NPort IA5000A-I/O Series
NPort IAW5000A-I/O Series
User's Manual

Edition 3.0, January 2018

www.moxa.com/product

NPort IA5000A-I/O
NPort IAW5000A-I/O
User's Manual

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

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**

Overview

The NPort IA5000A-I/O and NPort IAW5000A-I/O Series comprise wired and wireless serial device servers with digital I/O, providing maximum flexibility to integrate serial equipment into Ethernet networks, with rich sets of digital I/O, for a variety of industrial data acquisition applications. The digital input/output (DIO) on the device can be controlled over TCP/IP using the Modbus TCP protocol and can be configured and secured from a web browser.

The device also can be installed as a COM Port (patented Real COM) on a Windows/Linux PC to be compatible with legacy applications and is also equipped with Ethernet port(s) that allows data to be seamlessly transferred between the serial line, I/O point, LAN, and WAN, allowing the LAN and WLAN interfaces to be bridged together with one IP address. All models are ruggedly constructed, DIN-rail mountable, and designed with redundant power inputs to ensure uninterrupted operation for industrial applications.

Package Checklist

Standard

- NPort IA5000A-I/O or NPort IAW5000A-I/O wireless device server with digital I/O
- Antenna (for the NPort IAW5000A-I/O only)
- Quick installation guide (printed)
- Warranty card

Optional Accessories

- **Mini DB9F-to-TB Adapter:** DB9-female-to-terminal block adapter for RS-422/485 applications
- **WK-51-01:** Wall-mounting kit
- **DR-4524:** 45W/2A DIN-rail 24 VDC power supply with universal 85 to 264 VAC input
- **DR-75-24:** 75W/3.2A DIN-rail 24 VDC power supply with universal 85 to 264 VAC input
- **DR-120-24:** 120W/5A DIN-rail 24 VDC power supply with 88 to 132 VAC/176 to 264 VAC input by switch

NOTE Please notify your sales representative if any of the above items are missing or damaged

Product Features

- Serial device server with combination of 4 DIs and 2 DOs, or 8 DIs and 4 DOs
- Redundant dual DC power inputs and relay output supported
- Enhanced remote configuration with HTTPS, SSH
- MicroSD for configuration backup
- Per-port offline port buffering and serial data log
- 4kV serial surge protection
- **For NPort IA5000A-I/O Series:**
  - 6 or 12 digital I/Os to collect local data for status monitoring
  - Cascading Ethernet ports for easy wiring
- **For NPort IAW5000A-I/O Series:**
  - Link any serial, Digital I/O, or Ethernet device to an IEEE 802.11a/b/g/n network
  - Secure data access with WEP, WPA, WPA2
  - Built-in WLAN site survey tool
  - Ethernet Bridge function for flexible integration

2

Getting Started

The following topics are covered in this chapter:

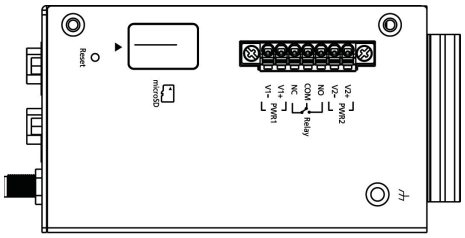
- **Overview**
- **Panel Layout**
- **LED Indicators**
- **Pull-Up/Down Resistors for RS-422/485**
- **Connecting the Hardware**
  - Connecting to the Network
  - Connecting the Power
  - Connecting to a Serial Device
- **Pin Assignments**
  - Serial Port Pin Assignments
  - RJ45 (Ethernet)
  - Power Inputs and Relay Output Pinouts
  - DI/DO Pinouts
- **I/O Wiring Diagram**
- **Mounting the Unit**
- **microSD Card**
  - microSD card Write Failure

Overview

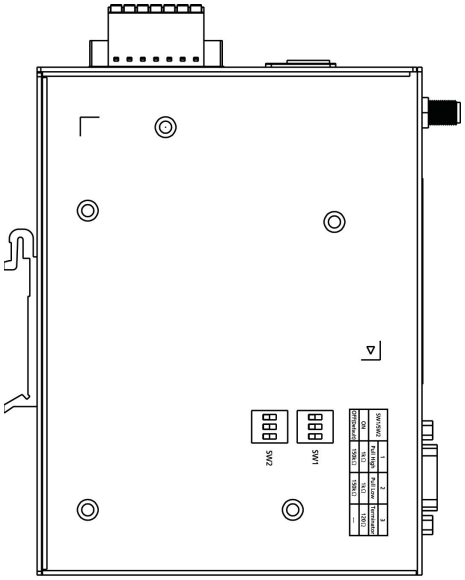
This chapter presents the hardware features of the IA5000A-I/O and IAW5000A-I/O and explains how to connect the hardware.

Panel Layout

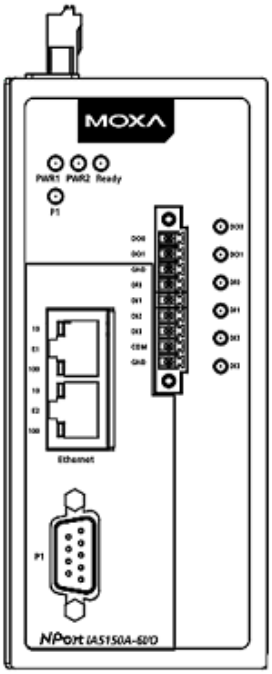
Top View

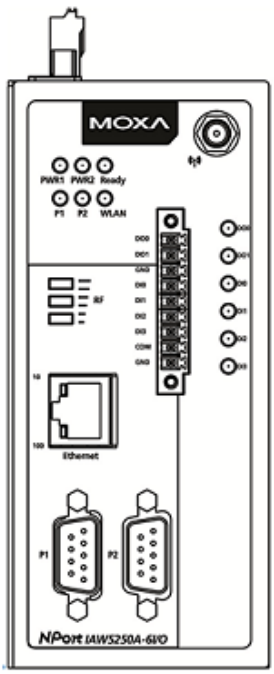


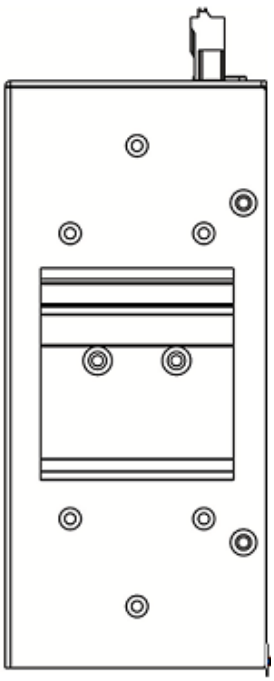
Side View



Front View and Back View







LED Indicators

Name	Color	Function
PWR 1, PWR 2	Green	Power is being supplied to power input PWR1, PWR2.
Ready	Red	Steady on: Power is on, and the NPort is booting up. Blinking: Indicates an IP conflict, or DHCP or BOOTP server did not respond properly, or a relay output occurred. When the above two conditions occur at the same time, check the relay output first. If the Ready LED is still blinking after resolving the relay output, then there is an IP conflict, or the DHCP or BOOTP server did not respond properly. Flashing quickly: MicroSD card failed
	Green	Steady on: Power is on, and the NPort is functioning normally. Blinking: The device server has been located by Administrator's Location function.
	Off	Power is off, or power error condition exists.
WLAN (for the NPort IAW5000A-I/O only)	Green	Steady on: Wireless enabled Blinking: NPort cannot establish WLAN connection with AP (Infrastructure) or station (Ad-Hoc)
	Off	Wireless not enabled.
Signal Strength (3 LEDs for the NPort IAW5000A-I/O only)	Green	1 Bottom: The signal strength (RSSI) is less than -74 dBm 2 Middle: The signal strength (RSSI) is between -65 to -74 dBm 3 Top: The signal strength (RSSI) is greater than -65 dBm
Ethernet	Amber	10 Mbps Ethernet connection
	Green	100 Mbps Ethernet connection
	Off	Ethernet cable is disconnected, or has a short.
P1, P2 (Serial)	Amber	Serial port is receiving data.
	Green	Serial port is transmitting data
	Off	No data is being transmitted or received through the serial port.
DI	Green	DI status on
	Off	DI status off
DO	Green	DO status on
	Off	DO status off

Pull-Up/Down Resistors for RS-422/485

In some critical RS-422/RS-485 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-up/down resistors correctly so that the electrical signal is not corrupted. For each serial port, DIP switches are used to set the pull-up/down resistor values. A built-in 120 Ω termination resistor can also be enabled.

SW1 (Serial 1) **SW2** (Serial 2)	**DIP 1** Pull-up resistor	**DIP 2** Pull-down resistor	**DIP 3** Terminal resistor
ON	1 KΩ	1 KΩ	120 Ω
OFF (Default)	150 KΩ	150 KΩ	N/A

ATTENTION

Do not use the 1 KΩ pull-up/down setting when using the RS-232 interface. Doing so will degrade the RS-232 signals and reduce the effective communication distance.

Connecting the Hardware

ATTENTION

Before connecting the hardware, follow these important wiring safety precautions:

Disconnect power source
Do not install or wire this unit or any attached devices with the power connected. Disconnect the power before installation by removing the power cord before installing and/or wiring your unit.

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

Use caution - unit may get hot
The unit will generate heat during operation, and the casing may be too hot to the touch. Take care when handling the unit. Be sure to leave enough space for ventilation.

The following guidelines will help ensure trouble-free signal communication with the NPort.

- Use separate paths to route wiring for power and devices to avoid interference. Do not run signal or communication wiring and power wiring in the same wire conduit. The rule of thumb is that wiring that shares similar electrical characteristics can be bundled together.
- If power wiring and device wiring paths must cross, make sure the wires are perpendicular at the intersection point.
- Keep input wiring and output wiring separate.
- Label all wiring to each device in the system for easier testing and troubleshooting

Connecting to the Network

Use the supplied Ethernet cable to connect the NPort to your Ethernet network. If the cable is properly connected, the NPort will indicate a valid connection to the Ethernet as follows:

- A green Ethernet LED indicates a valid connection to a 100 Mbps Ethernet network.
- An orange Ethernet LED indicates a valid connection to a 10 Mbps Ethernet network.
- A flashing Ethernet LED indicates that Ethernet packets are being transmitted or received.

Connecting the Power

The unit can be powered by connecting a power source to the terminal block.

1. We recommend using 24 to 16 AWG wire. Strip 9 to 10 mm of insulation off the end of the wire before inserting it into the terminal block hole.
2. The power input range is from 12 to 48 VDC.

To remove the wire from the terminal block, use a flathead screwdriver to push the orange slot next to the terminal block hole, and then pull the wire out.

Note that the unit does not have an on/off switch. It automatically turns on when it receives power. The PWR LED on the front panel will glow to indicate that the unit is receiving power. There are two DC power inputs for redundancy.

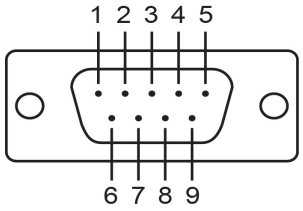
Connecting to a Serial Device

Use a serial cable to connect your serial device to a serial port on the NPort.

Pin Assignments

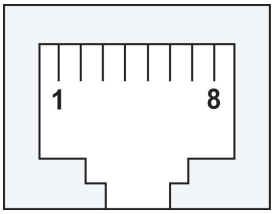
The IA5000A-I/O and IAW5000A-I/O Series use DB9 serial ports to connect to serial devices. Each port supports three serial interfaces that select by software: RS-232, RS-422, and RS-485 (both 2 and 4-wire).

Serial Port Pin Assignments



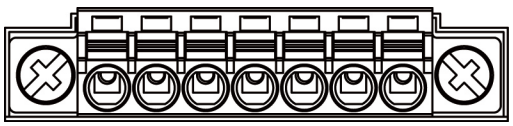
Pin	RS-232	RS-422/ RS-485 (4W)	RS-485 (2W)
1	DCD	TxD-(A)	–
2	RXD	TxD+(B)	–
3	TXD	RxD+(B)	Data+(B)
4	DTR	RxD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	–	–
7	RTS	–	–
8	CTS	–	–
9	–	–	–

RJ45 (Ethernet)



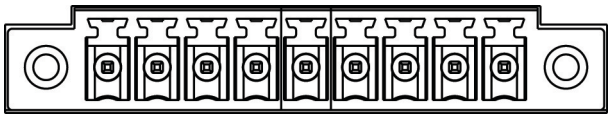
Pin	RS-232
1	Tx+
2	Tx-
3	Rx+
4	–
5	–
6	Rx-
7	–
8	–

Power Inputs and Relay Output Pinouts



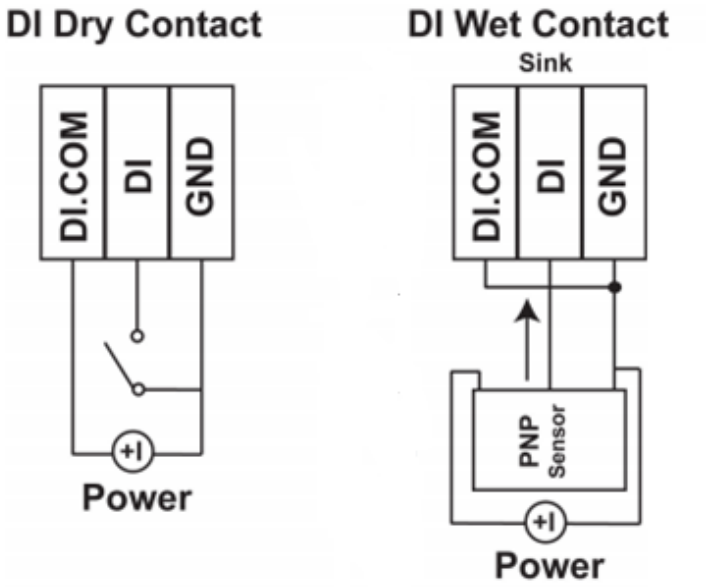
V2+	V2-				V1+	V1-
DC Power Input 2	DC Power Input 2	N.O.	Common	N.C.	DC Power Input 1	DC Power Input 1

DI/DO Pinouts



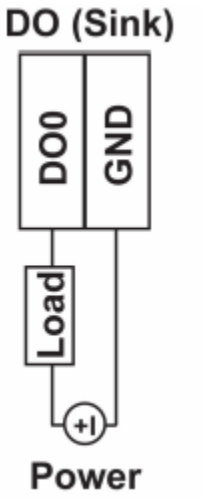
DO0	DO1	GND	DI0	DI1	DI2	DI3	COM	GND
Digital Output 0	Digital Output 1	Ground	Digital Input 0	Digital Input 1	Digital Input 2	Digital Input 3	Common	Ground

I/O Wiring Diagram



A **dry dontact** is a contact that works without a power source.

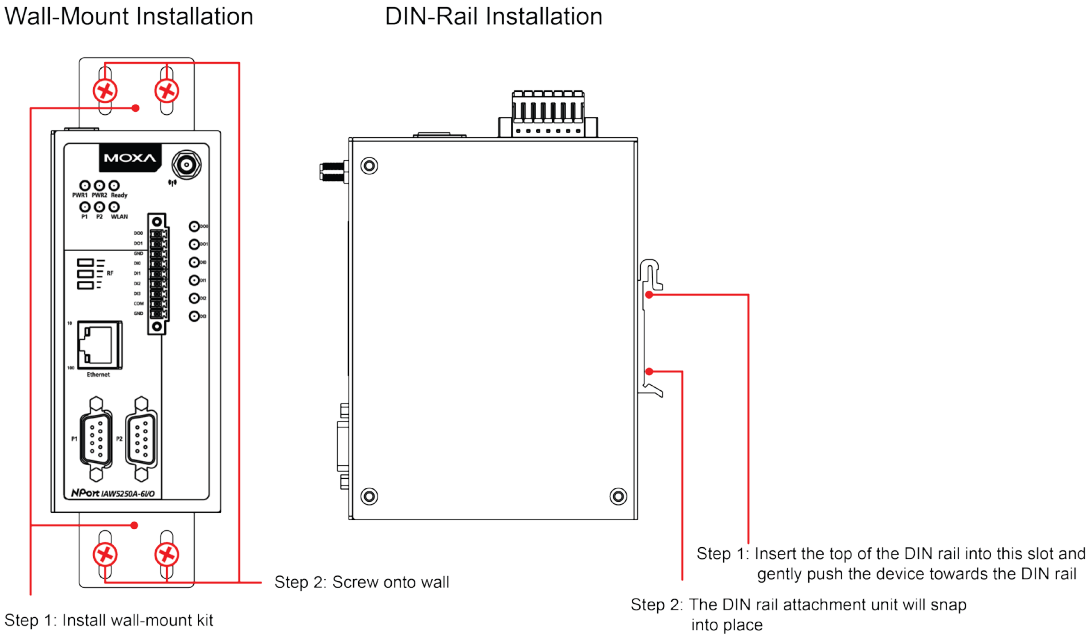
A **wet contact** is a contact that must work with a power source.



NOTE A "load" in a circuit schematic is a component or portion of the circuit that consumes electrical power. For the diagrams shown in this document, "load" refers to the devices or systems connected to the I/O unit.

Mounting the Unit

1. Connect the power adapter. Connect the 12–48 VDC power line or DIN-rail power supply to the NPort IA5000A-I/O and IAW5000A-I/O devices' terminal block.
2. Use a serial cable to connect the NPort to a serial device.
3. Use an Ethernet cable to connect the NPort to the PC for configuration setup.
4. The NPort IA5000A-I/O and IAW5000A-I/O are designed to be attached to a DIN rail or mounted on a wall. For DIN-rail mounting, properly insert the top of the DIN rail into the DIN rail slot until it "snaps" into place. For wall mounting, install the wall-mount kit (optional) first, and then screw the device onto the wall. The following figure illustrates the two mounting options:



microSD Card

The IA5000A-I/O and IAW5000A-I/O Series are equipped with a microSD card slot for easy configuration. The microSD card can be used to store an NPort's system configuration settings. The behavior of MicroSD card is described as below:

- Automatically load the configuration after system reboot
- Manually load and save the configuration through the web console

microSD card Write Failure

The following events will cause the microSD card to experience a write failure.

1. The microSD card has less than 20 MB of free space.
2. The NPort configuration file is read-only.
3. The microSD card's file system is corrupted.
4. The microSD card is damaged.

The NPort will halt the write action if any of the above conditions exists. The NPort's Ready LED will flash and the beeper will sound to inform the user of the write failure.

3

Initial IP Configuration

The following topics are covered in this chapter:

- **Overview**
- **Factory Default IP Settings**
- **Using ARP to Assign IP Address**
- **Using the Telnet Console to Assign IP Address**
- **Using the Serial Console to Assign IP Address**

Overview

This chapter presents several ways to assign the NPort's IP address for the first time. Please refer to Chapter 2 for instructions on connecting to the network.

The web console is the recommended method for configuring the NPort. Please refer to Chapter 6 to 12 for details on using the web console for configuration. With the NPort's default setting (Ethernet Bridge function disabled), please ensure the Ethernet cable is connected before powering up the NPort. Then, proceed to following IP configuration options.

Factory Default IP Settings

NPort IA5000A-I/O Series

Network Interface	IP Configuration	IP Address	Netmask
LAN	Static	192.168.127.254	255.255.255.0

NPort IAW5000A-I/O Series

Network Interface	IP Configuration	IP Address	Netmask
LAN	Static	192.168.126.254	255.255.255.0
WLAN	Static	192.168.127.254	255.255.255.0

If your NPort is configured to obtain its IP settings from a DHCP or BOOTP server, but it is unable to get a response, then it will use the factory default IP address and netmask.

ATTENTION

If you forget the IP address of your NPort, you can look it up using the Device Search Utility (DSU). After the DSU has found all NPorts on the network, each unit will be listed with its IP address. Please refer to Chapter 5 for additional information on using the DSU.

Using ARP to Assign IP Address

The ARP (Address Resolution Protocol) command can be used to assign an IP address to the NPort. The ARP command tells your computer to associate the NPort's MAC address with the specified IP address. You must then use Telnet to access the NPort, at which point the device server's IP address will be reconfigured. This method only works when the NPort is configured with default IP settings.

1. Select a valid IP address for your NPort. Consult with your network administrator if necessary.
2. Obtain the NPort's MAC address from the label on its bottom panel.
3. From the DOS prompt, execute the **arp** -s command with the desired IP address and the NPort's MAC address, as in the following example:

   ```
   arp -s 192.168.200.100 00-90-E8-xx-xx-xx
   ```

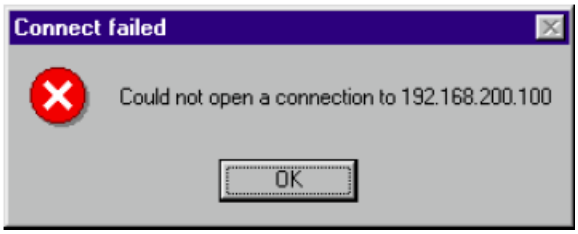
   In this example 192.168.200.100 is the new IP address that will be assigned to the NPort, and 00-90-E8-xx-xx-xx is the NPort's MAC address.

4. From the DOS prompt, execute a special Telnet command using port 6000, as in the following example:

   ```
   telnet 192.168.200.100 6000
   ```

   In this example, 192.168.200.100 is the new IP address that will be assigned to the NPort.

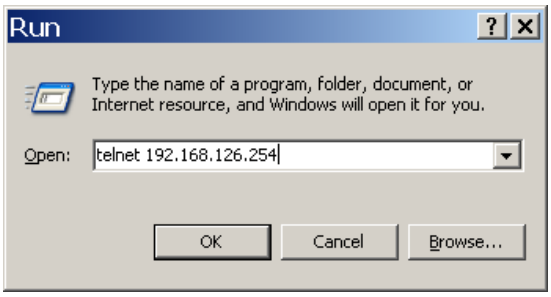
5. You will see a message indicating that the connection failed.



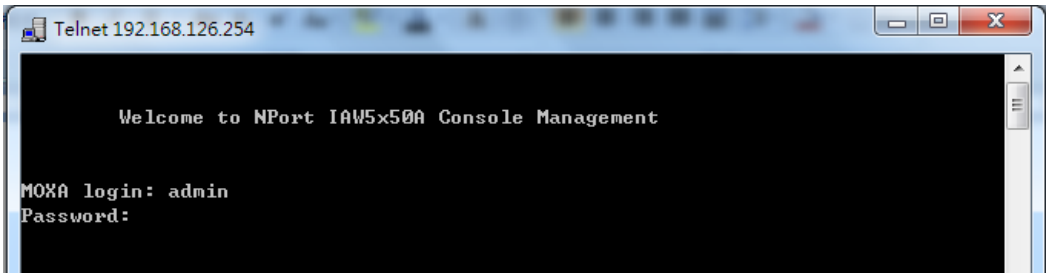
The NPort will automatically reboot with the new IP address. You can verify that the configuration was successful by connecting to the new IP address with Telnet, ping, the web console, or the DSU.

Using the Telnet Console to Assign IP Address

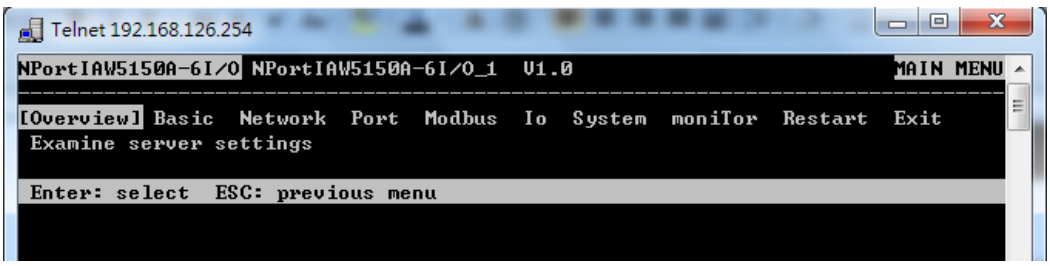
1. Select **Run...** from the Windows Start menu.
2. Enter **telnet 192.168.126.254** or **192.168.127.254** (the NPort's default IP address) and click **[OK]**.



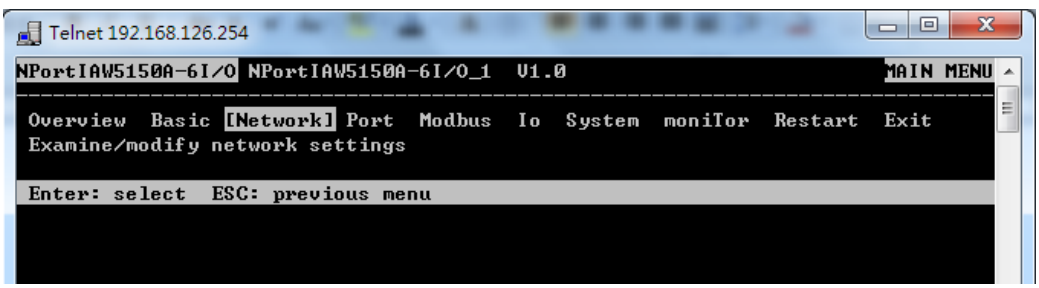
3. Enter your login account and password, then press **ENTER.**



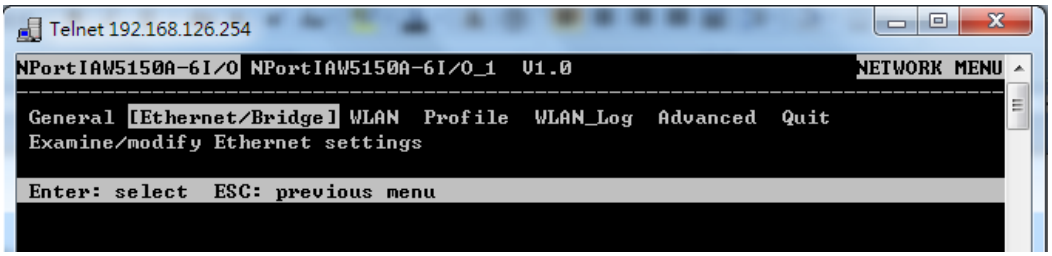
4. You will login to the **Overview** page.



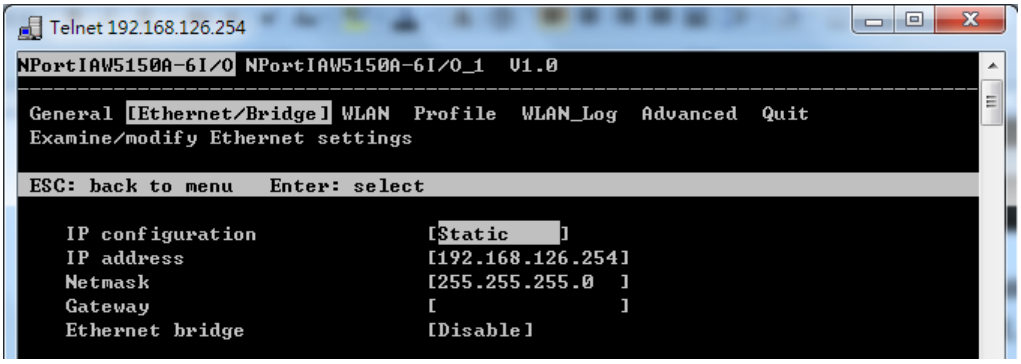
5. Press **N** or use the cursor keys to select **Network** and press **ENTER**.



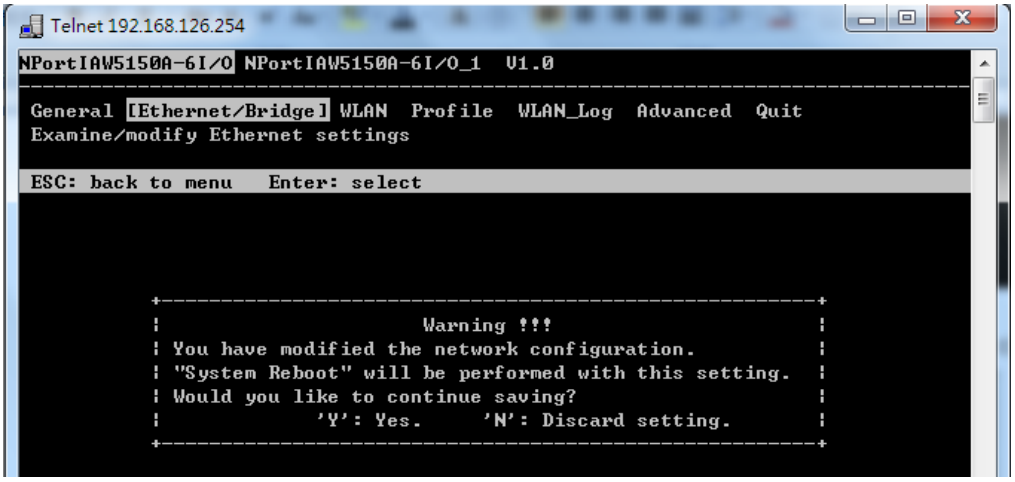
6. Press **E** or use the cursor keys to select **Ethernet** and press **ENTER**.



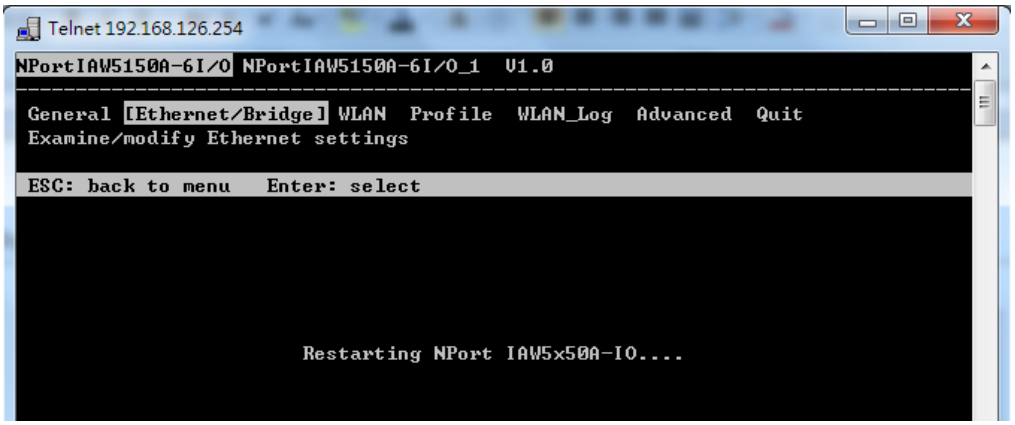
7. Use the cursor keys to navigate between the different fields. For **IP address**, **Netmask**, and **Gateway**, enter the desired values directly. For **IP configuration** and **LAN speed**, press **ENTER** to open a submenu and select between the available options.



8. Press **ESC** to return to the menu. When prompted, press **Y** to save the configuration changes.



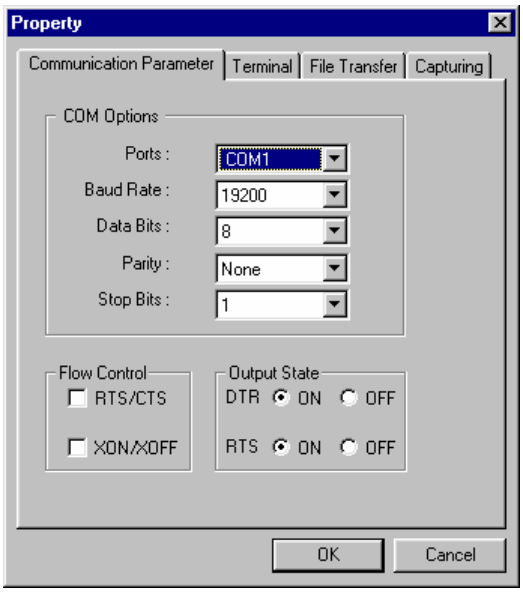
The NPort will reboot with the new IP settings. You can telnet to the new IP to log in again.



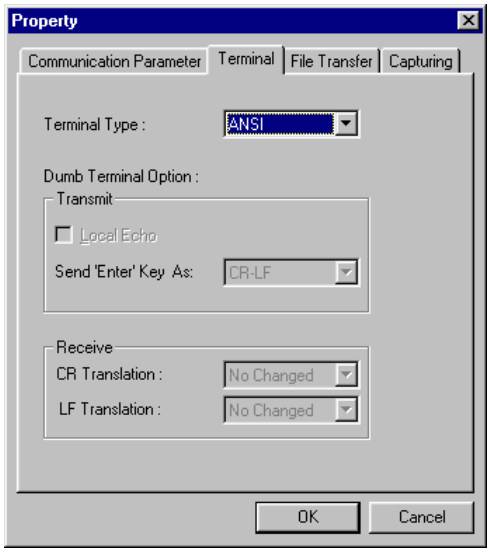
Using the Serial Console to Assign IP Address

Before using the NPort's serial console, turn off the power and use a serial cable to connect the NPort console port to your computer's serial port. Port 1 on the NPort serves as the console port. Use Port 1 connecting to the console port with a serial-based terminal or terminal emulator program, such as Windows HyperTerminal. You may also download PComm Lite at www.moxa.com. The terminal type should be set as ANSI or VT100, and the serial communication parameters should be set as 19200, 8, N, 1 (19200 for baud rate, 8 for data bits, None for parity, and 1 for stop bits). As soon as the connection is open, you will be presented with a text menu displaying the IA5000A-I/O and IAW5000A-I/O Series' general settings. Please refer to Chapter 4 for a description of the available settings. The following instructions, we recommend using PComm Terminal Emulator, which can be downloaded free of charge from www.moxa.com, to carry out the configuration procedure.

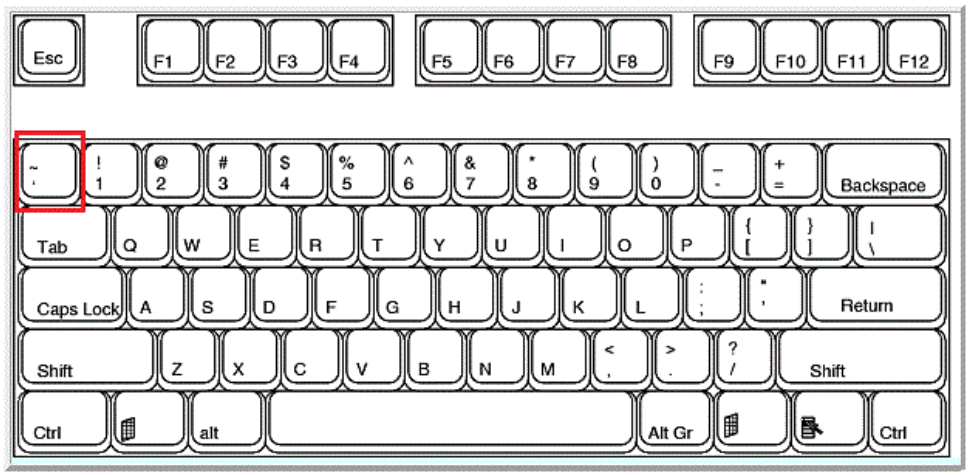
1. Connect your PC's serial port to the NPort's console port.
2. Open your terminal emulator program, such as Windows HyperTerminal. We recommend using PComm Terminal Emulator, which can be downloaded for free at www.moxa.com.
3. In your terminal emulator program, configure the communication parameters for the serial port on the PC. The parameters should be set to **19200** for baud rate, **8** for data bits, **None** for parity, and **1** for stop bits.



4. In your terminal emulator program, set the terminal type to **ANSI** or **VT100**. If you select **Dumb Terminal** as the terminal type, some of the console functions—especially the "Monitor" function—may not work properly.



5. Hold the **grave accent** key (`) down and power up the NPort.



The continuous string of grave accent characters triggers the NPort to switch from data mode to console mode.

6. The serial console will open and will be functionally identical to the Telnet console. Please refer to the Telnet console section for instructions on how to navigate the console and configure the IP settings.

4

Introduction to Operation Modes

The following topics are covered in this chapter:

- **Overview**
- **RealCOM Mode**
- **RFC2217 Mode**
- **TCP Server Mode**
- **TCP Client Mode**
- **UDP Mode**
- **Pair Connection Modes**
- **Ethernet Modem Mode**
- **Reverse Terminal Mode**

Overview

This chapter introduces the different serial port operation modes that are available on the NPort IA5000A-I/O and IAW5000A-I/O Series. Each serial port on the NPort is configured independently of the other ports, with its own serial communication parameters and operation mode. The serial port's operation mode determines how it interacts with the network, and different modes are available to encompass a wide variety of applications and devices.

RealCOM and **RFC2217** modes allow serial-based software to access the NPort serial port as if it were a local serial port on a PC. These modes are appropriate when your application relies on Windows or Linux software that was originally designed for locally attached COM or TTY devices. With these modes, you can access your devices from the network using your existing COM/TTY-based software, without investing in additional software.

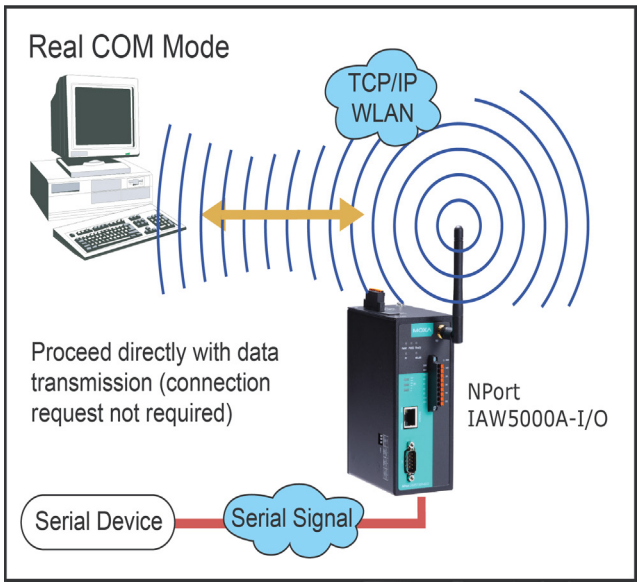
Three different socket modes are available for user-developed socket programs: **TCP Server**, **TCP Client**, and **UDP Server/Client**. For TCP applications, the appropriate mode depends on whether the connection will be hosted or initiated from the NPort serial port or from the network. The main difference 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 multicasting of data to groups of IP addresses and would be suitable for streaming media or non-critical messaging applications such as LED message boards.

Pair Connection Slave and **Master** modes are designed for serial-to-serial communication over Ethernet, in order to overcome traditional limitations with serial transmission distance.

In **Ethernet Modem** mode, the NPort acts as an Ethernet modem, providing a network connection to a host through the serial port.

RealCOM Mode

RealCOM mode is designed to work with NPort drivers that are installed on a network host. COM drivers are provided for Windows systems, and TTY drivers are provided for Linux and UNIX systems. The driver establishes a transparent connection to the attached serial device by mapping a local serial port to the NPort serial port. RealCOM mode supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.



ATTENTION

RealCOM drivers are installed and configured through NPort Windows Driver Manager.

RealCOM mode allows you to continue using your serial communications software to access devices that are now attached to your NPort device server. On the host, the NPort RealCOM driver automatically intercepts data sent to the COM port, packs it into a TCP/IP packet, and redirects it to the network. At the other end of the

connection, the NPort device server accepts the Ethernet frame, unpacks the TCP/IP packet, and sends the serial data to the appropriate device.

ATTENTION

In RealCOM mode, several hosts can have simultaneous access control over the NPort serial port. If necessary, you can limit access by using the NPort's Accessible IP settings. Please refer to Chapter 10 for additional information on Accessible IP settings.

RFC2217 Mode

RFC-2217 mode is similar to RealCOM mode, since it relies on a driver to transparently map a virtual COM port on a host computer to a serial port on the NPort. The RFC2217 standard defines general COM port control options based on the Telnet protocol and supports one connection at a time. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement virtual COM mapping.

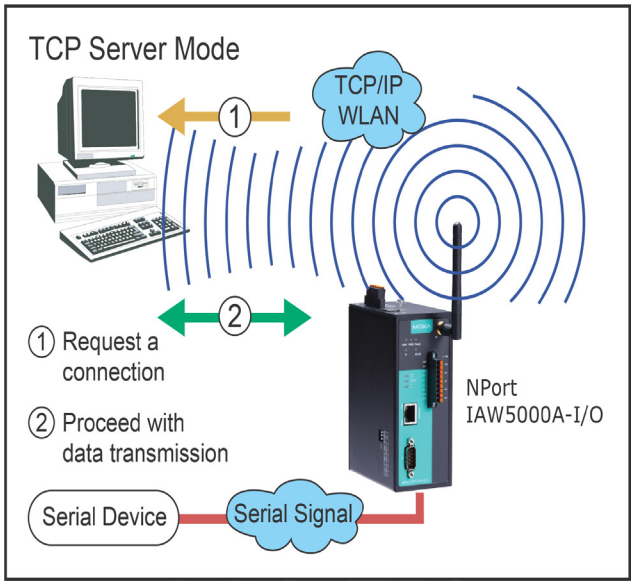
TCP Server Mode

In TCP Server mode, the NPort serial port is assigned an IP:port address that is unique on your TCP/IP network. It waits for the host computer to establish a connection to the attached serial device. This operation mode also supports up to eight simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

Data transmission proceeds as follows:

A host requests a connection to the NPort serial port.

Once the connection is established, data can be transmitted in both directions—from the host to the device, and from the device to the host.

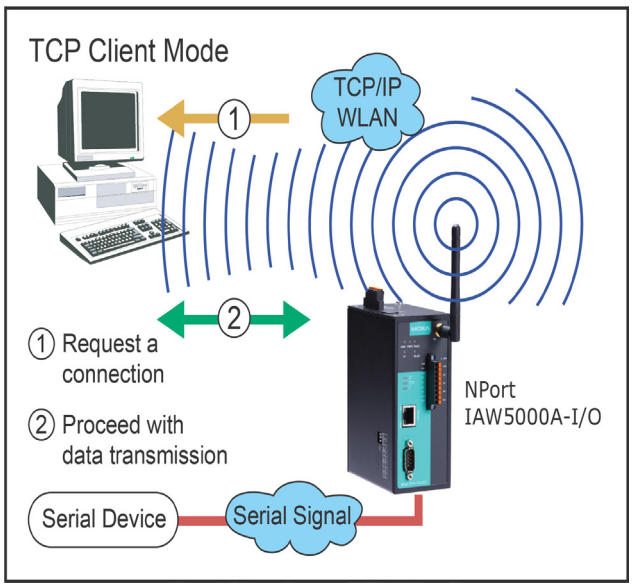


TCP Client Mode

In TCP Client mode, the NPort actively establishes a TCP connection to a specific network host when data is received from the attached serial device. After the data has been transferred, the NPort can automatically disconnect from the host computer through the Inactivity time settings. Please refer to Chapter 8 for details on these parameters.

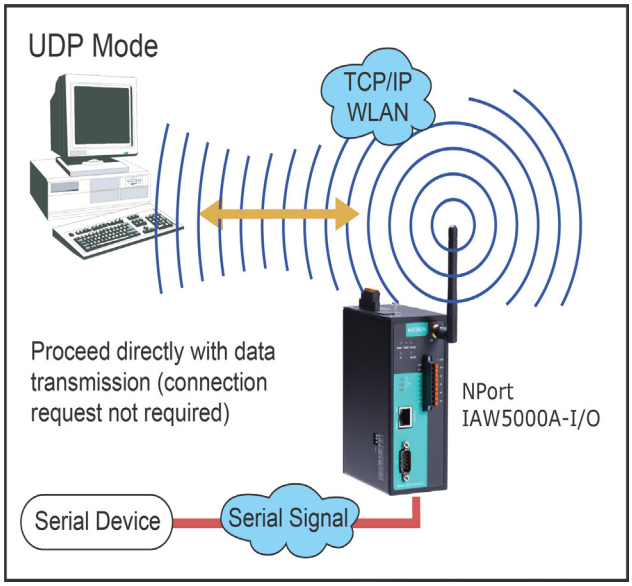
Data transmission proceeds as follows:

The NPort requests a connection from the host. The connection is established and data can be transmitted in both directions between the host and device.



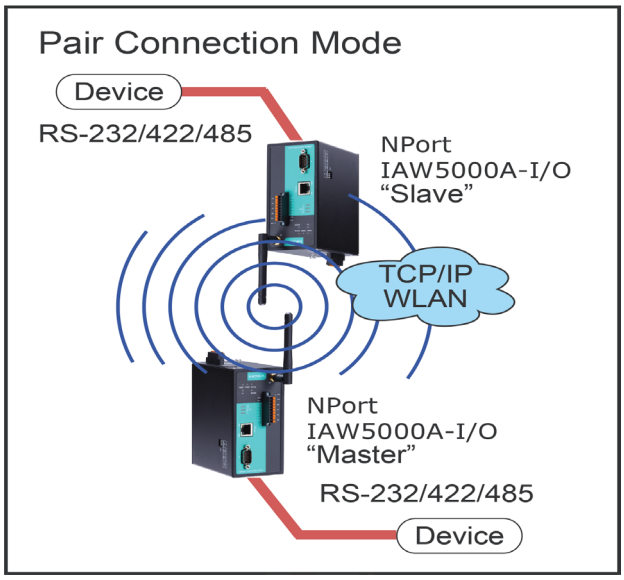
UDP Mode

UDP is similar to TCP but is faster and more efficient. Data can be broadcast to or received from multiple network hosts. However, UDP does not support verification of data and would not be suitable for applications where data integrity is critical. It is ideal for message display applications.



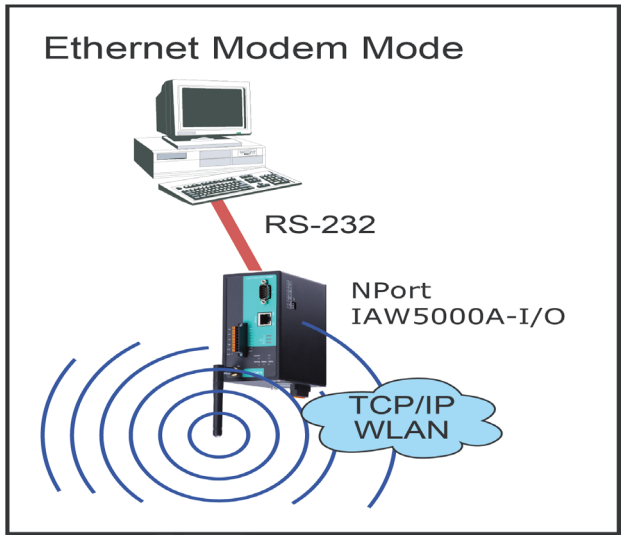
Pair Connection Modes

Pair Connection Master and Slave modes connect two NPort device servers over a network for serial-to-serial communication. A device attached to one NPort can then communicate transparently to a device attached to the other NPort, as if the two devices were connected by a serial cable. Both data and modem control signals are exchanged, except for DCD signals. This can be used to overcome traditional limitations with serial communication distance and introduces many new possibilities for serial-based device control.



Ethernet Modem Mode

Ethernet Modem mode is designed for use with legacy operating systems, such as MS-DOS, that do not support TCP/IP Ethernet. By connecting the properly configured NPort serial port to the MS-DOS computer's serial port, it is possible to use legacy software to transmit data over the Ethernet when the software was originally designed to transmit data over a modem.



Reverse Terminal Mode

Reverse terminal applications are similar to terminal applications as they also use an NPort to manage the connection between a terminal and a server. The difference is that with reverse terminal applications, the terminal is connected through the network and the server is connected through the serial port, rather than the other way around. In practice, a reverse terminal session typically involves a network administrator telnetting to a device that has a dedicated serial console port used specifically for configuration purposes.

For example, many routers, switches, UPS units, and other devices have Console/AUX or COM ports to which a terminal can be physically connected for console management. The device's console port can be connected to a serial port on the NPort, allowing a network administrator to telnet to the device remotely through the network. Although modern network equipment generally allows other options for remote configuration through the network, there are situations in which it is

necessary or desirable to configure a device by serial console (e.g., for security reasons, when using older-generation equipment, or as a backup configuration method when the network is down).

The Reverse Terminal mode is widely used for device management in control rooms. The system waits for a host on the network to initiate a connection. Since TCP Server mode does not assist with conversion of CR/LF commands, reverse terminal applications that require this conversion should use Reverse Terminal mode.

5

Use Real COM Mode to Communicate with Serial Devices

The following topics are covered in this chapter:

Overview

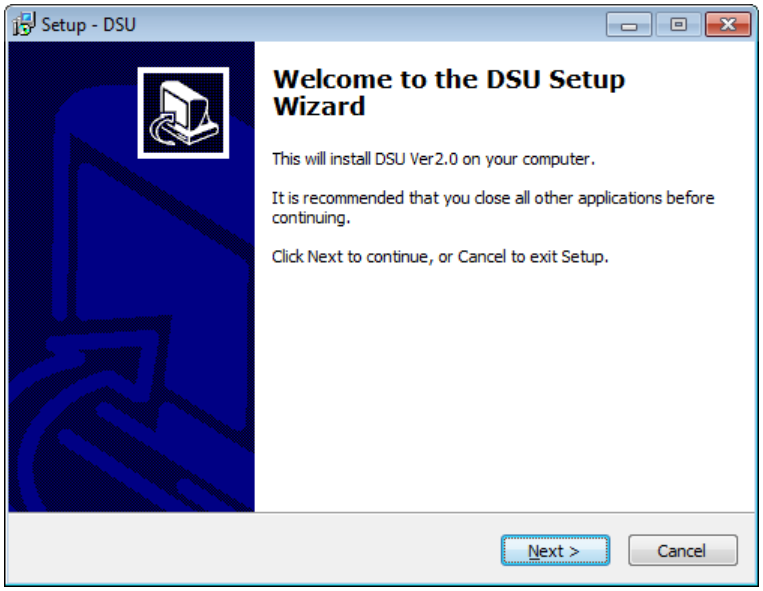
This chapter will instruct you on how to install the necessary software and provide the steps to mapping virtual COM port to help user's software keep working as usual.

1. Install the Device Search Utility to find the specific NPort on the Ethernet network.
2. Log in to the Web console to configure the device to work on Real COM mode.
3. Install the NPort driver and mapping COM port.

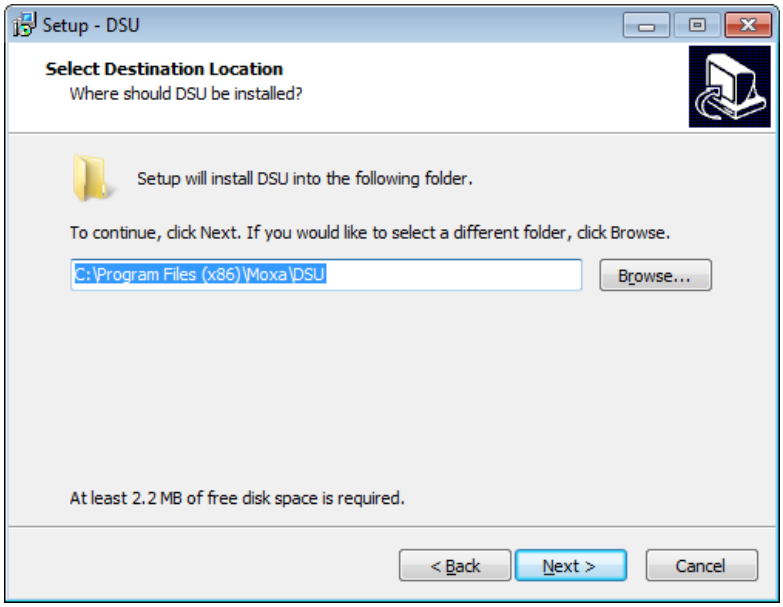
Device Search Utility

Installing the Device Search Utility

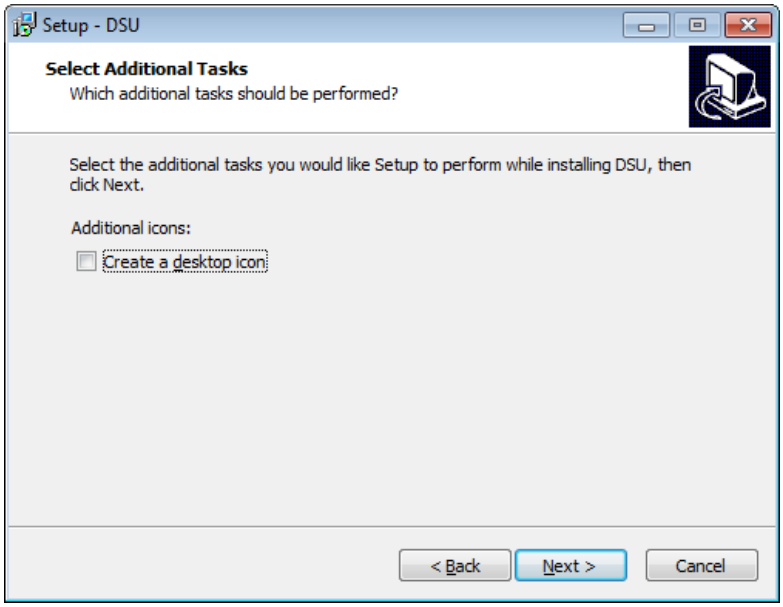
1. Download Device Search Utility from Moxa website, https://www.moxa.com/support/download.aspx?type=support&id=10137, to install the Device Search Utility. Once the program starts running, click **Yes** to proceed.
2. Click **Settings** when the Welcome screen opens, to proceed with the installation.



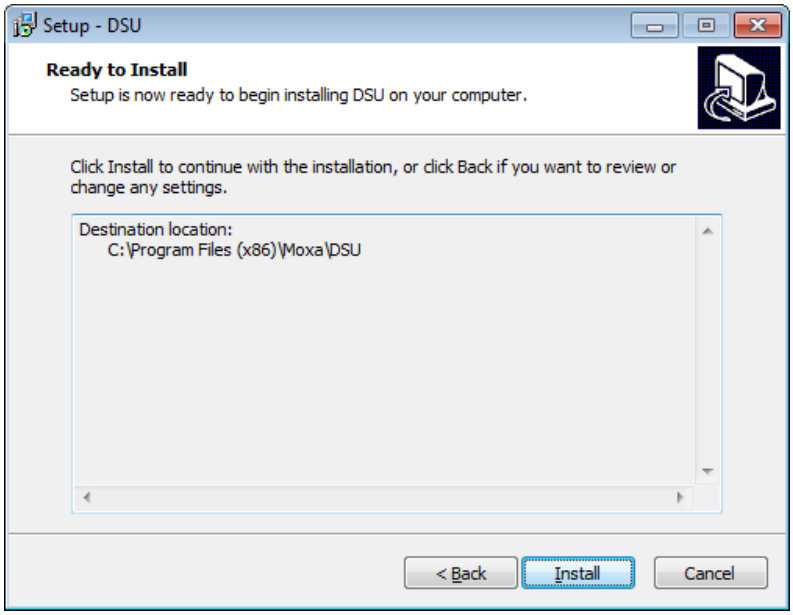
3. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



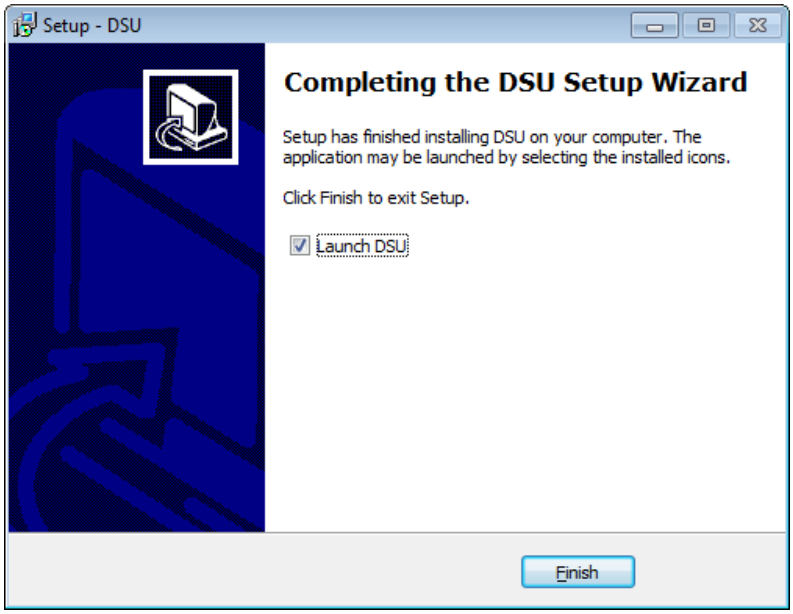
4. Check the checkbox if you want the DSU to create a desktop icon, or just click **Next** to install the program's shortcuts in the appropriate Start Menu folder.



5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of the NPort Search Utility.

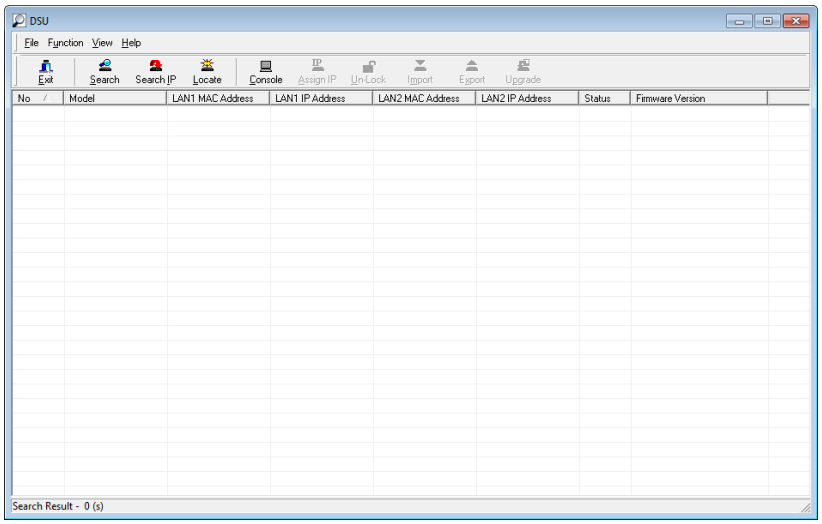


Find a Specific NPort on the Ethernet Network via the DSU

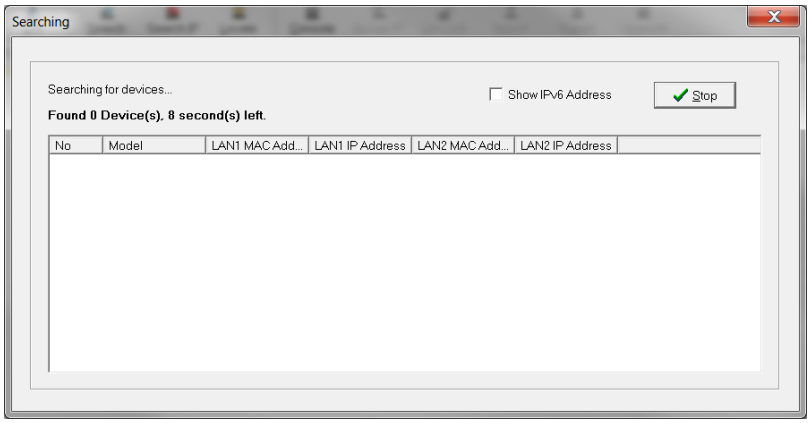
The Broadcast Search function is used to locate all the NPort device servers that are connected to the same LAN as your computer. After locating a NPort device server, you will be able to change its IP address.

Since the Broadcast Search function searches by MAC address and not by IP address, all NPort device servers connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

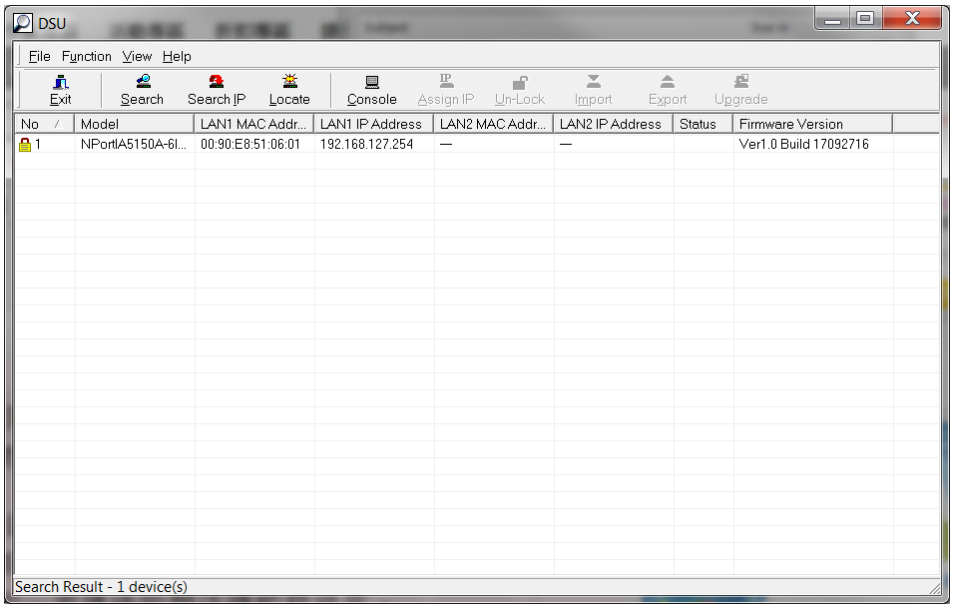
1. Open the DSU and then click the **Search** icon.



The Searching window indicates the progress of the search.



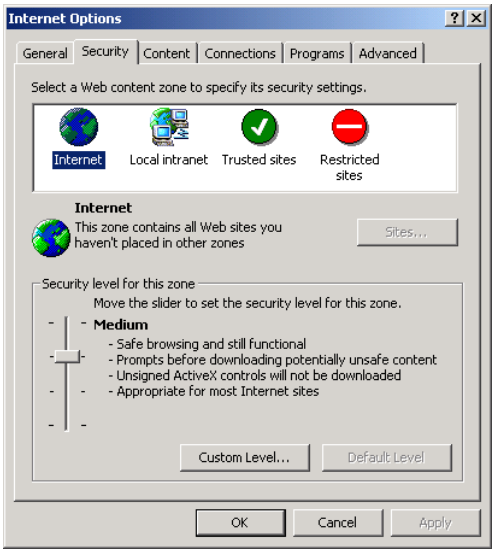
2. When the search is complete, all the NPort device servers that were located will be displayed in the DSU window.

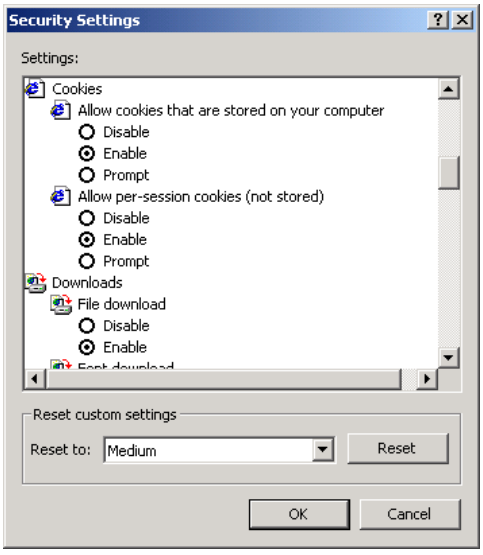


3. To modify the configuration of the highlighted NPort device servers, click on the Console icon to open the web console. This will take you to the web console, where you can make all configuration changes. Please refer to Chapter 6 to 12, "Web Console: Basic Settings", for information on how to use the web console.

Opening Your Browser

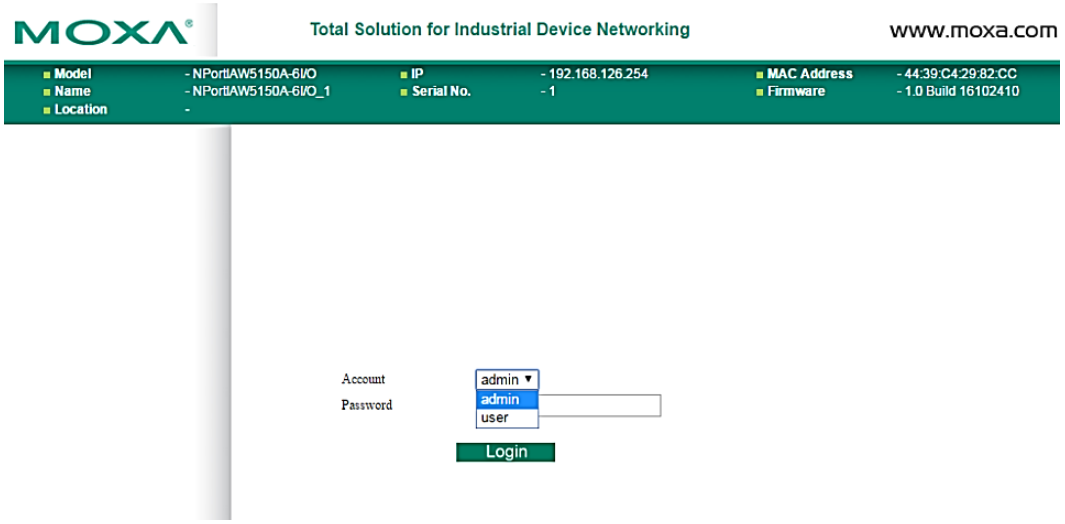
1. Open your browser with the cookie function enabled. (To enable your browser for cookies, right-click on your desktop Internet Explorer icon, select **Properties**, click on the Security tab, and then select the three Enable options as shown in the figure below.)





2. After using the DSU to find a specific NPort, type the IP address to log in to the web console. If this is the first time you configure the NPort, you may directly type the default IP address, 192.168.127.254 in the Address input box. Use the correct IP address if it is different from the default and then press Enter.

4. On the first page of the web console, type **admin** for the default account name and **moxa** for the default password.



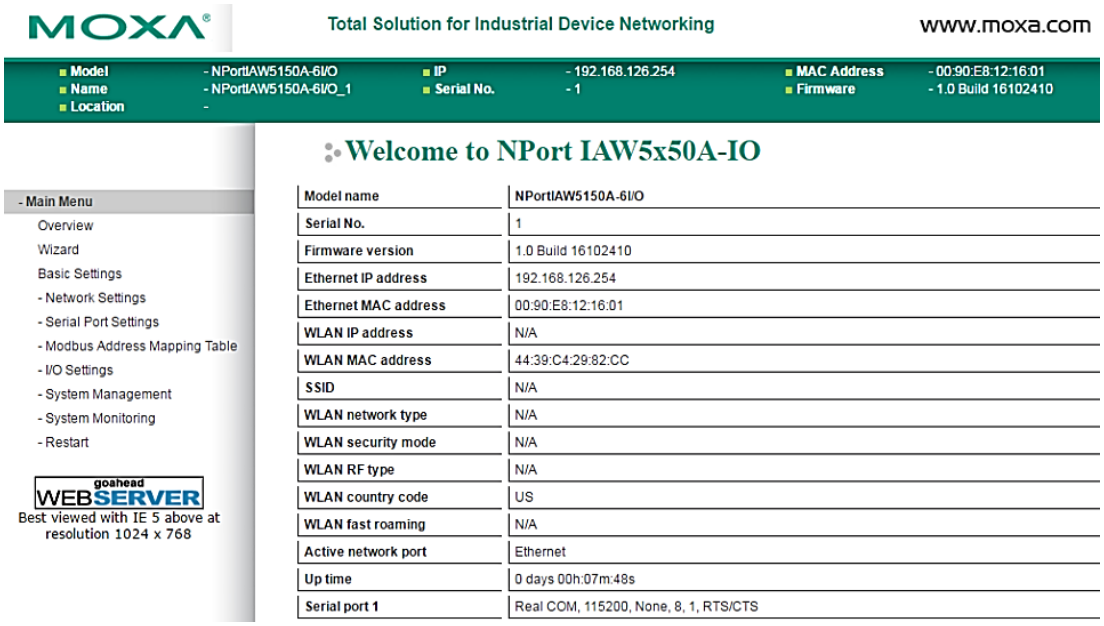
ATTENTION

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**. Device servers use cookies only for "password" transmission.

ATTENTION

Refer to Chapter 3, "Initial IP Address Configuration," to see how to configure the IP address. Examples shown in this chapter use the Factory Default IP address (192.168.127.254).

The NPort IA5000A-I/O or IAW5000A-I/O homepage will open. On this page, you can see a brief description of the Web Console



ATTENTION

If you forgot the password, the ONLY way to start configuring the NPort is to load the factory defaults by using the reset button.

ATTENTION

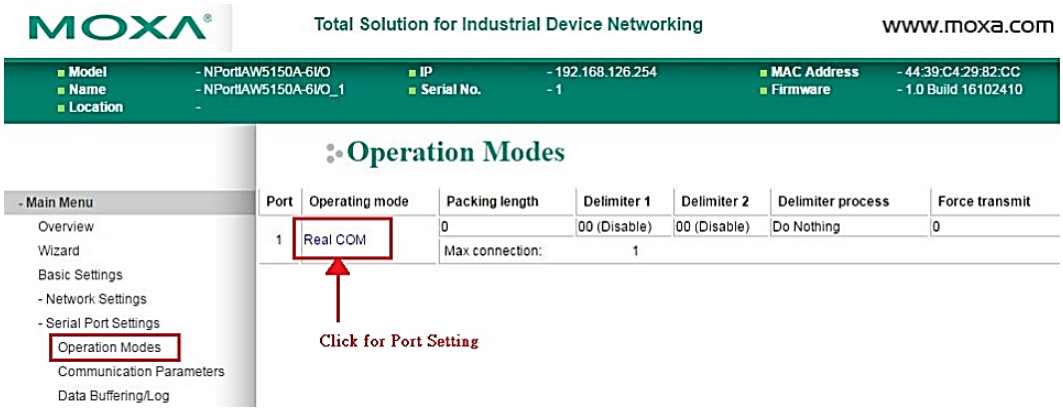
Remember to export the configuration file when you have finished the configuration. After using the reset button to load the factory defaults, your configuration can be easily reloaded into the NPort by using the Import function. Refer to Chapter 10 "Web Console: System Management", for more details about using the Export and Import functions.

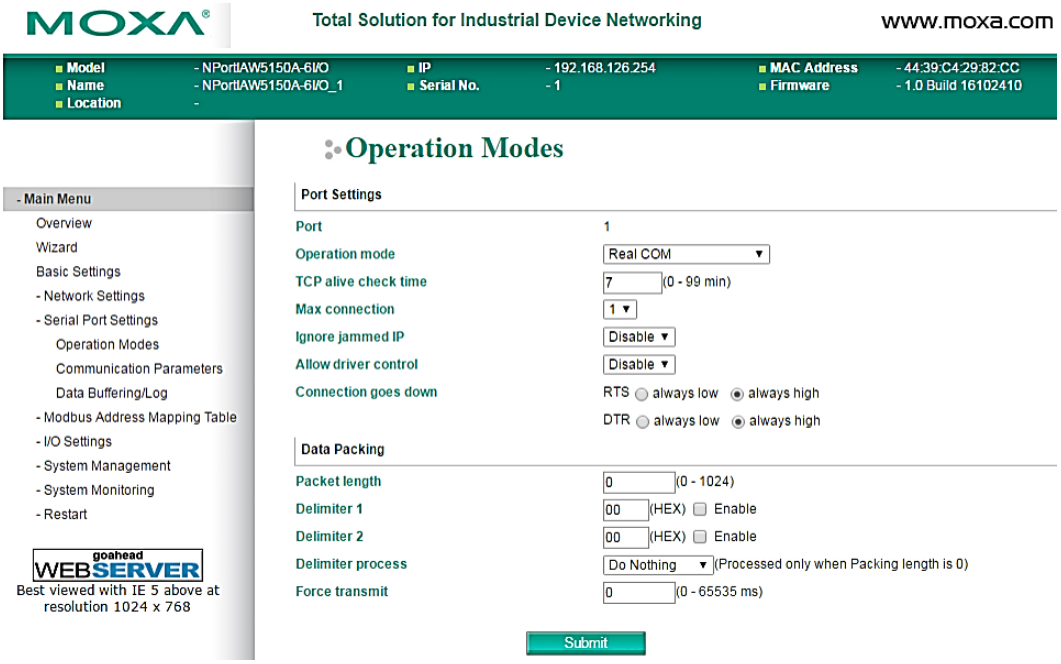
ATTENTION

If your NPort application requires using password protection, you must enable the cookie function in your browser. If the cookie function is disabled, you will not be allowed to enter the Web Console Screen.

Configure Operation Mode to Real COM Mode

Click on **Operation Modes**, located under Serial Settings, to display the serial port settings for four serial ports. To modify the serial operation mode settings for a particular port, click on **Operation Modes** of the serial port in the window on the right-hand side.



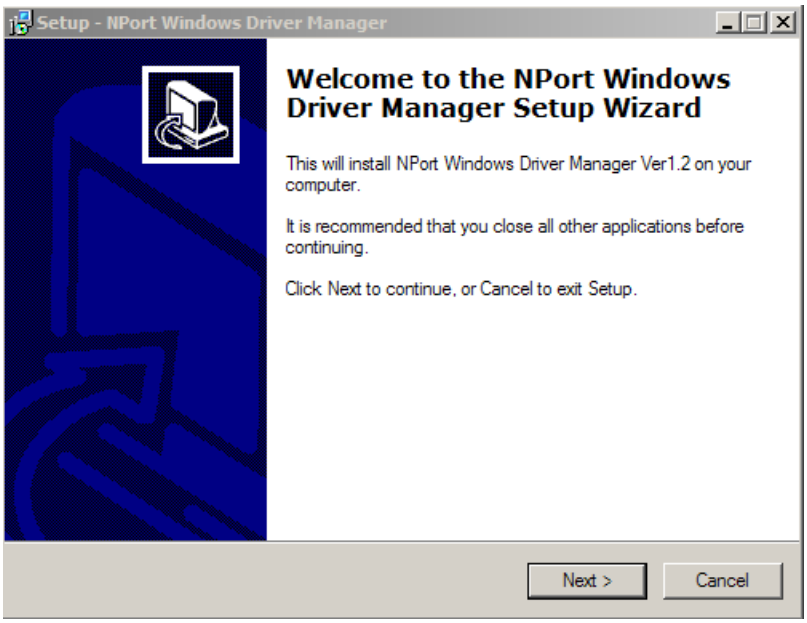


NPort Windows Driver Manager

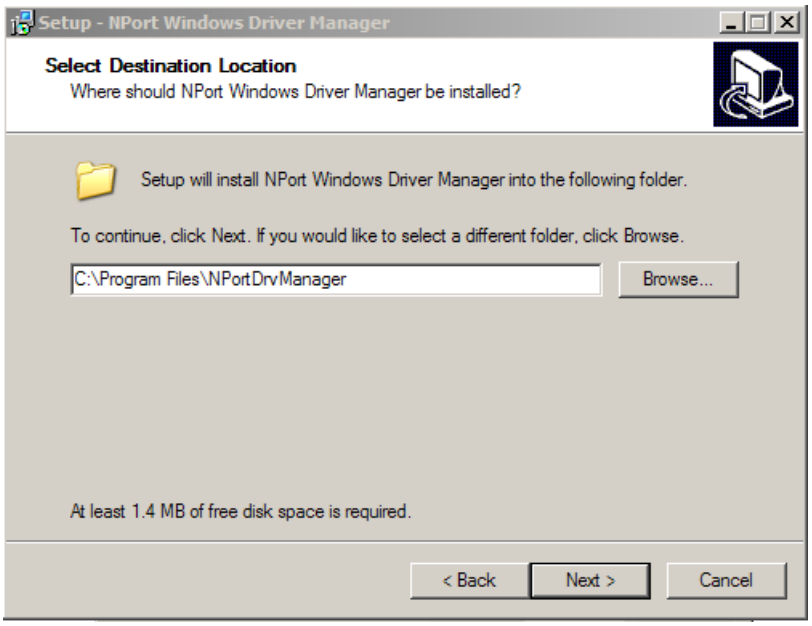
Installing the NPort Windows Driver Manager

The NPort Windows Driver Manager is intended for use with NPort device server 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 device server. When the drivers are installed and configured, devices that are attached to serial ports on the NPort device server will be treated as if they were attached to your PC's own COM ports.

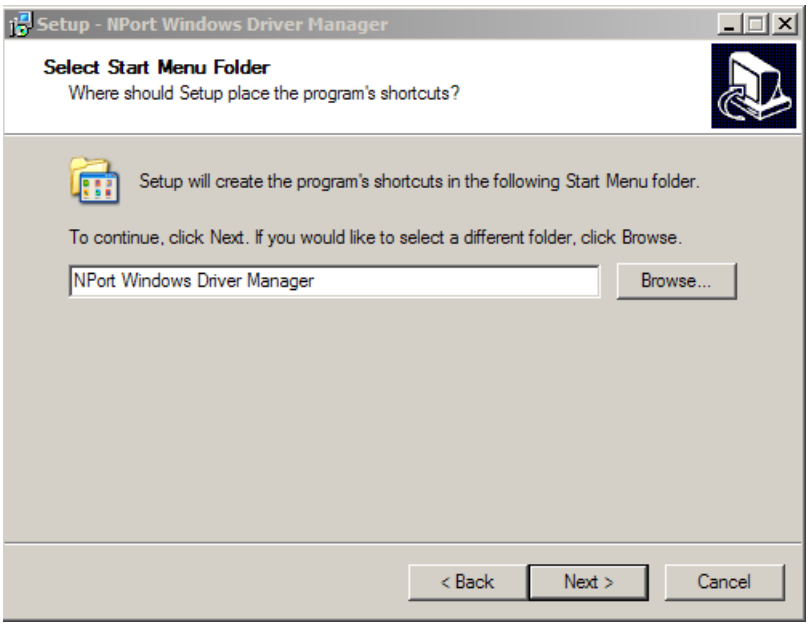
1. Download NPort Windows Driver Manager from Moxa's website, https://www.moxa.com/support/download.aspx?type=support&id=974, to install the NPort Windows Driver. Once the installation program starts running, click **Yes** to proceed.
2. Click **Next** when the Welcome screen opens, to proceed with the installation.



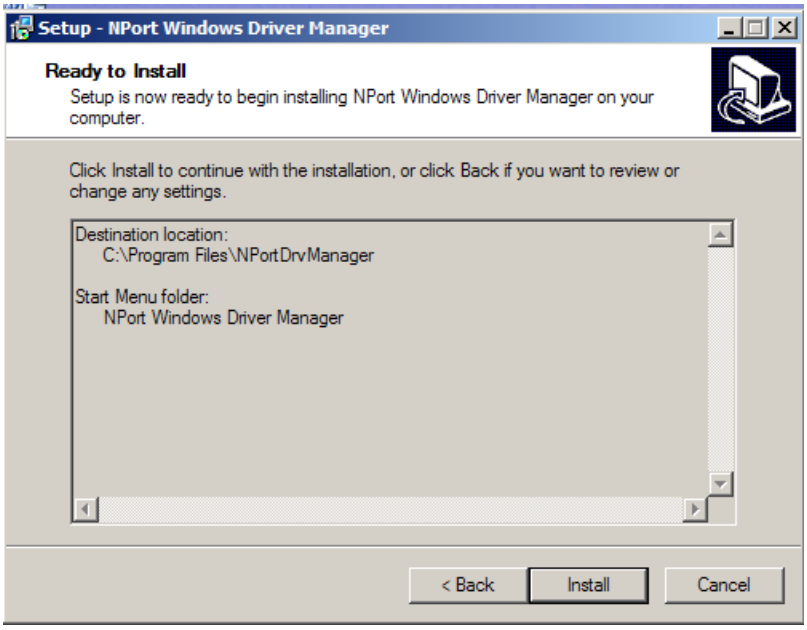
Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



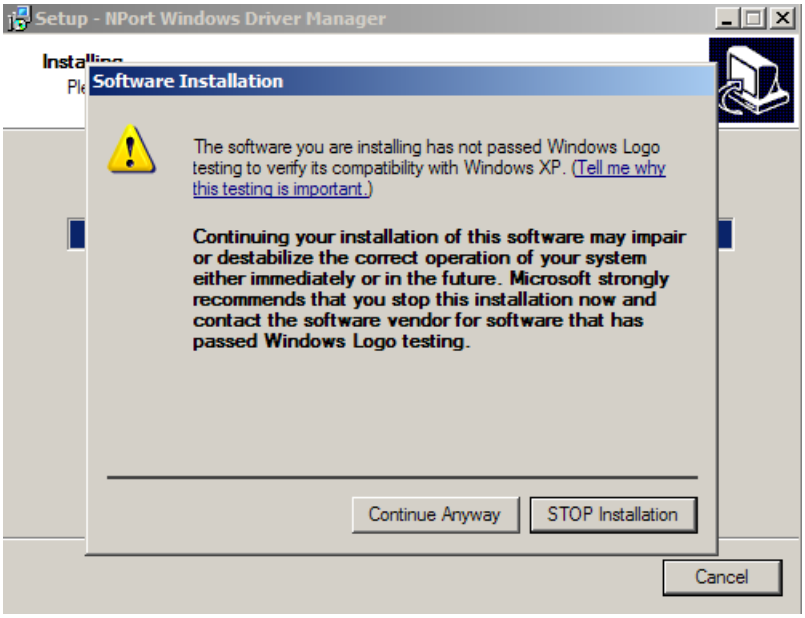
3. Click **Next** to install the program's shortcuts in the appropriate Start Menu folder.



4. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.

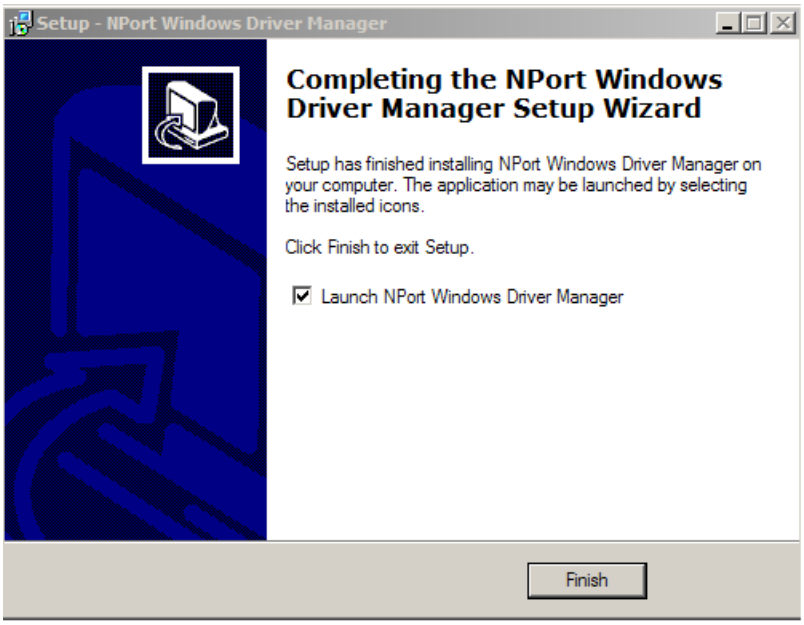


5. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen. The installer will display a message that the software has not passed Windows Logo testing. This is shown as follows:



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

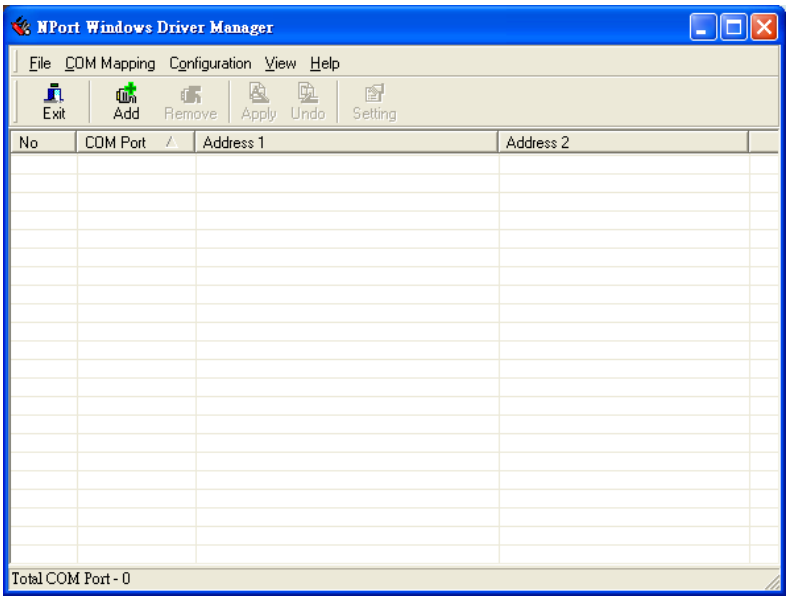
6. Click **Finish** to complete the installation of the NPort Windows Driver Manager.



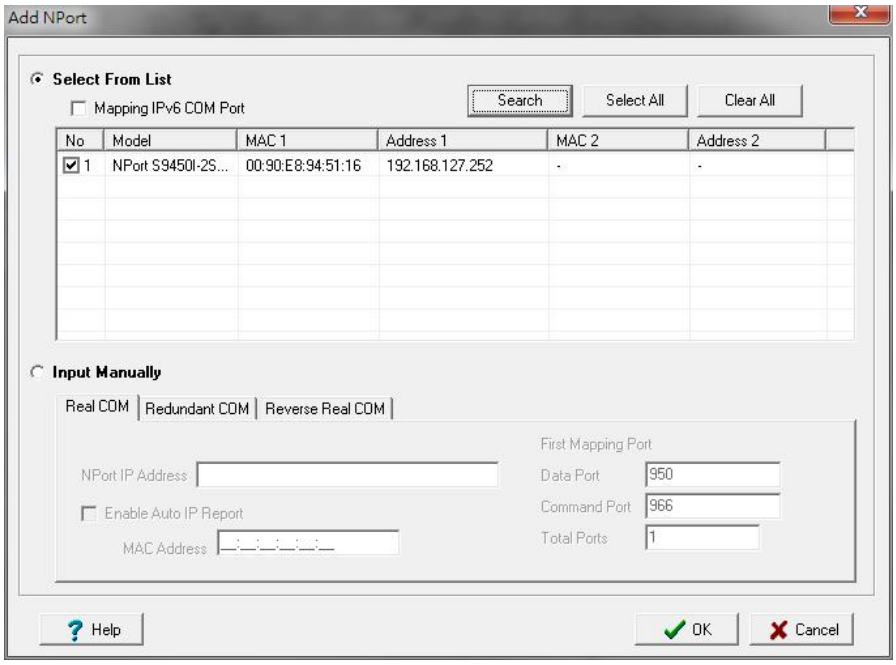
Using NPort Windows Driver Manager

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

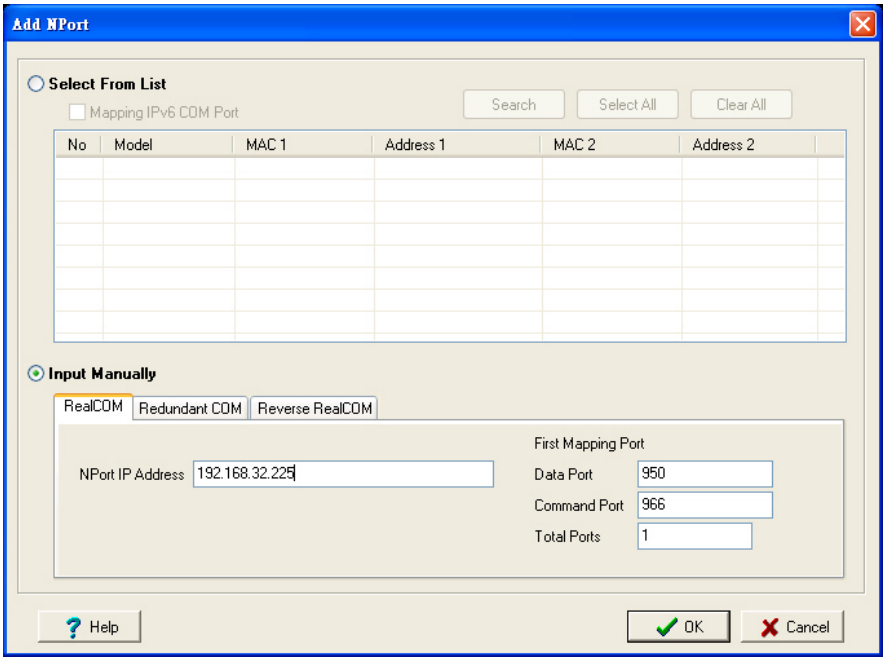
1. Go to **Start** → **NPort Windows Driver Manager** → **NPort Windows Driver Manager** to start the COM mapping utility.
2. Click the **Add** icon.



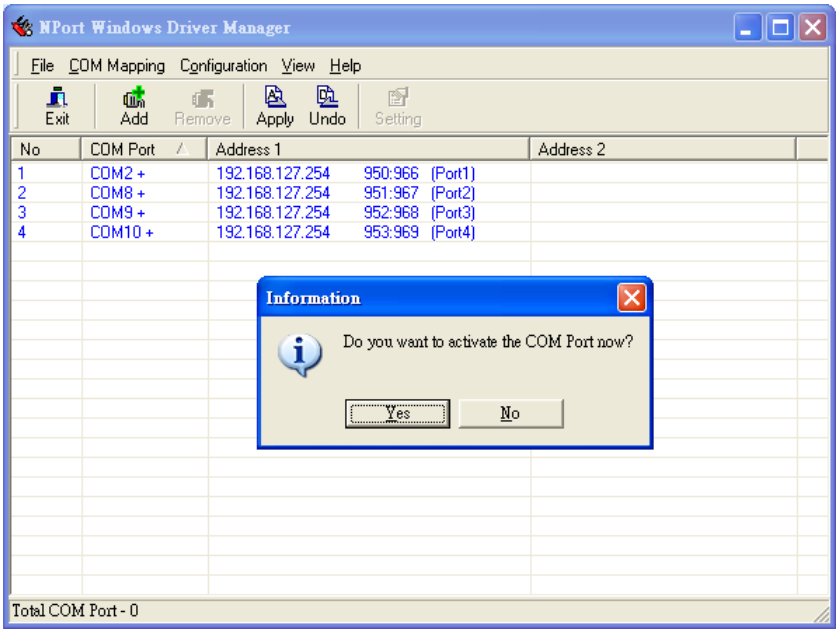
3. Click **Search** to search for the NPort device servers. From the list that is generated, select the server to which you will map COM ports, and then click **OK**.



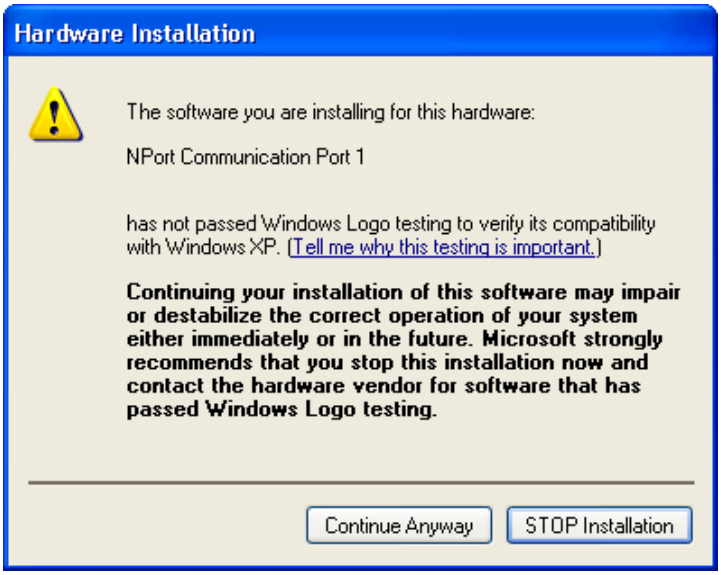
4. Alternatively, you can select **Input Manually** and then manually enter the NPort IP Address, 1st Data Port, 1st Command Port, and Total Ports to which COM ports will be mapped. Click **OK** to proceed to the next step. Note that the Add NPort page supports FQDN (Fully Qualified Domain Name), in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



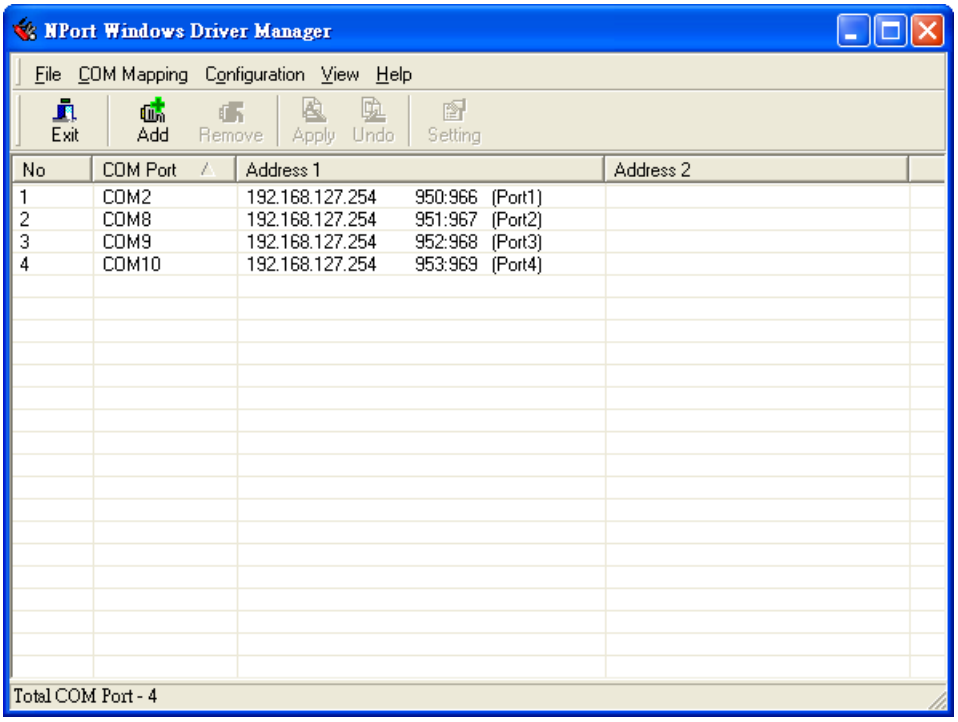
5. COM ports and their mappings will appear in blue until they are activated. Activating the COM ports saves the information in the host system registry and makes the COM port available for use. The host computer will not have the ability to use the COM port until the COM ports are activated. Click **Yes**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



6. A message will display during activation of each port, indicating that the software has not passed Windows Logo certification. Click **Continue Anyway** to proceed.



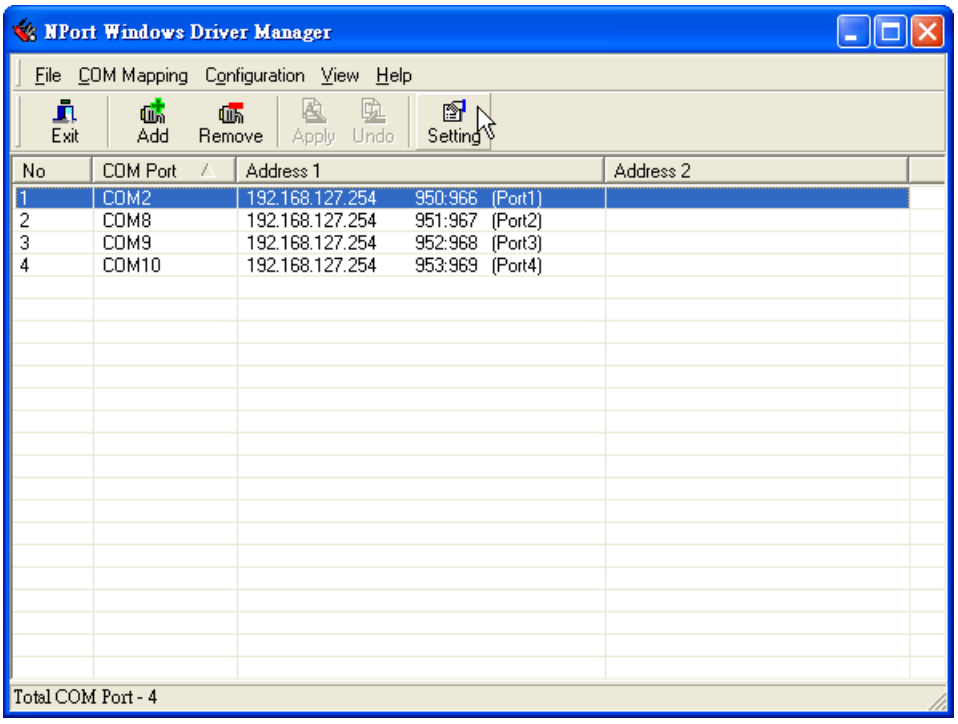
7. Ports that have been activated will appear in black.



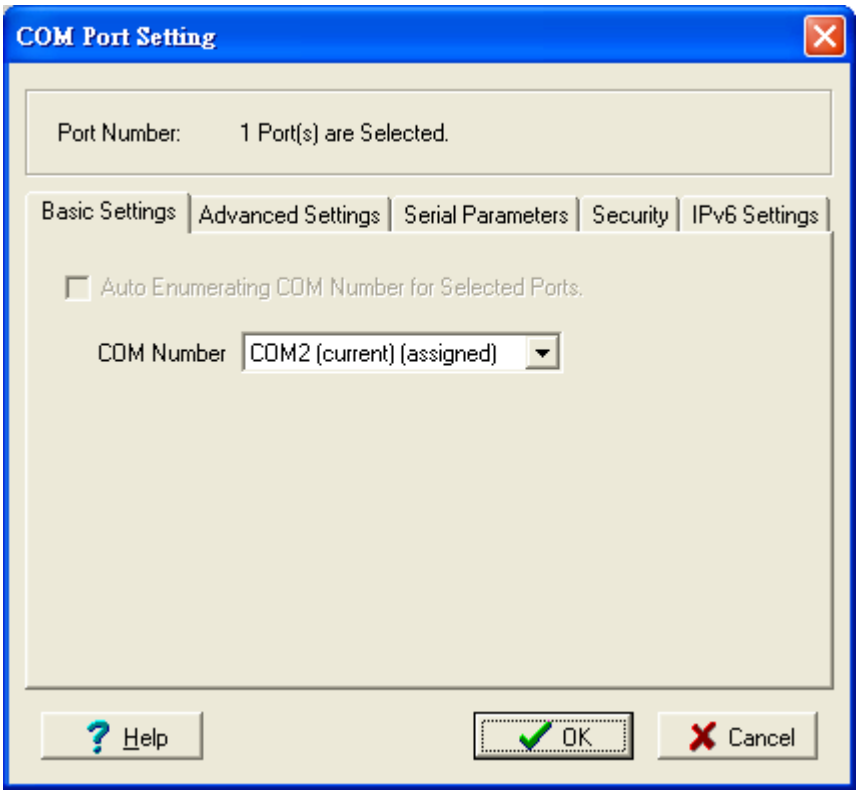
8. Use terminal software to open the mapped COM port to communicate with the serial device. You may download PComm Lite, a useful tool to check the serial communication, from Moxa's website: http://www.moxa.com/support/download.aspx?type=support&id=167

Configure the mapped COM ports with Advanced Functions

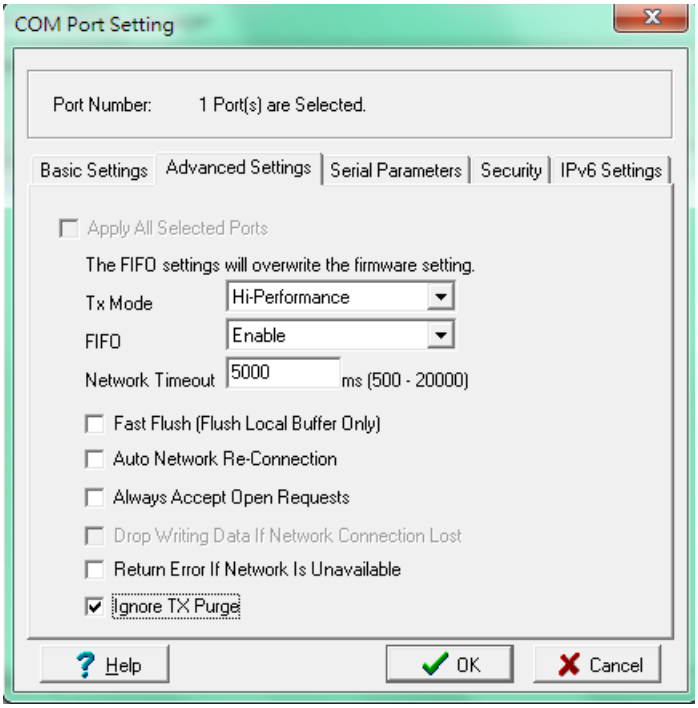
For Real COM Mode, to reconfigure the settings for a particular serial port on the NPort device server, select the row corresponding to the desired port and then click the **Setting** icon.



1. On the **Basic Setting** window, use the **COM Number** drop-down list to select a COM number to be assigned to the NPort device server's serial port that is being configured. 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.



2. Click the **Advanced Settings** tab to modify Tx Mode, FIFO, and Flash Flush.



Tx Mode

Hi-Performance is the default for Tx mode. After the driver sends data to the NPort device service, the driver immediately issues a "Tx Empty" response to the program. Under **Classical** mode, the driver will not send the "Tx Empty" response until confirmation has been received from the NPort device 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 device 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 result in a faster response and lower throughput.

Network Timeout

You can use this option to prevent blocking if the target NPort is unavailable.

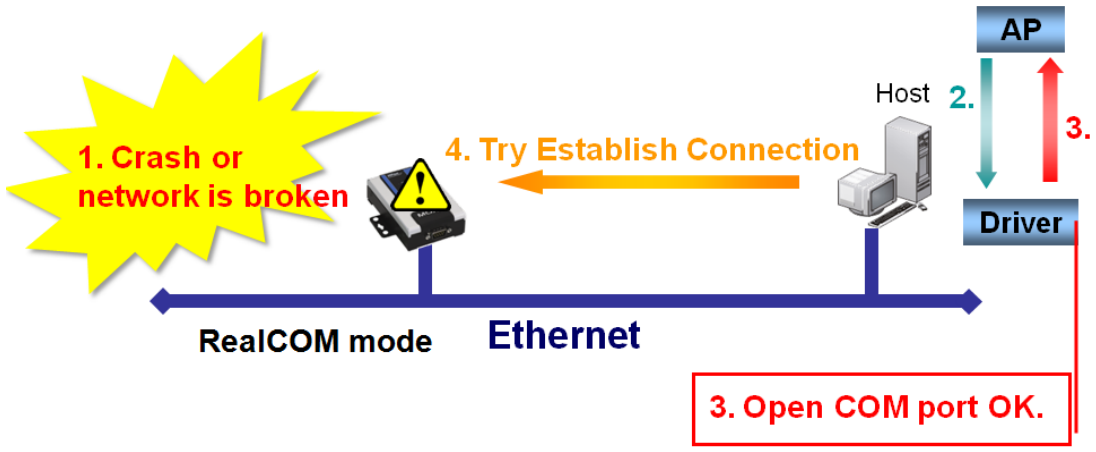
Auto Network Re-Connection

With this option enabled, the driver will repeatedly attempt to reestablish the TCP connection if the NPort device server 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.

For example, if the NPort is down or the network is broken as described in figure below. At that moment, the terminal software tries to open the mapped COM port, and the driver will respond with the message:"Success" for the terminal software to open the COM port. At the same time, the driver will try to establish the connection to the specific NPort. If the connection is established, then the mapped COM port will work properly.



Return error if network is unavailable

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

Fast Flush (only flushes the local buffer)

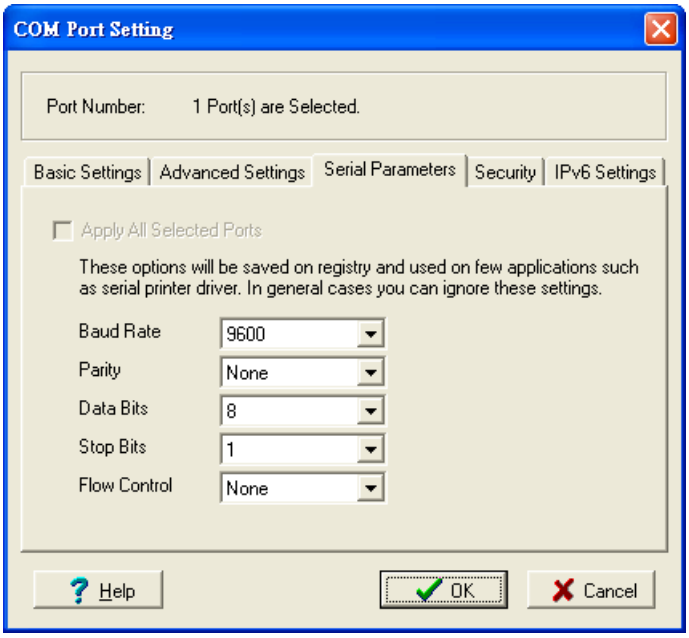
For some applications, the user's program will use the Win32 "PurgeComm()" function before it reads or writes data. After a program uses this PurgeComm() function, the NPort driver continues to query the NPort's firmware several times to make sure no data is queued in the NPort's firmware buffer, rather 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 due to the additional time spent communicating across the Ethernet. This is why PurgeComm() works significantly faster with native COM ports on a PC than with mapped COM ports on the NPort device server. 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 device server 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.

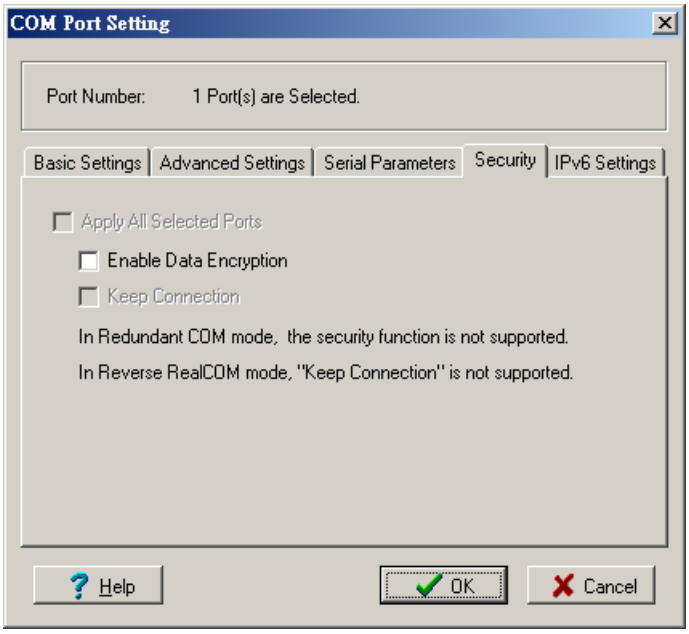
Ignore TX Purge

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.

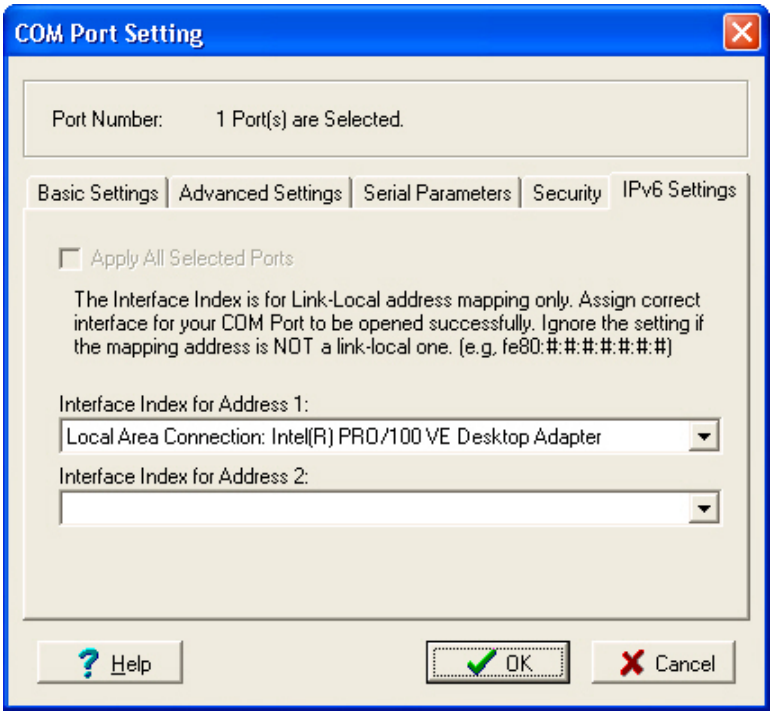
3. The **Serial Parameters** window in the following figure shows the default settings when the NPort device server is powered on. However, the program can redefine the serial parameters to different values after the program opens the port via Win 32 API.



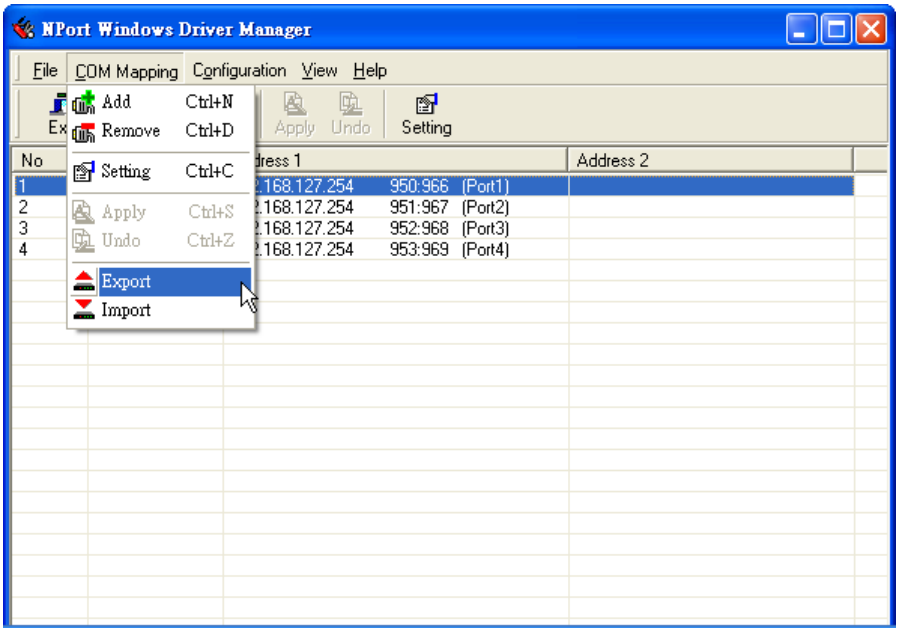
4. The Enable Data Encryption function is available only for the NPort 6000 Series. When the user also enables the same function on the NPort 6000's firmware, the data transmitted on the Ethernet network will be encrypted between the NPort 6000 and the host.



5. The IPv6 Settings function is available only for the NPort 6000 Series.



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



Linux Real TTY Drivers

Basic Procedures

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

1. Set up the NPort device server. After verifying that the IP configuration works, and you can access the NPort device server (by using ping, telnet, etc.), configure the desired serial port on the NPort device server 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 device server is **192.168.127.254,** and the default username and password are **admin** and **moxa**, respectively.

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

Installing Linux Real TTY Driver Files

1. Obtain the driver file from Moxa's website, at http://www.moxa.com.
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 device server 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. Modifies 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 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 number of 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, map tty ports, and unload the driver. To do this, you only need to enter the directory **/usr/lib/npreal2/driver**, and 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.

The UNIX Fixed TTY Driver

Installing the UNIX Driver

1. Log in to UNIX and create a directory for the Moxa TTY. To create a directory named /usr/etc, execute the command:
   # **mkdir –p /usr/etc**

2. Copy **moxattyd.tar** to the directory you created. If you created the **/usr/etc** directory above, you would execute the following commands:

   # **cp moxattyd.tar /usr/etc**
   # **cd /usr/etc**

3. Extract the source files from the tar file by executing the command:

   # tar xvf moxattyd.tar
   The following files will be extracted:
   README.TXT
   moxattyd.c --- source code
   moxattyd.cf --- an empty configuration file
   Makefile --- makefile
   VERSION.TXT --- fixed tty driver version
   FAQ.TXT

4. Compile and Link

   For SCO UNIX:
   # make sco
   For UnixWare 7:
   # make svr5
   For UnixWare 2.1.x, SVR4.2:
   # make svr42

Configuring the UNIX Driver

Modify the configuration

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

ttyp1 192.168.1.1 950

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

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

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

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

Device naming rule

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

pts/[*n*]

For all other UNIX operating systems, use:

ttyp[*n*]

Starting moxattyd

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

Adding an additional server

1. Modify the text file **moxattyd.cf** to add an additional server. Users may use vi or any text editor to modify the file. For more configuration information, look at the file **moxattyd.cf**, which contains detailed descriptions of the various configuration parameters.
2. Find the process ID (PID) of the program **moxattyd**.

   # ps -ef | grep moxattyd
3. Update configuration of **moxattyd** program.

   # kill -**USR1 [*PID*]**

   (e.g., if moxattyd PID = 404, **kill -USR1 404**)

   This completes the process of adding an additional server.

6

Web Console: Basic Settings

The following topics are covered in this chapter:

- **Overview**
- **Basic Settings**

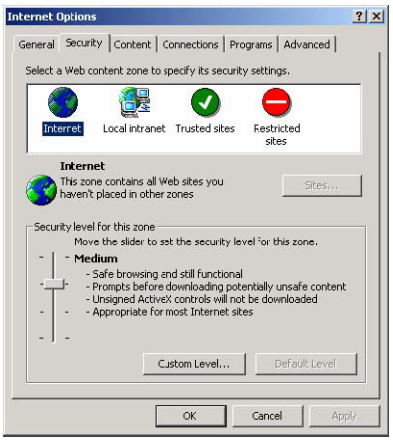
Overview

This chapter introduces the NPort web console and explains how to configure the basic settings.

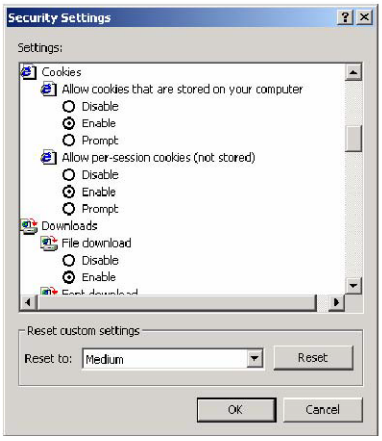
The NPort can be configured from anywhere on the network through its web console. Simply point the browser to the device server's IP address to open the web console. Network settings, operation mode, and other items can all be configured through the browser.

Web Browser Settings

In order to use the web console, you will need to have cookies enabled for your browser. Please note that the web console uses cookies only for password transmission. For Internet Explorer, cookies can be enabled by right-clicking the Internet Explorer icon on your desktop and selecting Properties from the context menu.



On the Security tab, click "Custom Level…" and enable these two items:
Allow cookies that are stored on your computer.
Allow per-session cookies (not stored).



ATTENTION

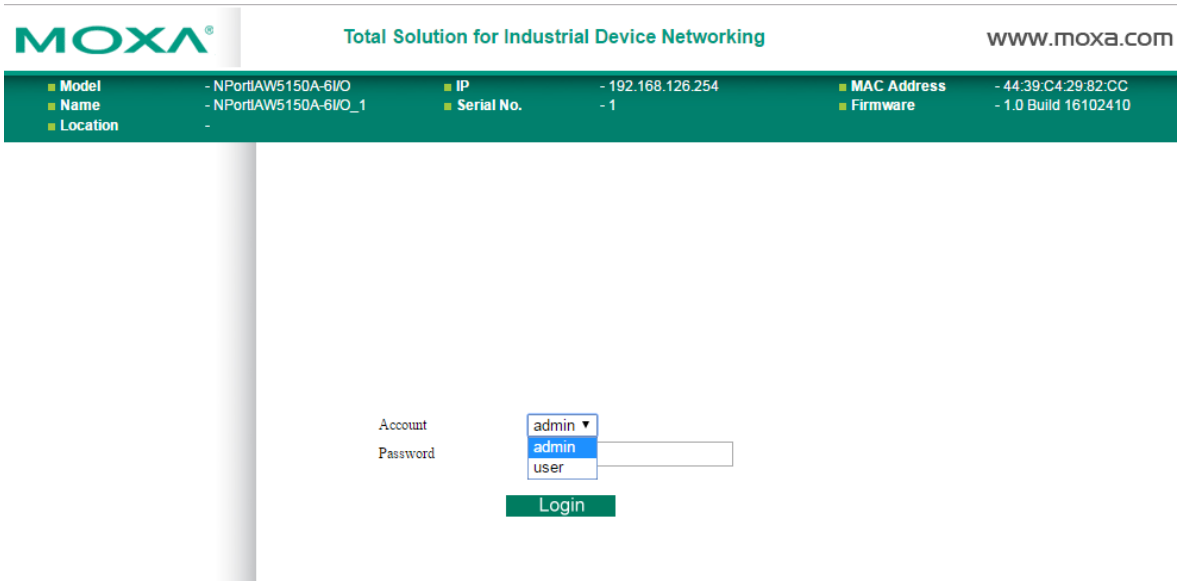
If you are not using Internet Explorer, cookies are usually enabled through a web browser setting such as "allow cookies that are stored on your computer" or "allow per-session cookies."

Navigating the Web Console

To open the web console, enter your device server's IP address in the website address line. If you are configuring the NPort for the first time over an Ethernet cable, you will use the default IP address, **192.168.126.254** for the NPort IAW5000A-I/O Series, and **192.168.127.254** for the NPort IA5000A-I/O Series.

There are two account types: **admin** and **user**. If you enter the system with **admin** account, you will have the right to read and write. If you enter the system with **user** account, you will only have the right to read.

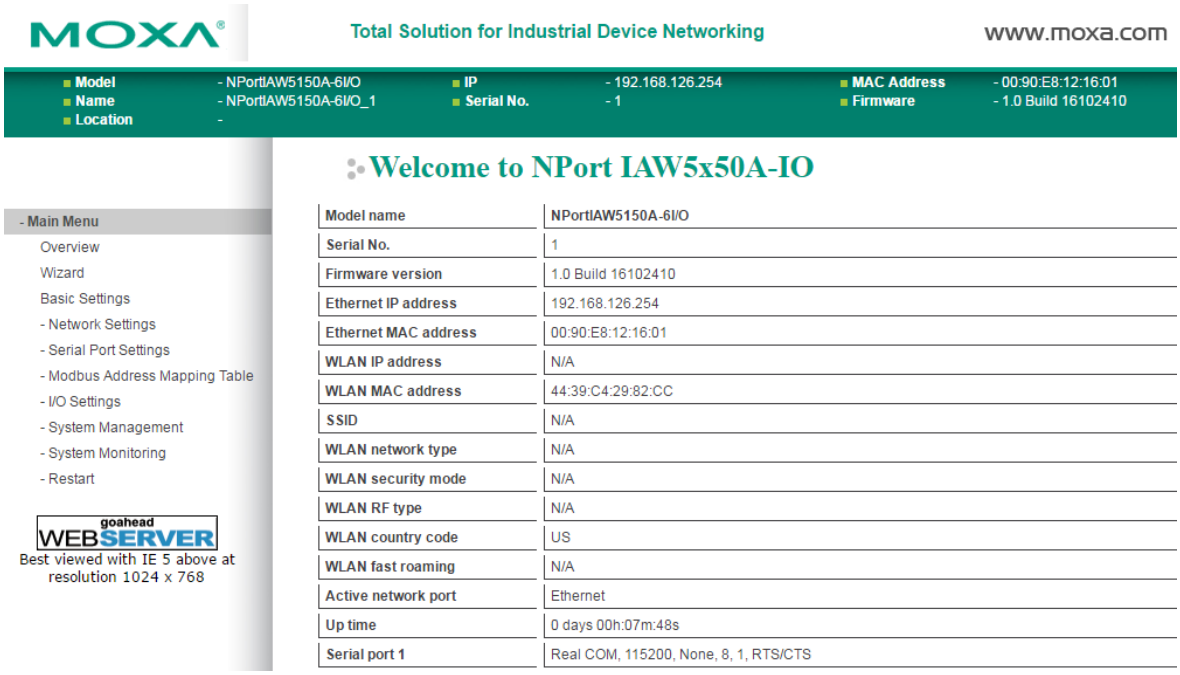
If prompted, enter the console password. You will only be prompted for a password if you have enabled password protection on the device server. The password will be transmitted with MD5 encryption over the Ethernet.



ATTENTION

If you have forgotten the password, you can use the reset button to load factory defaults, but this will erase all previous configuration information.

The web console will appear as shown below.



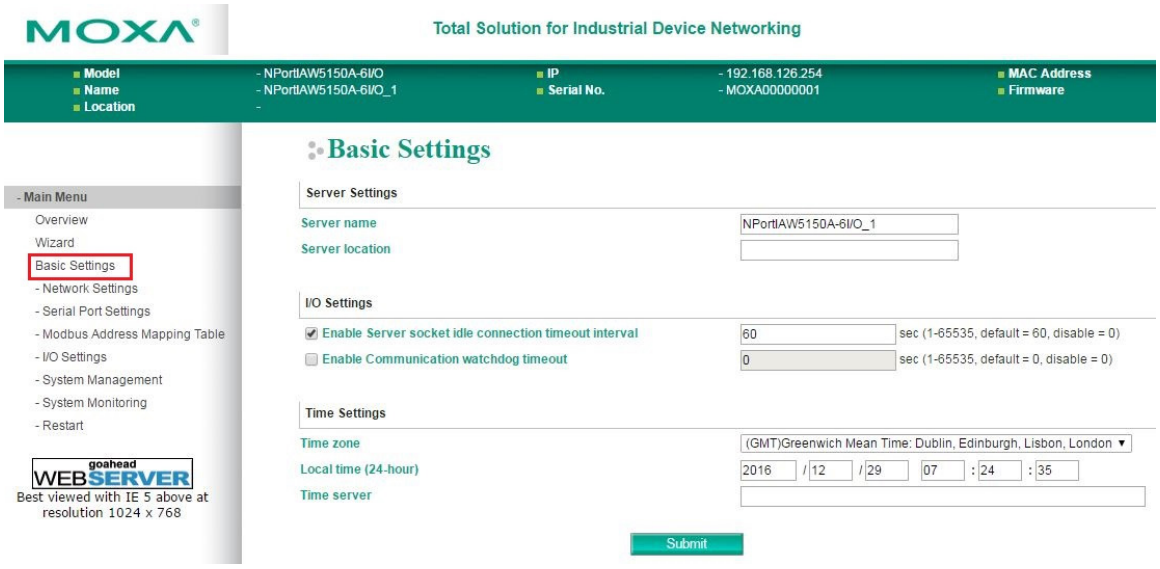
Settings are presented on pages that are organized by folder. Select the desired folder in the left navigation panel to open that page. The page will be displayed in the main window on the right. Certain folders can be expanded by clicking the adjacent "–" symbol.

For example, if you click **Basic Settings** in the navigation panel, the main window will show a page of basic settings that you can configure.

After you have made changes on a page, you must click **[Submit]** in the main window before jumping to another page. Your changes will be lost if you do not click **[Submit]**.

Once you click **[Submit]** button, the device server will reboot and with a beep alarm.

Basic Settings



On the **Basic Settings** page, you can configure:

Server Name

Default	NPortIA5150A-6I/O_<serial no.> or NPort IA5250A-6I/O_<serial no.> NPortIAW5150A-6I/O_<serial no.> or NPort IAW5250A-6I/O_<serial no.> NPortIA5150A-12I/O_<serial no.> or NPort IA5250A-12I/O_<serial no.> NPortIAW5150A-12I/O_<serial no.> or NPort IAW5250A-12I/O_<serial no.>
Options	free text (e.g., "Server 1")
Description	This is an optional free text field to help you differentiate one device server from another. It does not affect operation of the NPort device server.

Server Location

Default	
Options	free text (e.g., "Bldg 1, 2nd Floor")
Description	This is an optional free text field to help you differentiate one device server from another. It does not affect operation of the NPort device server.

Enable Server socket idle connection timeout interval

Default	Enabled (60 secs)
Options	1-65535, default = 60, disable = 0
Description	The NPort will automatically disconnect the Modbus/TCP connection from the server after a specified time period to free up the port for the next connection if function is enabled.

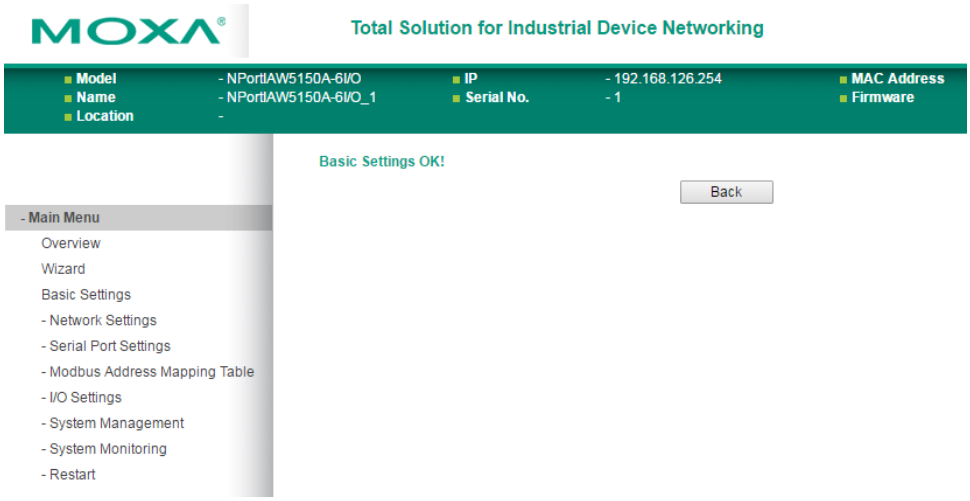
Enable Communication watchdog timeout

Default	Disabled
Options	1-65535, default = 60, disable = 0
Description	This function will activate **Safe Mode** when a specified period of time has passed and there is a loss of Modbus/TCP network connectivity. **Safe Mode** is specially designed for products with output channels to output a suitable value or status when the NPort cannot be controlled by a remote PC (such as in the event of a network failure). By default, the watchdog is disabled. Users can configure how each output channel responds on the **I/O Settings** page. To enable the Communication Watchdog function, select the **Enable Communication Watchdog** checkbox, set the timeout value, and then restart the server. When the watchdog is enabled, the NPort will enter **Safe Mode** when there is a disruption in communication that exceeds the specified time limit. User may go to **System Alert Status** under **System Monitoring** tab to see the host connection status and clear the alert if the **Modbus/TCP connection** resumes.

Time Zone

Default	(GMT)Greenwich Mean Time
Options	(GMT)Greenwich Mean Time (GMT-01:00)Azores, Cape Verde Is. (GMT-02:00)Mid-Atlantic etc.
Description	This field shows the currently selected time zone and allows you to select a different time zone.

Local Time

Default	
Options	Date (yy:mm:dd), Time (hh:mm:ss)
Description	The NPort has a built-in real-time clock that allows you to add time information to functions such as the automatic warning e-mail or SNMP trap. This field shows the current time according to the NPort's built-in real-time clock. This is not a live field, so you will need to refresh the browser to get an updated reading. Change the correct date or time, and click **[Submit]**. The change will take effect directly, and shows **Basic Setting OK!**. 

ATTENTION

There is a risk of explosion if the real-time clock battery is replaced incorrectly!
The real time clock is powered by a lithium battery. We strongly recommend that you obtain assistance from a Moxa support engineer before replacing the battery. Please contact the Moxa RMA service team if you need to change the battery.

Time Server

Default	
Options	IP address or domain name (e.g., "192.168.1.1" or "time.nist.gov")
Description	This optional field specifies your time server's IP address or domain name, if a time server is used in your network. The NPort supports SNTP (RFC-1769) for automatic time calibration. The device server will request time information from the specified time server every 10 minutes.

7

Web Console: Network Settings

The following topics are covered in this chapter:

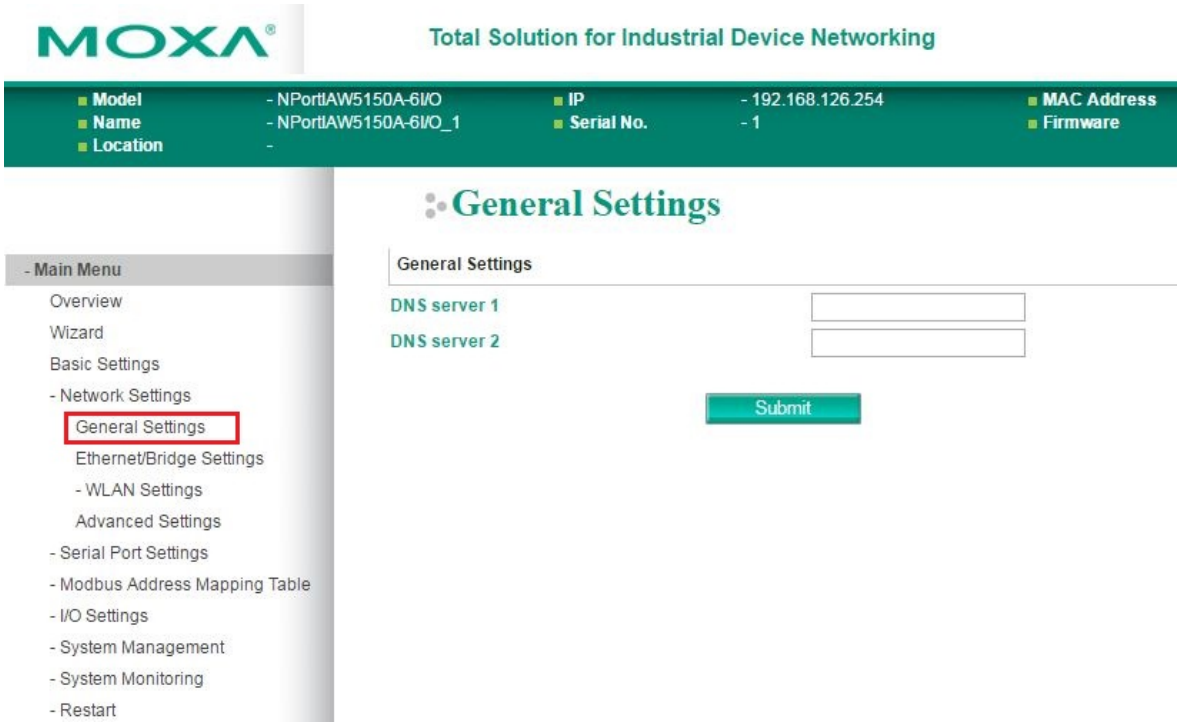
- **Overview**
- **Network Settings**
  - General Settings
  - Ethernet/Bridge Settings
  - WLAN Settings
  - Advanced Settings

Overview

This chapter explains how to configure all settings located under the **Network Settings** folder in the NPort web console.

Network Settings

General Settings



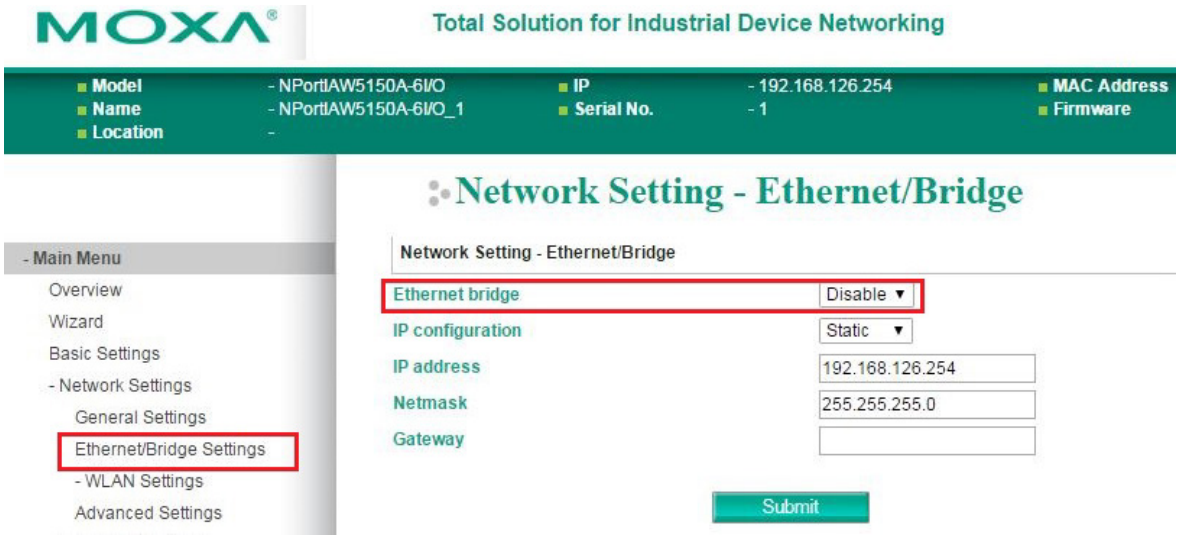
On the **General Settings** page in the **Network Settings** folder, you can modify **DNS server 1 and 2**.

DNS Server 1 and 2

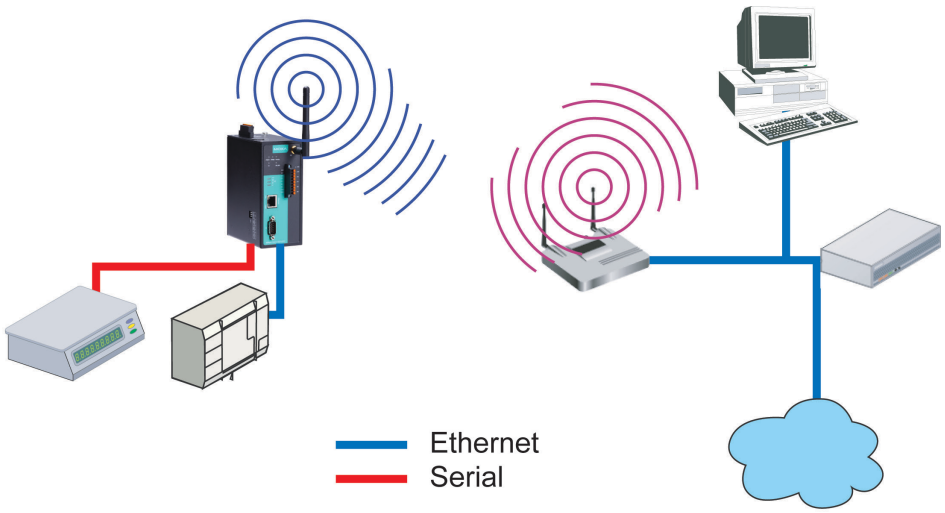
Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the DNS server's IP address, if applicable. With the DNS server configured, the NPort device server can use domain names instead of IP addresses to access hosts. Domain Name System (DNS) is how Internet domain names are identified and translated into IP addresses. A domain name is an alphanumeric name, such as www.moxa.com, that it is usually easier to remember than the numeric IP address. A DNS server is a host that translates a text-based domain name into an IP address in order to establish a TCP/IP connection. When the user wants to visit a particular website, the user's computer sends the domain name (e.g., www.moxa.com) to a DNS server to request that website's numeric IP address. When the IP address is received from the DNS server, the user's computer uses that information to connect to the website's web server. The NPort will play the role of a DNS client, actively querying the DNS server for the IP address associated with a particular domain name.

Ethernet/Bridge Settings

To enable the Ethernet-to-Wireless function, go to the **Ethernet/Bridge Settings** page and enable **Ethernet Bridge**.



Ethernet Bridge (for NPort IAW5000A-I/O Series)

Default	Disabled
Options	Enabled / Disabled
Description	This field specifies whether to enable **Ethernet Bridge** mode or not. When **Ethernet Bridge** is enabled, the LAN and WLAN interfaces are bridged together. Data can be seamlessly transferred between serial lines, LAN, and WLAN. The LAN and WLAN will use the LAN IP setting, and WLAN IP setting will be disabled. **Disabled:** When disabled, you can use either the LAN or WLAN. **Enabled:** When enabled, you can use both the LAN and the WLAN. 

IP Configuration

Default	Static
Options	Static, DHCP, DHCP/BOOTP, BOOTP
Description	This field determines how the NPort's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

IP Address

Default	192.168.127.254 for the NPort IA5000A-I/O Series 192.168.126.254 for the NPort IAW5000A-I/O Series' wired RJ45 Ethernet port
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address that will be assigned to your NPort device server. 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. If your device server will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

Netmask

Default	255.255.255.0
Options	Netmask setting (e.g., "255.255.0.0")
Description	This field is for the subnet mask. A subnet mask represents all of 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 device server 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 device server, a connection is established directly from the device server. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

Gateway

Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address of the gateway, if applicable. A gateway is a network computer 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 device server needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

ATTENTION

In dynamic IP environments, the NPort will send 3 requests every 30 seconds to the DHCP or BOOTP server until the network settings have successfully been assigned. The first request will time out after one second; the second request will time out after three seconds, and the third request will timeout after five second. If the DHCP or BOOTP server is unavailable, the NPort will use the factory default network settings.

WLAN Settings (for the NPort IAW5000A-I/O Series)

WLAN

The **WLAN** page is located under **WLAN Settings** in the **Network Settings** folder. You can modify **IP configuration**, **IP address**, **Netmask**, and **Gateway** for your WLAN.

The NPort IAW5000A-I/O Series supports IEEE 802.11a/b/g/n wireless network interfaces. The supported IP configurations are static and dynamic (BOOTP, DHCP, or BOOTP+DHCP). Users can set up the IP configuration with the serial console, or the Web/Telnet consoles through the NPort's Ethernet interface. For detailed information about configuring **IP configuration**, **IP address**, **Netmask**, and **Gateway**, see the previous section, **Ethernet/Bridge Settings**.

IP Configuration

Default	Static
Options	Static, DHCP, DHCP/BOOTP, BOOTP
Description	This field determines how the NPort's IP address will be assigned. Static: IP address, netmask, and gateway are user-defined. DHCP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. DHCP/BOOTP: IP address, netmask, gateway, DNS, and time server are assigned by DHCP server. IP address is assigned by BOOTP server if DHCP server does not respond. BOOTP: IP address is assigned by BOOTP server.

IP Address

Default	192.168.127.254
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address that will be assigned to your NPort device server. 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 WLAN environment. If your device server will be assigned a dynamic IP address, set the "IP configuration" parameter appropriately.

Netmask

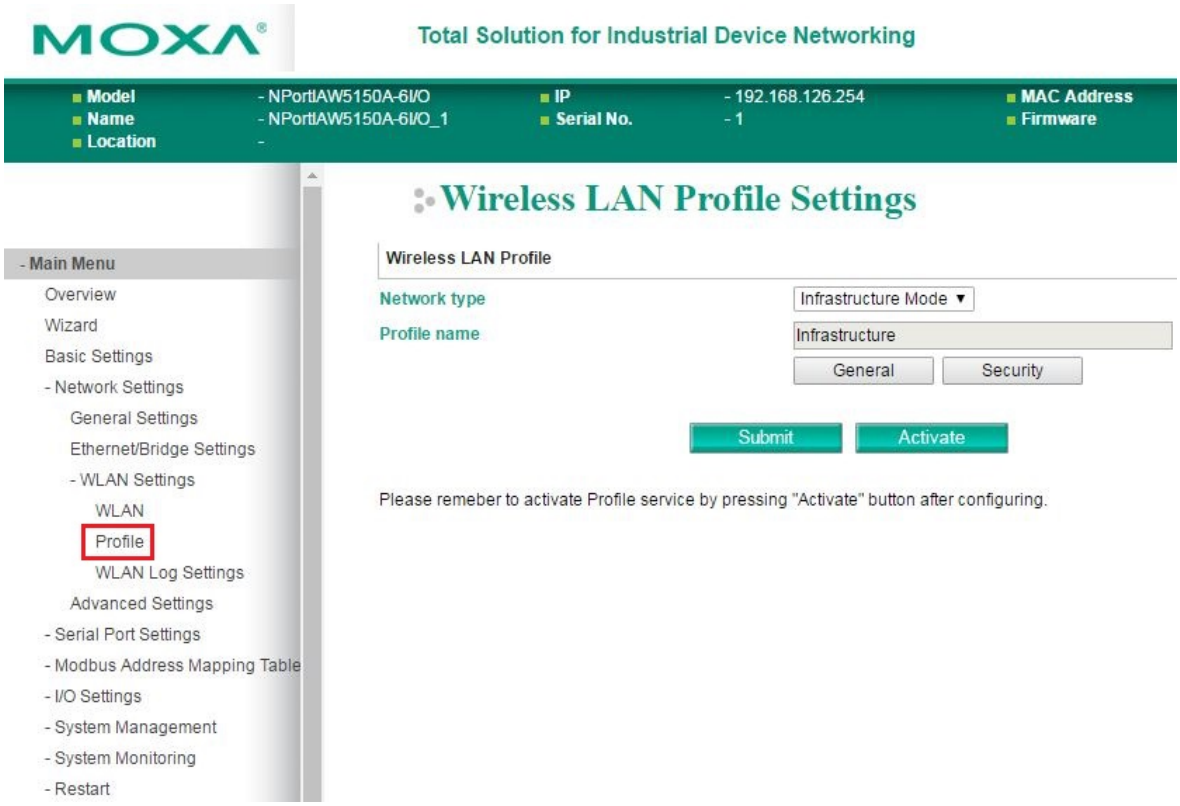
Default	255.255.255.0
Options	Netmask setting (e.g., "255.255.0.0")
Description	This field is for the subnet mask. A subnet mask represents all of the network hosts at one geographic location, in one building, or on the same local area network. When a packet is sent out over the network, the NPort device server 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 device server, a connection is established directly from the device server. Otherwise, the connection is established through the gateway as specified in the "Gateway" parameter.

Gateway

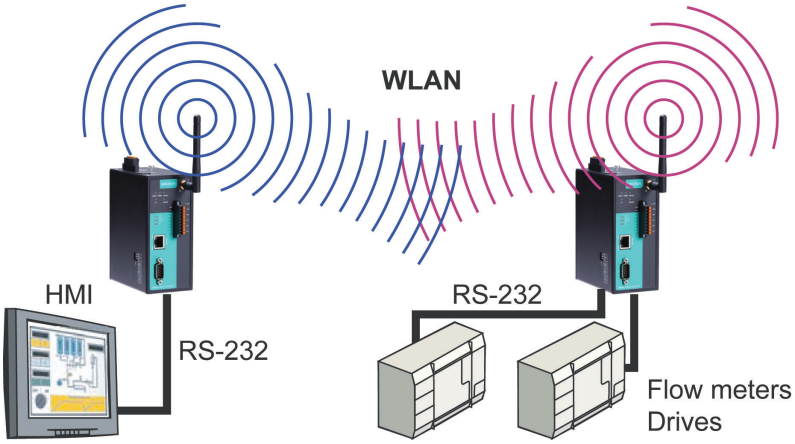
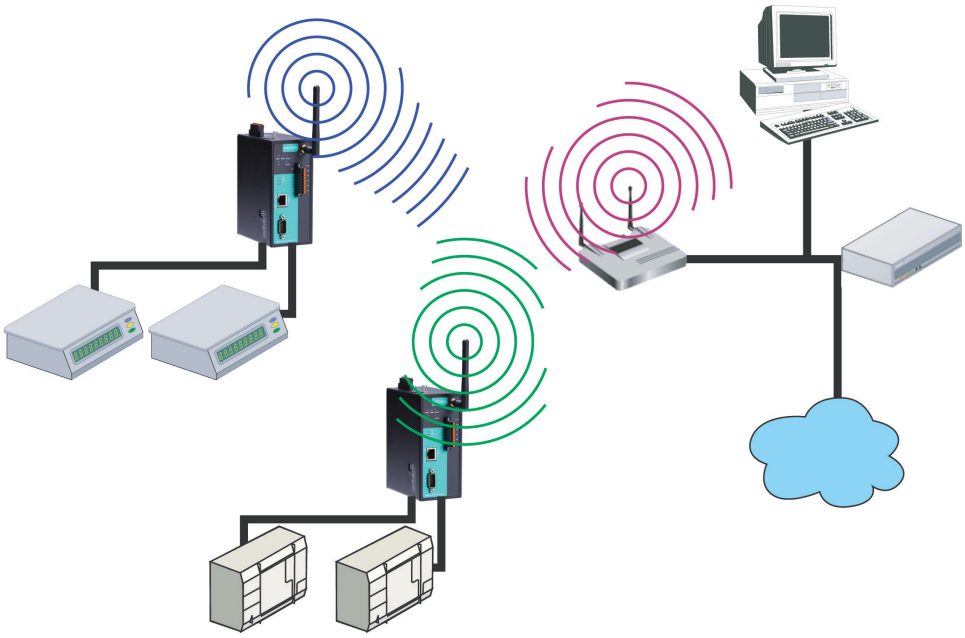
Default	
Options	IP address (e.g., "192.168.1.1")
Description	This field is for the IP address of the gateway, if applicable. A gateway is a network computer that acts as an entrance to another network. Usually, the computers that control traffic within the network or at the local Internet service provider are gateway nodes. The NPort device server needs to know the IP address of the default gateway computer in order to communicate with the hosts outside the local network environment. Consult your network administrator if you do not know how to set this parameter.

Profile

The **Profile** page is located under **WLAN Settings** in the **Network Settings** folder. This is where you configure the NPort for Ad-hoc or Infrastructure operation. Different settings are available depending on whether you select Ad-hoc Mode or Infrastructure Mode.



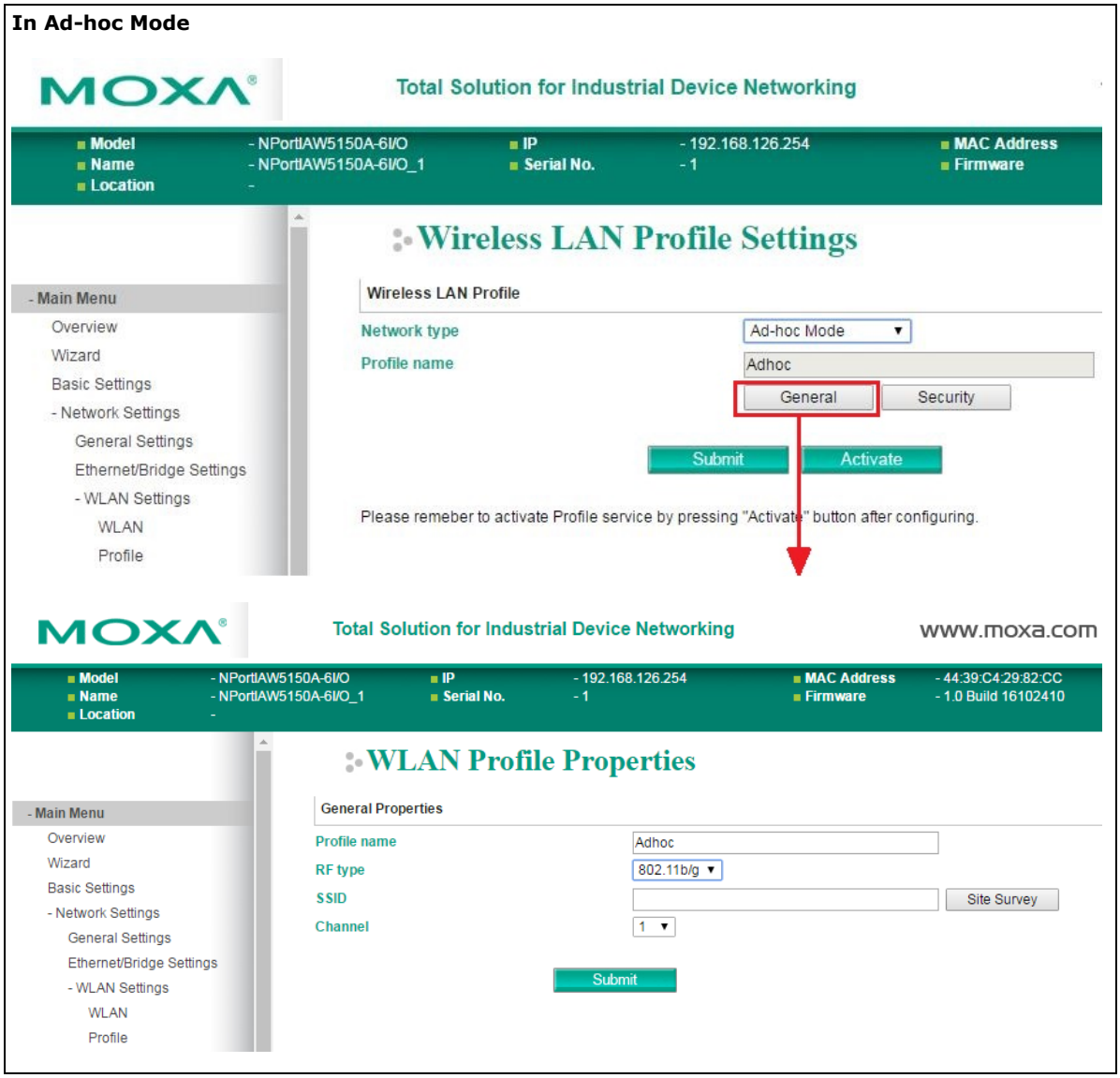
Network Type

Default	Infrastructure Mode
Options	Infrastructure Mode, Ad-hoc Mode
Description	This field specifies whether the NPort will operate in Ad-hoc or Infrastructure Mode. For all wireless networking devices, there are two possible modes for communication with another wireless device. Devices that are configured for Ad-hoc Mode automatically detect and communicate directly with each other and do not require a wireless access point (AP) or gateway. Wireless devices that are configured for Infrastructure Mode do not communicate directly with each other, but through a wireless access point (AP). Devices must be configured for the same mode in order to communicate with each other. Devices in Ad-Hoc Mode will only recognize other devices in Ad-Hoc Mode, and likewise for devices in Infrastructure Mode. **Example of Ad-Hoc Mode**  **Example of Infrastructure Mode**  After setting the Network type, you will need to adjust the General and Security settings for the profile. In Ad-hoc Mode, only one profile is available. In Infrastructure Mode, three profiles can be defined.

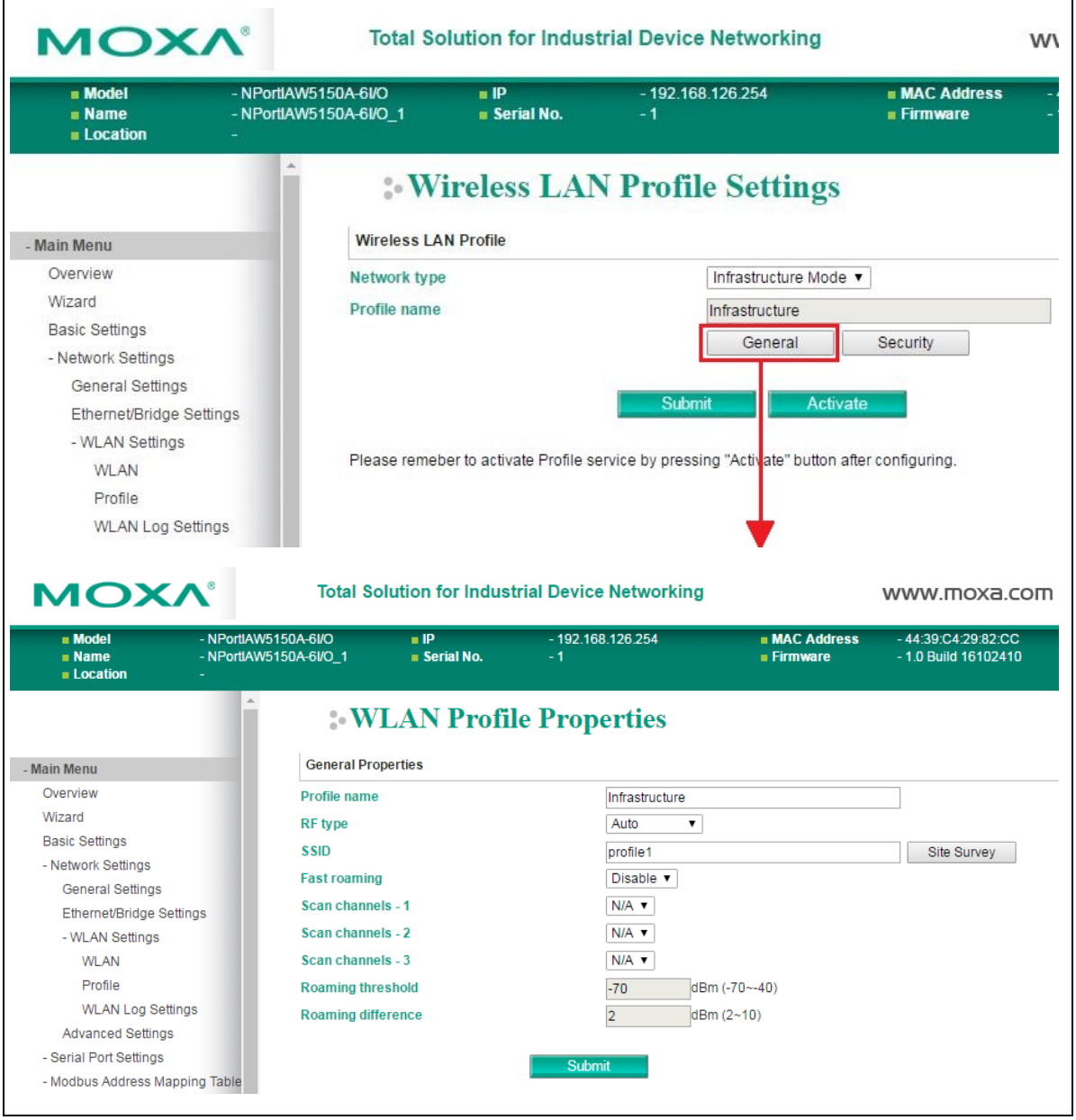
General Settings for WLAN Profile

The **General** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. You can type a profile name to help you differentiate one profile from another. It does not affect operation of the NPort. After selecting Ad-hoc or Infrastructure Mode, click **[General]** to open the General page for the selected profile. In Ad-hoc Mode, only one profile is available.

In Ad-hoc Mode



In Infrastructure Mode



On the General page, you can configure **Profile name**, **RF Type**, and input an **SSID** provided by your WiFi AP. Additional settings are also available depending on whether you select **Ad-hoc Mode** or **Infrastructure Mode**.

Profile Name

Default	Ad-hoc (in Ad-hoc Mode) Infrastructure (in Infrastructure Mode)
Options	free text (e.g., "Primary Connection")
Description	This is a free text field to help you differentiate one profile from another. It does not affect operation of the NPort.

RF Type

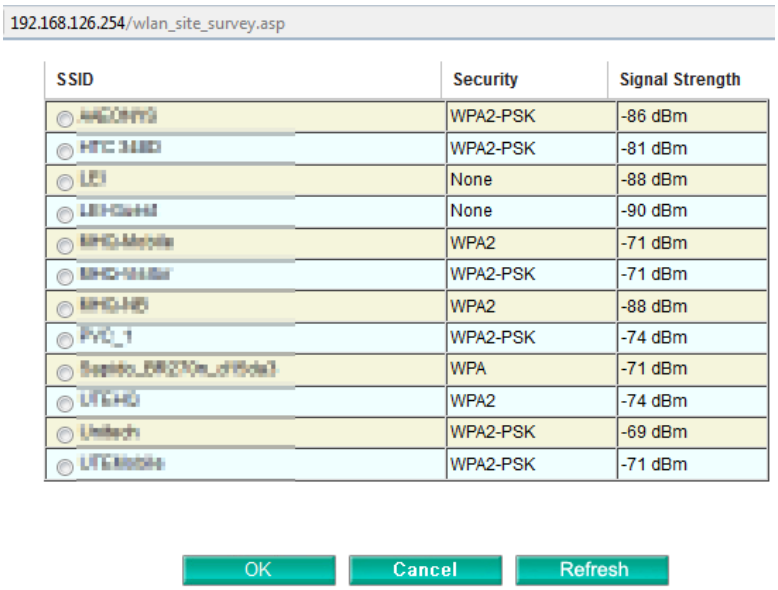
Default	802.11b/g for Ad-Hoc Mode. Auto for Infrastructure Mode.
Options	802.11b/g only for Ad-Hoc Mode. Auto, 802.11a, 802.11b/g, 802.11a/n, 802.11b/g/n for Infrastructure Mode.
Description	This field determines which wireless standard will be used by the selected profile. 802.11a, 802.11b/g, 802.11a/n and 802.11b/g/n are supported. Auto: In Ad-hoc Mode, the NPort will scan the 2.4G wireless band and will automatically select the appropriate wireless standard for communication with any other wireless devices that are detected. In Infrastructure Mode, the NPort will automatically select between 802.11a, 802.11b/g, 802.11a/n and 802.11b/g/n according to the settings of the AP. 802.11a: The Unlicensed National Information Infrastructure (UNII) 5 GHz band is used for communication, which is different from the RF band used by 802.11b and 802.11g. Consequently, 802.11a devices will not be able to communicate with 802.11b or 802.11g devices. (Multimode 802.11a/b/g APs or client adapters can be used to resolve this.) Transmission rates up to 54Mbps are supported. 802.11b/g: This option means our device will support for 802.11b or 802.11g. 802.11b: This is the well-known "Wi-Fi" standard, also referred to as "802.11 High-Rate (HR)." Wireless communication is in the 2.4 GHz ISM band, using the DSSS spread spectrum transmission scheme. 802.11b supports data rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps. 802.11a/n: The option means our device will support up to 150 Mbps bandwidth to communicate to a 802.11a/n AP. 802.11b/g/n: This option means our device will support up to 72.2 Mbps bandwidth to communicate to a 802.11b/g/n AP.

SSID

Default	Default
Options	Free text (e.g., "Coffeeshop WLAN")
Description	This field specifies the SSID, or name, of the wireless network (SSID) that will be used by the NPort. Wireless devices must use the same SSID in order to communicate with each other.

Site Survey

When you click **Site Survey**, the device server will scan for all the APs it can find nearby. It shows all the signal strengths between the device server and the APs. You may check the checkbox and click **OK** to create a profile for the specified AP.



Channel (Ad-hoc mode only)

Default	1
Options	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Description	This field is for Ad-Hoc Mode only and specifies the radio channel to use for the wireless network.

Fast Roaming (Infrastructure mode only)

Default	Disable
Options	Disable, Enable
Description	This field is only available in Infrastructure Mode and is used to specify the NPort IAW5000A-I/O roaming behavior. Roaming is the ability to connect to different APs so wireless communication is not confined to one area or one particular AP. The NPort IAW5000A-I/O will only roam between APs, as specified by the SSID. Disable: Fast Roaming function will be disabled. NPort IAW5000A-I/O will scan all available channels and roam between APs as specified by the SSID. It scans the channel when booting up and will associate with the highest signal strength AP. Only when the associated AP is loses, then it will re-associate again. Enable: Fast Roaming function will be enabled. NPort IAW5000A-I/O will only scan the pre-defined "**Scan Channels - 1, Scan Channels - 2 & Scan Channels – 3**" and roam between APs as specified by the SSID. It scans the channel and will associate with the highest signal strength AP. It also scans the channel regularly and will re-associate with the highest signal strength AP (if there is) by automatically.

Scan channels – 1, Scan channels – 2, Scan channels – 3 (Infrastructure mode only)

Default	N/A
Options	1 through 14, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161
Description	This field is for fast roaming under Infrastructure Mode and specifies the radio channel to use for the wireless network. Choose the channel according to the factory setting of AP.

Roaming Threshold

Default	-70 (Disable)
Options	numbers
Description	When the signal strength between the device and the AP is below -70 dBm (the default number), the device server will start to scan for a new AP to establish the connection.

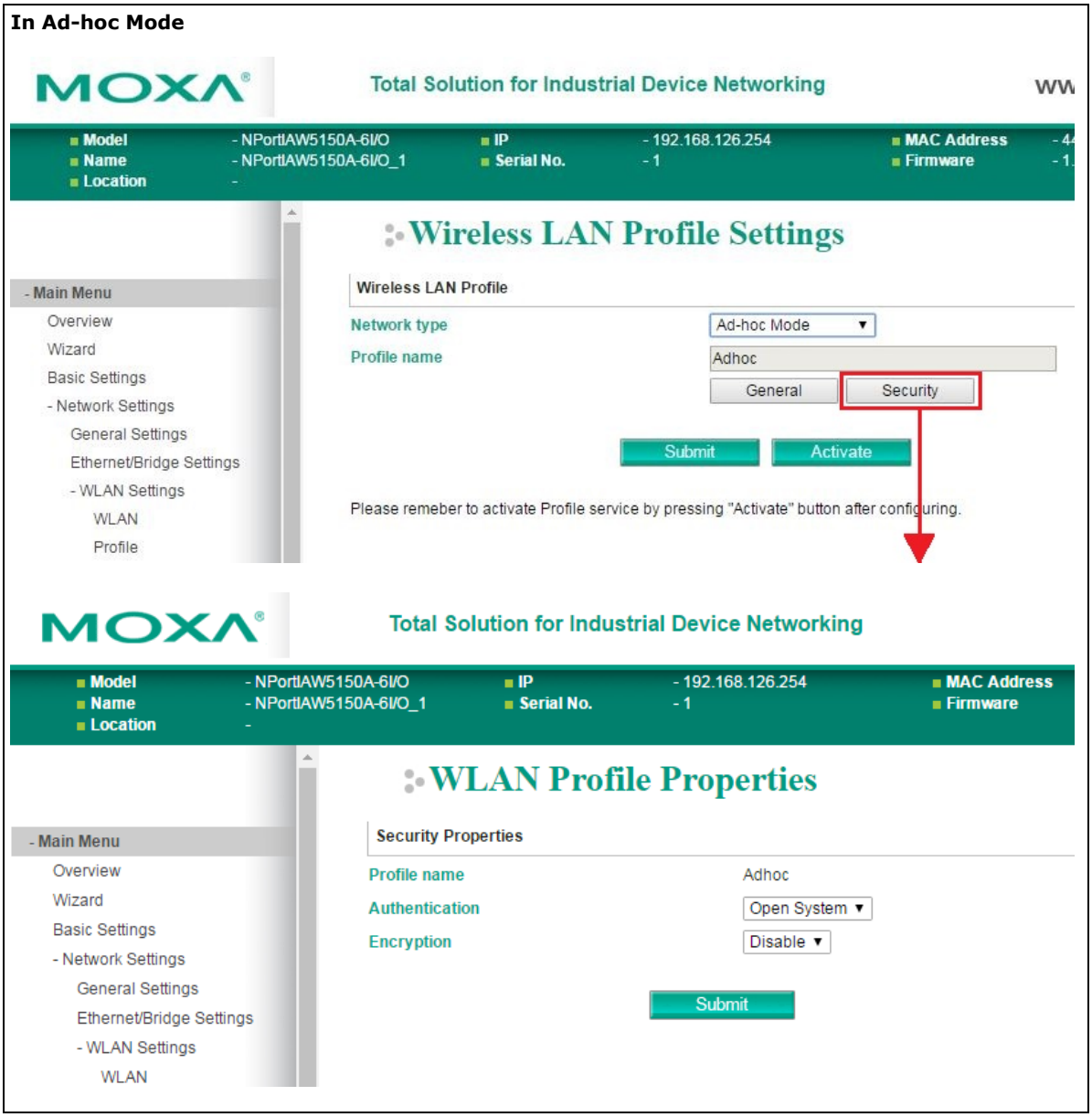
Roaming Difference

Default	2 (Disable)
Options	numbers
Description	When the device server finds a new AP, the signal strength between device server and the new AP must be 2 dBm stronger than the signal strength between the device server and the the old AP for the device server to establish a new connection with the new AP. For example, if the signal strength with the old AP is -70 dBm and it is -69 dBm with the new AP, then the device server will keep the connection with the old one. If the signal strength with the new AP is -68 dBm, the device server will switch the connection to the new AP.

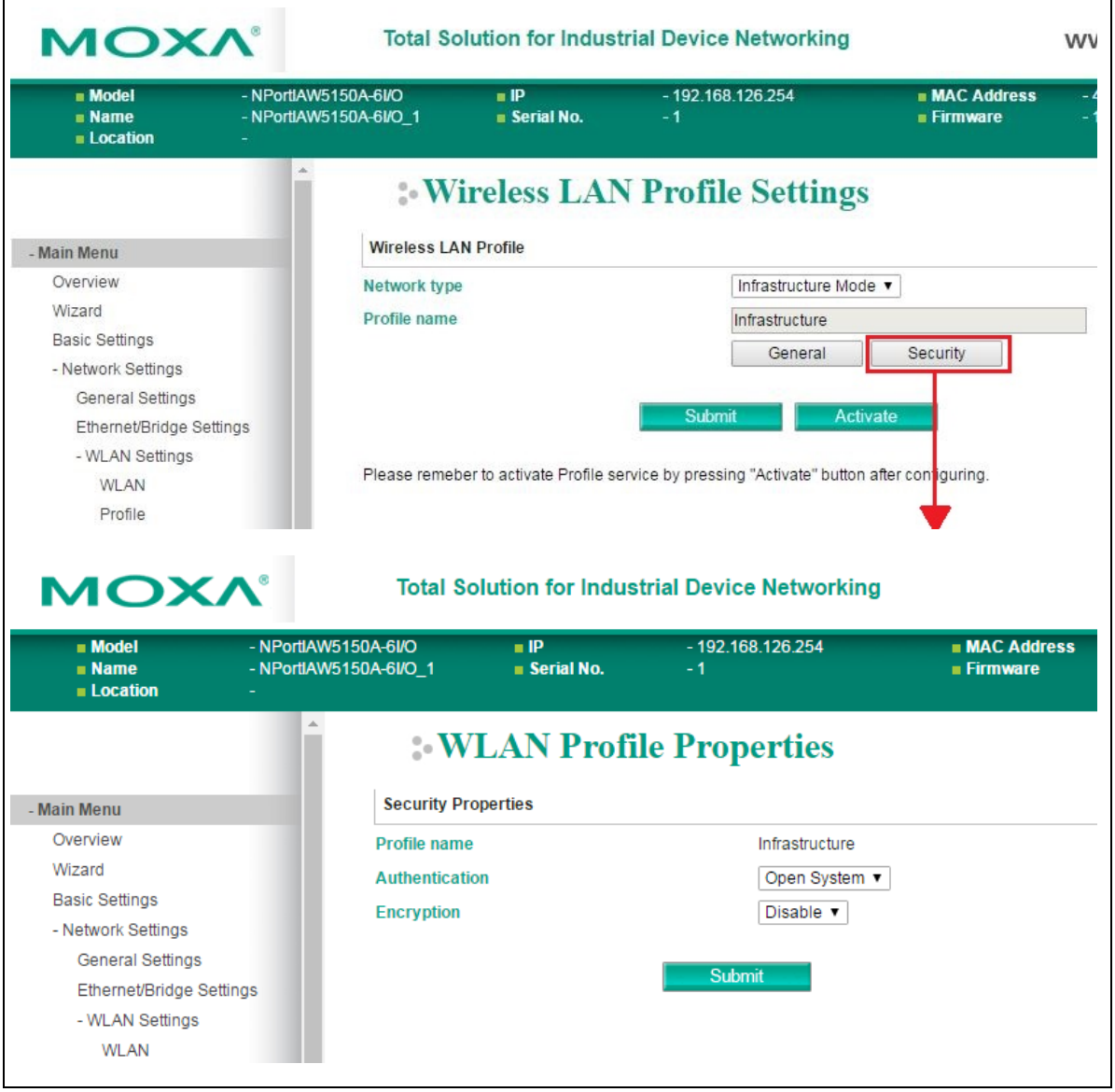
Security Settings for WLAN Profile

The **Security** page is opened through the **Profile** page, under **WLAN Settings** in the **Network Settings** folder. After selecting Ad-hoc or Infrastructure Mode, click **[Security]** to open the Security page for the selected profile. In Ad-hoc Mode, only one profile is available, whereas three profiles are available in Infrastructure Mode.

In Ad-hoc Mode



In Infrastructure Mode



You will need to configure **Authentication** and **Encryption**. These settings must match the settings on the wireless device at the other end of the connection (such as the AP). Different settings and options are available depending on how **Authentication** and **Encryption** are configured.

Authentication

Default	Open System
Options	Open System, Shared Key, WPA, WPA-PSK, WPA2, WPA2-PSK
Description	This field specifies how wireless devices will be authenticated. Only authenticated devices will be allowed to communicate with the NPort. If a RADIUS server is used, this setting must match the setting on the RADIUS server. Open System: The NPort will simply announce a desire to associate with another station or access point. No authentication is required. For Ad-hoc Mode, this is the only option for authentication, since Ad-hoc Mode was designed for open communication. Shared Key: This option is only available in Infrastructure Mode. Authentication involves a more rigorous exchange of frames to ensure that the requesting station is authentic. WEP encryption is required. WPA: This is a managed authentication option that is only available in Infrastructure Mode. WPA was created by the Wi-Fi Alliance, the industry trade group that owns the Wi-Fi trademark and certifies devices with the Wi-Fi name. It is based on Draft 3 of the IEEE 802.11i standard. Each user uses a unique key for authentication, distributed from an IEEE 802.1X authentication server, also known as a RADIUS server. This option is also referred to as WPA Enterprise Mode, since it is intended to meet rigorous enterprise security requirements. Tunneled authentication is supported, depending on the EAP method selected. WPA-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. Instead of a unique key for each user, a pre-shared key (PSK) is manually entered on the access point to generate an encryption key that is shared among all users. Consequently, this method does not scale well for enterprise. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option is also referred to as WPA Personal Mode, since it is designed for the needs and capabilities of small home and office WLANs. WPA2: This is a managed authentication option that is only available in Infrastructure Mode. WPA2 implements the mandatory elements of 802.11i. Supported encryption algorithms include TKIP, Michael, and AES-based CCMP, which is considered fully secure. Since March 13, 2006, WPA2 has been mandatory for all Wi-Fi-certified devices. This option may also be referred to as WPA Enterprise Mode. Tunneled authentication is supported, depending on the EAP method selected. WPA2-PSK: This is an unmanaged authentication option that is only available in Infrastructure Mode. It employs WP2 encryption algorithms but relies on a PSK for authentication. A PSK that uses a mix of letters, numbers and non-alphanumeric characters is recommended. This option can also be referred to as WPA Personal Mode.

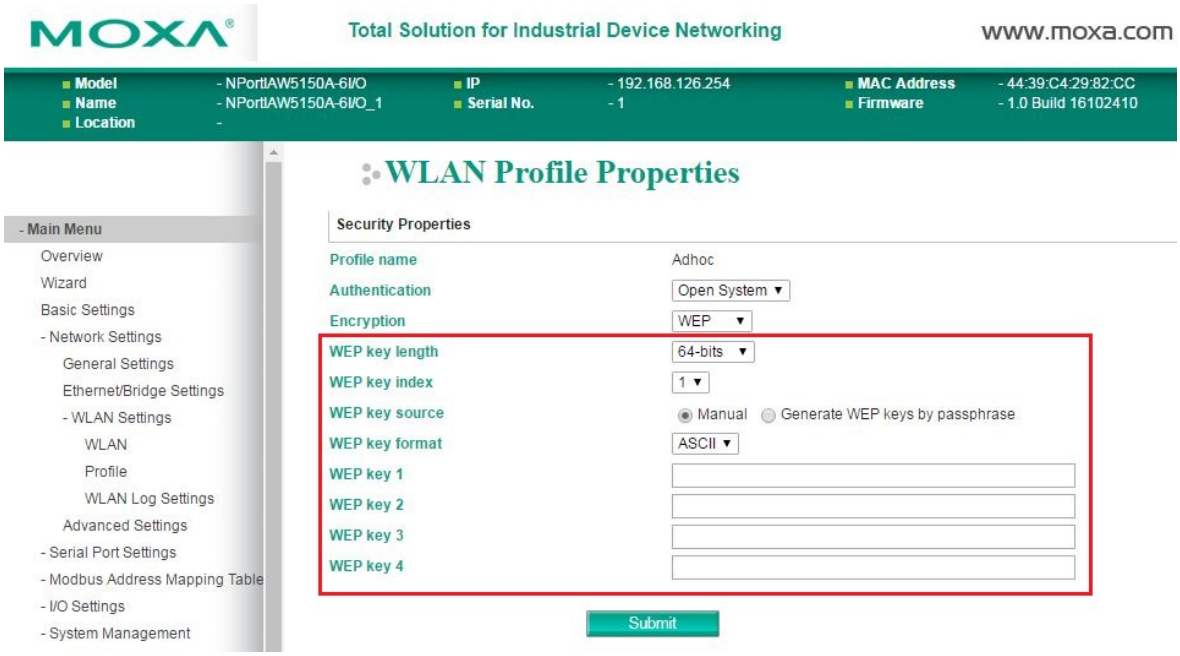
Encryption

Default	Disable
Options	Disable, WEP, TKIP, AES-CCMP
Description	This field specifies the type of encryption to use during wireless communication. Different encryption methods are available depending on the **Authentication setting**. Also, each encryption method has its own set of parameters that may also require configuration. Disable: No encryption is applied to the data during wireless communication. This option is only available if **Authentication** is set to **Open** System. WEP: Wired Equivalent Privacy (WEP) is only available for Open System and Shared Key authentication methods. Data is encrypted according to a key. The NPort supports both 64 and 128-bit keys. This method may deter casual snooping but is not considered very secure. TKIP: Temporal Key Integrity Protocol (TKIP) is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. TKIP is part of a draft standard from the IEEE 802.11i working group and utilizes the RC4 stream cipher with 128-bit keys for encryption and 64-bit keys for authentication. TKIP improves on WEP by adding a per-packet key mixing function to de-correlate the public initialization vectors (IVs) from weak keys. AES-CCMP: This is a powerful encryption method that is only available for WPA, WPA2, WPA-PSK, and WPA2-PSK authentication methods. Advanced Encryption Standard (AES) is the block cipher system used by the Robust Secure Network (RSN) protocol and is equivalent to the RC4 algorithm used by WPA. CCMP is the security protocol used by AES, equivalent to TKIP for WPA. Data undergoes a Message Integrity Check (MIC) using a well-known and proven technique called Cipher Block Chaining Message Authentication Code (CBC-MAC). The technique ensures that even a one-bit alteration in a message produces a dramatically different result. Master keys are not used directly but are used to derive other keys, each of which expire after a certain amount of time. Messages are encrypted using a secret 128-bit key and a 128-bit block of data. The encryption process is complex, but the administrator does not need to be aware of the intricacies of the computations. The end result is encryption that is much harder to break than even WPA.

PSK Passphrase

Default	
Options	free text (e.g., “This is the WLAN passphrase”)
Description	This field is only available for WPA-PSK and WPA2-PSK authentication methods. If the NPort’s passphrase does not match the AP’s passphrase, the connection will be denied. A PSK of sufficient strength—one that uses a mix of letters, numbers and non-alphanumeric characters—is recommended.

Security Settings for WEP Encryption



When Encryption is set to WEP on the **Security** page for the WLAN profile, you will be able to configure **WEP key length**, **WEP key index**, and **WEP key source**. Other settings will be displayed depending on how **WEP key source** is configured.

WEP Key Length

Default	64bits
Options	64bits, 128bits
Description	This field specifies the length of the WEP key. 64bits is the industry standard for WEP, but 128bits provides better protection.

WEP Key Index

Default	1
Options	1 through 4
Description	This field specifies the primary WEP key to use for the WLAN.

WEP Key Source

Default	Manual
Options	Manual, Generate WEP keys by passphrase
Description	This field specifies whether the WEP key will be generated manually or through a user-specified passphrase. A passphrase is equivalent to a free-text password that will be used to generate the WEP key. A passphrase is typically easier to remember and enter than a long and complicated WEP key.

WEP Passphrase

Default	
Options	free text (e.g., "This is the WEP passphrase")
Description	This field is only available if WEP key source is set to "Generate WEP keys by passphrase". A standard hexadecimal password will be generated using the supplied passphrase. For example, if "404tech" is entered, the WEP key will be "DB971608E942FC39BD89FC4ADB".

WEP Key Format

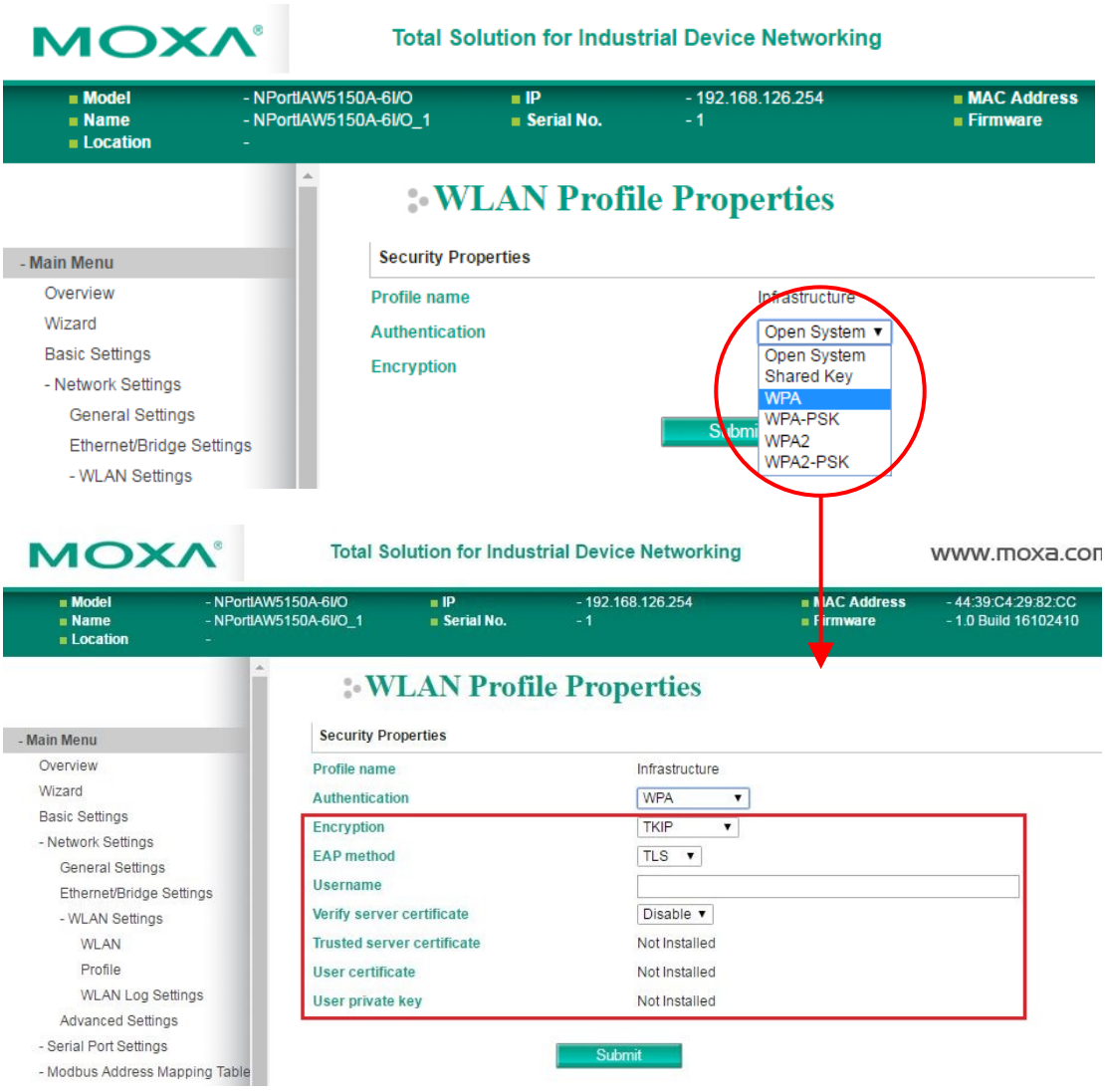
Default	ASCII
Options	ASCII, HEX
Description	This field is only available if WEP key source is set to "Manual". It specifies the format you will use to enter the WEP key.

WEP Key 1 Through 4

Default	
Options	free text in ASCII or HEX
Description	These fields are only available if WEP key source is set to "Manual". Enter each WEP key in ASCII or HEX as specified in WEP key format. The number of characters required for each key depends on WEP key length and WEP key format.

WEP Key Length	WEP Key Format	Key Length
64bits	ASCII	5 characters
	HEX	10 characters
128bits	ASCII	13 characters
	HEX	26 characters

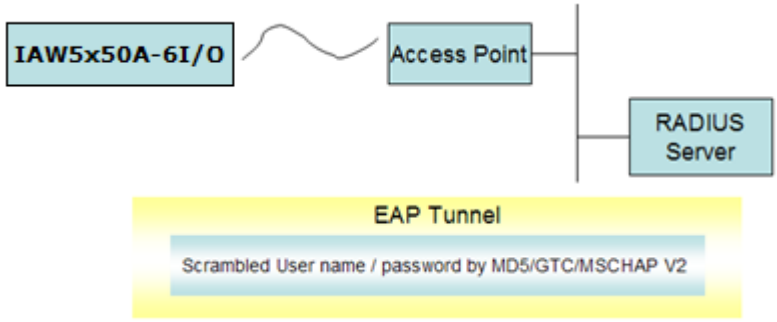
Security Settings for WPA, WPA2



When WPA or WPA2 is used for authentication, you will also need to configure **EAP method** in the **Security** settings for the WLAN profile. Other settings will also be displayed depending on how **EAP method** is configured.

There are two parts to WPA and WPA2 security, authentication and data encryption.

- Authentication occurs before access is granted to a WLAN. Wireless clients such as the NPort IAW5000A-I/O Series are first authenticated by the AP according to the authentication protocol used by the RADIUS server. Depending on the WLAN security settings, an EAP tunnel can be used to scramble the username and password that is submitted for authentication purposes.



- Encryption occurs after WLAN access has been granted. For all wireless devices, data is first encrypted before wireless transmission, using mutually agreed-upon encryption protocol.

EAP Method

Default	PEAP
Options	TLS, PEAP, TTLS, LEAP
Description	This field specifies the EAP method to use for authentication. Four methods are supported. TLS: Transport Layer Security (TLS) was created by Microsoft and accepted by the IETF as RFC 2716: PPP EAP TLS Authentication Protocol. Passwords and tunneled authentication are not used. A user certificate and user private key are used to identify the NPort. The NPort's user certificate and user private key must already be installed on the RADIUS server. PEAP: Protected Extensible Authentication Protocol (PEAP) is a proprietary protocol which was developed by Microsoft, Cisco and RSA Security. TTLS: Tunneled Transport Layer Security (TTLS) is a proprietary protocol which was developed by Funk Software and Certicom, and is supported by Agere Systems, Proxim, and Avaya. TTLS is being considered by the IETF as a new standard. For more information on TTLS, read the draft RFC EAP Tunneled TLS Authentication Protocol. LEAP: Lightweight Extensible Authentication Protocol (LEAP) is a proprietary protocol which was developed by Cisco. LEAP doesn't check certificate during the authentication process.

Tunneled Authentication

Default	PAP (when using TTLS) GTC (when using PEAP)
Options	GTC, MD5, MSCHAP V2 (when using PEAP) PAP, CHAP, MSCHAP, MSCHAP V2, EAP-MSCHAP V2, EAP-GTC, EAP-MD5 (when using TTLS)
Description	This field specifies the encryption method to use during the authentication process. Different methods are available depending on the EAP Method setting.

Username

Default	
Options	free text (e.g., "Smith_John")
Description	This field specifies the username that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

Password

Default	
Options	free text (e.g., "Password123")
Description	This field specifies the password that will be used to gain access to the WLAN. The correct username and password must be provided for access to be granted.

Anonymous Username

Default	
Options	free text (e.g., "Anyuser")
Description	This field specifies the anonymous username to use when initiating authentication. After the RADIUS Server has been verified by certificate, the true username and password will be used to complete the authentication process.

Verify Server Certificate

Default	Disable
Options	Disable, Enable
Description	Disable: The certificate from the RADIUS server will be ignored. Enable: The certificate from the RADIUS server will be used to authenticate access to the WLAN. The RADIUS server's trusted server certificate must already be installed on the NPort. To install a trusted server certificate, visit the corresponding page in the System Management> Certificate folder.

Trusted Server Certificate

This field is available for PEAP, TLS, and TTLS EAP methods only. It displays information on the trusted server certificate that is installed on the NPort. To install a trusted server certificate, visit the corresponding page in the **System Management > Certificate** folder.

User Certificate

This field is available only when EAP method has been set to TLS. It displays information on the user certificate that is installed on the NPort. To install a user certificate, visit the corresponding page in the **System Management > Certificate** folder.

User Private Key

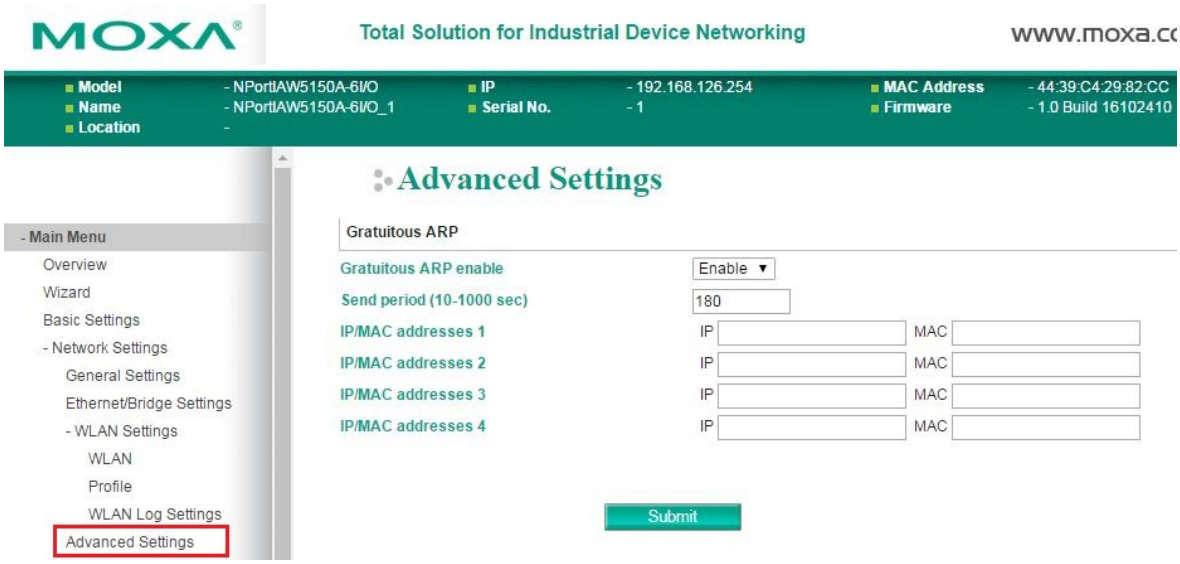
This field is available only when EAP method has been set to TLS. It displays information on the user private key on the NPort.

WLAN Log Setting

WLAN Log Settings

Default	Disable
Options	Disable, Enable
Description	When the wireless connection between the device server and the AP is not stable, you may enable this function to have more information available for troubleshooting. You may find **System Monitoring → System Status → WLAN Log** for the detail logs. Before calling Moxa for help, please enable this function first to collect some information.

Advanced Settings



On the **Advanced Settings** page in the **Network Settings** folder, you can modify **Gratuitous ARP**.

Gratuitous ARP

Default	Enabled
Options	Enable / Disable
Description	Gratuitous ARP requests provide duplicate IP address detection. The NPort sends broadcast packets to update ARP tables on other devices (e.g., AP, PC) periodically. We can use this function to notify networked devices that the NPort is still alive. Morever, the NPort can send Gratuitous ARP for legacy devices that do not have this function. If you want the NPort to send Gratuitous ARP for legacy devices, you should enter the legacy devices' IP and Mac addresses in "IP/MAC address" field.

Send Period

Default	180 seconds
Options	10-1000 seconds
Description	This field specifies how long the NPort periodically sends Gratuitous ARP.

IP/MAC Addresses (for the NPort IAW5000A-I/O Series)

Default	N/A
Options	IP address and MAC address of the legacy device (e.g., IP: "192.168.1.1", MAC: "11:22:33:44:AA:11"). This function only available when **Ethernet Bridge** is enabled.
Description	**IP address:** legacy device IP address. **MAC address:** legacy devices MAC address.

8

Web Console: Serial Port Settings

The following topics are covered in this chapter:

- **Overview**
  - Serial Port Settings
  - Communication Parameters
  - Data Buffering/Log

Overview

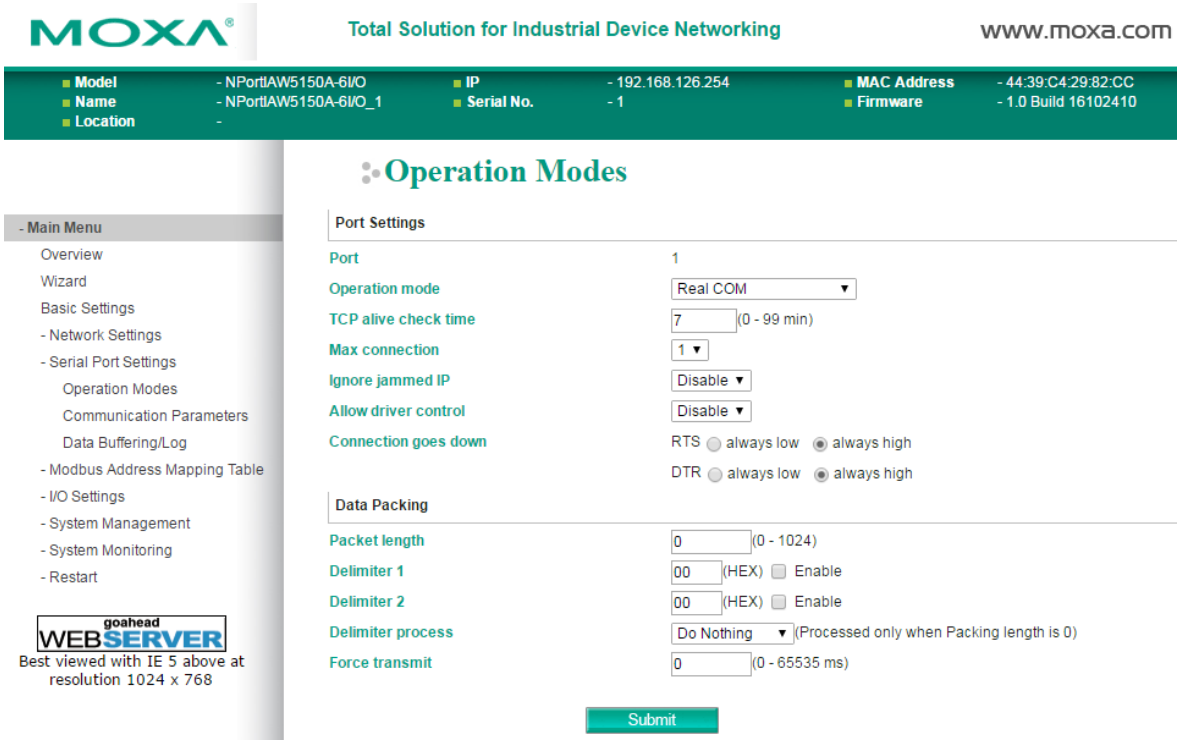
This chapter explains how to configure all settings located under the **Serial Port Settings** folder in the NPort web console.

Serial Port Settings

Operation Modes

Each serial port on the NPort is configured through the hyperlink below the column of **Operating mode**.

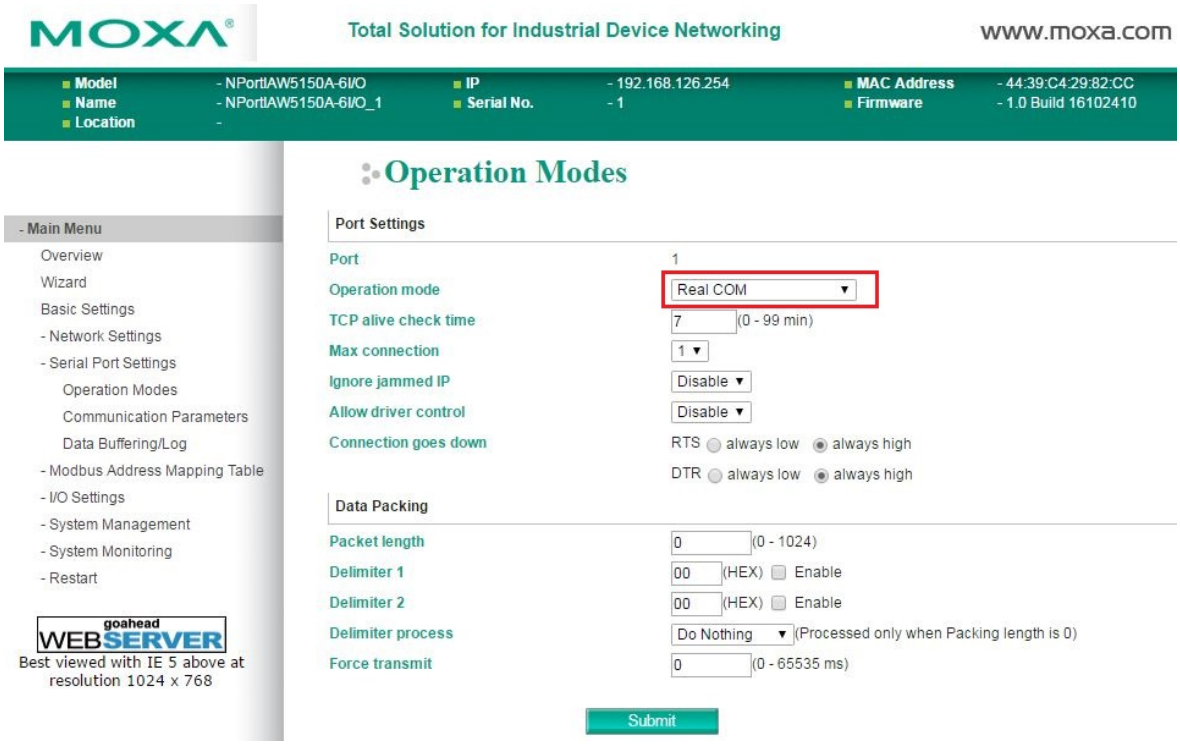
Click the link of **Real COM**, it will show the Port settings page. The Operation Modes page for each serial port is where you configure the serial port's operation mode and related settings. For an introduction to the different operation modes, please refer to Chapter 4.



Operation Mode

Default	Real COM
Options	Real COM, RFC2217, TCP Server, TCP Client, UDP, Pair Connection Master, Pair Connection Slave, Ethernet Modem, Reverse Terminal
Description	Along with Application, this field specifies the serial port's operation mode, or how it will interact with network devices. Depending on how Application is configured, different options are available for Mode. Depending on how Mode is configured, additional settings will be available for configuration. For an introduction to the different operation modes, please refer to Chapter 4. Real COM: This serial port will operate in Real COM mode. RFC2217: This serial port will operate in RFC2217 mode. TCP Server: This serial port will operate in TCP Server mode. TCP Client: This serial port will operate in TCP Client mode. UDP: This serial port will operate in UDP mode. Pair Connection Master: This serial port will operate in Pair Connection Master mode. Pair Connection Slave: This serial port will operate in Pair Connection Slave mode. Ethernet Modem: This serial port will operate in Ethernet Modem mode. Reverse Terminal: This serial port will operate in Reverse Terminal mode.

Settings for Real COM Mode



When **Operation Mode** is set to Real COM on a serial port's **Operation Modes** page, you will be able to configure additional settings including **TCP alive check time**, **Max connection**, **Ignore jammed IP, Allow driver control, connection goes down, Packet length, Delimiter 1, Delimiter 2, Delimiter process,** and **Force transmit.**

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Max connection

Default	1
Options	1 to 8
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only one specific host can access this serial port, and the RealCOM driver on that host will have full control over the port. 2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the Real COM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the NPort rather than by your application program. Application software that is based on the Rea lCOM driver will receive a driver response of "success" when using any of the Win32 API functions. The NPort will send data only to the Real COM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.

ATTENTION

When Max connection is 2 or greater, the serial port's communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the NPort. Any host that opens the COM port connection must use identical serial communication settings.

Ignore jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Allow driver control

Default	Disable
Options	Disable, Enable
Description	This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. Disable: Driver control commands will be ignored. Enable: Control commands will be accepted, with the most recent command received taking precedence.

Connection goes down

Default	always high
Options	always low, always high
Description	This field specifies what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Always low: The selected signal will change to low when the Ethernet connection goes down. Always high The selected signal will remain high when the Ethernet connection goes down.

Packet length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. 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 will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

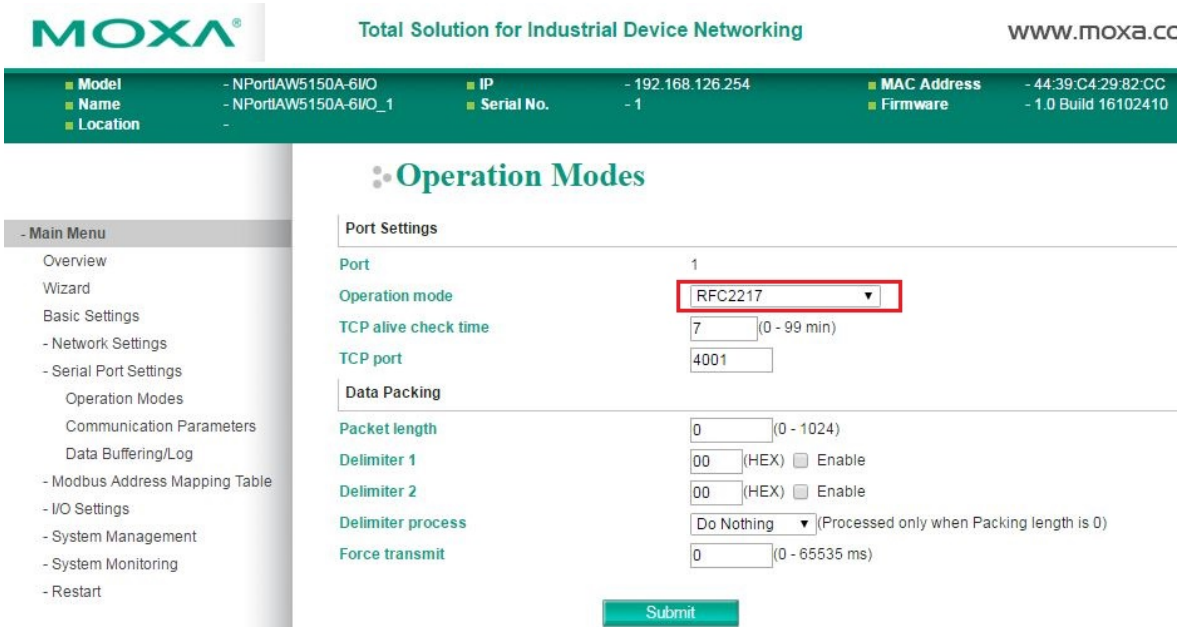
Delimiter process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on 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. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for RFC2217 Mode



When **Operation Mode** is set to **RFC2217** on a serial port's **Operation Modes** page, you will be able to configure additional settings, including **TCP alive check time**, **TCP port**, **Packet length, Delimiter 1, Delimiter 2, Delimiter process,** and **Force transmit.**

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

TCP Port

Default	4001
Options	
Description	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

Packet length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. 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 will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

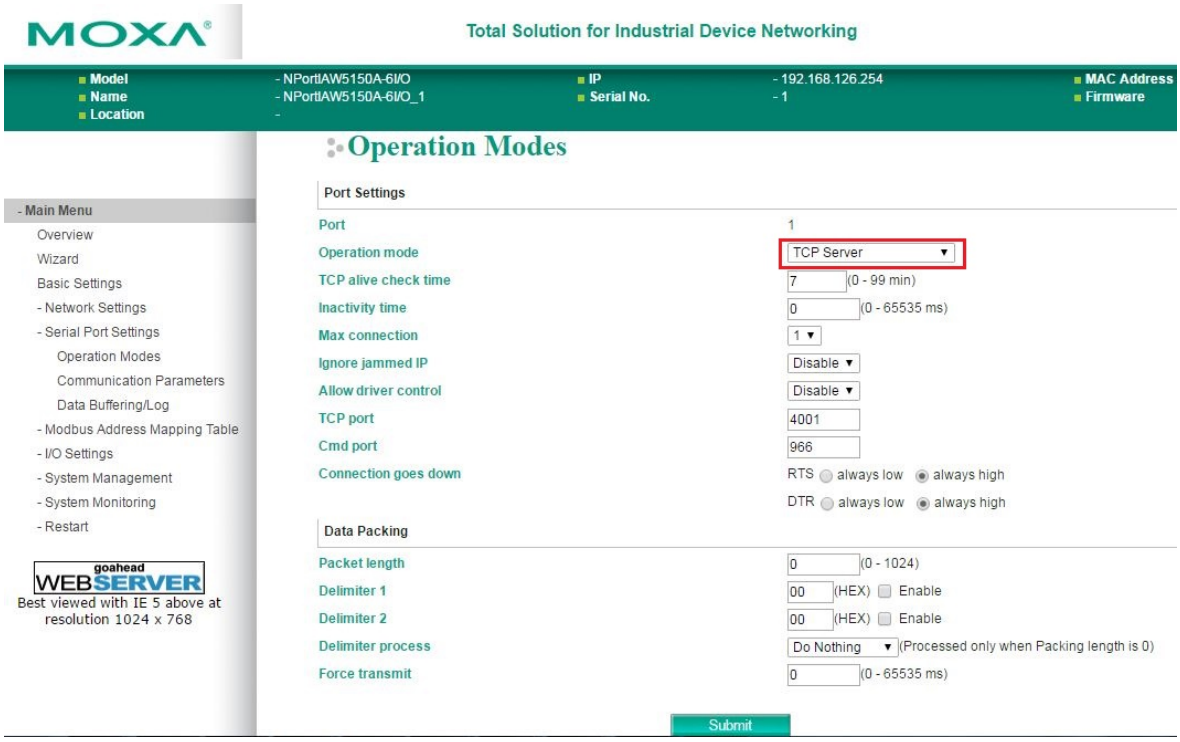
Delimiter process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on 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. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Server Mode



When **Operation Mode** is set to **TCP Server** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, **Max connection, Ignore jammed IP, Allow driver control, TCP port, Cmd port, Connection goes down, Packet length, Delimiter 1, Delimiter 2, Delimiter process,** and **Force transmit.**

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Inactivity time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, 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

Default	1
Options	1 to 8
Description	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only one specific host can access this serial port, and the RealCOM driver on that host will have full control over the port. 2 to 8: This serial port will allow the specified number of connections to be opened simultaneously. With simultaneous connections, the RealCOM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the NPort rather than by your application program. Application software that is based on the RealCOM driver will receive a driver response of "success" when using any of the Win32 API functions. The NPort will send data only to the RealCOM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in-first-out basis.

ATTENTION

When Max connection is 2 or greater, the serial port's communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the NPort. Any host that opens the COM port connection must use identical serial communication settings.

Ignore jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Allow driver control

Default	Disable
Options	Disable, Enable
Description	This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port. Disable: Driver control commands will be ignored. Enable: Control commands will be accepted, with the most recent command received taking precedence.

TCP port

Default	4001
Options	0 to 9999
Description	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.

Cmd port

Default	966
Options	
Description	This field specifies the TCP port number for listening to SSDK commands from the host.

Connection goes down

Default	always high
Options	always low, always high
Description	This field specifies what happens to the RTS and DTR signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS or DTR signals sent through the serial port. Always low: The selected signal will change to low when the Ethernet connection goes down. Always high The selected signal will remain high when the Ethernet connection goes down.

Packet length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. 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 will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

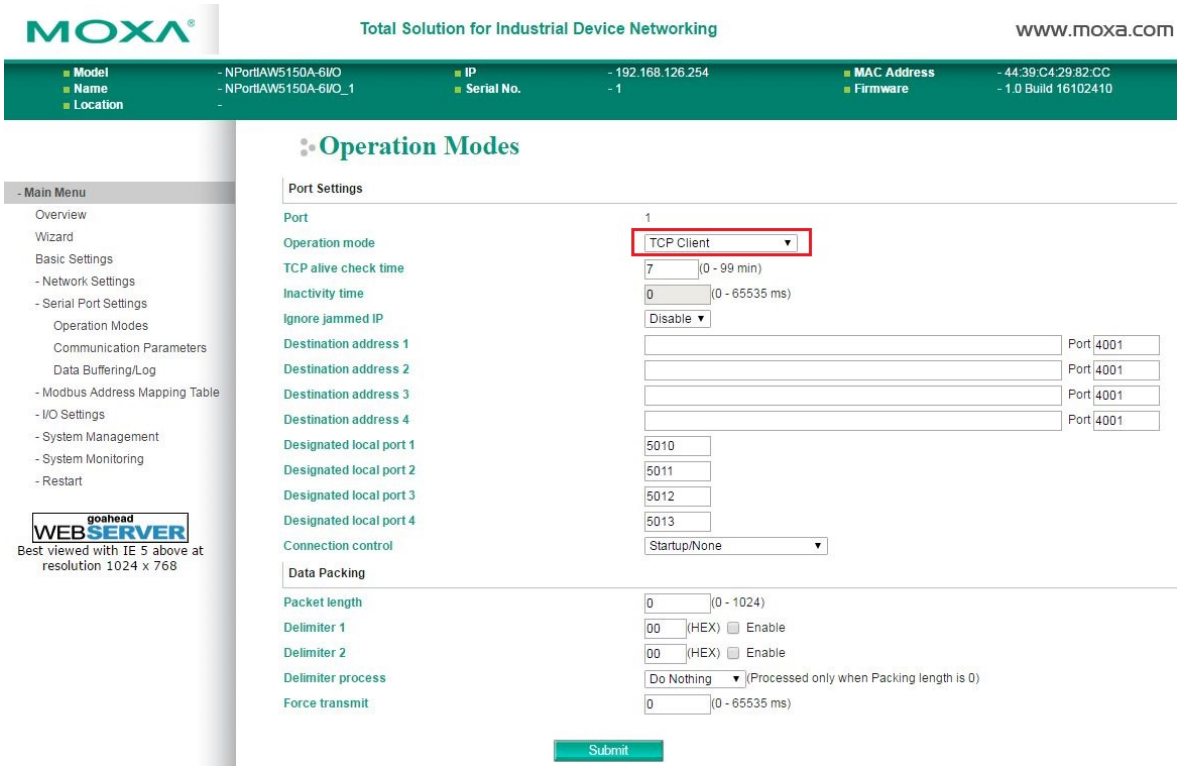
Delimiter process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that 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. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on 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. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for TCP Client Mode



When **Operation Mode** is set to **TCP Client** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, **Ignore jammed IP , Destination address 1-4, Designated local port 1-4, Connection control, and Packet length, Delimiter 1, Delimiter 2, Delimiter process,** and **Force transmit.**

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Inactivity time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, 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.

Ignore jammed IP

Default	Disable
Options	Disable, Enable
Description	This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port. Disable: All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded. Enable: Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.

Destination address 1 to 4

Default	4001
Options	IP address and port (e.g., "192.168.1.1" and "4001")
Description	This field specifies the remote host(s) that will access the attached device. At least one destination must be provided. This field supports the use of domain names and names defined in the host table.

ATTENTION

In TCP Client mode, up to 4 connections can be established between the serial port and TCP hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

Designated local port 1 to 4

Default	5010 to 5013
Options	1 to 65535
Description	This field specifies the TCP port number that will be used for data transmission with the serial port.

Connection control

Default	Startup/None
Options	Startup/None, Any Character/None, Any Character/Inactivity Time, DSR On/DSR Off, DSR On/None, DCD On/DCD Off, DCD On/None
Description	This field specifies how connections to the device are established and closed. Startup/None: The connection will be opened as the NPort starts up. The connection will only be closed manually. Any Character/None: The connection will be opened as soon as a character is received from the attached device. The connection will only be closed manually. Any Character/Inactivity Time: The connection will be opened as soon as a character is received from the attached device. The connection will be closed if no data is received for the time specified in Inactivity time. DSR On/DSR Off: The TCP connection is opened when the DSR signal is on, and closed when the DSR signal is off. DSR On/None: The TCP connection is opened when the DSR signal is on. The connection will only be closed manually. DCD On/DCD Off: The TCP connection is opened when the DCD signal is on, and closed when the DCD signal is off. DCD On/None: The TCP connection is opened when the DCD signal is on. The connection will only be closed manually.

Packet length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. 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 will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

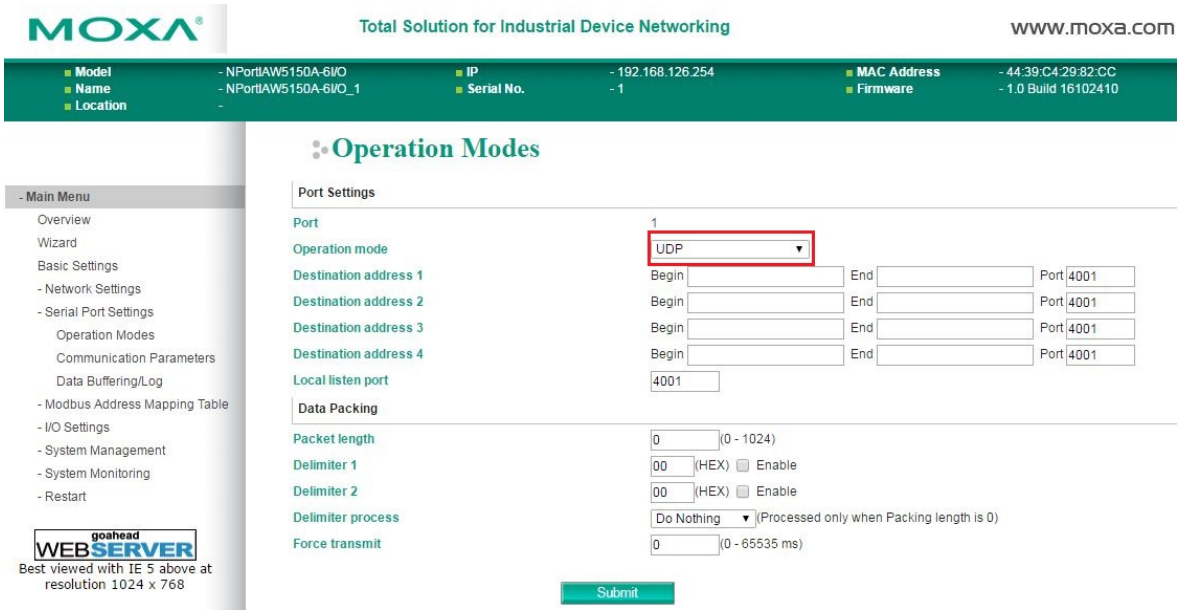
Delimiter process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that 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. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on 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. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for UDP Mode



When **Operation Mode** is set to **UDP** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **Destination address 1** through **4**, **Local listen port**, **Packet length, Delimiter 1, Delimiter 2, Delimiter process,** and **Force transmit.**

Destination address 1 to 4

Default	
Options	IP address range and port (e.g., "192.168.1.1" to "192.168.1.64" and "4001")
Description	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided. The maximum selectable IP address range is 64 addresses. However, you can enter multicast addresses in the Begin field, in the form xxx.xxx.xxx.255. For example, enter "192.127.168.255" to allow the NPort to broadcast UDP packets to all hosts with IP addresses between 192.127.168.1 and 192.127.168.254.

Local listen port

Default	4001
Options	
Description	This field specifies the UDP port that the NPort listens to and that other devices must use to contact the attached serial device.

Packet length

Default	0
Options	0 to 1024
Description	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.

Delimiter 1 and 2

Default	Disabled
Options	Disabled, Enabled, 00 to FF
Description	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. 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 will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

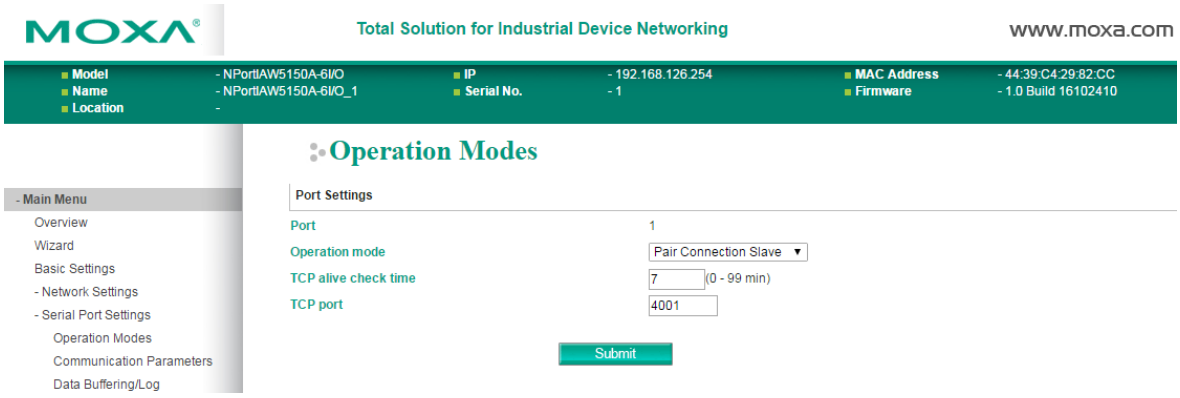
Delimiter process

Default	Do Nothing
Options	Do Nothing, Delimiter + 1, Delimiter + 2, Strip Delimiter
Description	This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled. Do nothing: Data accumulated in the serial port's buffer will be packed, including delimiters. Delimiter + 1: One additional character must be received before the data in the serial port's buffer is packed. Delimiter + 2: Two additional characters must be received before the data in the serial port's buffer is packed. Strip Delimiter: Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.

Force transmit

Default	0 ms
Options	0 to 65535
Description	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that 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. 0: If serial data is not received, the NPort will wait indefinitely for additional data. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on 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. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.

Settings for Pair Connection Master Mode and Pair Connection Slave Mode



When **Operation Mode** is set to **Pair Connection Master** or **Pair Connection Slave** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Destination address** and **TCP port.** A Pair Connection application involves one serial port communicating over an IP network to another serial port as if the two serial ports were connected by a serial cable. Pair Connection modes can be used to extend RS-232 transmission to unlimited distances.

An NPort device server is needed at both ends of the connection. The serial port at one end must be set to Pair Connection Master mode, and the serial port at the other end must be set to Pair Connection Slave mode. It does not matter which serial port is master and which serial port is slave.

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

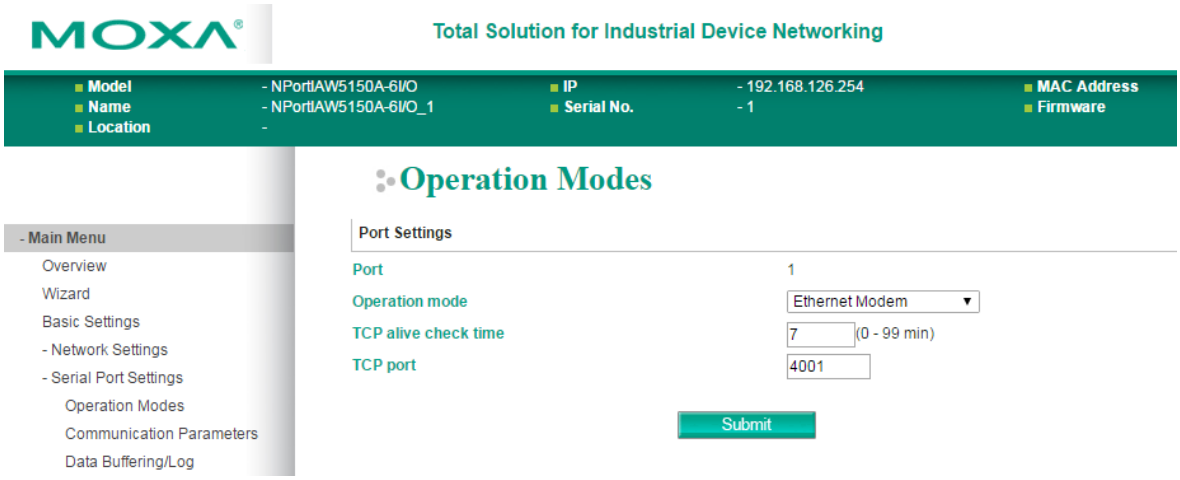
Destination address

Default	
Options	IP address and port (e.g., "192.168.1.1" and "4001")
Description	This field specifies the IP address for the NPort at the opposite end of the Pair Connection, and the TCP port number for communication with the serial port. The port number must match with that serial port's TCP port setting.

TCP port

Default	4001
Options	
Description	This field specifies the TCP port to use for communication with the attached serial device. The serial port at the opposite end of the Pair Connection must use this port number to establish the connection.

Settings for Ethernet Modem Mode



When **Application** is set to **Ethernet Modem Mode**, the NPort will accept AT commands such as "ATD 192.127.168.1:4001" from the serial port. A TCP connection will then be requested from the specified remote Ethernet Modem or PC. When the remote unit accepts this TCP connection, the NPort will return the "**CONNECT** {*baudrate*}" signal to the serial port and will then enter data mode. Please refer to Appendix C for details on Ethernet modem commands.

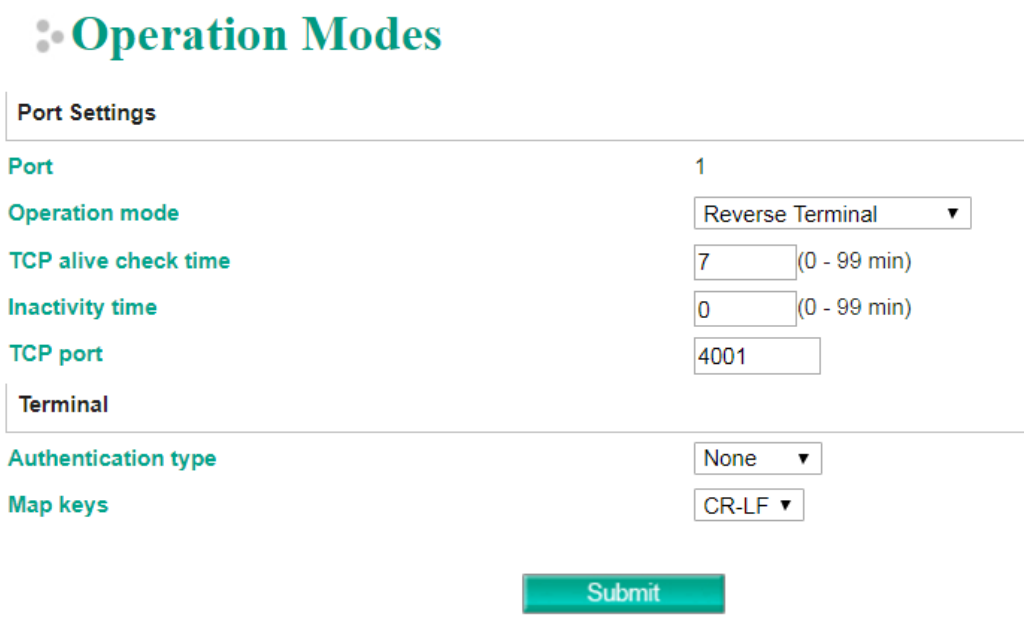
TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

TCP port

Default	4001
Options	
Description	This field specifies the TCP port to use for communication with the attached serial device.

Settings for Reverse Terminal Mode



When Operation mode is set to Reverse Terminal Mode, you will be able to configure additional settings such as TCP alive check time, Inactivity time, and TCP port.

TCP alive check time

Default	7 min
Options	0 to 99 min
Description	This field specifies how long the NPort will wait for a response to "keep alive" packets before closing the TCP connection. The NPort checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the NPort will force the existing TCP connection to close.

Inactivity time

Default	0 ms
Options	0 to 65535 ms
Description	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, 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.

TCP port

Default	4001
Options	
Description	This field specifies the TCP port to use for communication with the attached serial device.

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 User Table.
RADIUS	Verify the ID against the external RADIUS server.
None	Authentication is not required.

Map keys <CR-LF> (default=CR-LF)

This specifies how the ENTER key is mapped from the Ethernet port through the serial port.

Option	Description
<CR-LF>	carriage return + line feed (i.e., the cursor will jump to the next line, and return to the first character of the line)
<CR>	carriage return (i.e., the cursor will return to the first character of the line)
<LF>	line feed (i.e., the cursor will jump to the next line, but not move horizontally)

Communication Parameters

The **Communication Parameters** page for each serial port is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.

Alias

Default	
Options	free text (e.g., "Secondary console connection")
Description	This is an optional free text field to help you differentiate one serial port from another. It does not affect operation of the NPort device server.

ATTENTION

Serial communication settings should match the attached serial device. Check the communication settings in the user's manual for your serial device.

Baud rate

Default	115200
Options	50, 75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600, Other
Description	This field specifies the baudrate for the serial port. Nonstandard baudrates are supported through the "Other" setting. When set to "Other", you may manually enter a baudrate of your choice, up to 921600. 50 to 921600: The serial port will operate at the specified baudrate Other: The serial port will operate at a baudrate that is manually entered by the user.

Parity

Default	None
Options	None, Odd, Even, Space, Mark
Description	This field specifies the type of parity bit used for each character frame.

Data bit

Default	8
Options	5, 6, 7, 8
Description	This field specifies the number of data bits used to encode each character of data.

Stop bit

Default	1
Options	1, 1.5, 2
Description	This field specifies the number of stop bits used for each character frame.

Flow control

Default	RTS/CTS
Options	None, RTS/CTS, XON/XOFF, DTR/DSR
Description	This field specifies the type of flow control used by the serial port.

FIFO

Default	Enable
Options	Enable, Disable
Description	This field specifies whether the serial port will use the built-in FIFO. A 128-byte FIFO is provided to each serial port for both Tx and Rx directions. To prevent data loss during serial communication, this should be set to Disabled if the attached serial device does not have a FIFO.

Interface

Default	RS-232
Options	RS-232, RS-422, RS-485 2-wire, RS-485 4-wire
Description	This field specifies the type of interface the serial port will use.

Data Buffering/Log

On the serial port's **Data Buffering/Log** page, you can enable or disable **Port buffering** and **Serial data logging**.

Port buffering

Default	Disable
Options	Enable, Disable
Description	This field specifies whether the serial port will use port buffering when the network connection (Ethernet or WLAN) is down. Port buffering can be used in RealCOM mode, TCP Server mode, TCP Client mode, and Pair Connection mode. For other modes, the port buffering settings will have no effect.

Serial data logging(64K)

Default	Disable
Options	Enable, Disable
Description	This field specifies whether data logs for the serial port will be stored on system RAM. Each serial port is allotted 64 KB for data logging. The data log is not saved when the NPort is powered off.

9

Web Console: Modbus Address Mapping & I/O Setting

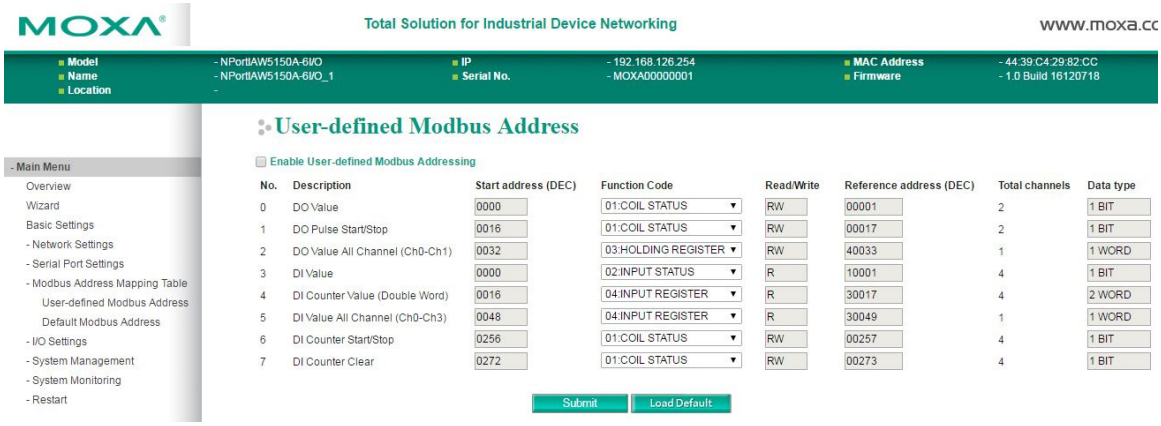
The following topics are covered in this chapter:

- **Modbus Address Mapping Table**
  - User-Defined Modbus Addressing
  - Default Modbus Address
- **I/O Settings**
  - DI Channels
  - DO Channels

Modbus Address Mapping Table

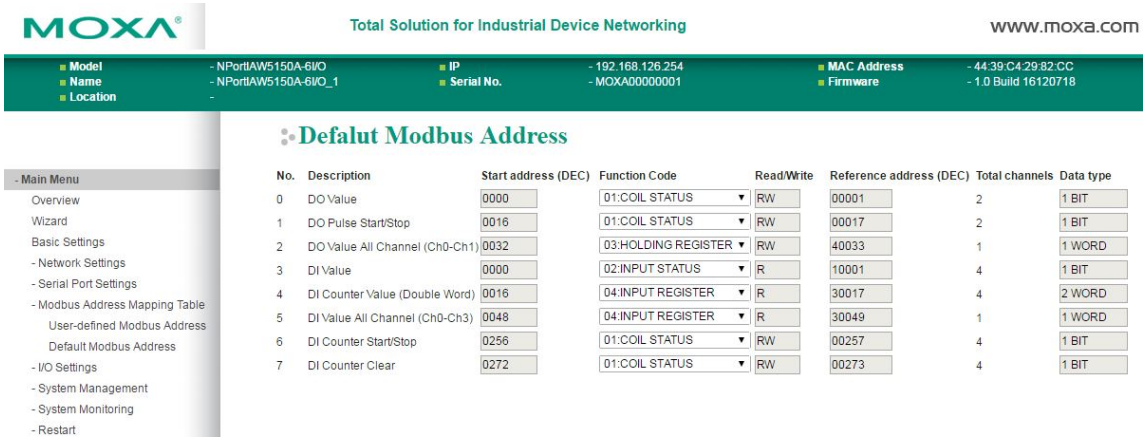
User-Defined Modbus Addressing

The NPort IA5000A-I/O and NPort IAW5000A-I/O Series play a role as the Modbus TCP slave and input and output addresses can be configured on this page. Select the **Enable User-defined Modbus Addressing** checkbox, and then configure the start address of each Modbus function. If you do not want to use the Modbus function, deselect the **Enable User-defined Modbus Addressing** checkbox**.**



Default Modbus Address

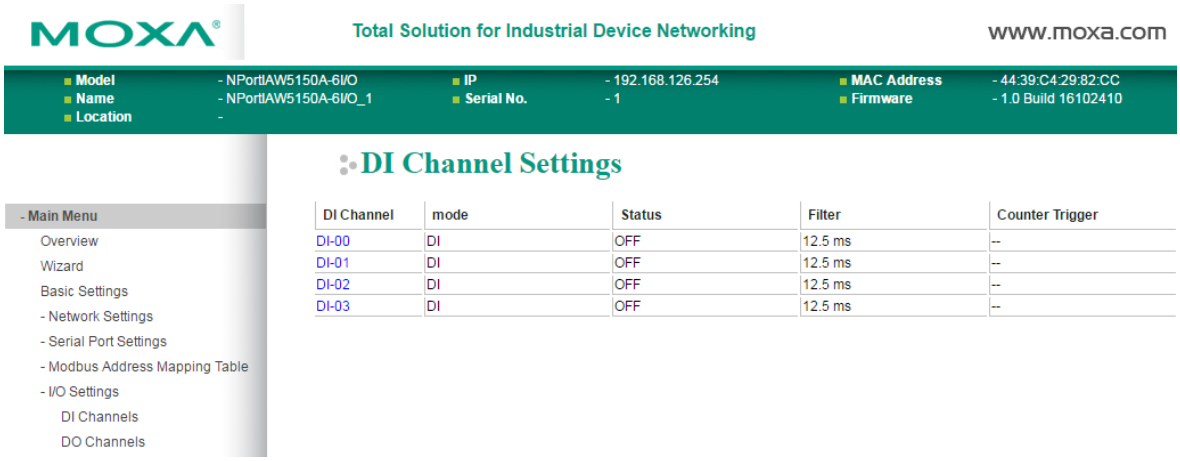
You can view the default Modbus address for all I/O devices on the **Default Modbus Address settings** page. However, only the starting address will be displayed for each item with multiple reference addresses. For example, if the reference addresses for DI Value start from 10001 and the second DI channel's reference address is 10002, only the first DI channel's Modbus address of 10001 will be displayed. See the diagram below.



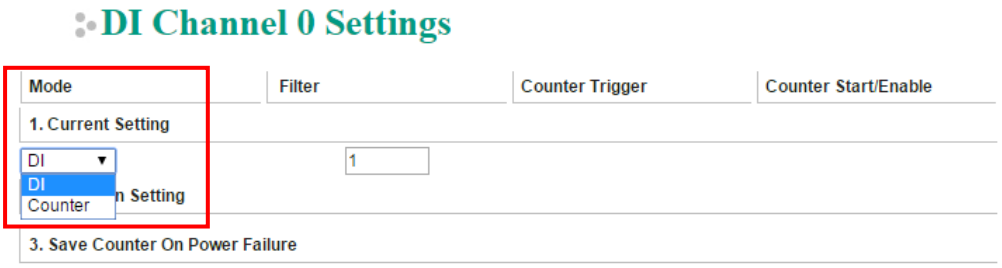
I/O Settings

DI Channels

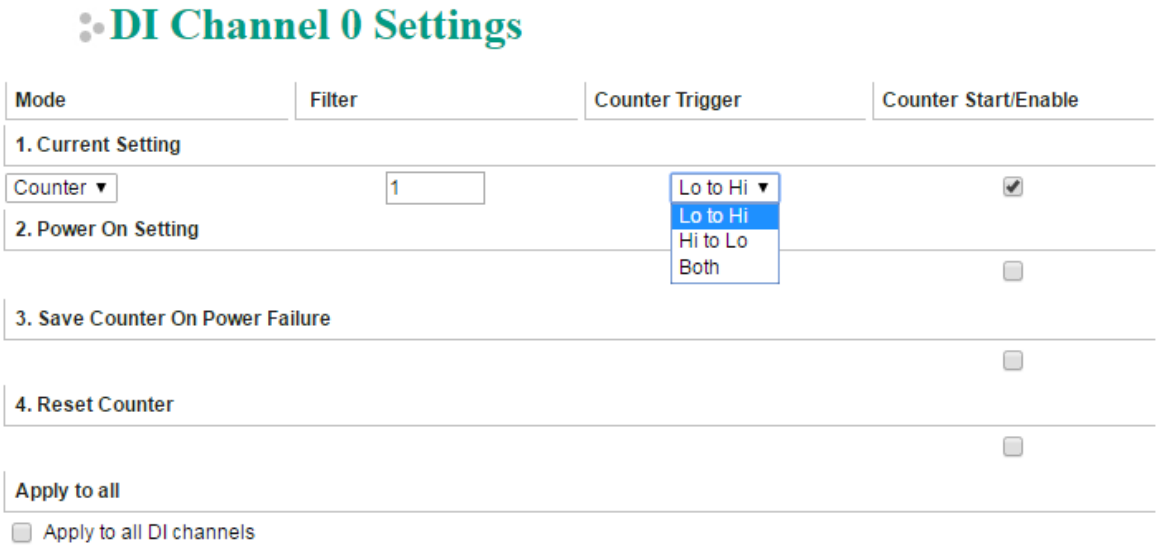
The status of each DI (digital input) channel appears on the **DI Channel Settings** page.



You can also configure each channel's digital input mode and parameters by clicking on the channel. DI channels can operate in **DI** mode or **Event Counter** mode.



Activate **Event Counter** mode by selecting the **Counter Start** field and configure the **Counter Trigger** by selecting **Lo to Hi**, **Hi to Lo**, or **Both** from the drop-down menu. If the **Counter Start** field is not selected, you can still activate the counter by using Modbus commands.



NOTE Confirm that the Counter Filter is not set to 0; otherwise, the counter will never be activated.

Power On Setting: You may configure DI channels in **Event Counter** mode whether or not counting begins when powering up.

Save Counter On Power Failure: The NPort IA5000A-I/O and IAW5000A-I/O will automatically save the counter value when there is a power failure if this function is selected.

Reset Counter: Select this function to reset the counter.

You can apply the DI settings to all DI Channels by selecting the **Apply to all DI Channels** checkbox.

The DI channel's Alias Name and logic definition can also be configured on this page.

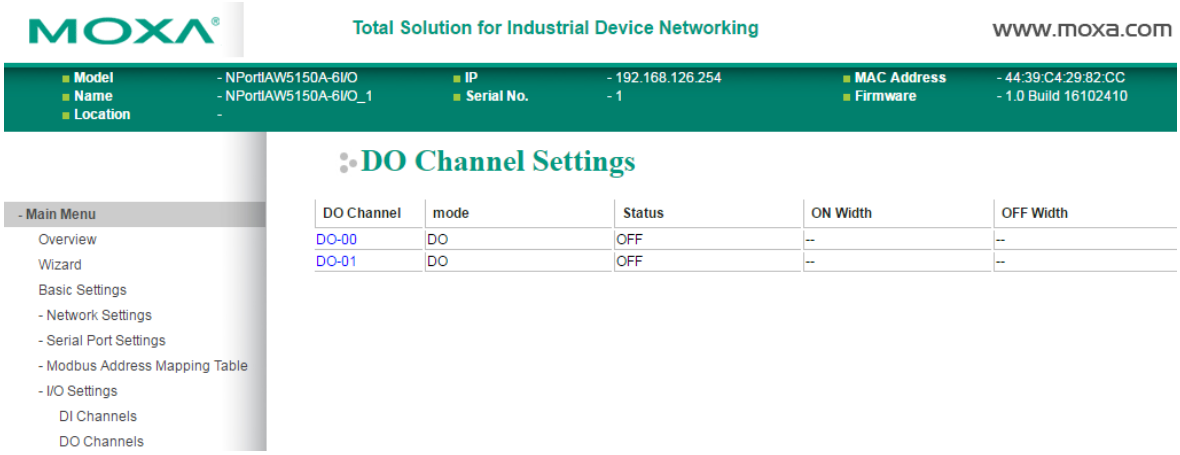
DI Channel Specifications

Note1:	Filter unit=12.5ms, range=1~65535.
Note2:	
Sensor Type	-> Wet Contact and Dry Contact.
Dry Contact	-> OFF : Open.
	-> ON : Short to GND.
Wet Contact (Sink/NPN)	-> OFF : 10 - 30VDC.
	-> ON : 0 - 3 VDC.
Wet Contact (Source/PNP)	-> OFF : 0 - 3 VDC.
	-> ON : 10 - 30VDC.

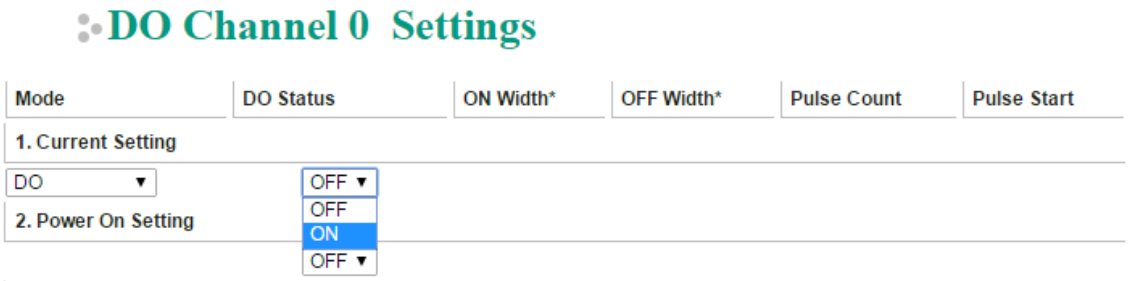
WARNING: Be sure to Save/Restart your settings.

DO Channels

On the **I/O Setting: DO (Digital Output) Channels** page; you can configure each DO channel by clicking on the channel.



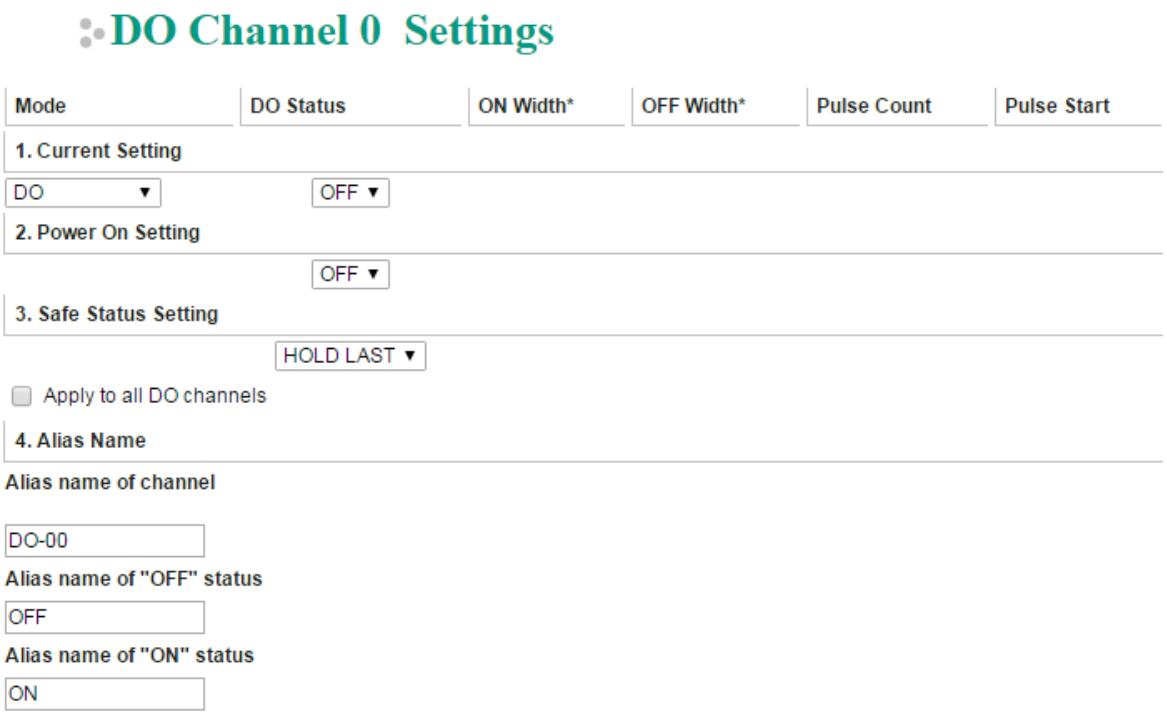
DO channels can operate in DO mode when the status is either ON or OFF.



If you select **Pulse Output** mode, you can specify the **ON Width** and **OFF Width** to generate a square wave.

Pulse width unit = 25ms, range = 1-65535.

When configuring individual channels, if **Power On Setting** is selected, the pulse output will start as soon as the NPort is powered on. If the **Safe Status Setting** is selected, the pulse output will start only when the NPort has entered **Safe Status** mode. In contrast, when neither of these settings is selected and the **Pulse Start** field is selected, the NPort will automatically stop the pulse output when the NPort is either powered on or in **Safe Status** mode.



NOTE Safe Status is controlled by the Communication Watchdog under Basic Settings, which is disabled by default. If the Communication Watchdog is disabled, the NPort will never enter Safe Mode and your Safe Status settings will have no effect.

The DO channel's Alias Name and logic definition can also be configured on this page. You can apply the DO settings to all channels by clicking on the **Apply to all DO channels** checkbox.

10

Web Console: System Management

The following topics are covered in this chapter:

- **Overview**
- **System Management**
  - Misc. Network Settings
  - Auto Warning Settings
  - Maintenance
  - Certificate

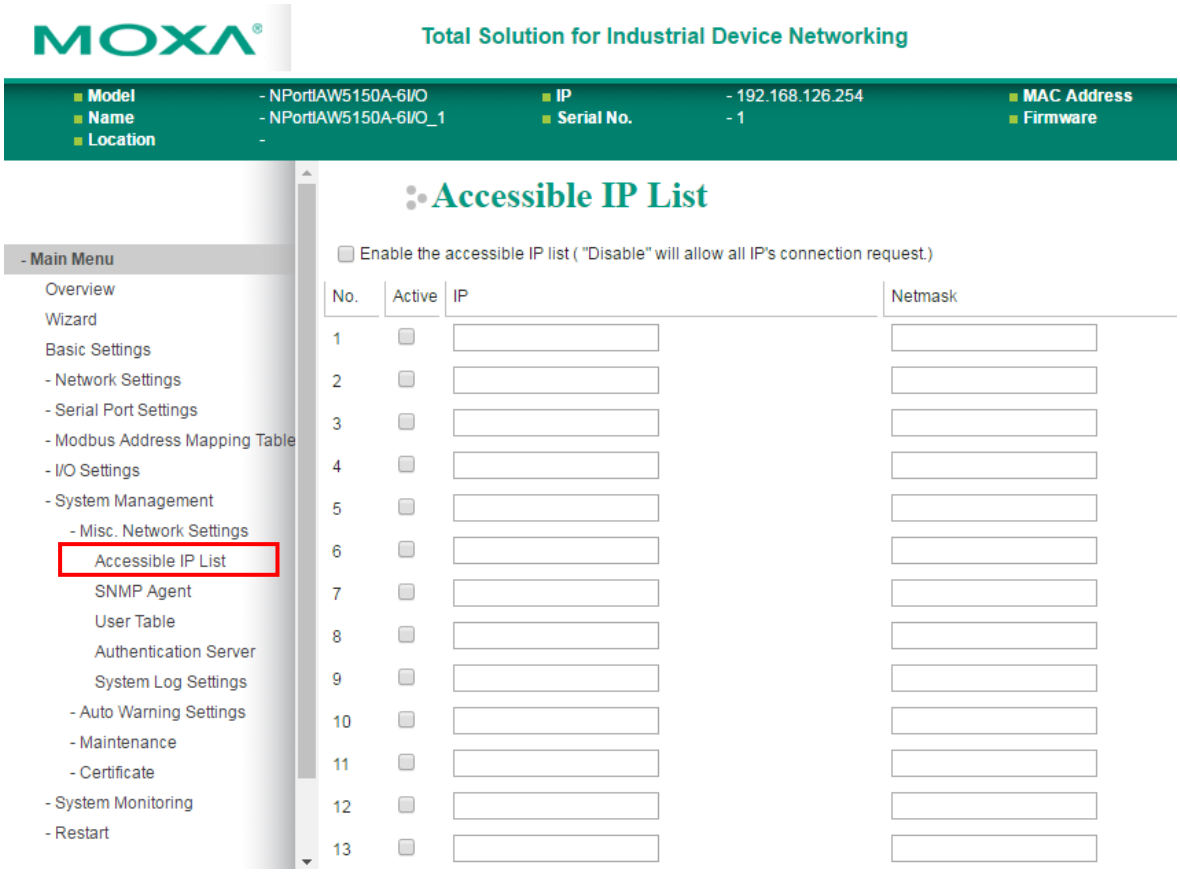
Overview

This chapter explains how to configure all settings located under the **System Management** folder in the NPort web console.

System Management

Misc. Network Settings

Accessible IP List



The **Accessible IP List** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used this restrict access to the NPort by IP address. Only IP addresses on the list will be allowed access to the NPort. You may add a specific address or range of addresses by using a combination of IP address and netmask, as follows:

To allow access to a specific IP address
Enter the IP address in the corresponding field; enter 255.255.255.255 for the netmask.

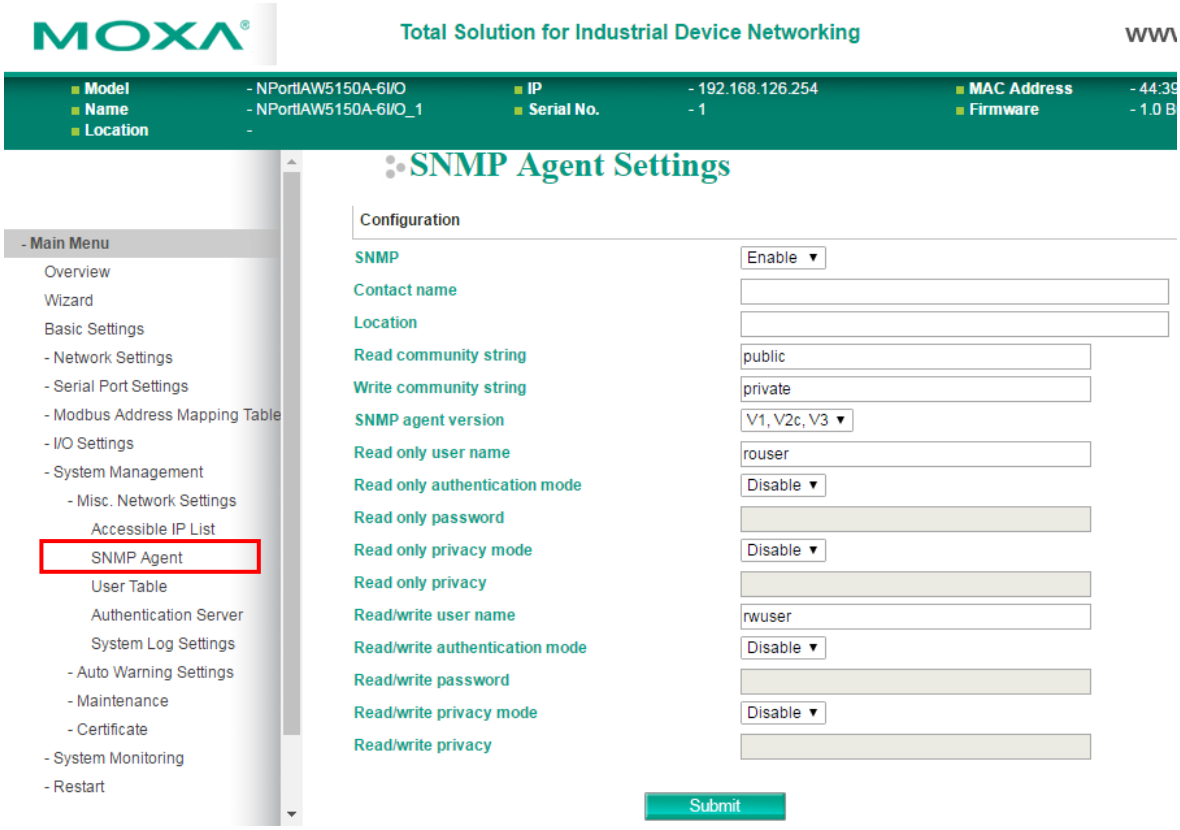
To allow access to hosts on a specific subnet
For both the IP address and netmask, use 0 for the last digit (e.g., "192.168.1.0" and "255.255.255.0").

To allow access to all IP addresses
Make sure that **Enable the accessible IP list** is not checked.

Refer to the following table for more configuration examples.

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	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

SNMP Agent Settings



The **SNMP Agent** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used to configure the SNMP Agent on the NPort.

SNMP

Default	Enable
Options	Enable, Disable
Description	This field enables or disables the SNMP Agent. If enabled, you will need to configure other SNMP Agent settings. You will need to enter a community name under Read community string.

Contact Name

Default	
Options	free text (e.g., "J Smith")
Description	This is an optional free text field that can be used to specify the SNMP emergency contact name, telephone, or pager number.

Location

Default	
Options	free text (e.g., "Building XYZ")
Description	This is an optional free text field that can be used to specify the location for SNMP agents such as the NPort.

Read Community String

Default	public
Options	free text (e.g., "public community")
Description	This field specifies the read community string used for the SNMP Agent. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.

Write Community String

Default	private
Options	free text (e.g., "private community")
Description	This field specifies the write community string used for the SNMP Agent. This is a text password mechanism that is used to weakly authenticate changes to agents of managed network devices.

SNMP Agent Version

Default	V1, V2c, V3
Options	V1, V2c, V3 / V1, V2c / V3 only
Description	This field specifies which version(s) of SNMP to support.

Read Only User Name

Default	rouser
Options	free text (e.g., "guest")
Description	This field specifies a user name to use for read only access.

Read Only Authentication Mode

Default	Disable
Options	Disable, MD5, SHA
Description	This field specifies the type of authentication to use for read-only access.

Read Only Password

Default	
Options	free text (e.g., "password123")
Description	This field specifies the password that users must enter for read-only access, if read only authentication is enabled.

Read Only Privacy mode

Default	Disable
Options	Disable, DES_CBC
Description	This field specifies whether DES_CBC data encryption will be used during read-only access.

Read Only Privacy

Default	
Options	free text (e.g., "read only key")
Description	This field specifies the encryption key for read-only access, if read-only privacy is enabled.

Read/Write User Name

Default	rwuser
Options	free text (e.g., "admin")
Description	This field specifies a user name to use for read/write access.

Read/Write Authentication Mode

Default	Disable
Options	Disable, MD5, SHA
Description	This field specifies the type of authentication to use for read/write access.

Read/Write Password

Default	
Options	free text (e.g., "password123")
Description	This field specifies the password that users must enter for read/write access, if read only authentication is enabled.

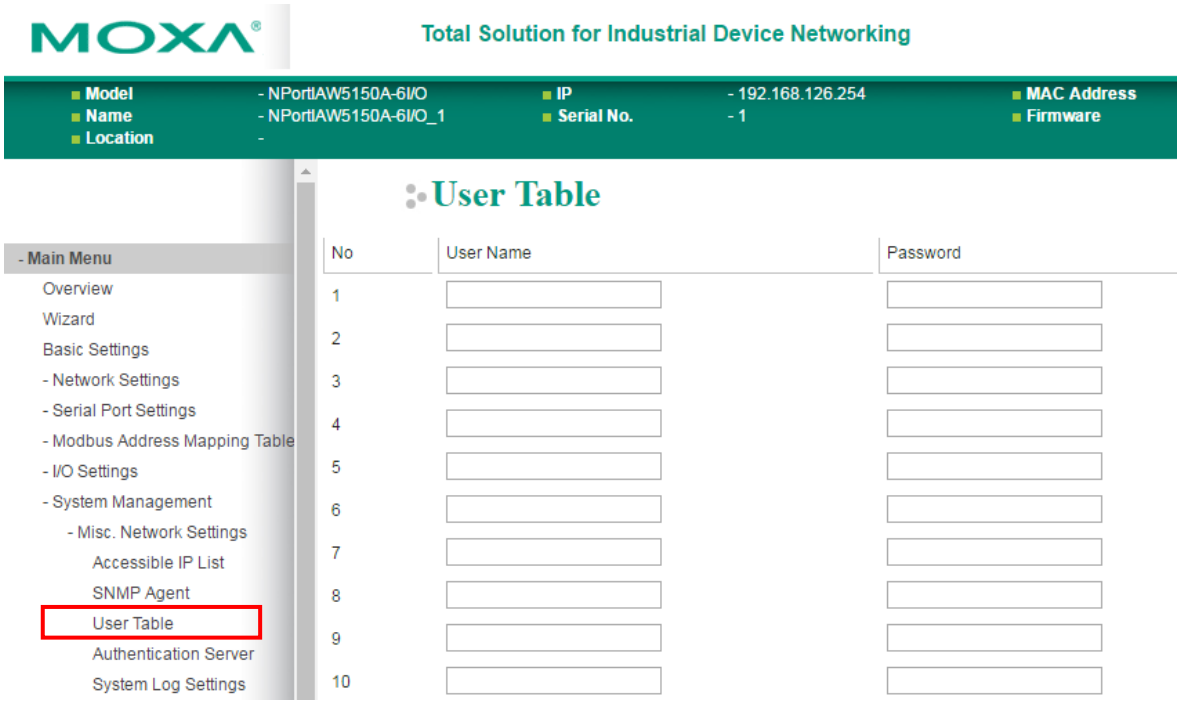
Read/Write Privacy mode

Default	Disable
Options	Disable, DES_CBC
Description	This field specifies whether DES_CBC data encryption will be used during read/write access.

Read/Write Privacy

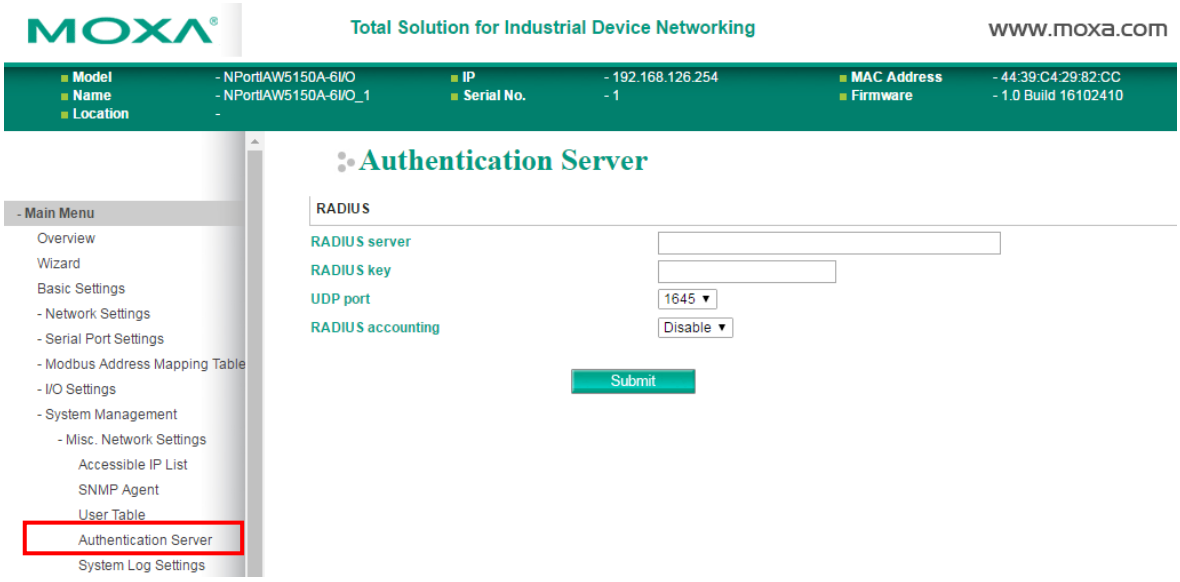
Default	
Options	free text (e.g., "read write key")
Description	This field specifies the encryption key for read/write access, if read-/write privacy is enabled.

User Table



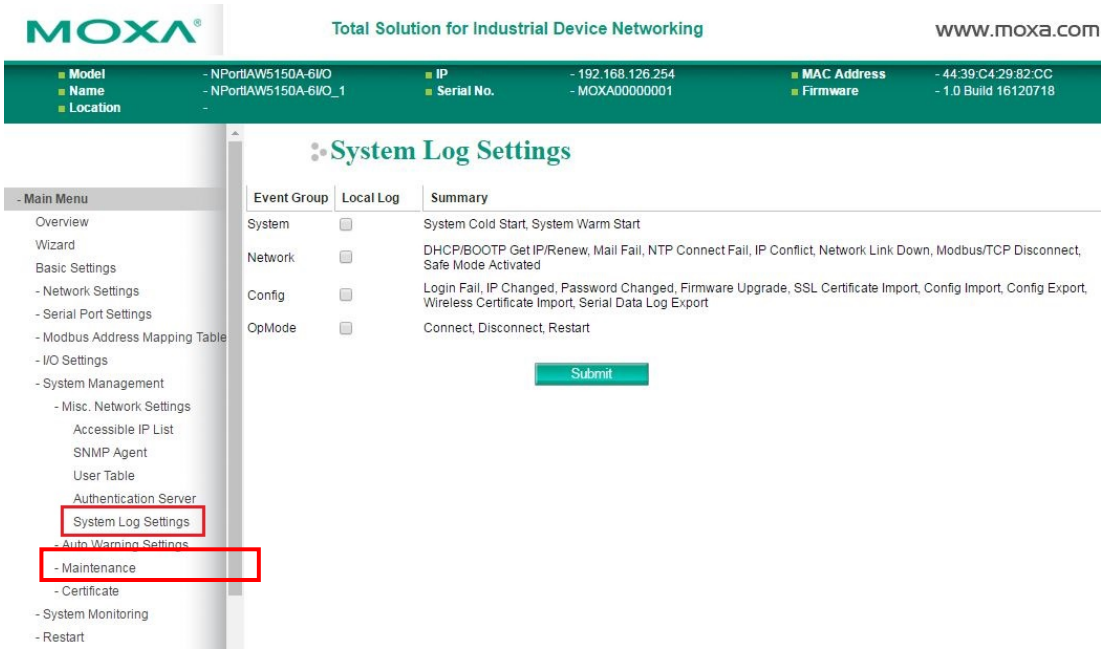
The NPort User Table can be used to authenticate users for reverse terminal access and is useful if you do not have an external RADIUS server for authentication. The NPort User Table stores up to 64 entries, with fields for User Name and Password.

Authentication Server



RADIUS server: If you are using a RADIUS server for user authentication, enter its IP address here.
RADIUS key: If you are using a RADIUS server for user authentication, enter its password here.
UDP port (default=1645): If you are using a RADIUS server, enter its UDP port assignment here.
RADIUS accounting: Use this field to enable or disable RADIUS accounting.

System Log Settings



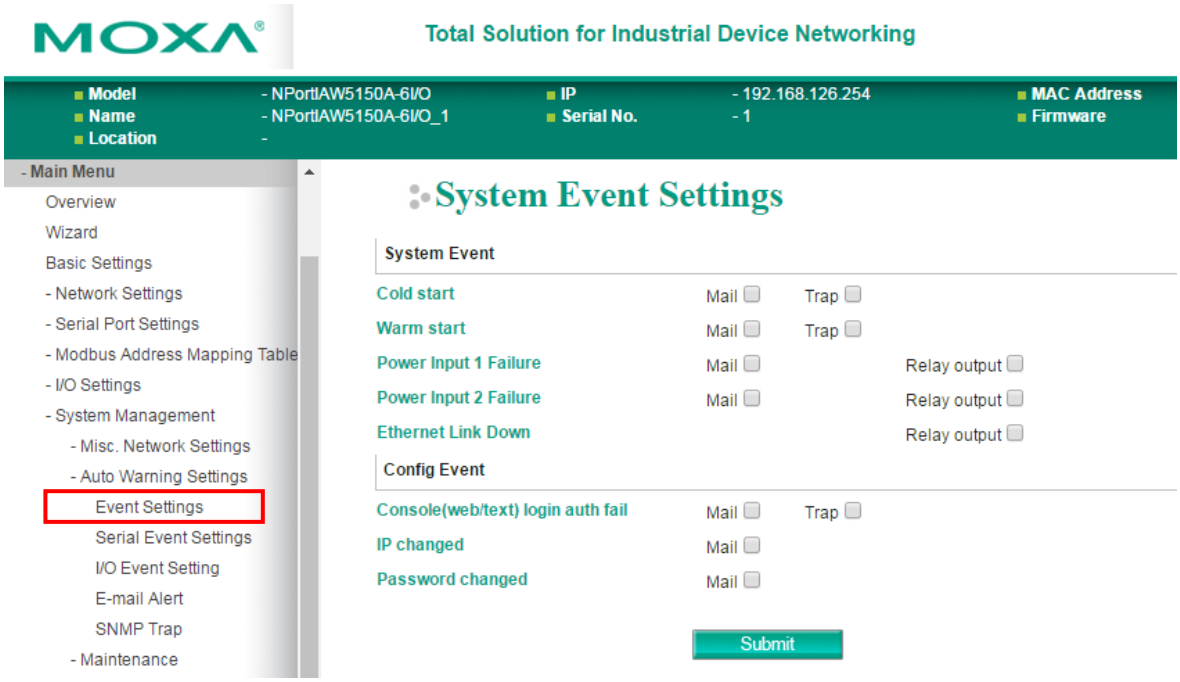
The **System Log** page is located under **Misc. Network Settings** in the **System Management** folder.

This is where you select the type of events that will be logged by the NPort.

Group	Event
System	System Cold Start, System Warm Start
Network	DHCP/BOOTP Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down, Modbus/TCP Disconnect, Safe Mode Activated
Config	Login Fail, IP Changed, Password Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export, Wireless Certificate Import, Serial Data Log Export
Op Mode	Connect, Disconnect, Restart

Auto Warning Settings

Event Settings



The **Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the NPort will notify you of system and configuration events. Depending on the event, different options for notification are available, as shown above. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

Event	Description
Cold start	The NPort was powered on, or was restarted after a firmware upgrade.
Warm start	The NPort restarted without powering off.
Power Input 1 Failure	The NPort was not receiving power from PWR1. (The NPort device server has two DC power inputs for redundancy.)
Power Input 2 Failure	The NPort was not receiving power from PWR2. (The NPort device server has two DC power inputs for redundancy.)
Ethernet Link Down	The Ethernet connection has failed.
Console login auth fail	An attempt has been made to open the web, Telnet, or serial console, but the password was incorrect.
IP changed	The IP address has been changed.
Password changed	The password to the console has been changed.

Serial Event Settings

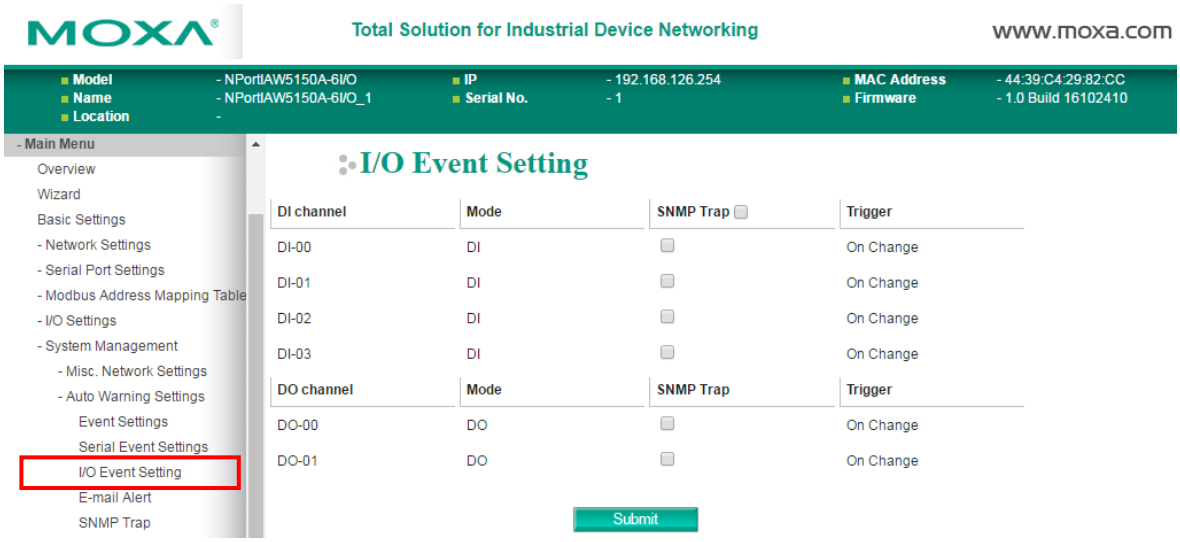
The **Serial Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the NPort will notify you of DCD and DSR events for each serial port. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending an SNMP trap.

A change in the DCD (Data Carrier Detect) signal indicates that the modem connection status has changed. If the DCD signal changes to low, it indicates that the connection line is down. A change in the DSR (Data Set Ready) signal indicates that the data communication equipment is powered off. If the DSR signal changes to low, it indicates that the data communication equipment is powered down.

ATTENTION

SNMP indicates a change in DCD or DSR signals but does not differentiate between the two. A change in either signal from "–" to "+" is indicated by "link up" and a change in either signal from "+" to "–" is indicated by "link down."

I/O Event Setting



The IA5000A-I/O and IAW5000A-I/O Series provide the following private trap triggers:

Event	Description
DI-change status	Sends SNMP trap when DI status changes.
DO-change status	Sends SNMP trap when DO status changes.

*SNMP Trap does not support Counter & Pulse Output function.

E-mail Alert

The **E-mail Alert** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how and where e-mail is sent when e-mail is used for automatic notification of system and serial port events.

ATTENTION

Consult your network administrator or ISP for the mail server settings to use for your network. If these settings are not configured correctly, e-mail notification may not work properly.

Mail Server (SMTP)

Default	
Options	free text (e.g., "192.168.3.3")
Description	This field specifies the IP address of the mail server that will be used when sending automatic warning e-mails. If the mail server requires authentication, select "My server requires authentication" and enter the username and password.

From e-mail address

Default	
Options	free text (e.g., "jsmith@xyz.com")
Description	This field specifies the e-mail address that will be listed in the e-mail's "From" field.

To e-mail address 1 to 4

Default	
Options	free text (e.g., "admin@abc.com")
Description	These fields specify the destination e-mail address(es) for the automatic e-mail warnings.

SNMP Trap

The **SNMP Trap** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify the SNMP trap settings to use for automatic notification of system and serial port events.

SNMP Trap Server IP

Default	
Options	IP address (e.g., "192.168.5.5")
Description	This field specifies the IP address of the SNMP trap server that will receive SNMP traps.

Trap Version

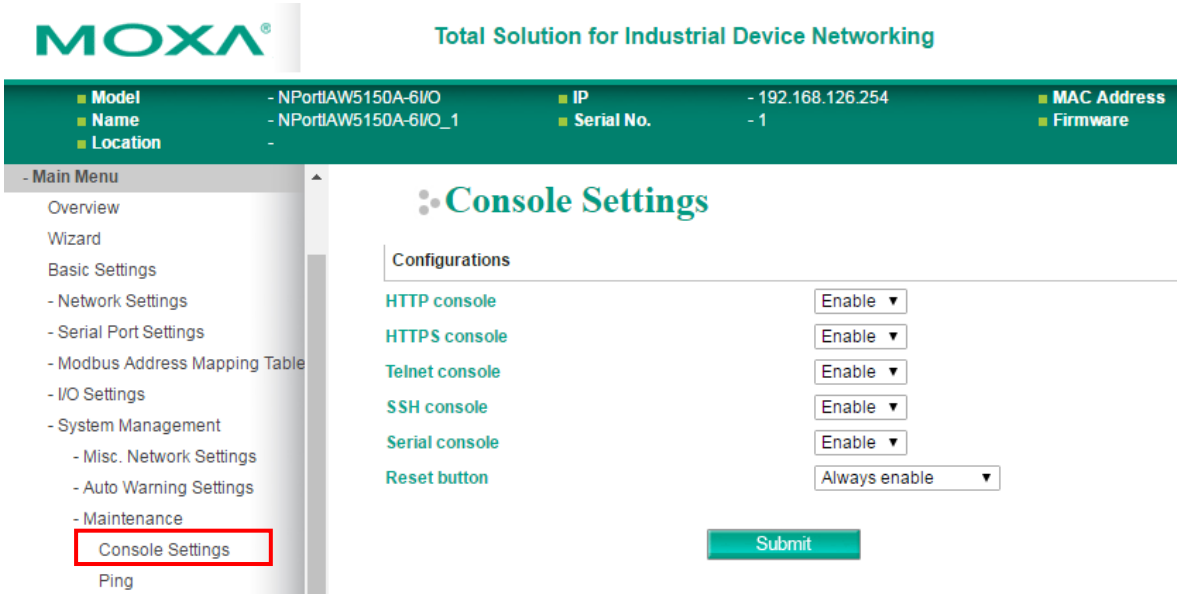
Default	v1
Options	v1, v2c
Description	This field specifies the SNMP trap version to use.

Trap Community

Default	
Options	free text (e.g., "public access")
Description	This field specifies the SNMP trap community.

Maintenance

Console Settings



The **Console Settings** page is located under **Maintenance** in the **System Management** folder. This is where you enable or disable access to the various NPort configuration consoles, as well as the behavior of the reset button. You may modify **HTTP console**, **HTTPS console**, **Telnet console**, **SSH console**, **Serial Console**, and **Reset button**.

HTTP Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the HTTP (web) console.

HTTPS Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the HTTPS (web) console.

Telnet Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the Telnet console.

SSH Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the SSH console.

Serial Console

Default	Enable
Options	Enable, Disable
Description	This field enables or disables access to the serial console.

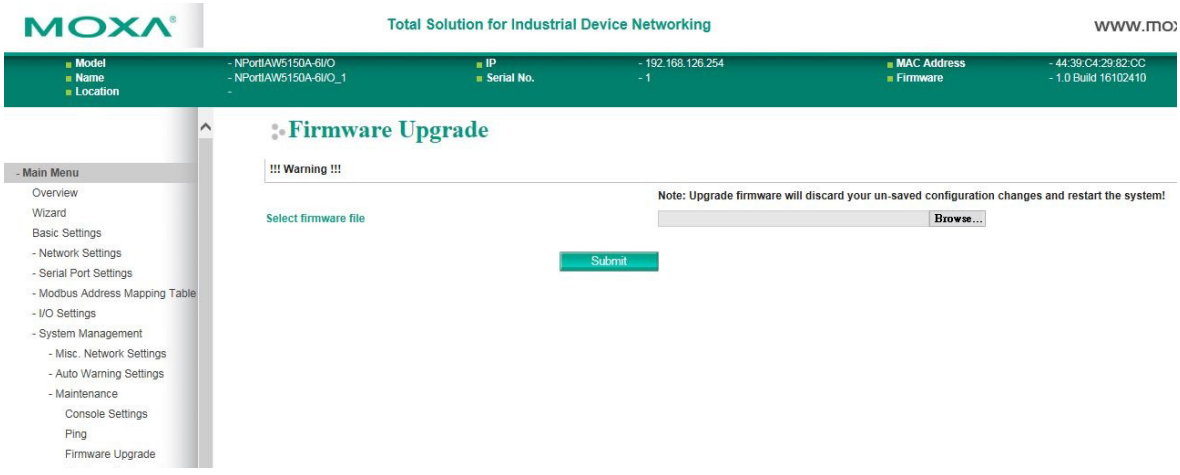
Reset Button

Default	Always Enable
Options	Always Enable, Disable after 60 sec
Description	This field specifies the behavior of the hardware reset button. Always Enable: The reset button will be operate as usual. Disable after 60 sec: The reset button will only be effective for the first 60 seconds that the NPort is powered on.

Ping

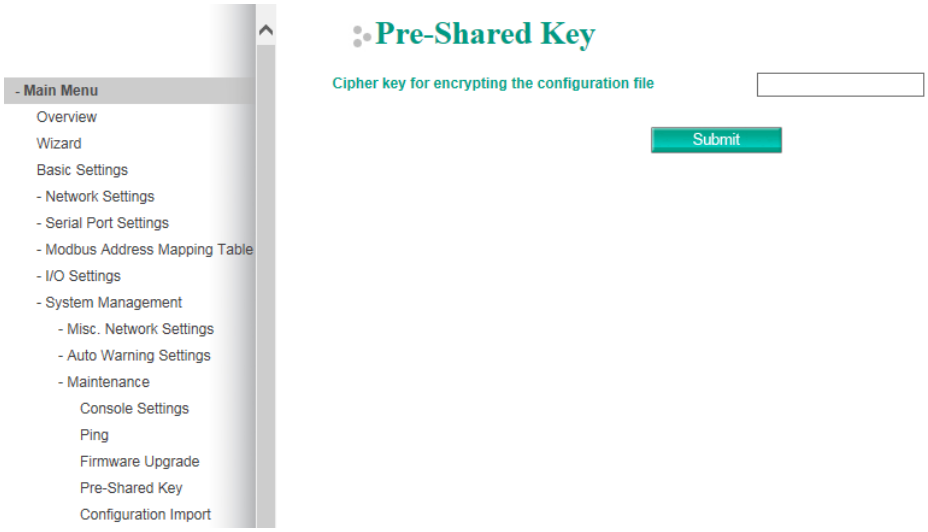
The **Ping** page is located under **Maintenance** in the **System Management** folder. It provides a convenient way to test an Ethernet connection or verify an IP address. Enter the IP address or domain name in the Destination field and click **[Activate].** The results will be displayed immediately.

Firmware Upgrade



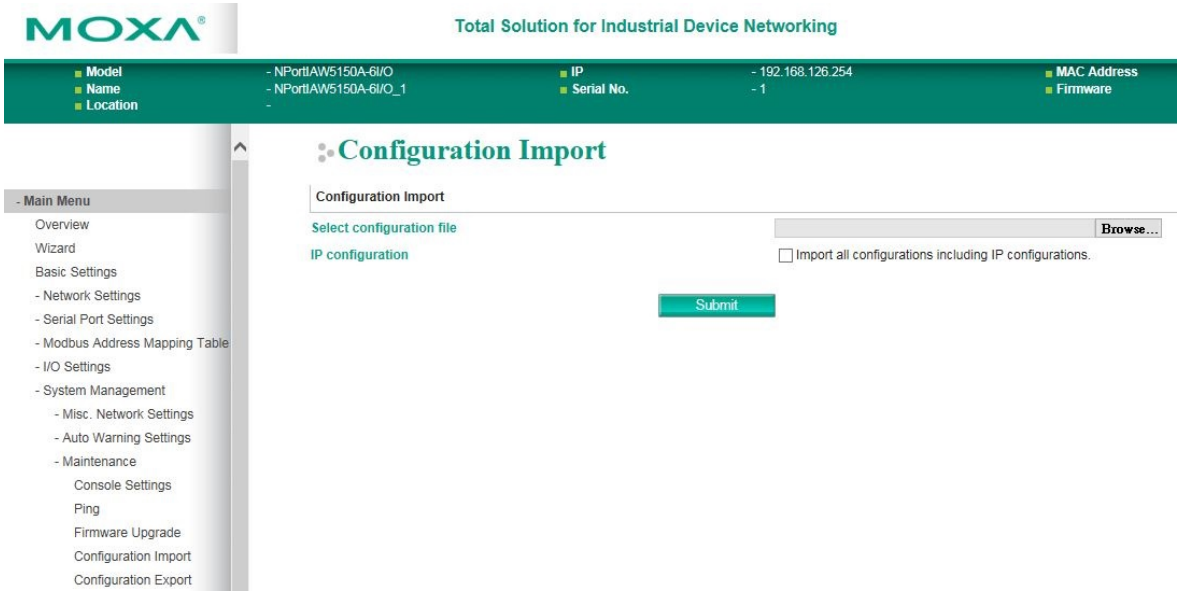
The **Firmware Upgrade** page is located under **Maintenance** in the **System Management** folder. This is where you can update the NPort firmware. After obtaining the latest firmware from www.moxa.com, select or browse for the firmware file in the **Select firmware file** field. Before clicking **[Submit]**, it is a good idea to save the NPort configuration using the **Configuration Export** page, since the firmware upgrade process may cause all settings to revert to factory defaults.

Pre-Shared Key



The device server can share or back up its configuration by exporting all settings to a file, which can then be imported into another device server. The exported file will be encrypted by a pre-shared key by the user. (The default cipher key is **moxa**)

Configuration Import

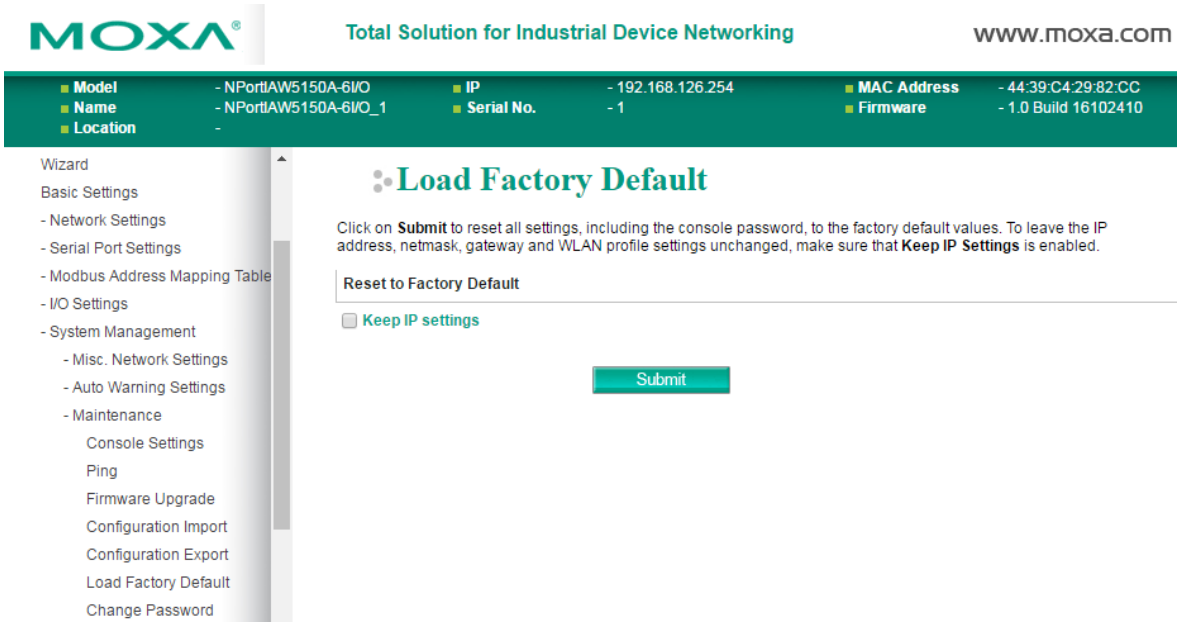


The **Configuration Import** page is located under **Maintenance** in the **System Management** folder. This is where you can load a previously saved or exported configuration. Select or browse for the configuration file in the **Select configuration file** field. If you also wish to import the IP configuration (i.e., IP address, netmask, and gateway), make sure that **Import all configurations including IP configurations** is checked.

Configuration Export

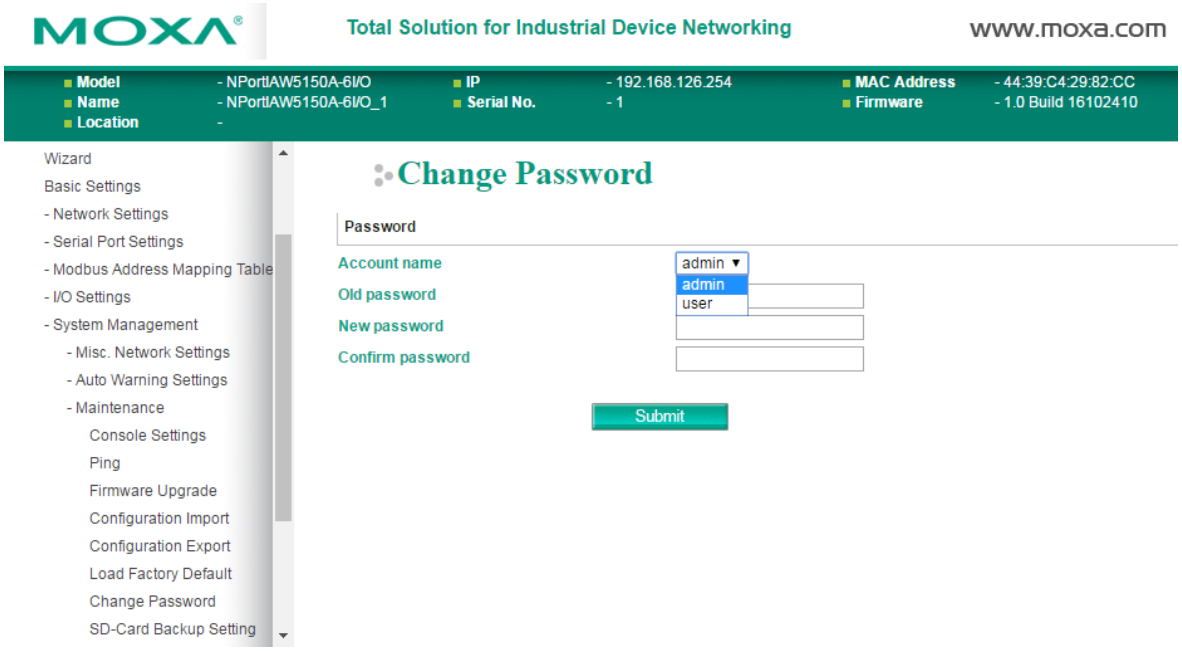
The **Configuration Export** page is located under **Maintenance** in the **System Management** folder. This is where you can save the NPort's current configuration to a file on the local host. Click **[Export]** to begin the process. A window should appear asking you to open or save the configuration text file.

Load Factory Default



The **Load Factory Default** page is located under **Maintenance** in the **System Management** folder. Click **[Submit]** to reset all settings to the factory defaults. You can preserve the NPort's existing IP settings (i.e., IP address, netmask, gateway, WLAN profile, and all certificates) by making sure **Keep IP settings** is checked before clicking **[Submit]**.

Change Password



The **Change Password** page is located under **Maintenance** in the **System Management** folder. To change the password, choose the account name first, and then enter the old password in the **Old password** field. Leave this blank if the NPort is not currently password-protected. Enter the new password twice, once in the **New password** field and once in the **Confirm password**. Leave these fields blank to remove password protection.

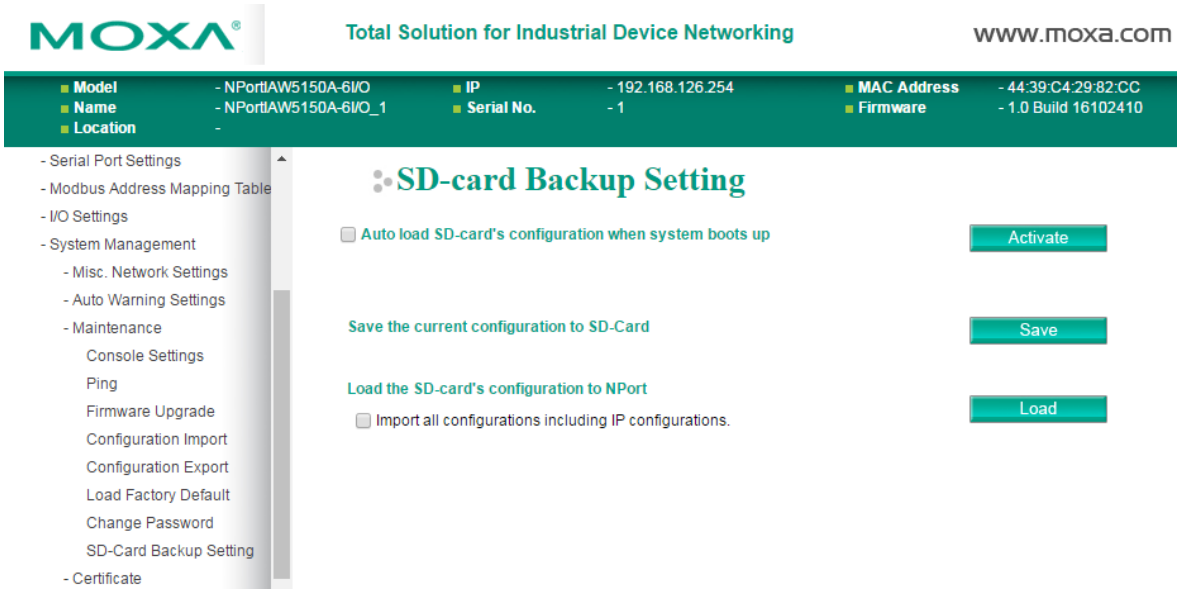
ATTENTION

If you forget the password, the ONLY way to configure the NPort is by loading the factory defaults with the reset button. All settings will be lost.

Before setting the password, you may want to first export the configuration to a file. Your configuration can then be easily imported back into the NPort if necessary.

SD card Back-up Setting

The NPort IA5000A-I/O and IAW5000A-I/O Series are equipped with a microSD card slot for easy configuration. The microSD card can be used to store an NPort's system configuration settings.



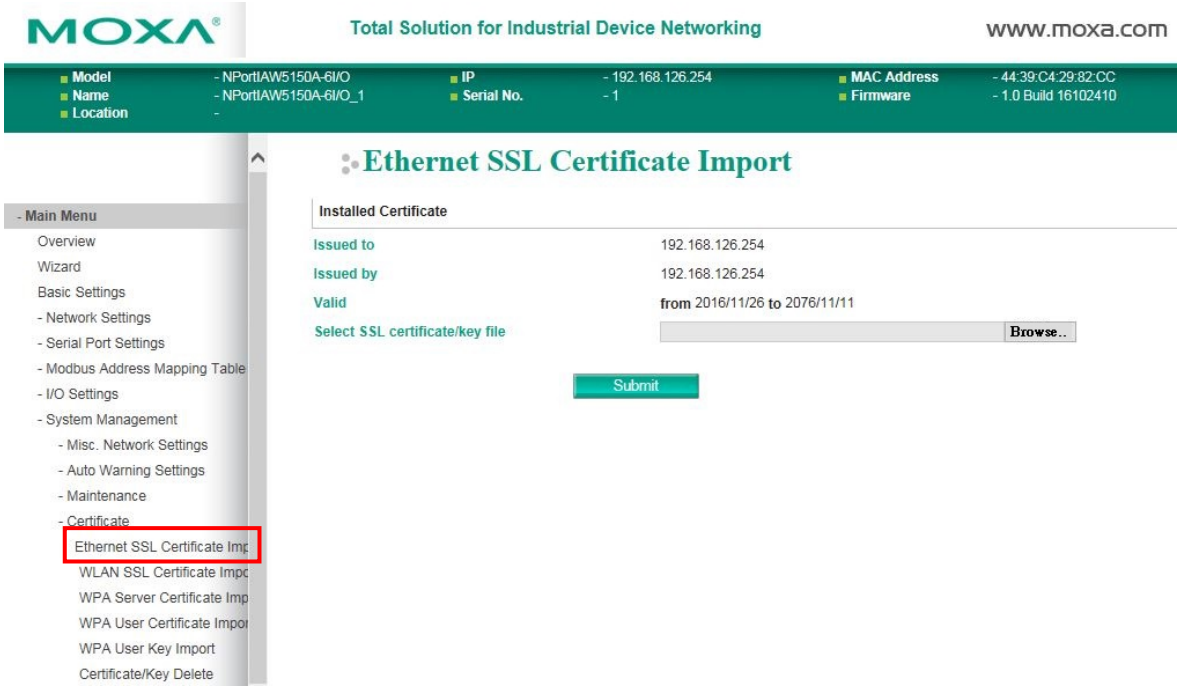
Auto load SD card's configurations when system boots up: By checking this option, the NPort will import the configuration file saved in the SD card to the NPort device when the system boots up. Click **[Activate]** to submit the change.

Save the current configuration to SD card: Users can manually save the current configuration to SD card by clicking **[Save]** button. This will overwrite the configuration file that was previously saved in the SD card if any.

Load the SD card's configuration to NPort: If a user does not want the configuration in SD card be loaded to the NPort device automatically upon system boot up, one can manually load the SD card's configuration to the NPort by clicking **[Load]** button. If you also wish to import the IP configuration (i.e., IP address, netmask, and gateway), make sure that **Import all configurations including IP configurations** is checked.

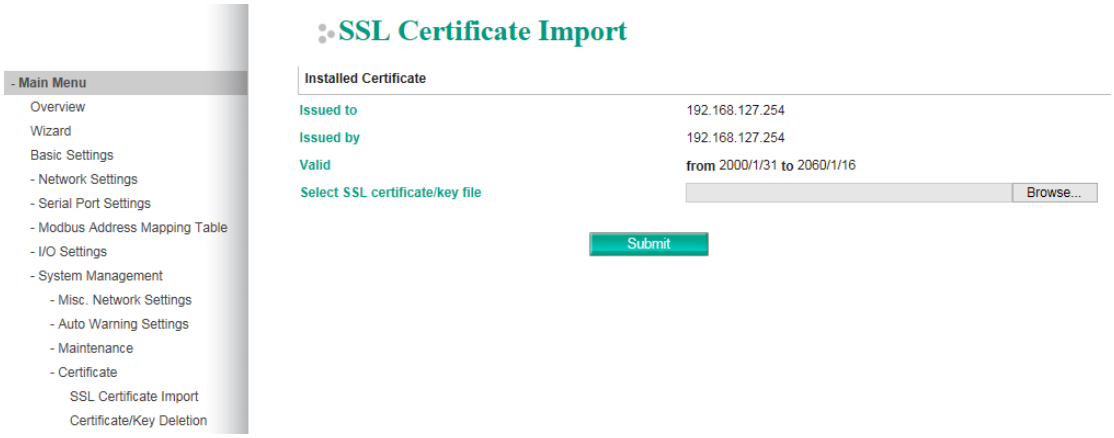
Certificate

Ethernet SSL Certificate Import (for the NPort IAW5000A-I/O Series)



The **Ethernet SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the Ethernet SSL certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

SSL Certificate Import



The **SSL Certificate Import** page is where you can load the SSL certificate for the HTTPS web console for use. Select or browse the certificate file in the **Select SSL certificate/key file** field

WLAN SSL Certificate Import (for the NPort IAW5000A-I/O Series)

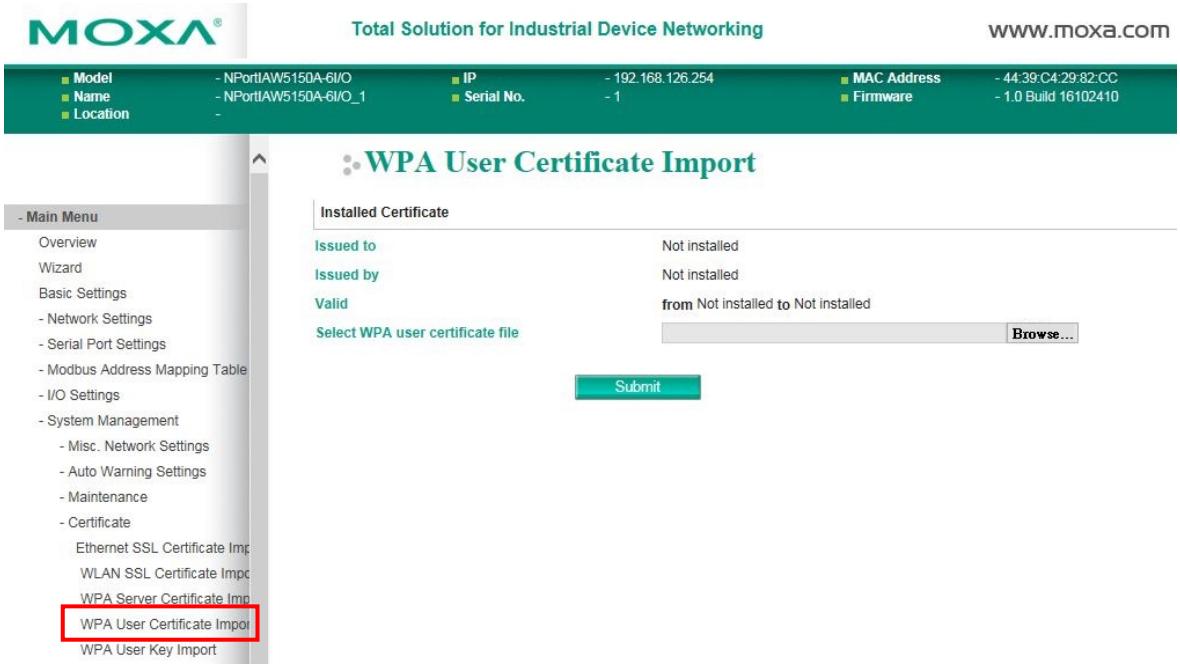
The **WLAN SSL Certificate Import** page is located under **Certificate** in the **System Management** folder. By default, the WLAN SSL certificate is automatically generated by the NPort based on the IP address of the wireless interface. You can also import a certificate. Select or browse for the certificate file in the **Select SSL certificate/key file** field.

WPA Server Certificate Import (for the NPort IAW5000A-I/O Series)

The **WPA Server Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA server certificate. Select or browse for the certificate file in the **Select WPA server certificate file** field.

You must install the trusted server certificate from the RADIUS server in order to enable **Verify server certificate** in the WLAN **Security** settings. This certificate will then be used by the NPort to authenticate the RADIUS server.

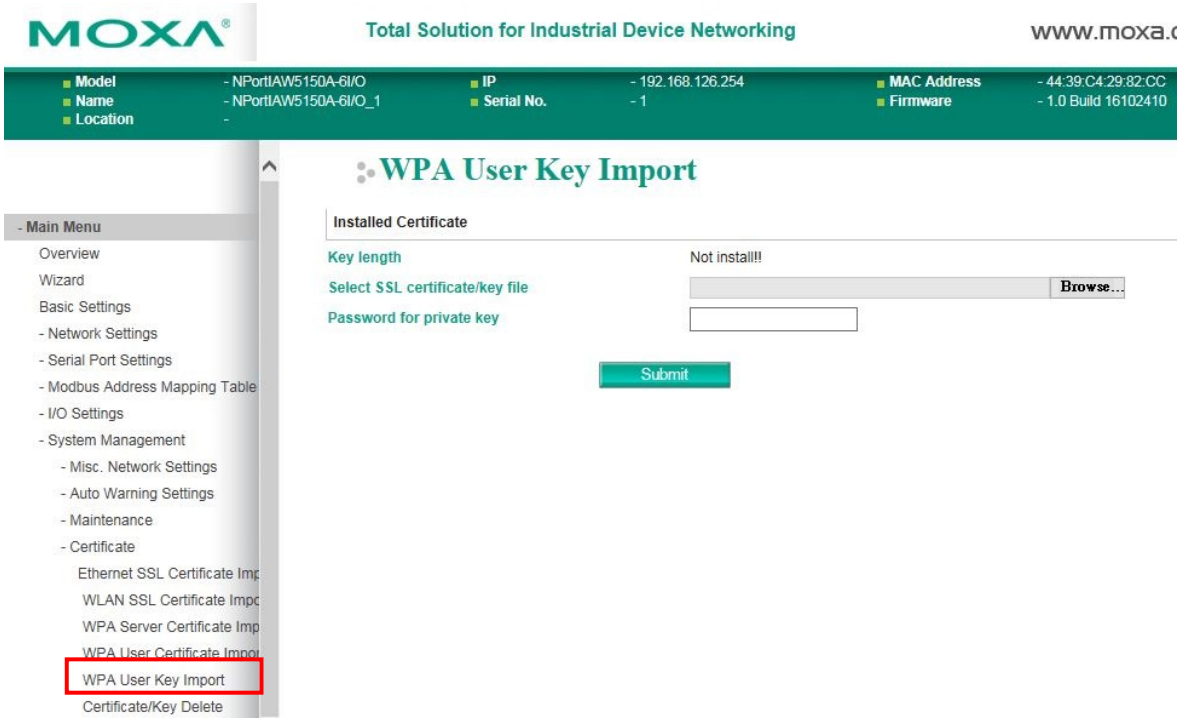
WPA User Certificate Import (for the NPort IAW5000A-I/O Series)



The **WPA User Certificate Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user certificate. Select or browse for the certificate file in the **Select WPA user certificate file** field.

The user certificate of the NPort must be installed in the RADIUS server when the NPort uses WPA (WPA2)/TLS. The trusted server certificate of the RADIUS server must also be installed in the NPort.

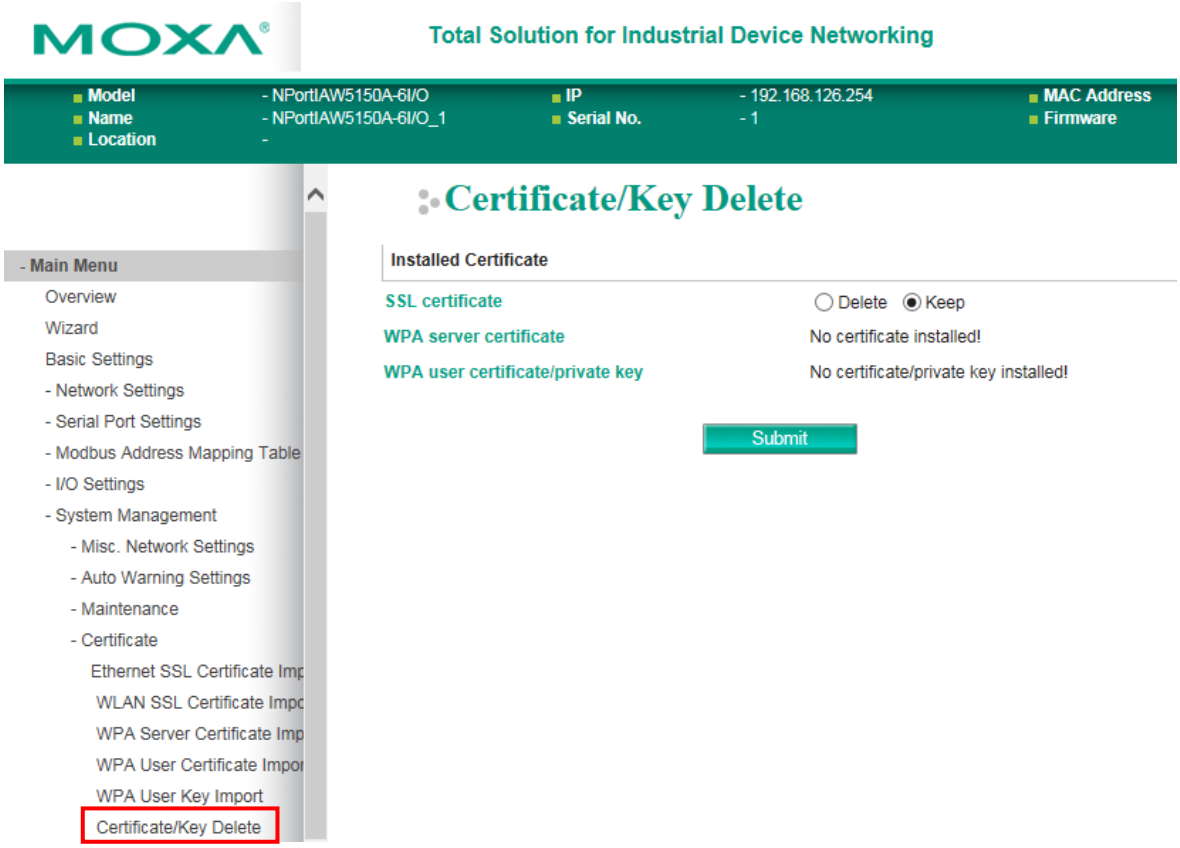
WPA User Key Import (for the NPort IAW5000A-I/O Series)



The **WPA User Key Import** page is located under **Certificate** in the **System Management** folder. This is where you can load the WPA user certificate. Select or browse for the user private key file in the **Select WPA user privacy key file** field and enter the **Password for the private key**.

The user private key of the NPort must be installed in the RADIUS server when the NPort uses WPA(WPA2)//TLS. The trusted server certificate of RADIUS server must also be installed on the NPort.

Certificate/Key Delete



The **Certificate/Key Delete** page is located under **Certificate** in the **System Management** folder. This page is where you can delete certificates or WPA keys that have been installed on the model. When you click **[Submit]**, any certificate or key that has been set to "Delete" will be deleted from the NPort.

11

Web Console: System Monitoring

The following topics are covered in this chapter:

- **Overview**
- **System Monitoring**
  - Serial Status
  - System Status

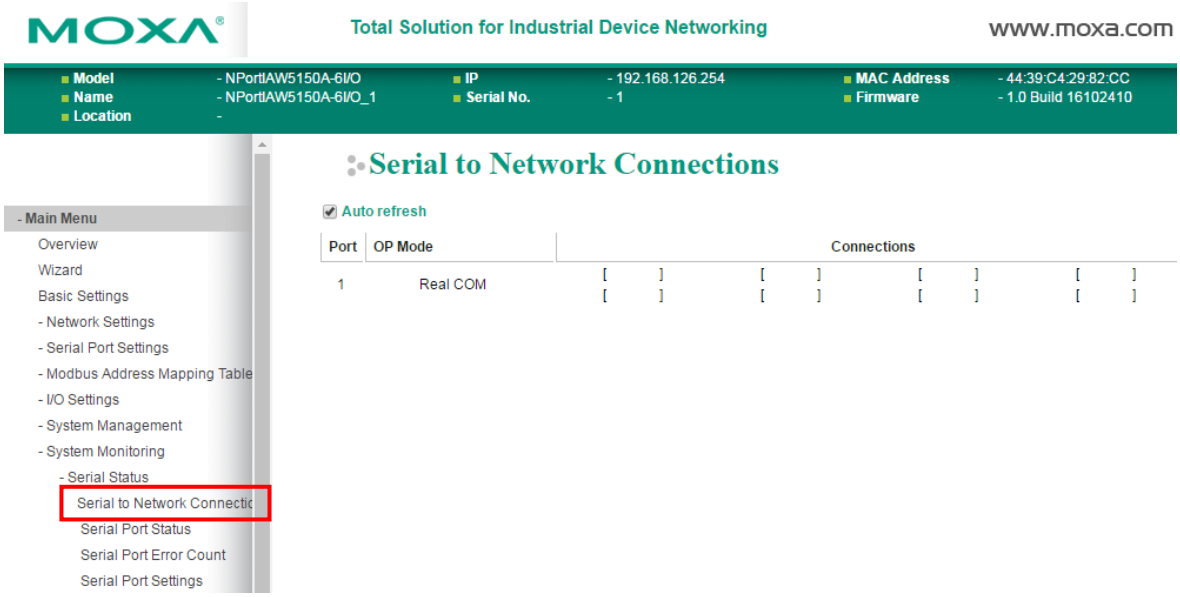
Overview

This chapter explains how to use the **System Monitoring** functions on the NPort web console. These functions allow you to monitor many different aspects of operation.

System Monitoring

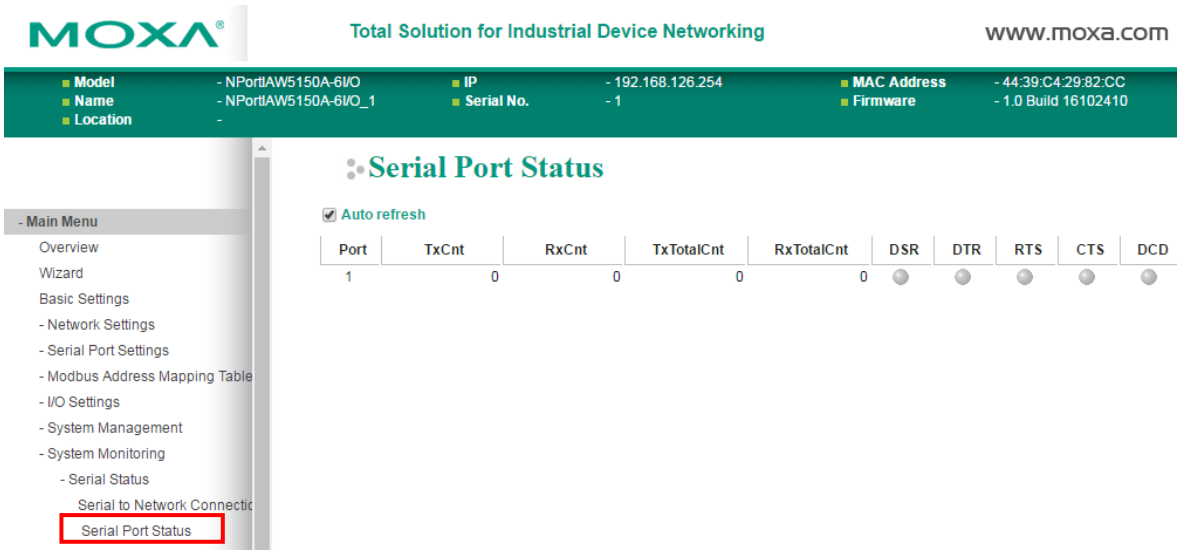
Serial Status

Serial to Network Connections



The **Serial to Network Connections** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the current operation mode and host connection status for each serial port.

Serial Port Status



The **Serial Port Status** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can monitor the signal and data transmission status for each serial port.

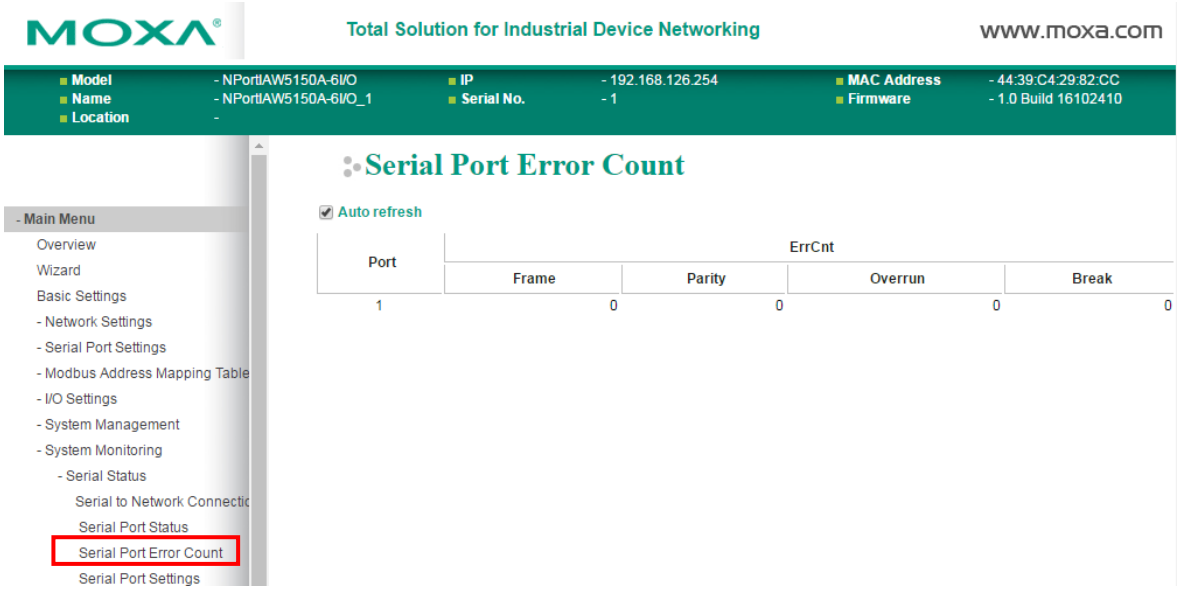
TxCnt: number of Tx packets (to device) for the current connection

RxCnt: number of Rx packets (from device) for the current connection

TxTotalCnt: number of Tx packets since the NPort was powered on

RxTotalCnt: number of Rx packets since the NPort was powered on

Serial Port Error Count



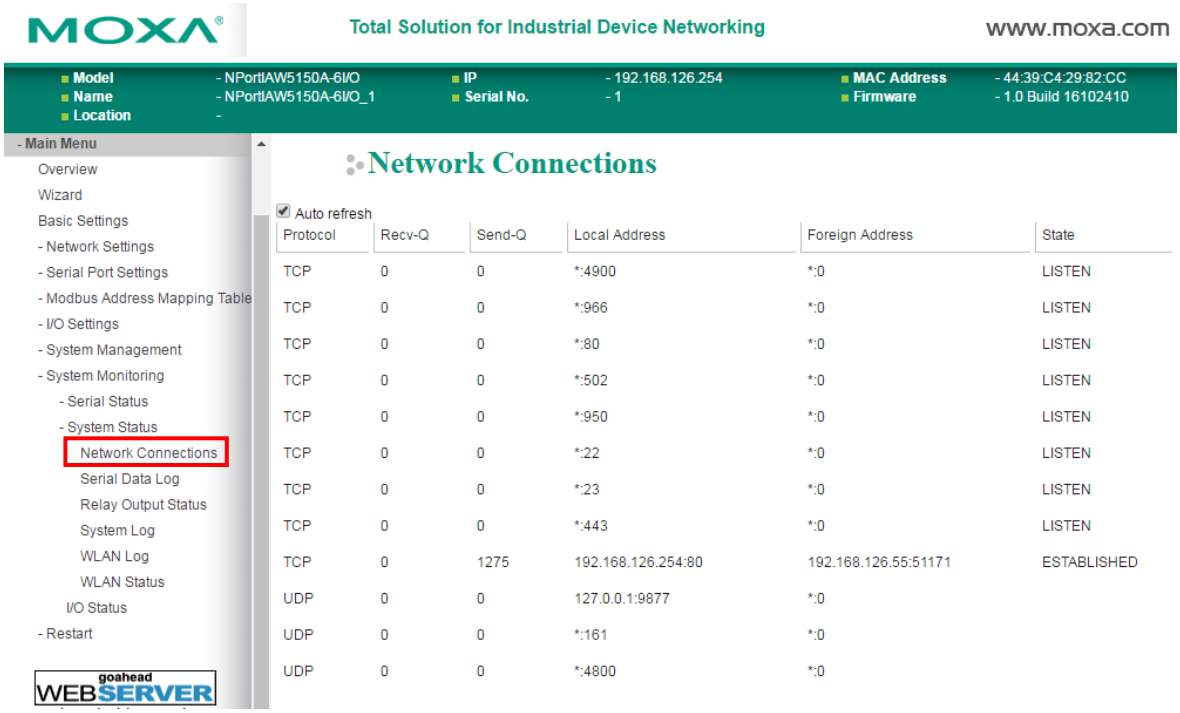
The **Serial Port Error Count** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current number of frame, parity, overrun and break errors for each serial port.

Serial Port Settings

The **Serial Port Settings** page is located under **Serial Status** in the **System Monitoring** folder. On this page, you can view the current communication settings for each serial port.

System Status

Network Connections



The **Network Connections** page is located under **System Status** in the **System Monitoring** folder. On this page, you can view the current status of any network connection to the NPort.

Serial Data Log

Data logs for each serial port can be viewed in ASCII or HEX format. After selecting the serial port and format, you may click **Select** all to select the entire log if you wish to copy and paste the contents into a text file. The **Clear log** and **Refresh** buttons allow you to clear or refresh the log contents.

The **Serial Data Log** page is located under **System Status** in the **System Monitoring** folder. This is where you can download the current data log for a serial port. Select the desired serial port in the **Select port** field. Select the desired data format in the **Download format** field. Click **[Clear log]** to clear the log contents.

The data log includes all data sent or received by the specified serial port since the NPort was powered on. The maximum size of the log is 64 KB.

System Alert Status

The **System Alert Status** page is located under **System Status** in the **System Monitoring** folder. This is where you can check which event triggered the warning.

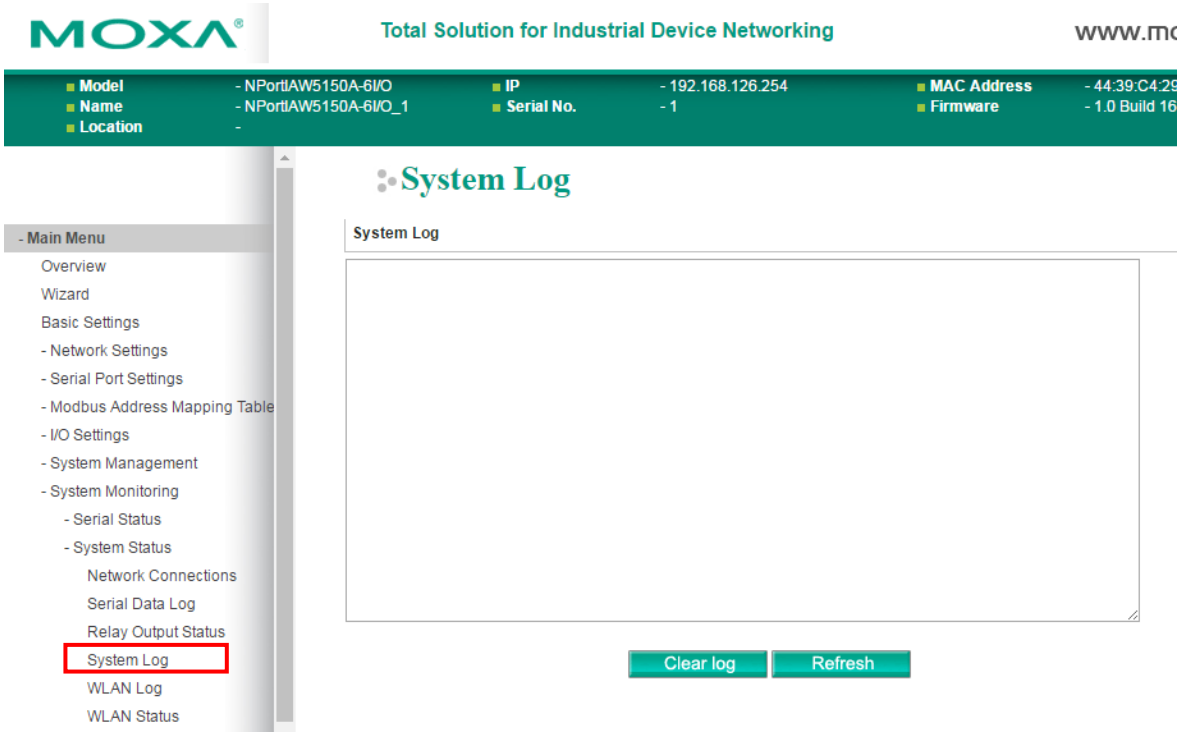
Relay Output Status

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.

Modbus/TCP Connection Watchdog Status

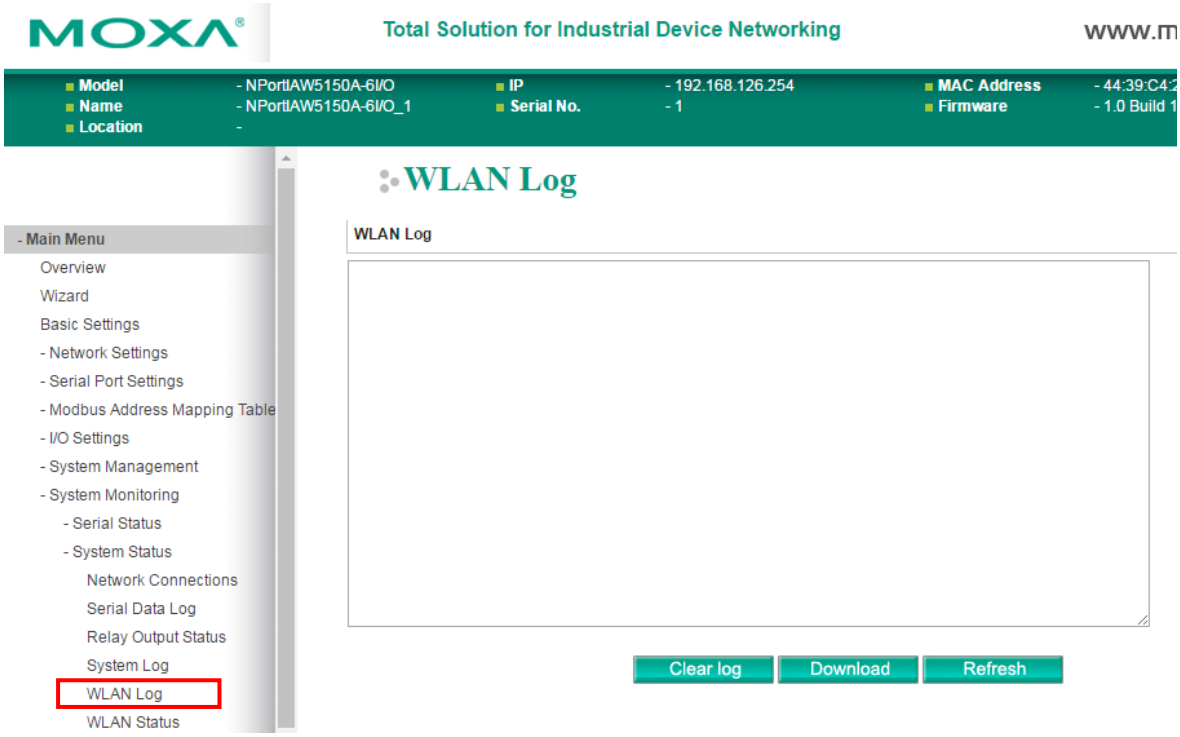
If the **Communication Watchdog Timeout** function is enabled (Please refer to Chapter 2: "Basic Settings"), the NPort will enter **Safe Mode** when a specified period of time has passed and there is a loss of Modbus/TCP network connectivity. The user may see the host connection status in the **System Alert** section under **System Monitoring** and clear the alert when the host connection resumes.

System Log



The **System Log** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the log of NPort system events. Click **[Clear log]** to clear the log contents. Click **[Refresh]** to refresh the log contents.

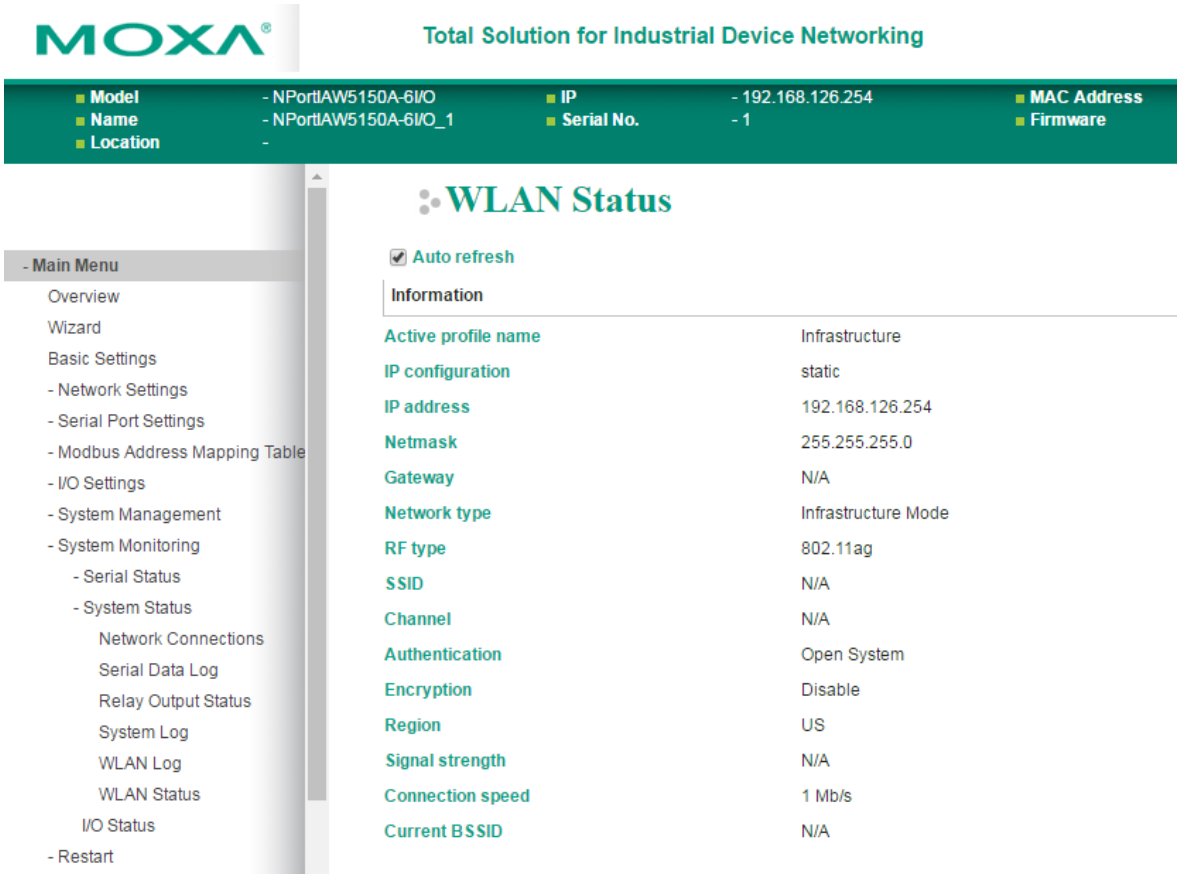
WLAN Log (for the NPort IAW5000A-I/O Series)



The **WLAN Log** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the log between the device server and the access points. It's a good tool for an engineer to troubleshoot if there is any issue with the wireless connection. Click **[Clear log]** to clear the log contents. Click **[Download]**

to save the log to a txt file for an engineer to troubleshoot, e.g., Moxa's Technical Support Team. Click **[Refresh]** to refresh the log contents.

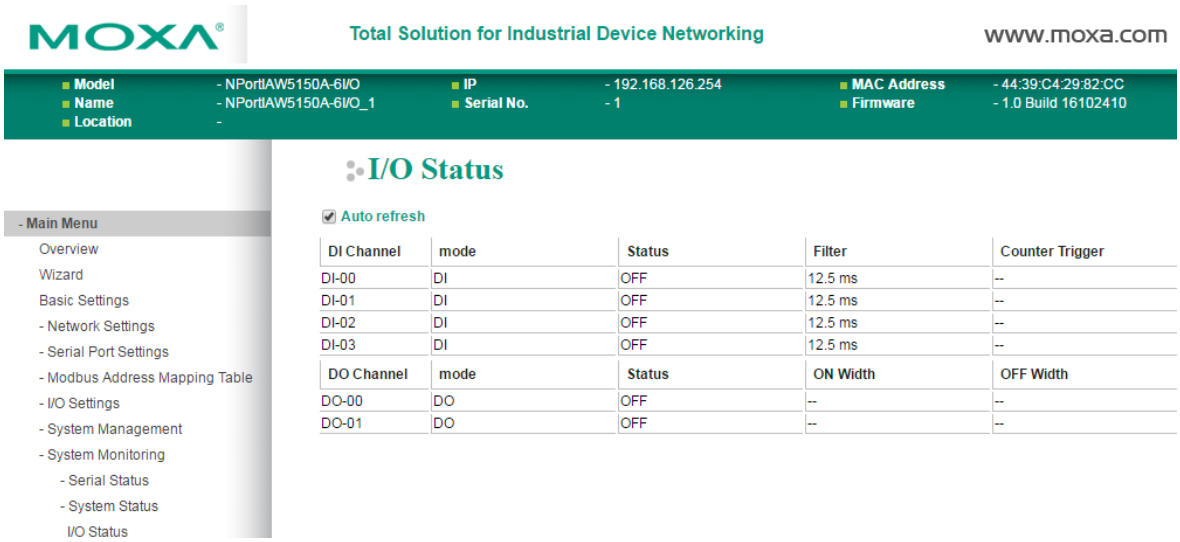
WLAN Status (for NPort IAW5000A-I/O Series)



The **WLAN Status** page is located under **System Status** in the **System Monitoring** folder. This is where you can view the current WLAN settings and status.

I/O Status

The **I/O Status** page is located under **System Monitoring** folder. On this page, you can monitor the current status and communication settings of DI and DO channels.



12

Web Console: Restart

The following topics are covered in this chapter:

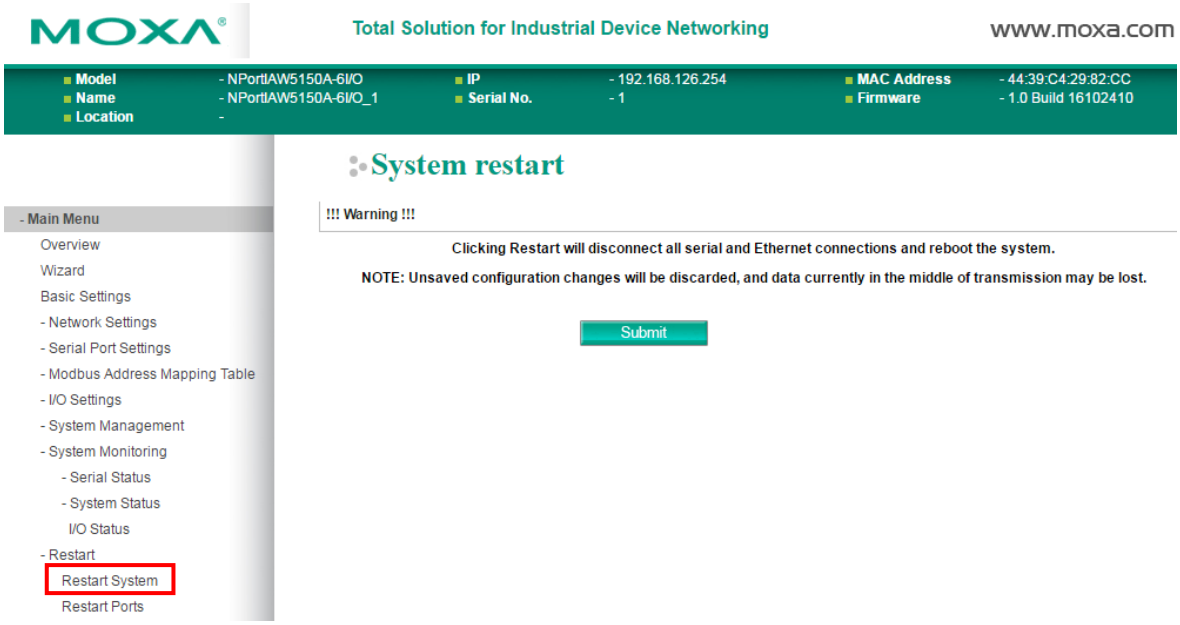
- **Overview**
- **Restart**
  - Restart System
  - Restart Ports

Overview

This chapter explains how to use save your configuration changes and restart the NPort using the NPort web console. Configuration changes will not be effective until they are saved and the NPort is rebooted.

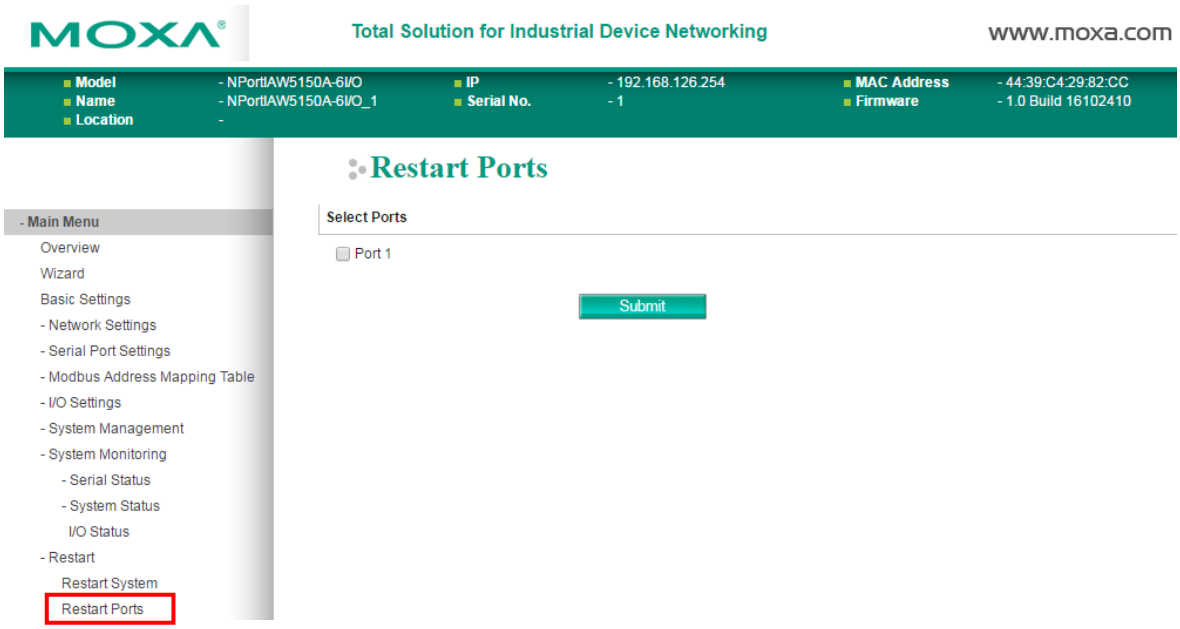
Restart

Restart System



The **Restart System** page is located in the **Restart** folder. Click **[Restart]** to restart the NPort, and the new settings will take effect upon restart.

Restart Ports



The **Restart Ports** page is located in the **Restart** folder. Select the desired serial and click **[Select All]** to select all serial ports. Click **[Submit]** to restart the selected serial ports.

13

Android API Instructions

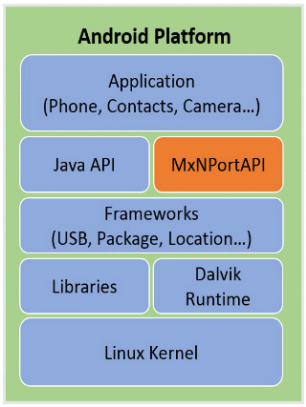
The following topics are covered in this chapter:

Overview

If you want to remote control your serial devices on an Android platform, then the MxNPortAPI is a simple application programming tool that 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 about the provided functions, please refer to the "MxNPortAPI Function Groups" section.

This MxNPortAPI is layered between the Android application and Android network manager framework. This Android library is compatible with Java 1.7, Android 3.1 (Honeycomb - API version 12), and later versions.

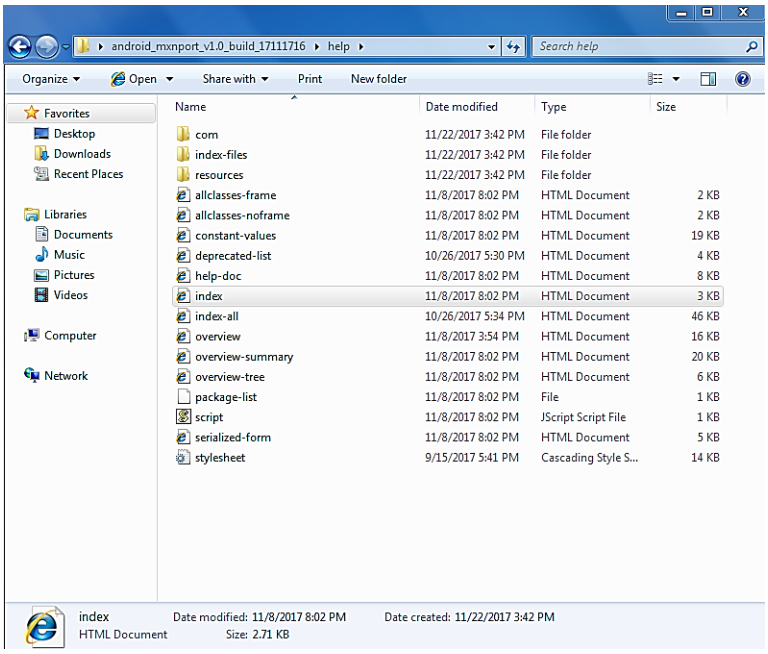


How to Start MxNPortAPI

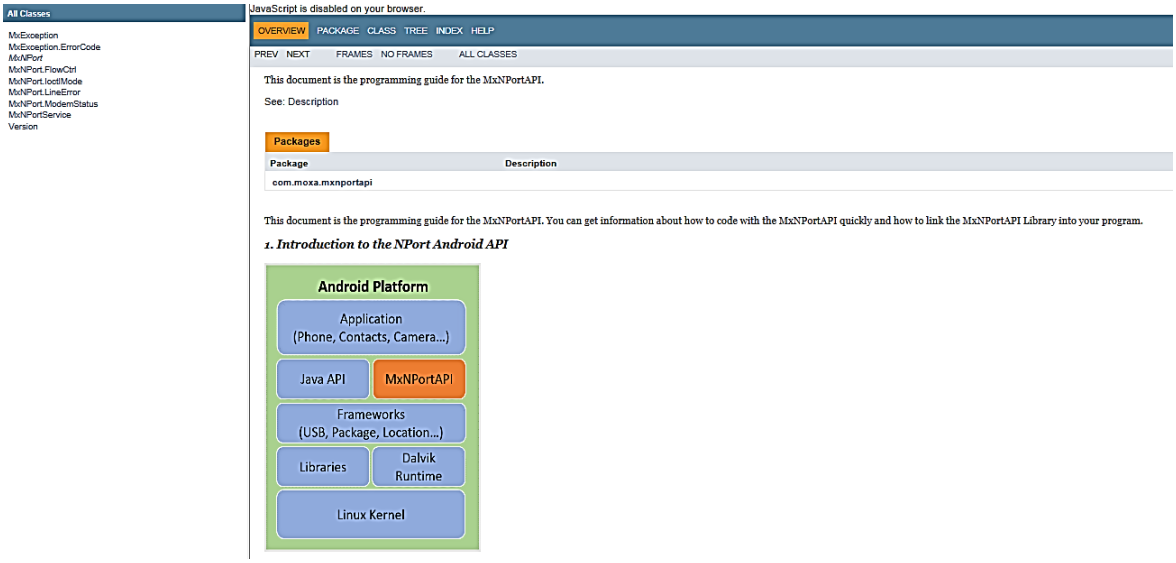
You can download the MxNPortAPI from Moxa's website at http://www.moxa.com and develop the application program in popular OSs, such as Windows, Linux, or Mac.

(You can refer the Android studio website to see the system requirements for development environment: https://developer.android.com/studio/index.html?hl=zh-tw#Requirements).

To start your application program, please unzip the MxNPortAPI file and refer to the index (.html) under the Help directory.



For more details about the installation, please 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();
```

A

SNMP Agents with MIB II & RS-232-Like Groups

The NPort has built-in SNMP (Simple Network Management Protocol) agent software that supports SNMP Trap, RFC1317 RS-232 like groups and RFC 1213 MIB-II. The following table lists the standard MIB-II groups, as well as the variable implementation for the NPort.

RFC1213 MIB-II Supported SNMP Variables

System MIB

SysDescr	SysContact	SysServices
SysObjectID	SysName	
SysUpTime	SysLocation	

Interfaces MIB

itNumber	ifOperStatus	ifOutOctets
ifIndex	ifLastChange	ifOutUcastPkts
ifDescr	ifInOctets	ifOutNUcastPkts
ifType	ifInUcastPkts	ifOutDiscards
ifMtu	ifInNUcastPkts	ifOutErrors
ifSpeed	ifInDiscards	ifOutQLen
ifPhysAddress	ifInErrors	ifSpecific
ifAdminStatus	ifInUnknownProtos	

IP MIB

ipForwarding	ipOutDiscards	ipAdEntIfIndex
ipDefaultTTL	ipOutNoRoutes	ipAdEntNetMask
ipInreceives	ipReasmTimeout	ipAdEntBcastAddr
ipInHdrErrors	ipReasmReqds	ipAdEntReasmMaxSize
ipInAddrErrors	ipReasmOKs	IpNetToMediaIfIndex
ipForwDatagrams	ipReasmFails	IpNetToMediaPhysAddress
ipInUnknownProtos	ipFragOKs	IpNetToMediaNetAddress
ipInDiscards	ipFragFails	IpNetToMediaType
ipInDelivers	ipFragCreates	IpRoutingDiscards
ipOutRequests	ipAdEntAddr	

ICMP MIB

IcmpInMsgs
IcmpInErrors
IcmpInDestUnreachs
IcmpInTimeExcds
IcmpInParmProbs
IcmpInSrcQuenchs
IcmpInRedirects
IcmpInEchos
IcmpInEchoReps
IcmpInTimestamps
IcmpTimest ampReps
IcmpInAddrMasks
IcmpOutMsgs
IcmpOutErrors
IcmpOutDestUnreachs
IcmpOutTimeExcds
IcmpOutParmProbs
IcmpOutSrcQuenchs
IcmpOutRedirects
IcmpOutEchos
IcmpOutEchoReps
IcmpOutTimestamps
IcmpOutTimestampReps
IcmpOutAddrMasks
IcmpOutAddrMaskReps

UDP MIB

UdpInDatagrams
UdpNoPorts
UdpInErrors
UdpOutDatagrams
UdpLocalAddress
UdpLocalPort

Address Translation

AtIfIndex
AtPhysAddress
AtNetAddress

TCP MIB

tcpRtoAlgorithm
tcpRtoMin
tcpRtoMax
tcpMaxConn
tcpActiveOpens
tcpPassiveOpens
tcpAttempFails
tcpEstabResets
tcpCurrEstab
tcpInSegs
tcpOutSegs
tcpRetransSegs
tcpConnState
tcpConnLocalAddress
tcpConnLocalPort
tcpConnRemAddress
tcpConnRemPort
tcpInErrs
tcpOutRsts

SNMP MIB

snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps

RFC1317: RS-232 MIB Objects

Generic RS-232-like Group

rs232Number

RS-232-like General Port Table

rs232PortTable
rs232PortEntry
rs232PortIndex
rs232PortType
rs232PortInSigNumber
rs232PortOutSigNumber
rs232PortInSpeed
rs232PortOutSpeed

RS-232-like Asynchronous Port Group

rs232AsyncPortTable	rs232AsyncPortIndex	rs232AsyncPortStopBits
rs232AsyncPortEntry	rs232AsyncPortBits	rs232AsyncPortParity

The Input Signal Table

rs232InSigTable	rs232InSigPortIndex	rs232InSigState
rs232InSigEntry	rs232InSigName	

The Output Signal Table

rs232OutSigTable	rs232OutSigPortIndex	rs232OutSigState
rs232OutSigEntry	rs232OutSigName	

B

Well-Known Port Numbers

Listed below are well-known port numbers that may cause network problems if they are assigned to an NPort serial port. Refer to RFC 1700 for well-known port numbers or refer to the following introduction from IANA.

The port numbers are divided into three ranges: Well-Known Ports, Registered Ports, and Dynamic and/or Private Ports.

- **Well-Known Ports** range from 0 through 1023.
- **Registered Ports** range from 1024 through 49151.
- **Dynamic and/or Private Ports** range from 49152 through 65535.

The well-known ports are assigned by 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, please 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	Simple Mail Transfer Protocol (SMTP)
37	Time (Time Server)
42	Host name server (names server)
43	Whois (nickname)
49	Login Host Protocol (Login)
53	Domain Name Server (domain)
79	Finger protocol (Finger)
80	World Wide Web HTTP
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol
213	IPX
160 to 223	Reserved for future use
502	Modbus TCP Protocol

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	Gopher Protocol
79	Finger Protocol
80	World Wide Web HTTP
107	Remote Telnet Service
111	Sun Remote Procedure Call (Sunrpc)
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
161	Simple Network Mail Protocol (SNMP)
162	SNMP Traps
213	IPX (Used for IP Tunneling)

C

Ethernet Modem Commands

A serial port on the NPort can be set to Ethernet Modem mode, allowing a PC or device to connect to the NPort as if it was an Ethernet modem. This section provides additional detail about how the NPort operates in Ethernet Modem mode.

Dial-in Operation

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

ATS0=0: 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≧1: The NPort will accept the TCP connection immediately. It will send the "**CONNECT** {*baudrate*}" command to the serial port and will immediately enter data mode.

Dial-out

The NPort accepts ATD commands such as "**ATD 192.168.1.1:4001**" from the serial port. It will then request a TCP connection from the specified remote Ethernet modem or PC. Once the remote unit accepts this TCP connection, the NPort will send the "**CONNECT** {*baudrate*}" command to the serial port and will immediately enter data mode.

Disconnection Request from Local Site

When the NPort is in data mode, you can initiate disconnection by sending "**+++**". Some applications allow you to directly set the DTR signal to off, which will also initiate disconnection. The NPort will enter command mode, and you can then enter "**ATH**" to close the TCP connection "**NO CARRIER**" will be returned to the serial port.

ATTENTION

When entering "+++" to disconnect, the three "+" characters must be sent in quick succession, and the sequence must be prefaced and followed by a guard time to protect the raw data. You can change the disconnect character using register S2. You can set the guard time using register S12.

Disconnection Request from Remote Site

After the TCP connection has been closed by the remote Ethernet modem or PC, the NPort will send "**NO CARRIER**" to the serial port and will return to command mode.

AT Commands

Ethernet Modem mode supports the following common AT commands, as used with a typical modem:

No.	Command	Description	Remarks
1	ATA	Answer manually	
2	ATD	Dial up specified IP address and port number ATD 192.168.1.1:950 (example)	
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	On line 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 (default) 0=OK 1=connect 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&F	Restore manufacturer's settings	
17	AT&G	Select guard time	reply "OK" only
18	AT&R	Serial port RTS option command	reply "OK" only
19	AT&S	Serial port DSR control	reply "OK" only
20	AT&V	View settings	
21	AT&W	Write current settings to flash for next boot up	

S Registers

No.	Register	Description	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 "+++"	

D

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and your body.

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.

Labeling requirements

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.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

End Product Labeling

This transmitter module is authorized only for use in device where the antenna may be installed such that 20cm may be maintained between the antenna and users. The final end product must be labeled in a visible area with the following: "Contains FCC ID: SLE-IAW5000A ”

Information for the OEMs and Integrators

The following statement must be included with all versions of this document supplied to an

OEM or integrator, but should not be distributed to the end user.

1. This device is intended for OEM integrators only.
2. Please see the full Grant of Equipment document for other restrictions.

This radio transmitter FCC ID: SLE-IAW5000A has been approved by FCC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antenna List

No.	Manufacturer	Model No.	Antenna Type	Peak Gain
1	KINSUN	ANT-WDB-ARM-02 (Part No. 6602D03081)	Dipole Antenna	2.04 dBi for 2.4 GHz 0.38 dBi for 5 GHz

Note: The antenna connector is Reverse SMA type.