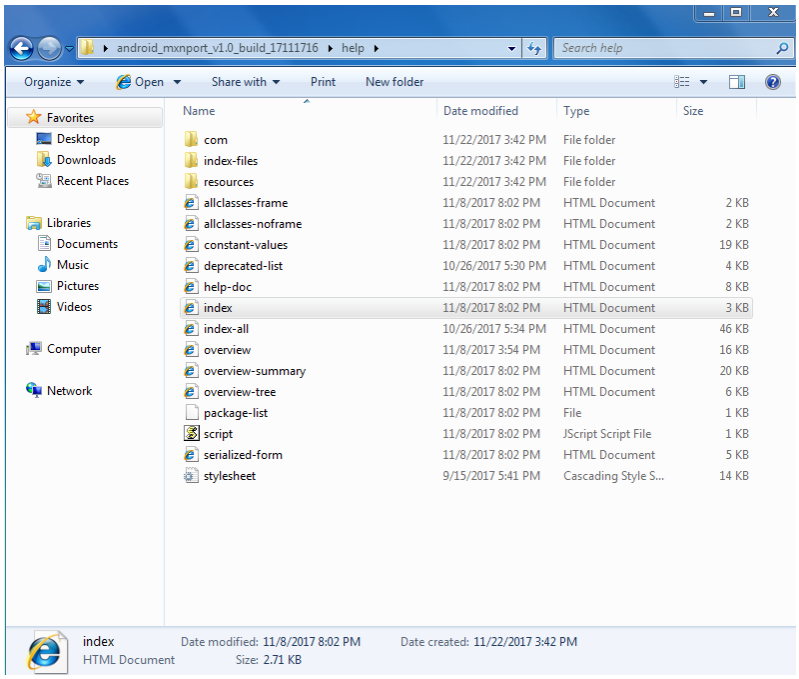


How to Start MxNPortAPI

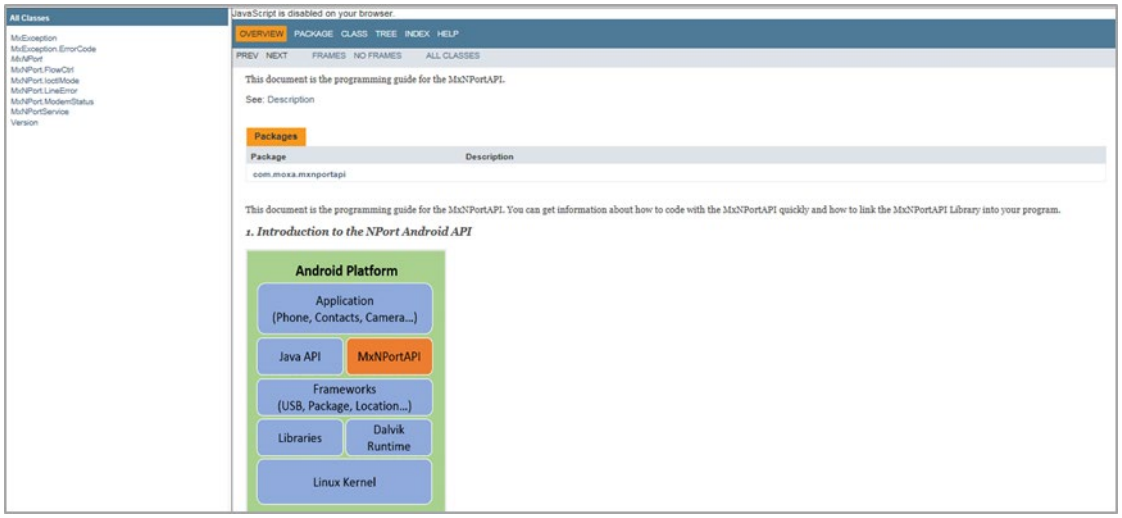
You can download the MxNPortAPI from Moxa's website at http://www.moxa.com, and develop the application program in popular Oss, such as Windows, Linux, or Mac. (You may find it in the **Resource** section under your product page.)

(You can refer to the Android studio website to see the system requirements for the development environment: https://developer.android.com/studio/index.html?hl=zh-tw#Requirements).

To start your application program, unzip the MxNPortAPI file and refer to the index (.html) under the Help directory.



For more details about the installation, refer to the Overview section.



MxNPortAPI Function Groups

The supported functions in this API are listed below:

Port Control	Input/Output	Port Status Inquiry	Miscellaneous
open	read	getBaud	setBreak
close	write	getFlowCtrl	
setIoctlMode		getIoctlMode	
setFlowCtrl		getLineStatus	
setBaud		getModemStatus	
setRTS		getOQueue	
setDTR			
flush			

Example Program

To make sure this API is workable with the device server on an Android platform, see the example program below:

```
Thread thread = new Thread()
{
    @Override
    public void run() {
        /* Enumerate and initialize NPorts on system */
         List<MxNPort> NPortList = MxNPortService.getNPortInfoList();
        if(NPortList!=null){

          MxNPort.IoctlMode mode = new MxNPort.IoctlMode();
            mode.baudRate = 38400;
            mode.dataBits = MxNPort.DATA_BITS_8;
            mode.parity = MxNPort.PARITY_NONE;
            mode.stopBits = MxNPort.STOP_BITS_1;

            MxNPort mxNPort = NPortList.get(0); /* Get first NPort device */
            try {
                byte[] buf = {'H','e','l','l','o',' ','W','o','r','l','d'};
                mxNPort.open(); /*open port*/
                mxNPort.setIoctlMode(mode); /*serial parameters setting*/
                mxNPort.write(buf, buf.length); /*write data*/
                mxNPort.close(); /*close port*/
            } catch (MxException e){
                 /*Error handling*/
            }
        }
     }
};
thread.start();
```

14. Introduction to LCM Display

Typically, you will use either NPort Administrator or the web console to configure the **NPort 5600-8-DT Series (standard temperature models), the NPort 5600 Series (standard temperature models) and the NPort 5410/5430 Series (standard temperature models)**. These are not the only options for configuration. For basic on-site configuration, you can use the LCM console built into the device server, without requiring a connection to the network or a laptop.

In this chapter, we will introduce the basic operation and menu options of LCM display.

Basic Operation

If the NPort works properly, the LCM panel will display a green color. The red Ready LED will also light up, showing that the NPort is receiving power. After the red Ready LED turns to green, you will see a display similar to:

```
N  P  5  4  1  0  _  6  1  4  0  5
1  9  2  .  1  6  8  .  1  2  7  .  2  5  4
```

This is where

- NP5410 is the NPort's name
- 61405 is the NPort's serial number
- 192.168.127.254 is the NPort's IP address

There are four push buttons on the NPort's nameplate. Going from left to right, the buttons are:

Button	Name	Action
menu	menu	activates the main menu, or returns to a lower level
△	up cursor	scrolls up through a list of items shown on the LCM panel's second line
▽	down cursor	scrolls down through a list of items shown on the LCM panel's second line
sel	select	selects the option listed on the LCM panel's second line

The buttons are manipulated in a manner similar to the way a modern cellular phone operates. As you move through the various functions and setting options, note that the top line shows the current menu or submenu name, and the bottom line shows the submenu name or menu item, which is activated by pressing the SEL button.

Detailed Menu Options

The best way to explain all the NPort's LCM functions is to refer to the tree graph shown on the next page. There are three main levels—1, 2, and 3—with each level represented by a separate column. The first thing to remember is that the menu button is used to move back and forth between the LCM panel's default screen and the main menu screen:

```
N  P  5  4  1  0  _  6  1  4  0  5
1  9  2  .  1  6  8  .  1  2  7  .  2  5  4
```


```
M  a  i  n     M  e  n  U
S  e  r  v  e  r     s  e  t  t  i  n  g     ↓
```

In addition, you only need to remember to:

- Use the SEL button to move up one level (i.e., left to right on the tree graph)
- Use the MENU button to move down one level (i.e., right to left on the tree graph)
- Use the cursor keys, r and s, to scroll between the various options within a level (i.e., up and down on the tree graph).

As you use the buttons to operate the LCM display, you will notice that with very few exceptions, moving up one level causes the bottom line of the display to move to the top line of the display. You will also notice that the bottom three options in level 2, and all of the options in level 3 have either a C or D attached. The meaning is as follows:

- C = configurable

  I.e., you may change the setting of this option
- D = display only

  I.e., the setting for this option is displayed, but it cannot be changed (This does NOT mean that the number does not change; only that you cannot change it)

Main Menu						
	Server setting	Serial number				*D*
		Server name				*C*
		Firmware ver				*D*
		Model name				*D*
	Network setting	Ethernet status				*D*
		MAC address				*D*
		IP config				*C*
		IP address				*C*
		Netmask				*C*
		Gateway				*C*
		DNS server 1				*C*
		DNS server 2				*C*
	Serial set	Select port				*C*
		Baudrate				*C*
		Data bit				*C*
		Stop bit				*C*
		Parity				*C*
		Flow control				*C*
		Tx/Rx fifo				*C*
		Interface				*C*
		Tx/Rx bytes				*D*
		Line status				*D*
	Op Mode set	Select port				*C*
		Select mode				*C*
		[mode]				
		Real COM	TCP server	TCP client	UDP svr/cli	
		Alive timeout	Alive timeout	Alive timeout	Delimiter 1	*C*
		Max connection	Inact. time	Inact. time	Delimiter 2	*C*
		Delimiter 1	Max connection	Delimiter 1	Force Tx	*C*
		Delimiter 2	Delimiter 1	Delimiter 2	Dest IP start-1	*C*
		Force Tx	Delimiter 2	Force Tx	Dest IP end-1	*C*
			Force Tx	Dest IP-1	Dest port-1	*C*
			Local TCP port	TCP port-1	Dest IP start-2	*C*
			Command port	Dest IP-2	Dest IP end-2	*C*
				TCP port-2	Dest port-2	*C*
				Dest IP-3	Dest IP start-3	*C*
				TCP port-3	Dest IP end-3	*C*
				Dest IP-4	Dest port-3	*C*
				TCP port-4	Dest IP start-4	*C*
				TCP connect	Dest IP end-4	*C*
					Dest port-4	*C*
					Local port	*C*

	Console	Web console Telnet console				C C
	Ping					C
	Save/Restart					C

The part of the LCM operation that still requires some explanation is how to edit the configurable options. In fact, you will only encounter two types of configurable options.

The first type involves entering numbers, such as IP addresses, Netmasks, etc. Here, you change the number one digit at a time. The up cursor (△) is used to decrease the highlighted digit, the down cursor (▽) is used to increase the highlighted digit, and the SEL button is used to move to the next digit. When the last digit has been changed, pressing SEL simply enters the number into the NPort's memory. The second type of configurable option is when there are only a few options from which to choose (although only one option will be visible at a time). Consider the PARITY attribute under PORT SETTING as an example. Follow the tree graph to arrive at the following PARITY screen. The first option, NONE, is displayed, with a down arrow all the way to the right. This is a sign that there are other options from which to choose.

```
P a r i t Y
N o n e                                    ↓
```

Press the down cursor button once to see Odd as the second option.

```
P a r i t Y                                ↑
O d d                                      ↓
```

Press the down cursor button again to see Even as the third option.

```
P a r i t Y                                ↑
E v e n                                    ↓
```

Press the down cursor button again to see Space as the fourth option.

```
P a r i t Y                                ↑
M a r k                                    ↓
```

Press the down cursor button yet again to see the last option, Space.

```
P a r i t Y                                ↑
S p a c e
```

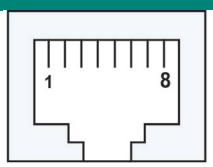
To choose the desired option, press the SEL button when the option is showing on the screen.

Port Pinout Diagrams

Ethernet Port Pinouts

Ethernet RJ45

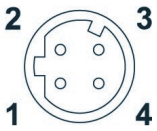
Pin	Signal
1	Tx+
2	Tx-
3	Rx+
6	Rx-



Ethernet M12 (For NPort 5000AI-M12 only)

Ethernet M12:

PIN	TX
1	TD+
2	RD+
3	TD–
4	RD–



Housing: shield

Power M12:

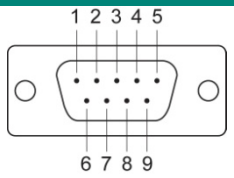
PIN	Description
1	Input V+
2	Not assigned
3	Input V-
4	Not assigned
5	Function ground

Serial Port Pinouts

DB9 Male RS-232 Port Pinouts

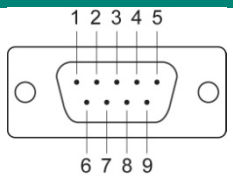
Pin Assignment

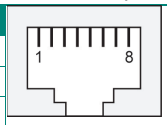
Pin	RS-232
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	–

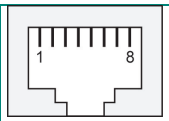


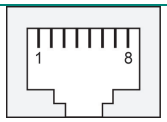
Applicable Products

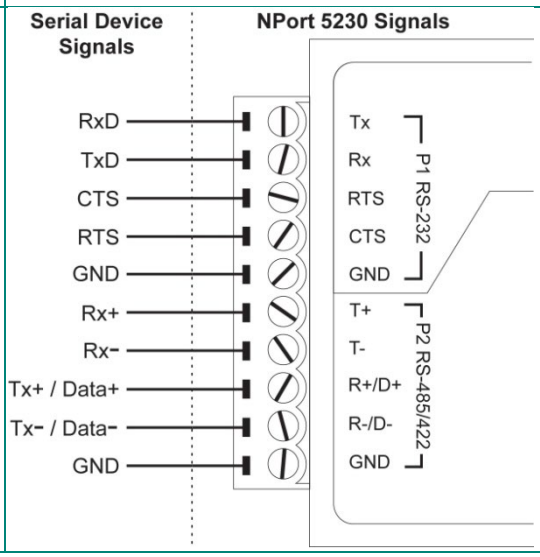
NPort 5110, NPort 5150, NPort 5110A, NPort 5150A, NPort P5150A, NPort_5000AI-M12, NPort 5210A, NPort 5250A, NPort 5410, NPort 5410/5450/5450I, NPort 5610-8-DT, 5650-8-DT, 5650I-8-DT, 5610-8-DTL/DTL-T, 5650-8-DTL/DTL-T, and 5650I-8-DTL/DTL-T, NPort IA5150/5250 NPort IA5150A/5250A

<table>
<tr><th></th><th>Pin Assignment</th><th>Applicable Products</th></tr>
<tr><td>DB9 Male RS-422/485 Port Pinouts</td><td>
<table>
<tr><th>Pin</th><th>RS-422 / 4-wire RS-485</th><th>2-wire RS-485</th></tr>
<tr><td>1</td><td>TxD-(A)</td><td>–</td></tr>
<tr><td>2</td><td>TxD+(B)</td><td>–</td></tr>
<tr><td>3</td><td>RxD+(B)</td><td>Data+(B)</td></tr>
<tr><td>4</td><td>RxD-(A)</td><td>Data-(A)</td></tr>
<tr><td>5</td><td>GND</td><td>GND</td></tr>
<tr><td>6</td><td>–</td><td>–</td></tr>
<tr><td>7</td><td>–</td><td>–</td></tr>
<tr><td>8</td><td>–</td><td>–</td></tr>
</table>


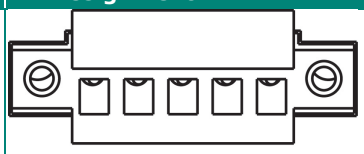
Note: The NPort IA5150A Series' DB9 ports only support RS-232 signals.
</td><td>NPort 5130, NPort 5150, NPort 5130A, NPort 5150A, NPort P5150A, NPort_5000AI-M12, NPort 5250A, NPort 5450/5450I, 5650-8-DT, 5650I-8-DT, 5650-8-DTL/DTL-T, and 5650I-8-DTL/DTL-T, NPort IA5150/5250, NPort IA5250A</td></tr>
<tr><td>8-pin RJ45 RS-232 Port Pinouts</td><td>
<table>
<tr><th>Pin</th><th>RS-232</th></tr>
<tr><td>1</td><td>DSR</td></tr>
<tr><td>2</td><td>RTS</td></tr>
<tr><td>3</td><td>GND</td></tr>
<tr><td>4</td><td>TxD</td></tr>
<tr><td>5</td><td>RxD</td></tr>
<tr><td>6</td><td>DCD</td></tr>
<tr><td>7</td><td>CTS</td></tr>
<tr><td>8</td><td>DTR</td></tr>
</table>


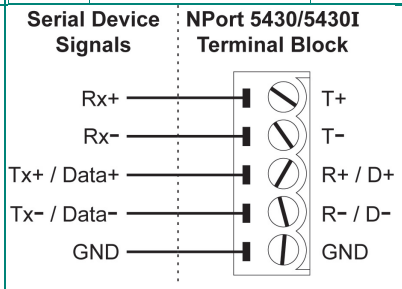
</td><td>NPort 5210/5210I, NPort 5610-8-DT-J, NPort 5610, NPort 5650-8-DT-J</td></tr>
<tr><td>8-pin RJ45 RS-422/485 Port Pinouts</td><td>
<table>
<tr><th>Pin</th><th>RS-422 4-wire RS-485</th><th>2-wire RS-485</th></tr>
<tr><td>1</td><td>–</td><td>–</td></tr>
<tr><td>2</td><td>–</td><td>–</td></tr>
<tr><td>3</td><td>TxD+</td><td>–</td></tr>
<tr><td>4</td><td>TxD-</td><td>–</td></tr>
<tr><td>5</td><td>RxD-</td><td>Data-</td></tr>
<tr><td>6</td><td>RxD+</td><td>Data+</td></tr>
<tr><td>7</td><td>GND</td><td>GND</td></tr>
<tr><td>8</td><td>–</td><td>–</td></tr>
</table>


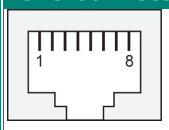
</td><td>NPort 5630</td></tr>
<tr><td>8-pin RJ45 RS-232/422/485 Port Pinouts</td><td>
<table>
<tr><th>Pin</th><th>RS-232</th><th>RS-422 4-wire RS-485</th><th>2-wire RS-485</th></tr>
<tr><td>1</td><td>DSR</td><td>–</td><td>–</td></tr>
<tr><td>2</td><td>RTS</td><td>TxD+</td><td>–</td></tr>
<tr><td>3</td><td>GND</td><td>GND</td><td>GND</td></tr>
<tr><td>4</td><td>TxD</td><td>TxD-</td><td>–</td></tr>
<tr><td>5</td><td>RxD</td><td>RxD+</td><td>Data+</td></tr>
<tr><td>6</td><td>DCD</td><td>RxD-</td><td>Data-</td></tr>
<tr><td>7</td><td>CTS</td><td>–</td><td>–</td></tr>
<tr><td>8</td><td>DTR</td><td>–</td><td>–</td></tr>
</table>


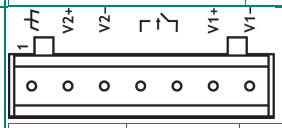
</td><td>NPort 5650, NPort 5650-8-DT-J</td></tr>
<tr><td>Terminal Block RS-232 & RS-422/485 Pinouts</td><td>


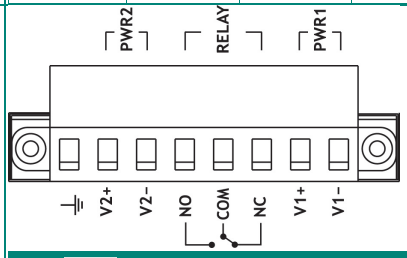
</td><td>NPort 5230</td></tr>
</table>

<table>
<tr><th></th><th>Pin Assignment</th><th>Applicable Products</th></tr>
<tr><td>Terminal Block RS-422/ 485 Port Pinouts</td><td>


<table>
<tr><th>Pin</th><th>2-wire RS-485</th><th>RS-422, 4-wire RS-485</th></tr>
<tr><td>1</td><td>–</td><td>TxD+(B)</td></tr>
<tr><td>2</td><td>–</td><td>TxD-(A)</td></tr>
<tr><td>3</td><td>Data+(B)</td><td>RxD+(B)</td></tr>
<tr><td>4</td><td>Data-(A)</td><td>RxD-(A)</td></tr>
<tr><td>5</td><td>GND</td><td>GND</td></tr>
</table>
</td><td>NPort 5230A, NPort IA5150, NPort IA5150A</td></tr>
<tr><td>Terminal Block RS-422/485 Pinouts</td><td>


</td><td>NPort 5430/5430I</td></tr>
<tr><td>Console Port Pinouts</td><td>


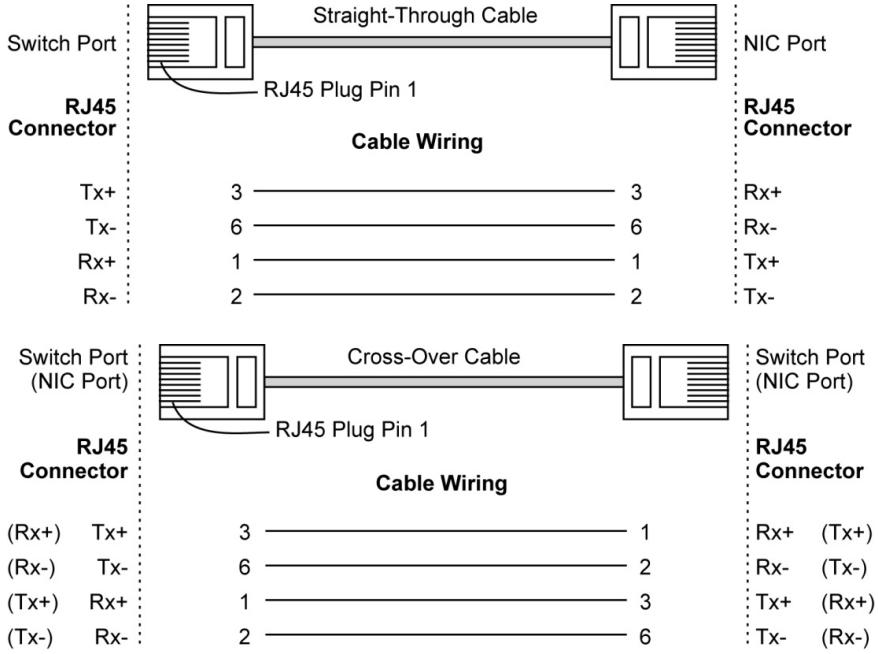
<table>
<tr><th>RJ45 Connector</th><th>Pin</th><th>RS-232</th></tr>
<tr><td></td><td>1</td><td>DSR</td></tr>
<tr><td></td><td>2</td><td>RTS</td></tr>
<tr><td></td><td>3</td><td>GND</td></tr>
<tr><td></td><td>4</td><td>TxD</td></tr>
<tr><td></td><td>5</td><td>RxD</td></tr>
<tr><td></td><td>6</td><td>DCD</td></tr>
<tr><td></td><td>7</td><td>CTS</td></tr>
<tr><td></td><td>8</td><td>DTR</td></tr>
</table>
</td><td>Applies only to DT models.</td></tr>
<tr><td>Power Input and Relay Output Pinouts</td><td>


<table>
<tr><th></th><th>V2+</th><th>V2-</th><th></th><th></th><th>V1+</th><th>V1-</th></tr>
<tr><td>Shielded Ground</td><td>DC Power input 1</td><td>DC Power input 1</td><td>Relay output</td><td>Relay output</td><td>DC Power input 2</td><td>DC Power input 2</td></tr>
</table>
</td><td>NPort IA5150/5250</td></tr>
<tr><td>Power Input and Relay Output Pinouts</td><td>


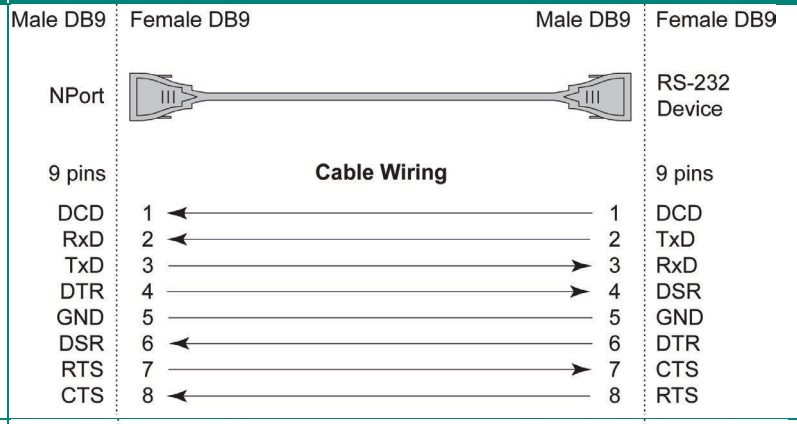
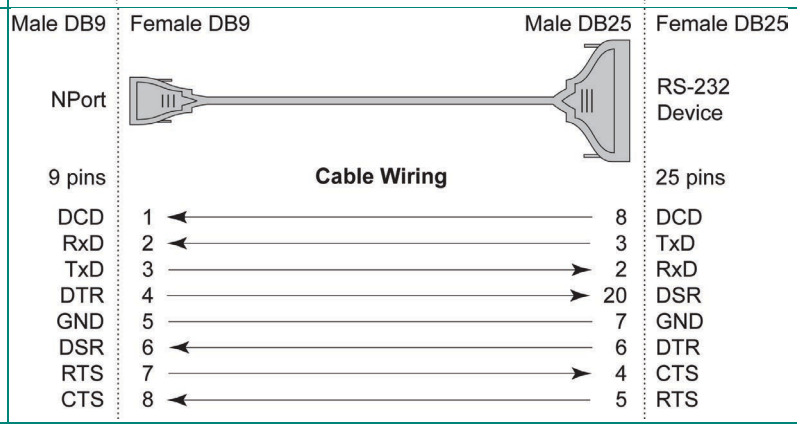
<table>
<tr><th></th><th>PWR1</th><th>PWR2</th><th>RELAY</th></tr>
<tr><td>Shielded Ground</td><td>DC Power Input</td><td>DC Power Input</td><td>Normal Open/Close, Relay output</td></tr>
</table>
</td><td>NPort IA5000A</td></tr>
</table>

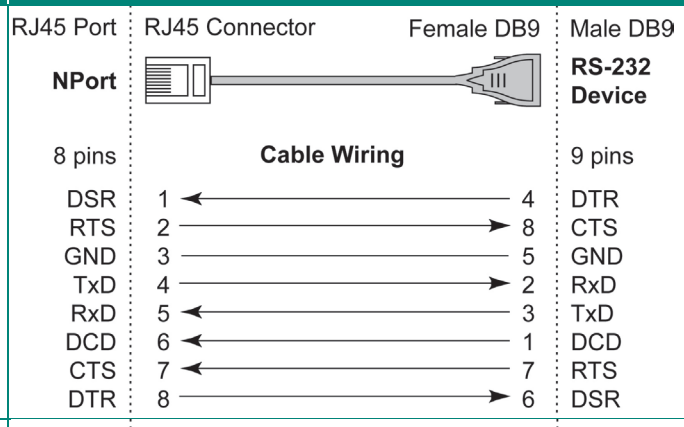
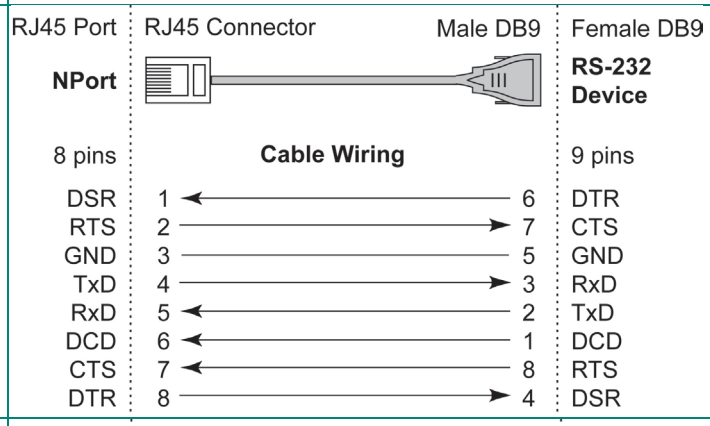
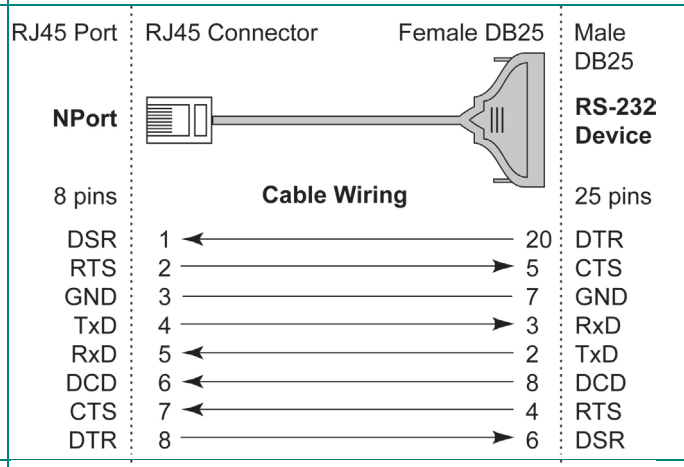
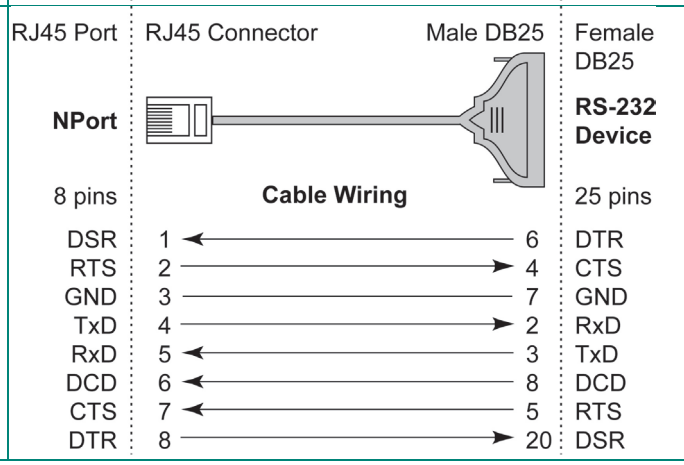
Cable Wiring Diagrams

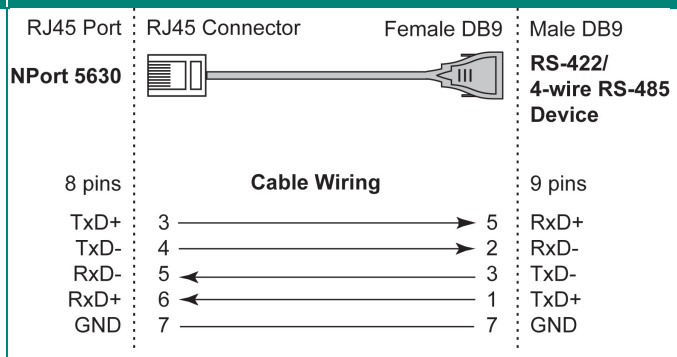
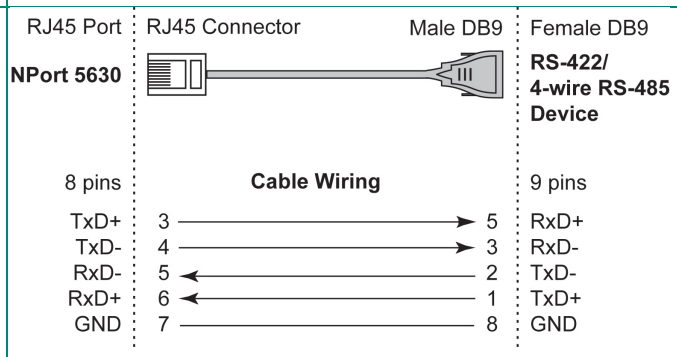
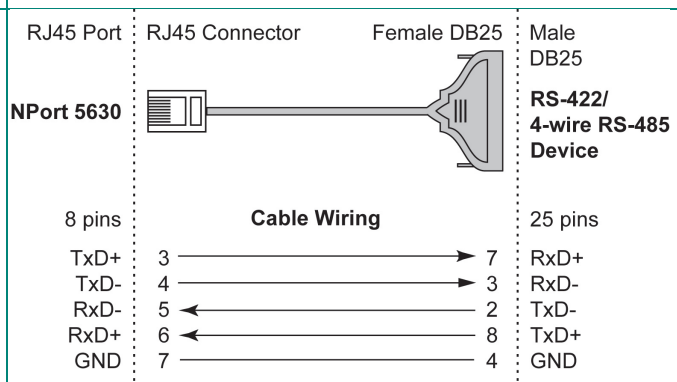
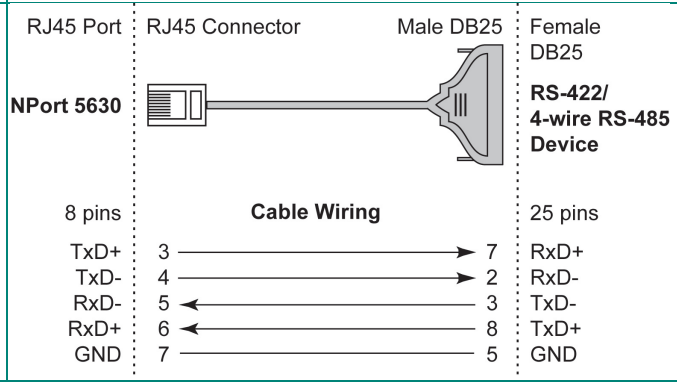
Ethernet Cables

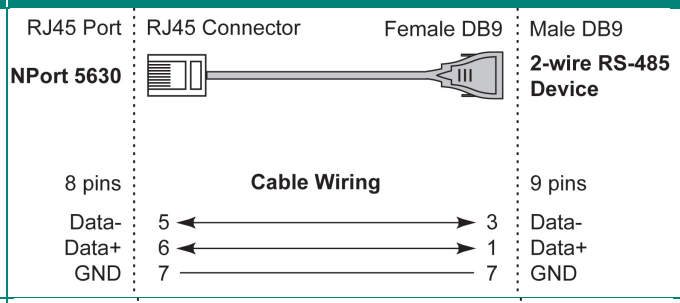
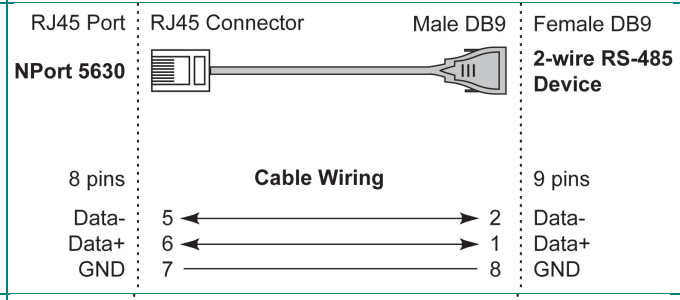
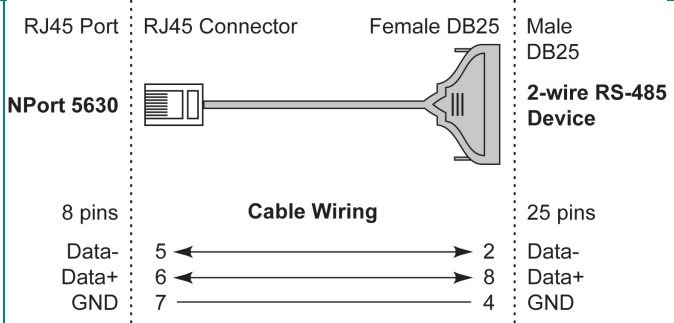
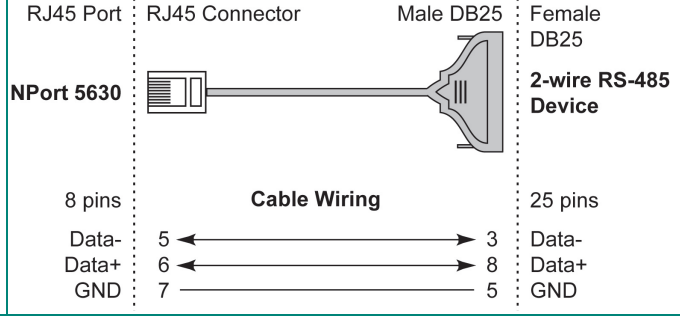


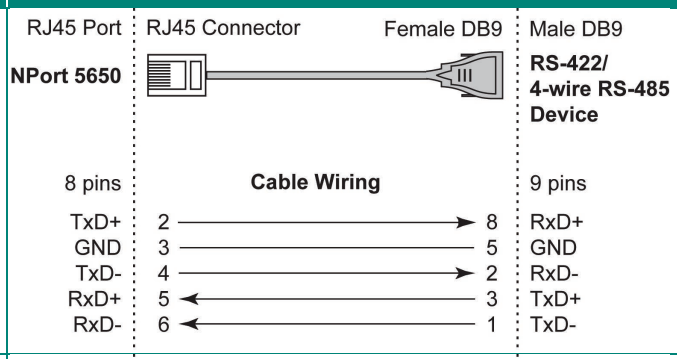
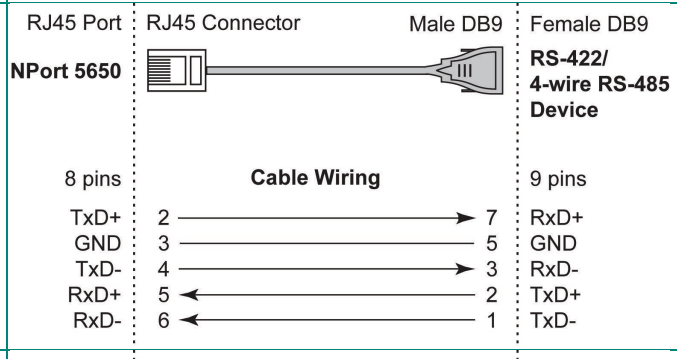
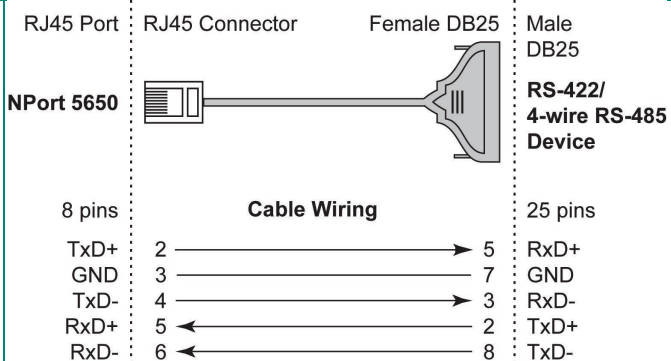
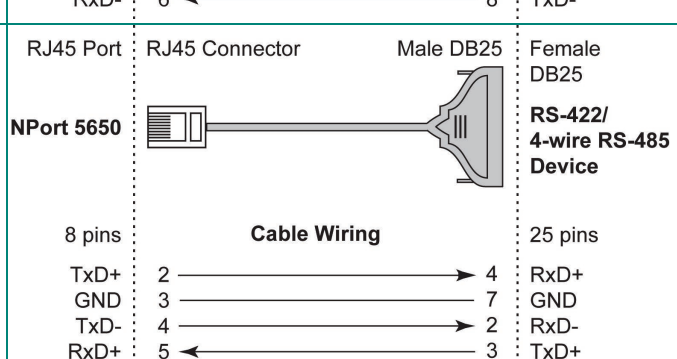
Serial Cables

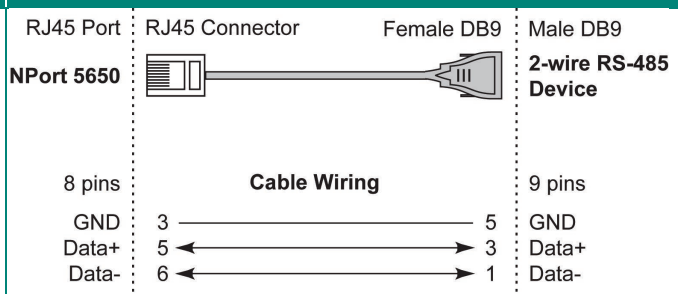
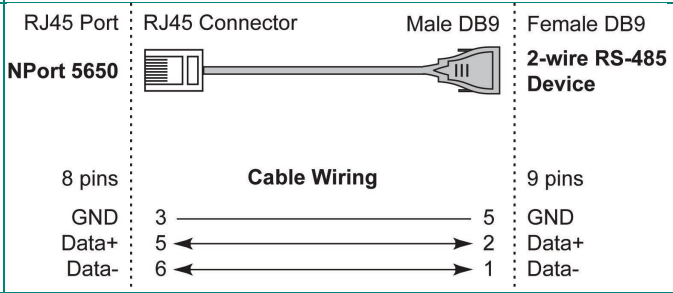
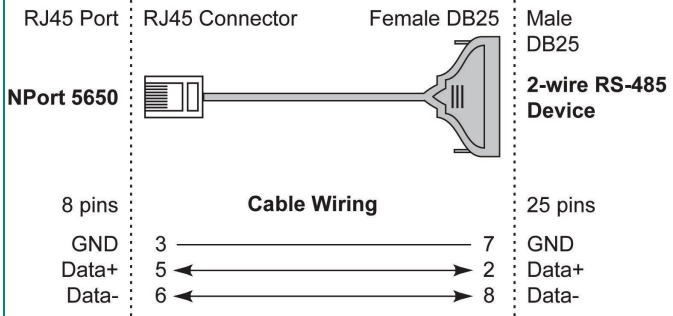
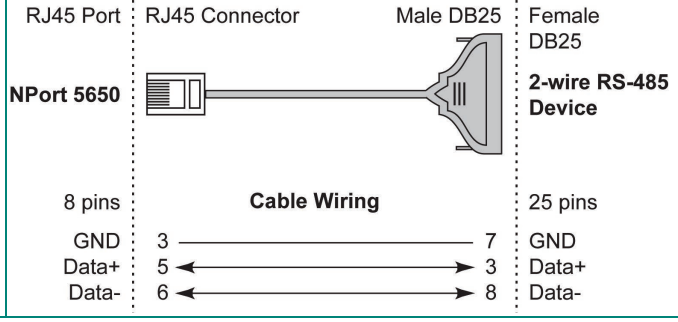
	Moxa Serial Cable Model Name	Serial Cable Wiring Diagrams
Female DB9 to Male DB9 (RS-232)	CBL-F9M9-150 CBL-F9M9-20	
Female DB9 to Male DB25 (RS-232)	N/A	

	Moxa Serial Cable Model Name	NPort 5210, NPort 5610/5650 (RS-232)
8-pin RJ45 to DB9 Female (RS-232)	CBL-RJ45SF9-150 CBL-RJ45F9-150	
8-pin RJ45 to DB9 Male (RS-232)	CBL-RJ45SM9-150 CBL-RJ45M9-150	
8-pin RJ45 to DB25 Female (RS-232)	CBL-RJ45SF25-150 CBL-RJ45F25-150	
8-pin RJ45 to DB25 Male (RS-232)	CBL-RJ45SM25-150 CBL-RJ45M25-150	

	Moxa Serial Cable Model Name	NPort 5630 (RS-422/4-wire RS-485)
8-pin RJ45 to DB9 Female (RS-422/4-wire RS-485)	CBL-RJ45SF9-150 CBL-RJ45F9-150	
8-pin RJ45 to DB9 Male (RS-422/4-wire RS-485)	CBL-RJ45SM9-150 CBL-RJ45M9-150	
8-pin RJ45 to DB25 Female (RS-422/4-wire RS-485)	CBL-RJ45SF25-150 CBL-RJ45F25-150	
8-pin RJ45 to DB25 Male (RS-422/4-wire RS-485)	CBL-RJ45SM25-150 CBL-RJ45M25-150	

	Moxa Serial Cable Model Name	NPort 5630 (2-wire RS-485)
8-pin RJ45 to DB9 Female (2-wire RS-485)	CBL-RJ45SF9-150 CBL-RJ45F9-150	
8-pin RJ45 to DB9 Male (2-wire RS-485)	CBL-RJ45SM9-150 CBL-RJ45M9-150	
8-pin RJ45 to DB25 Female (2-wire RS-485)	CBL-RJ45SF25-150 CBL-RJ45F25-150	
8-pin RJ45 to DB25 Male (2-wire RS-485)	CBL-RJ45SM25-150 CBL-RJ45M25-150	

	Moxa Serial Cable Model Name	NPort 5650 (RS-422/4-wire RS-485)
8-pin RJ45 to DB9 Female (RS-422/4-wire RS-485)	CBL-RJ45SF9-150 CBL-RJ45F9-150	
8-pin RJ45 to DB9 Male (RS-422/4-wire RS-485)	CBL-RJ45SM9-150 CBL-RJ45M9-150	
8-pin RJ45 to DB25 Female (RS-422/4-wire RS-485)	CBL-RJ45SF25-150 CBL-RJ45F25-150	
8-pin RJ45 to DB25 Male (RS-422/4-wire RS-485)	CBL-RJ45SM25-150 CBL-RJ45M25-150	

	Moxa Serial Cable Model Name	NPort 5650 (2-wire RS-485)
8-pin RJ45 to DB9 Female (2-wire RS-485)	CBL-RJ45SF9-150 CBL-RJ45F9-150	
8-pin RJ45 to DB9 Male (2-wire RS-485)	CBL-RJ45SM9-150 CBL-RJ45M9-150	
8-pin RJ45 to DB25 Female (2-wire RS-485)	CBL-RJ45SF25-150 CBL-RJ45F25-150	
8-pin RJ45 to DB25 Male (2-wire RS-485)	CBL-RJ45SM25-150 CBL-RJ45M25-150	

Cable Wiring for NPort 5600-8-DT/DTL Series

Serial Cable Wiring Diagrams

RS-232 Cables

NPort	RJ45	DB9(F)		DB9(M)	DB25(M)	DB25(F)	Serial Device
DSR	1	6	←	4	6	20	DTR
RTS	2	7	→	8	4	5	CTS
GND	3	5	—	5	7	7	GND
TxD	4	3	→	2	2	3	RxD
RxD	5	2	←	3	3	2	TxD
DCD	6	1	←	1	8	8	DCD
CTS	7	8	←	7	5	4	RTS
DTR	8	4	→	6	20	6	DSR

RS-422, 4-wire RS-485 Cables

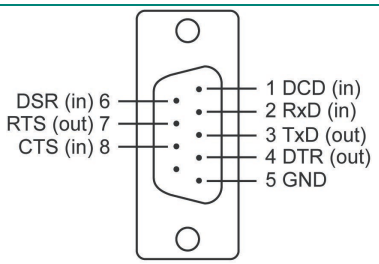
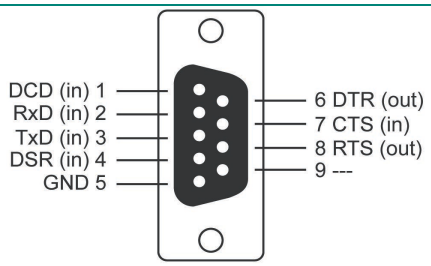
NPort	RJ45	DB9(F)		DB9(M)	DB25(M)	DB25(F)	Serial Device
TxD+	2	2	→	3	3	2	RxD+
GND	3	5	—	5	7	7	GND
TxD-	4	1	→	1	8	8	RxD-
RxD+	5	3	←	2	2	3	TxD+
RxD-	6	4	←	6	20	6	TxD-

2-wire RS-485 Cables

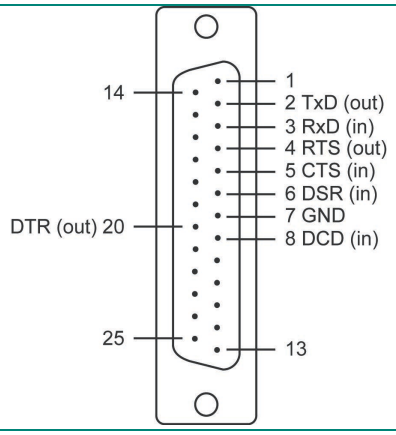
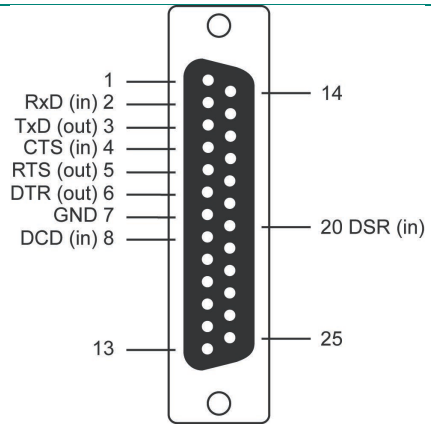
NPort	RJ45	DB9(F)		DB9(M)	DB25(M)	DB25(F)	Serial Device
GND	3	5	—	5	7	7	GND
Data+	5	3	↔	2	2	3	Data+
Data-	6	4	↔	6	20	6	Data-

Pin Assignments for DB9 and DB25 Connectors

Pin Assignments for DB9 Male and Female Connectors

DB9 Male Connector	DB9 Female Connector
	

Pin Assignments for DB25 Male and Female Connectors

DB25 Male Connector	DB25 Female Connector
	

B. Adjustable Pull High/Low Resistors for the RS-485 Port

In some critical environments, you may need to add termination resistors to prevent the reflection of serial signals. When using termination resistors, it is important to set the pull high/low resistors correctly so that the electrical signal is not corrupted. Since there is no resistor value that works for every environment, DIP switches or jumpers are used to set the pull high/low resistor values for each RS-485 port.

ATTENTION

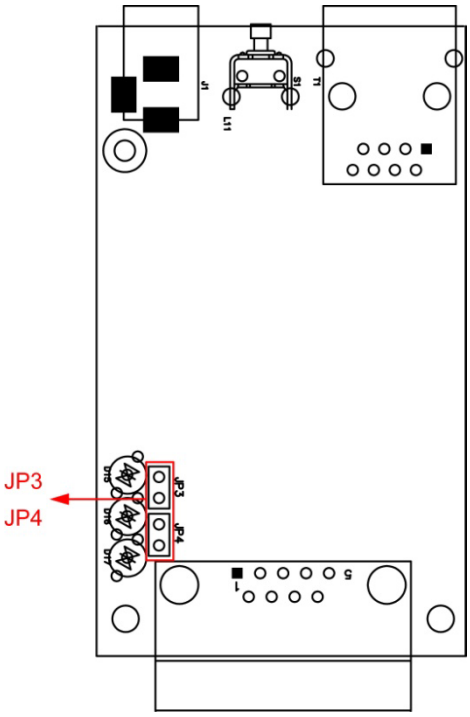
Do not use the 1 kΩ setting on NPorts when using the RS-232 interface. Doing so will degrade the RS-232 signals and shorten the maximum allowed communication distance.

Series	Pull H/L resistance	Terminator
NPort 5230	Fixed, 1 kΩ	N/A
NPort 5232		
NPort 5232I		
NPort 5130	Adjustable, ON = 1 kΩ / OFF = 150 kΩ default = 150 kΩ	N/A
NPort 5150		
NPort 5130A		
NPort 5150A		
NPort 5450AI-M12		
NPort 5430	Adjustable, ON = 1 kΩ / OFF = 150 kΩ default = 150 kΩ	120 Ω
NPort 5450		
NPort 5430I		
NPort 5450I		
NPort 5630		
NPort 5650		
NPort 5230A		
NPort 5250A		
NPort 5650-8-DT/DTL		
NPort P5150A		
NPort IA-5150/IA-5250		
NPort IA5150A/5250A		
NPort IA5450A		
NPort IA-5150I		

NPort 5130/5150 Series (Jumpers)

To set a pull high/low resistor to 150 kΩ, make sure that the two jumpers (JP3 and JP4) assigned to the serial port are not shorted by jumper caps. This is the default setting.

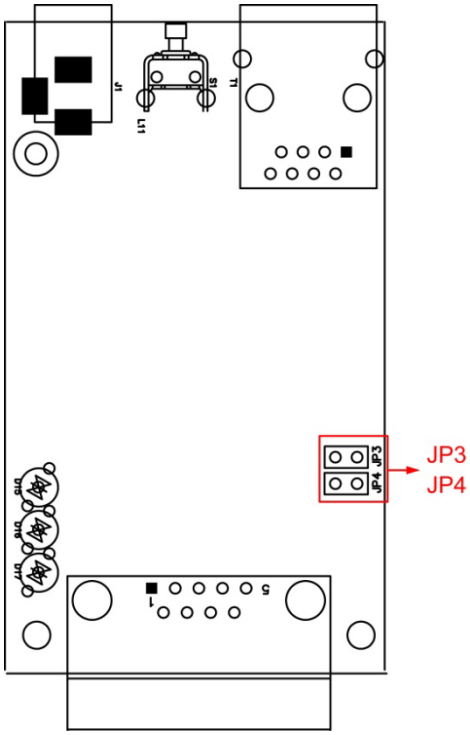
To set a pull high/low resistor to 1 kΩ, make sure that the two jumpers (JP3 and JP4) assigned to the serial port are shorted by jumper caps.



NPort 5130A/5150A (Jumpers)

To set a pull high/low resistor to 150 kΩ, make sure that the two jumpers (JP3 and JP4) assigned to the serial port are not shorted by jumper caps. This is the default setting.

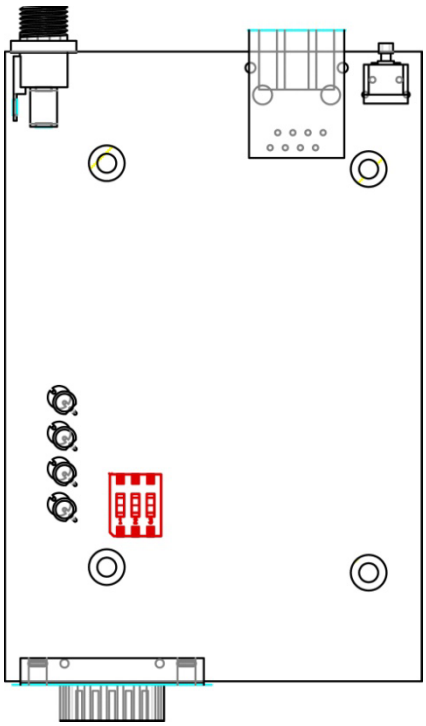
To set a pull high/low resistor to 1 kΩ, make sure that the two jumpers (JP3 and JP4) assigned to the serial port are shorted by jumper caps.

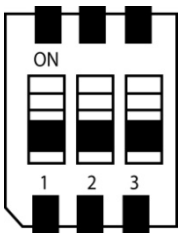


NPort P5150A (DIP Switches)

To set the pull high/low resistors to 150 KΩ, make sure both the assigned DIP switches are in the OFF position. This is the default setting.

To set the pull high/low resistors to 1 KΩ, make sure both the assigned DIP switches are in the ON position.





SW	1	2	3
	Pull-high resistor	Pull-low resistor	Terminator
ON	1 kΩ	1 kΩ	120 Ω
OFF	150 kΩ*	150 kΩ*	–*

*** Default**

NPort 5230/5232/5232I (Fixed)

The pull high/low value is 1 KΩ, and the value is fixed.

NPort 5430/5430I/5450/5450I Models (DIP Switches)

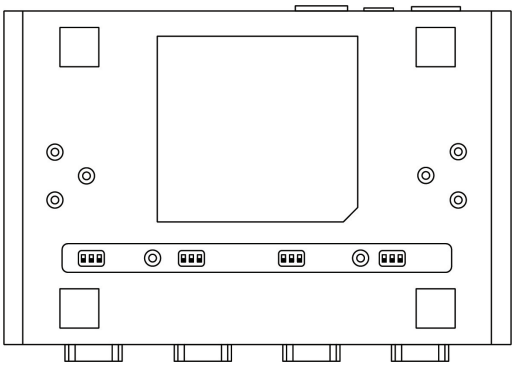
To set the pull high/low resistors to 150 KΩ, make sure both of the assigned DIP switches are in the OFF position. This is the default setting.

To set the pull high/low resistors to 1 KΩ, make sure both of the assigned DIP switches are in the ON position.

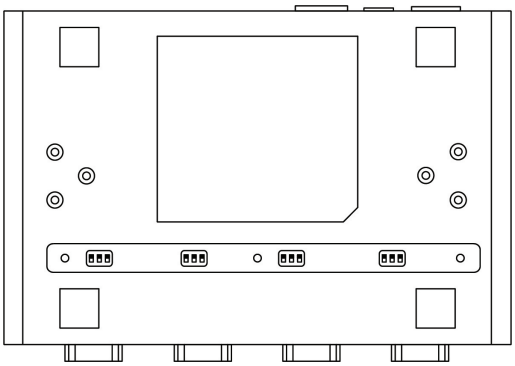
Pull high/low resistors for the RS-485 Port

	SW	1	2	3
		Pull High	Pull Low	Terminator
	ON	1 KΩ	1 KΩ	120 Ω
Default	OFF	150 KΩ	150 KΩ	–

HW version v1.3.0 or earlier



HW version v1.4.0 or later



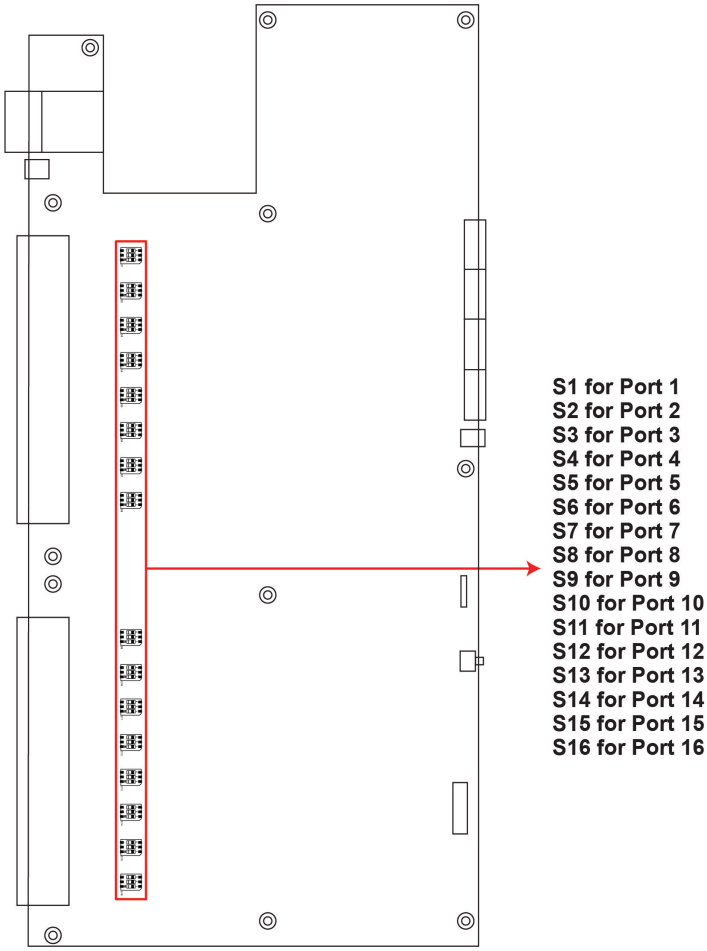
NPort 5630/5650 Series (DIP Switches)

To set the pull high/low resistors to 150 KΩ, make sure both of the assigned DIP switches are in the OFF position. This is the default setting.

To set the pull high/low resistors to 1 KΩ, make sure both of the assigned DIP switches are in the ON position.

Pull high/low resistors for the RS-485 Port

	SW	1	2	3
		Pull High	Pull Low	Terminator
	ON	1 KΩ	1 KΩ	120 Ω
Default	OFF	150 KΩ	150 KΩ	–



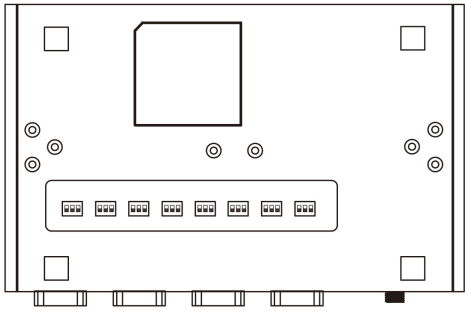
NOTE

In the NPort 5630 V3.4.0 and later, a DIP switch for the terminator has been added.

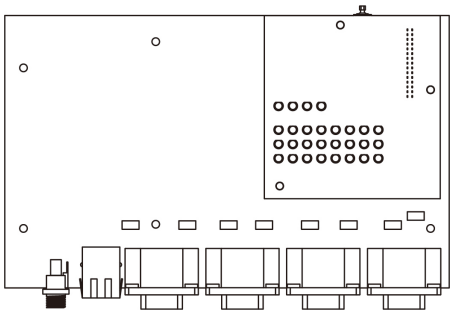
In the NPort 5650 V1.5.0 and later, a DIP switch for the terminator has been added.

NPort 5650-8-DT/DTL Series (DIP Switches)

- **NPort 5650-8-DT:** Use the DIP switches on the bottom panel to configure each device port's pull high/low resistors. You will need to unscrew the DIP switch cover to access the DIP switches.



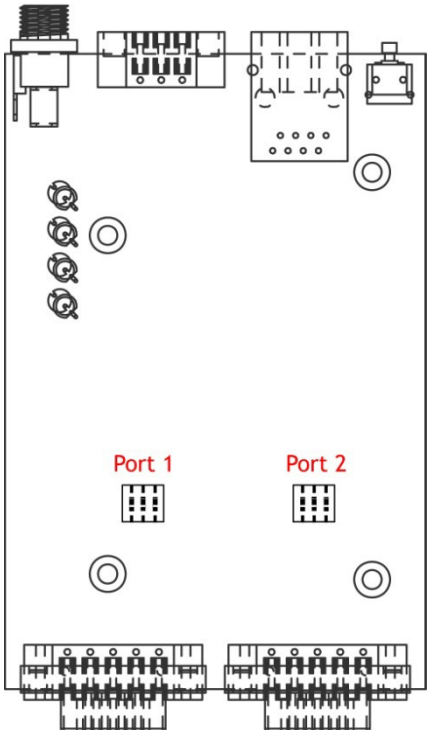
- **NPort 5650-8-DTL:** Remove the top cover to access the DIP switches used to configure each device port's pull high/low resistors (note that SW4 is reserved for future use).

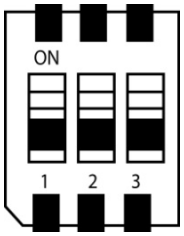


The pull high/low resistor values for each device port are set as follows:

	SW	1	2	3
		Pull High	Pull Low	Terminator
	ON	1 KW	1 KW	120 W
Default	OFF	150 KW	150 KW	–

NPort 5230A/5250A (DIP Switches)





SW	1	2	3
	Pull-high resistor	Pull-low resistor	Terminator
ON	1 KΩ	1 KΩ	120 Ω
OFF	150 KΩ*	150 KΩ*	–*

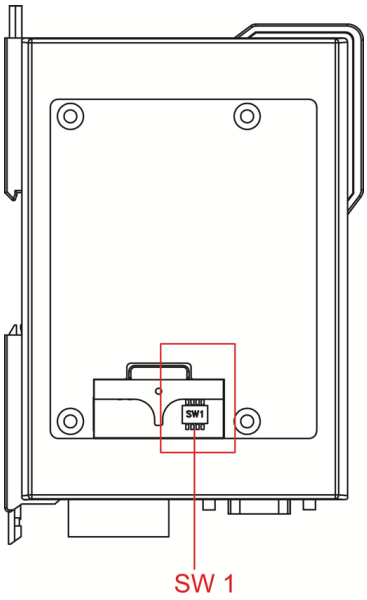
*** Default**

To set the pull high/low resistors to 150 KΩ, make sure both the assigned DIP switches are in the OFF position. This is the default setting.

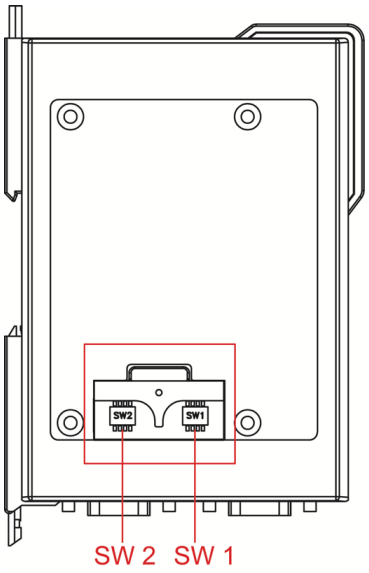
To set the pull high/low resistors to 1 KΩ, make sure both of assigned DIP switches are in the ON position.

NPort IA5000 Series (DIP Switches)

NPort IA5150 Models



NPort IA5250 Models



The DIP switches are located beneath the DIP switch panel on the side of the unit.

To add a 120 Ω termination resistor, set switch 3 to ON; set switch 3 to OFF (the default setting) to disable the termination resistor.

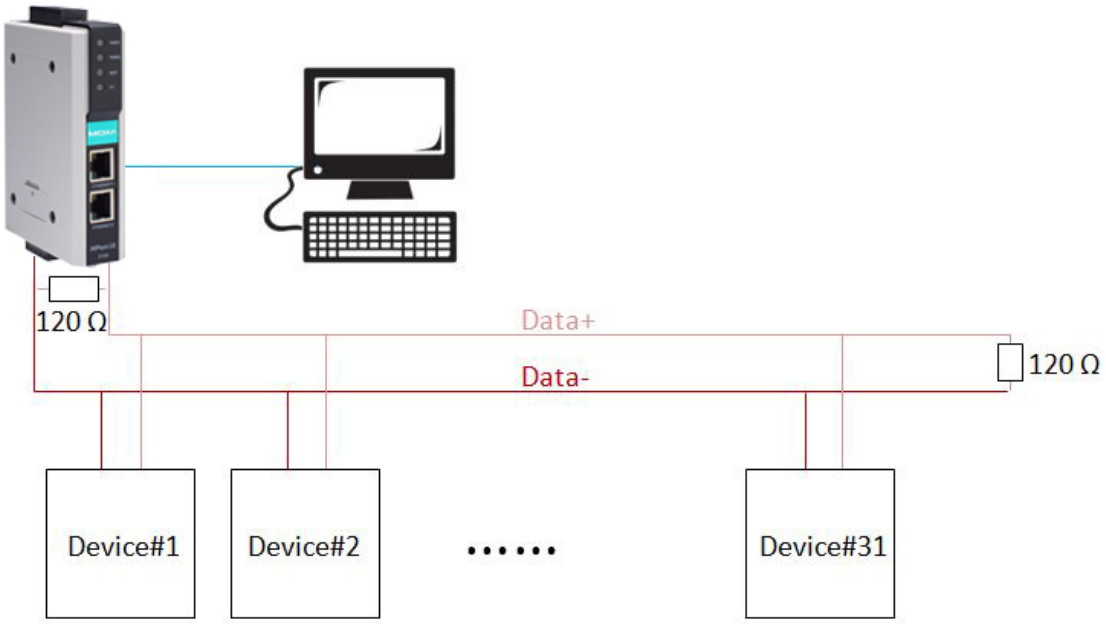
To set the pull high/low resistors to 150 KΩ, set switches 1 and 2 to OFF. This is the default setting.

To set the pull high/low resistors to 1 KΩ, set switches 1 and 2 to ON.

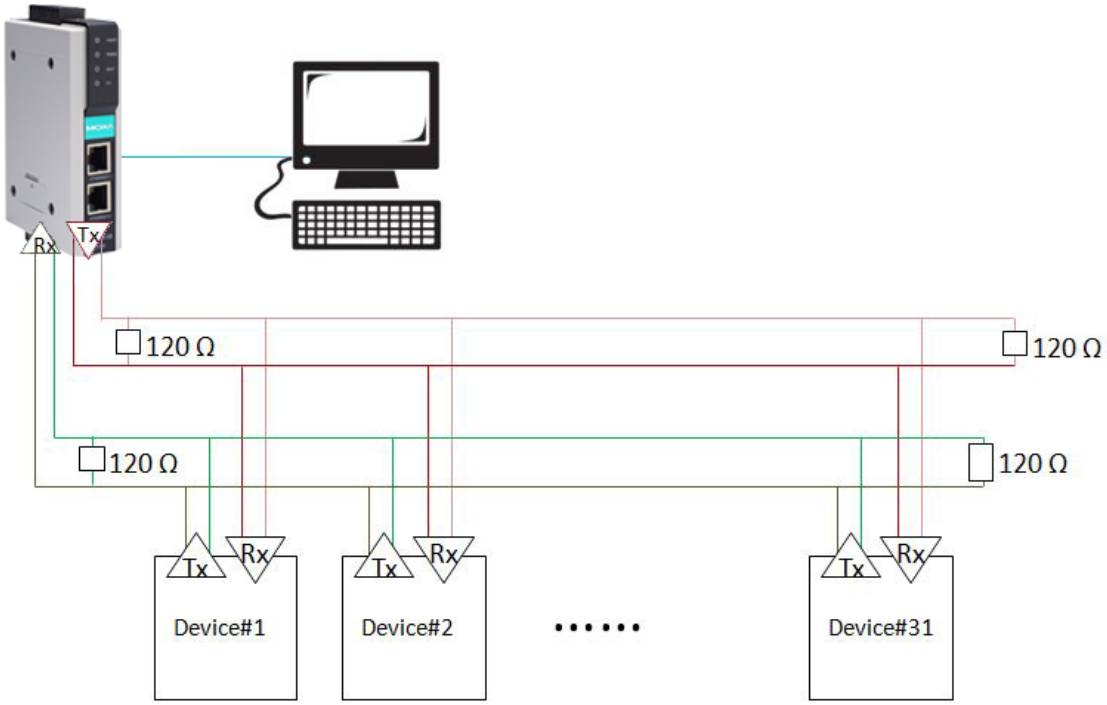
Switch 4 on the port's assigned DIP switch is reserved.

When setting up your RS-485 and RS-422 networks, use termination resistors to prevent signal reflections. The NPort IA5000 Series has built-in pull high/low resistors and terminators, so you can consider enabling them when they have a communication problem by the default settings with RS-485 and RS-422 networks. The following figures illustrate how to properly configure termination for a 2-wire RS-422/RS485 network, and a 4-wire RS485 network. You will usually only need to install termination resistors (typically 120 Ω) on the first and last devices on your network.

Setting up terminators for a 2-wire RS422/RS485 network



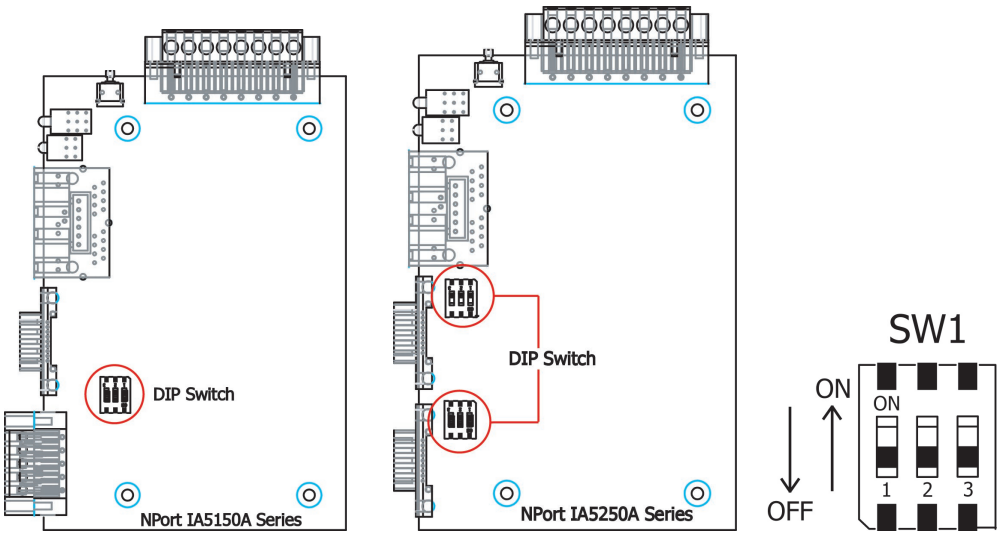
Setting up terminators for a 4-wire RS485 network



NPort IA5000A Series (DIP Switches)

The DIP switches are on the PCB board; you will need to take off the covers to access them. To set the pull-high resistor to 150 KΩ, flip DIP1 to "OFF," and then set the pull-low resistor to 150 KΩ, and then flip DIP2 to "OFF." To set the pull-high resistor to 1 KΩ, flip DIP1 to "ON," and then set the pull-low resistor to 1 KΩ, and then flip DIP2 to "ON." Make sure that DIP3 is "ON" to enable the 120Ω terminator. The default settings for the pull-high and pull-low resistors and the terminators are all at "OFF."

NPort IA5150A/IA5250A Series



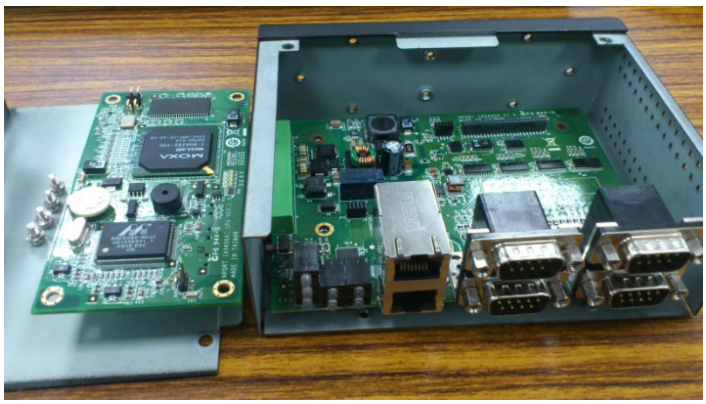
NPort IA5450A Series

Follow the instructions below to change the pull-high/low DIP switch settings.

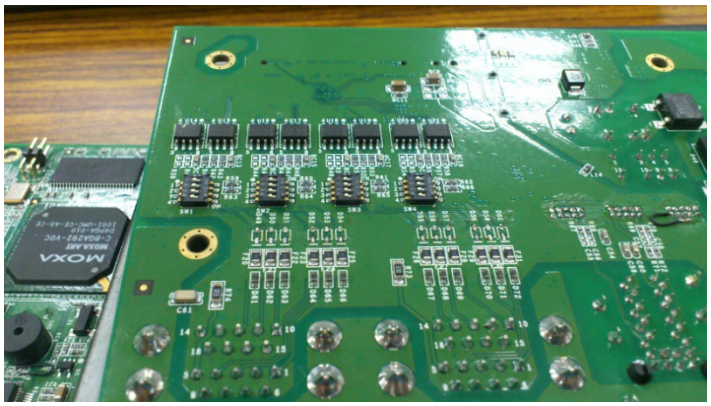
Step 1: Remove the case

Step 2: Remove the first tier

Step 3: Remove the 4 pillars



Step 4: Pull-high/low DIP switches are on the backside of the board



From right to left, the DIP switches are used for port 1 to port 4. SW1 is used for port 1, SW2 for port 2, SW3 for port 3, and SW4 for port 4. The functions of DIP1, DIP2, and DIP3 are shown in the following table (DIP4 is reserved).

Pull-high/low Resistors for the RS-485 Port

	SW	DIP1	DIP2	DIP3
		Pull-high	Pull-low	Terminator
	ON	1 kΩ	1 kΩ	120 kΩ
Default	**OFF**	150 kΩ	150 kΩ	–

C. Well-known Port Numbers

In this appendix, which is included for your reference, we provide a list of well-known port numbers that may cause network problems if you set the NPort to one of these ports. Refer to RFC 1700 for well-known port numbers, or refer 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, can only be used by system processes or by programs executed by privileged users. The following table shows famous port numbers among the well-known port numbers. For more details, visit the IANA website at http://www.iana.org/assignments/port-numbers.

TCP Socket	Application Service
0	reserved
1	TCP Port Service Multiplexor
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
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 – 223	Reserved for future use

UDP Socket	Application Service
0	reserved
2	Management Utility
7	Echo
9	Discard
11	Active Users (systat)
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 (TETP)
70	Gopler 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 (nnp
161	SNMP (Simple Network Mail Protocol)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

D. SNMP Agents with MIB II & RS-232/422/485 Like Groups

The NPort has built-in SNMP (Simple Network Management Protocol) agent software. It supports SNMP Trap, RFC1317 RS-232 like group and RFC 1213 MIB-II. The following table lists the standard MIB-II group, as well as the variable implementation for the NPort device server.

RFC1213 MIB-II Supported SNMP Variables:

System MIB	Interfaces MIB	IP MIB	ICMP MIB
SysDescr	itNumber	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	IcmpOutMsgs
	ifInDiscards	ipReasmReqds	IcmpOutErrors
	ifInErrors	ipReasmOKs	IcmpOutDestUnreachs
	ifInUnknownProtos	ipReasmFails	IcmpOutTimeExcds
	ifOutOctets	ipFragOKs	IcmpOutParmProbs
	ifOutUcastPkts	ipFragFails	IcmpOutSrcQuenchs
	ifOutNUcastPkts	ipFragCreates	IcmpOutRedirects
	ifOutDiscards	ipAdEntAddr	IcmpOutEchos
	ifOutErrors	ipAdEntIfIndex	IcmpOutEchoReps
	ifOutQLen	ipAdEntNetMask	IcmpOutTimestamps
	ifSpecific	ipAdEntBcastAddr	IcmpOutTimestampReps
		ipAdEntReasmMaxSize	IcmpOutAddrMasks
		IpNetToMediaIfIndex	IcmpOutAddrMaskReps
		IpNetToMediaPhysAddress	
		IpNetToMediaNetAddress	
		IpNetToMediaType	
		IpRoutingDiscards	

UDP MIB	TCP MIB	SNMP MIB	Address Translation MIB
UdpInDatagrams	tcpRtoAlgorithm	snmpInPkts	AtIfIndex
UdpNoPorts	tcpRtoMin	snmpOutPkts	AtPhysAddress
UdpInErrors	tcpRtoMax	snmpInBadVersions	AtNetAddress
UdpOutDatagrams	tcpMaxConn	snmpInBadCommunityNames	
UdpLocalAddress	tcpActiveOpens	snmpInASNParseErrs	
UdpLocalPort	tcpPassiveOpens	snmpInTooBigs	
	tcpAttempFails	snmpInNoSuchNames	
	tcpEstabResets	snmpInBadValues	
	tcpCurrEstab	snmpInReadOnlys	
	tcpInSegs	snmpInGenErrs	
	tcpOutSegs	snmpInTotalReqVars	
	tcpRetransSegs	snmpInTotalSetVars	
	tcpConnState	snmpInGetRequests	
	tcpConnLocalAddress	snmpInGetNexts	
	tcpConnLocalPort	snmpInSetRequests	
	tcpConnRemAddress	snmpInGetResponses	
	tcpConnRemPort	snmpInTraps	
	tcpInErrs	snmpOutTooBigs	
	tcpOutRsts	snmpOutNoSuchNames	
		snmpOutBadValues	
		snmpOutGenErrs	
		snmpOutGetRequests	
		snmpOutGetNexts	
		snmpOutSetRequests	
		snmpOutGetResponses	
		snmpOutTraps	
		snmpEnableAuthenTraps	

RFC1317: RS-232 MIB objects

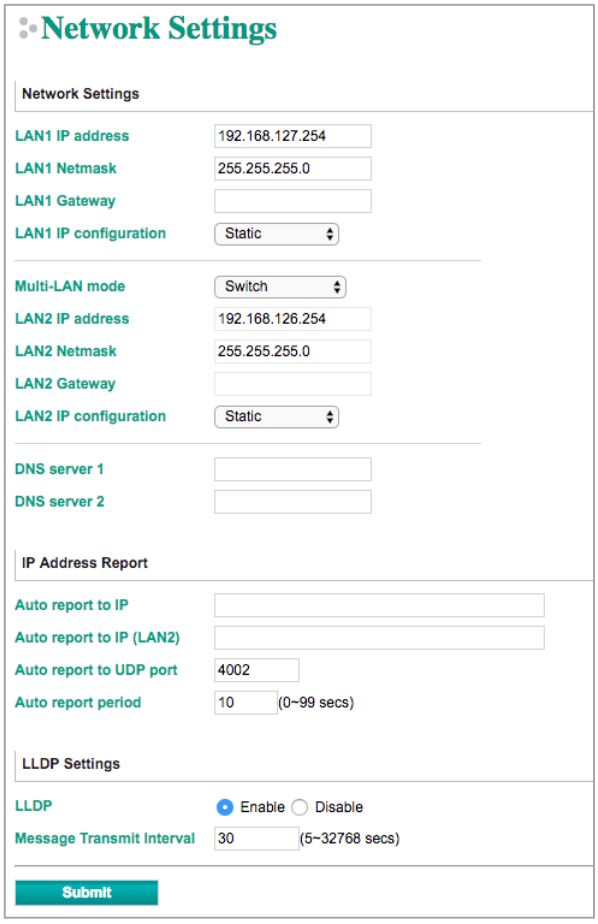
Generic RS-232-like Group	RS-232-like General Port Table	RS-232-like Asynchronous Port Group
rs232Number	rs232PortTable	rs232AsyncPortTable
	rs232PortEntry	rs232AsyncPortEntry
	rs232PortIndex	rs232AsyncPortIndex
	rs232PortType	rs232AsyncPortBits
	rs232PortInSigNumber	rs232AsyncPortStopBits
	rs232PortOutSigNumber	rs232AsyncPortParity
	rs232PortInSpeed	
	rs232PortOutSpeed	

The Input Signal Table	The Output Signal Table
rs232InSigTable	rs232OutSigTable
rs232InSigEntry	rs232OutSigEntry
rs232InSigPortIndex	rs232OutSigPortIndex
rs232InSigName	rs232OutSigName
rs232InSigState	rs232OutSigState

E. Auto IP Report Protocol

The NPort Series provides several ways to configure Ethernet IP addresses. One of them is DHCP Client. When you set up the NPort to use DHCP Client to configure Ethernet IP addresses, it will automatically send a DHCP request over the Ethernet to find the DHCP Server. And then the DHCP Server will send an available IP address to the NPort. The NPort will use this IP address for a period after receiving it. But the NPort will send a DHCP request again to the DHCP Server. Once the DHCP Server realizes that this IP address is to be released to another DHCP Client, the NPort then will receive a different IP address. For this reason, users sometimes find that the NPort will use different IP addresses, not a fixed IP address.

In order to know what IP address the NPort is using, you need to set up parameters in Network Settings via the Web browser. The figure below is the NPort Web console configuration window. Enter the IP address and the Port number of the PC that you want to send this information to.



And then you can develop your own programs to receive this information from the NPort. Here is NPort's Auto IP Report Protocol. We provide an example for you to easily develop your own programs. You can find this example on Moxa's website.

Auto IP Report Format

"Moxa", 4 bytes	Info[0]	Info[1]	…	Info[n]

Info [n]

Field	ID	Length	Data
Length	1	1	Variable, Length is "Length Field"

ID List

ID Value	Description	Length	Note
1	Server Name	Variable	ASCII char
2	Hardware ID	2	Little-endian
3	MAC Address	6	6 bytes MAC address. If the MAC address is "00-90-E8-01-02-03", the MAC[0] is 0, MAC[1] is 0x90(hex), MAC[2] is 0xE8(hex), and so on.
4	Serial Number	4, DWORD	Little-endian
5	IP Address	4, DWORD	Little-endian
6	Netmask	4, DWORD	Little-endian
7	Default Gateway	4, DWORD	Little-endian
8	Firmware Version	4, DWORD	Little-endian Ver1.3.4= 0x0103040
9	AP ID	4, DWORD	Little-endian

AP ID & Hardware ID Mapping Table

Product	Device ID	AP ID
NPort 5110	0x5110	0x80015110
NPort 5130	0x5130	0x80005100
NPort 5150	0x5150	0x80005100
NPort 5110A	0x511A	0x80015100
NPort 5130A	0x513A	0x80015100
NPort 5150A	0x515A	0x80015100
NPort 5210	0x0322	0x80000312
NPort 5230	0x0312	0x80000312
NPort 5232	0x0332	0x80000312
NPort 5232I	0x1332	0x80000312
NPort 5210A	0x521A	0x80015200
NPort 5250A	0x525A	0x80015200
NPort 5410	0x0504	0x80005000
NPort 5410 v3	0x05401	0x80005400
NPort 5430	0x0534	0x80005000
NPort 5430 v3	0x05402	0x80005400
NPort 5430I	0x1534	0x80005000
NPort 5430I v3	0x5403	0x80005400
NPort 5450 v3	0x5404	0x80005400
NPort 5450-T v3	0x5406	0x80005400
NPort 5450I v3	0x5405	0x80005400
NPort 5450I-T v3	0x5407	0x80005400
NPort 5610-8	0x5618	0x80005610
NPort 5610-16	0x5613	0x80005610
NPort 5630-8	0x5638	0x80005610
NPort 5630-16	0x5633	0x80005610
NPort 5610-8-DT	0x5700	0x80015610
NPort 5650-8-DT	0x5702	0x80015610
NPort 5650I-8-DT	0x5703	0x80015610
NPort 5610-8-DT-J	0x5704	0x80015610
NPort 5650-8-DT-J	0x5706	0x80015610
NPort 5150AI-M12	0x515B	0x80015101
NPort 5250AI-M12	0x525B	0x80015201
NPort 5450AI-M12	0x545B	0x80015401
NPort-IA5150	0x5151	0x80005250
NPort-IA5150I	0x5152	0x80005250
NPort-IA5150-S-SC	0x5153	0x80005250
NPort-IA5150I-S-SC	0x5154	0x80005250
NPort-IA5150-M-SC	0x5155	0x80005250
NPort-IA5150I-M-SC	0x5156	0x80005250
NPort-IA5250	0x5251	0x80005250
NPort-IA5250I	0x5250	0x80005250

Product	Device ID	AP ID
NPort IA5150A	0x527A	0x80005201
NPort IA5150A-M-SC	0x52BA	0x80005201
NPort IA5150AI	0x528A	0x80005201
NPort IA5250A	0x529A	0x80005201
NPort IA5250AI	0x52AA	0x80005201
NPort IA5450A	0x540A	0x80015400
NPort IA5450AI	0x541A	0x80015400
NPort P5150A	0x5157	0x80015100

F. Compliance Notice

CE Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take appropriate measures.

Federal Communications Commission Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his or her own expense.

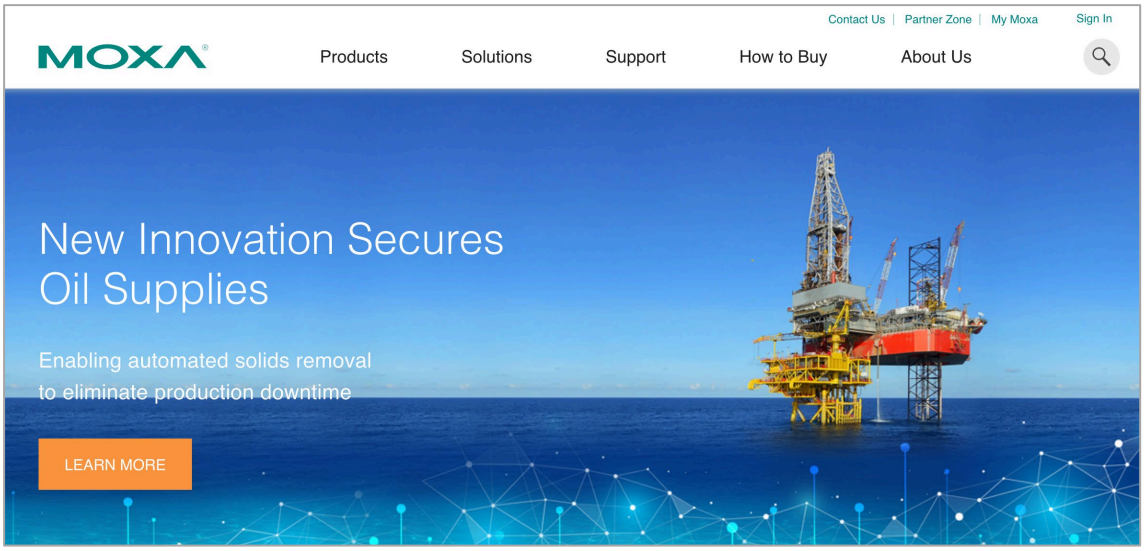
G. How to Become a Registered User on the Moxa Website

Why you should become a Moxa.com registered user, it benefits you to receive all updates of your purchased or interested products, including software such as firmware, driver, and documentation, like datasheet, Quick Installation Guide (QIG).

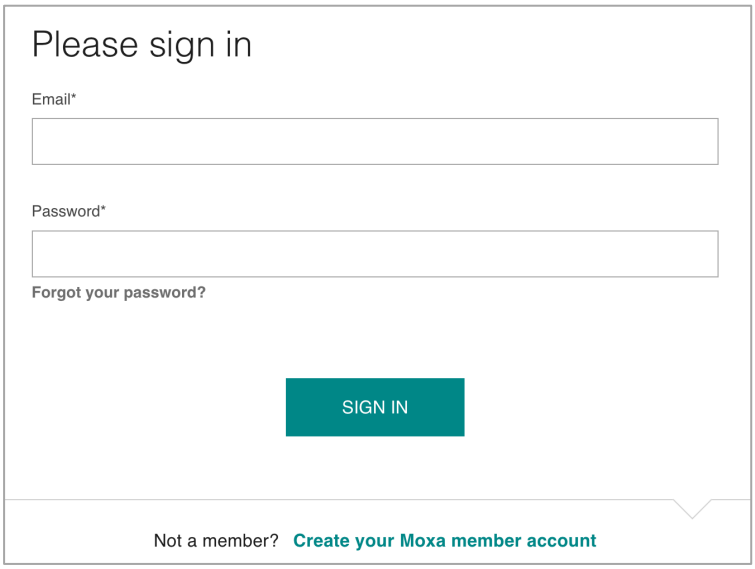
To become a registered user and receiving all updates, you need to do following:

Register a Moxa account

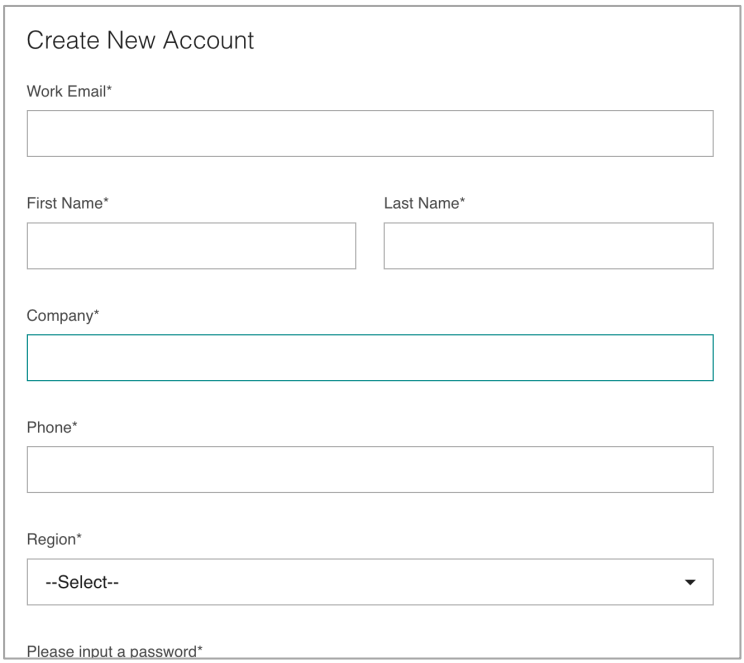
1. Go to Moxa.com and click '**Sign in**' at the top-right corner.



2. In the sign-in page, click "Create your Moxa member account" at below.



3. Fill up the necessary fields.



Request for product updates

1. Go to the product's page that you would like to receive updates, click "**+FOLLOW UPDATE**"

2. Once completes, see the FOLLOW UPDATES button changes.