Flow control

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

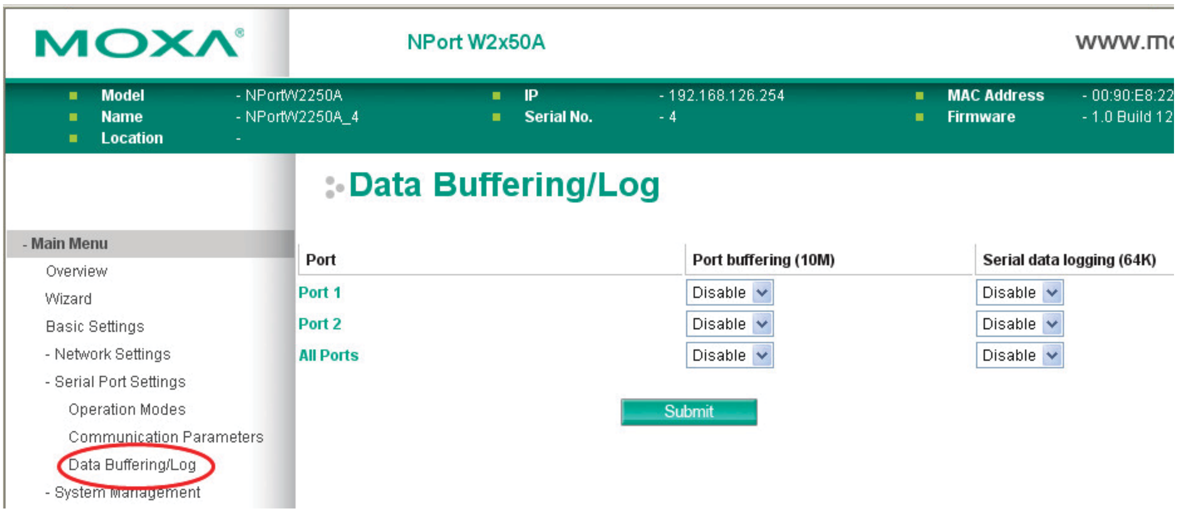
FIFO

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22
Firmware - 1.0 Build 12

Data Buffering/Log

Port	Port buffering (10M)	Serial data logging (64K)
Port 1	Disable	Disable
Port 2	Disable	Disable
All Ports	Disable	Disable

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 Real COM 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: System Management

The following topics are covered in this chapter:

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

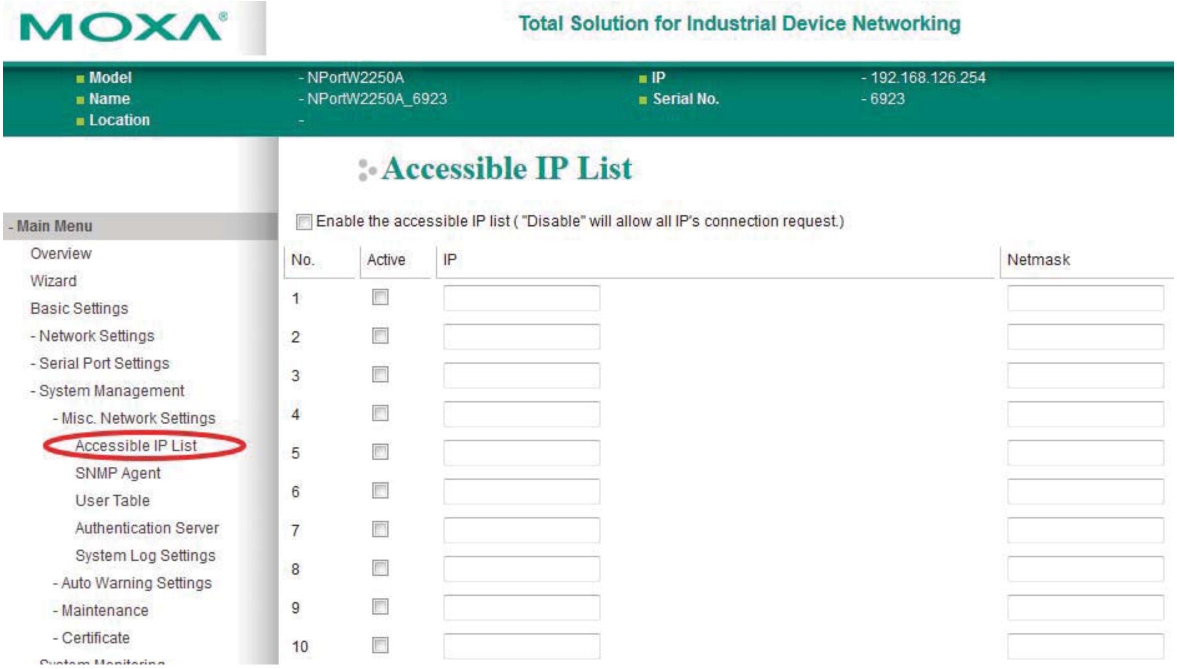
Overview

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



Model - NPortW2250A
Name - NPortW2250A_6923
Location -
IP - 192.168.126.254
Serial No. - 6923

Accessible IP List

□ Enable the accessible IP list ("Disable" will allow all IP's connection request.)

No.	Active	IP	Netmask
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		

The **Accessible IP List** page is located under **Misc. Network Settings** in the **System Management** folder. This page is used to 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.

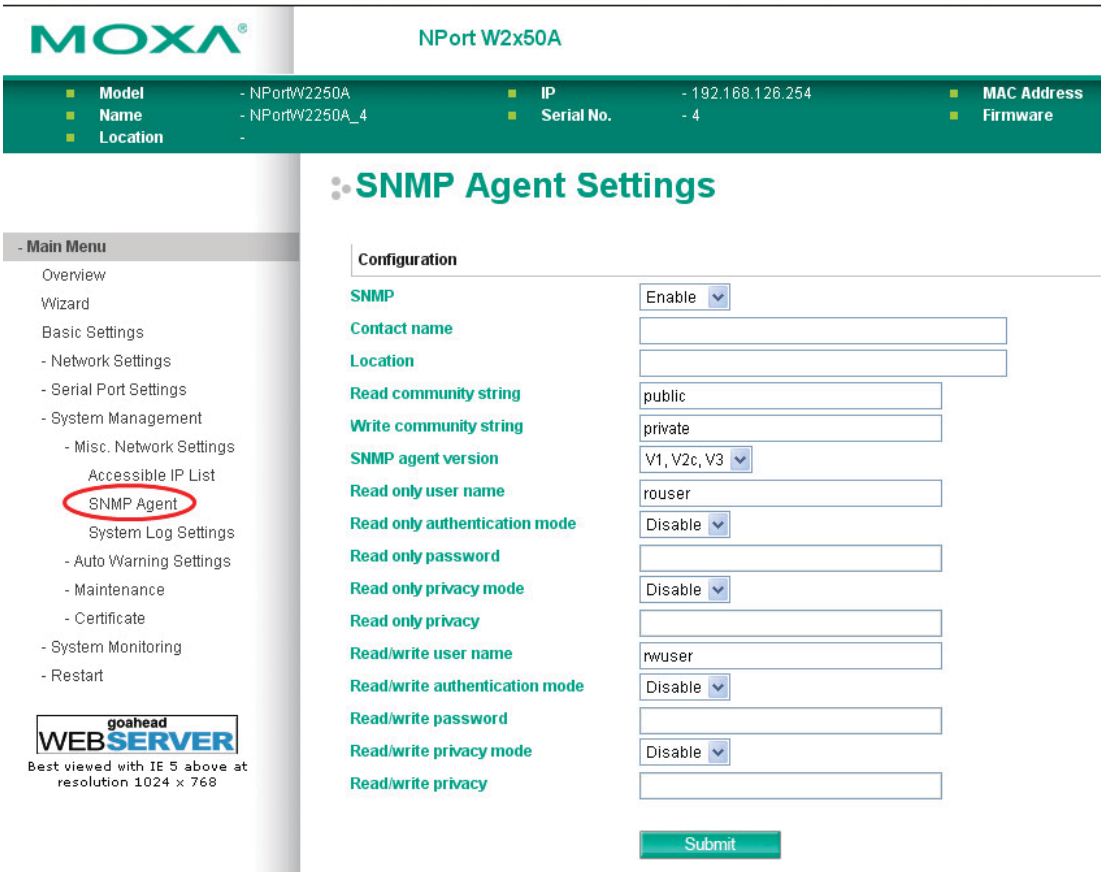
To allow access to hosts on a specific subnet
For both the IP address and netmask, use 0 for the last digit (e.g., “192.168.1.0” and “255.255.255.0”).

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

SNMP Agent Settings

Configuration

SNMP	Enable
Contact name	
Location	
Read community string	public
Write community string	private
SNMP agent version	V1, V2c, V3
Read only user name	rouser
Read only authentication mode	Disable
Read only password	
Read only privacy mode	Disable
Read only privacy	
Read/write user name	rwuser
Read/write authentication mode	Disable
Read/write password	
Read/write privacy mode	Disable
Read/write privacy	

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 username 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
Description	This field specifies whether 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 username 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.

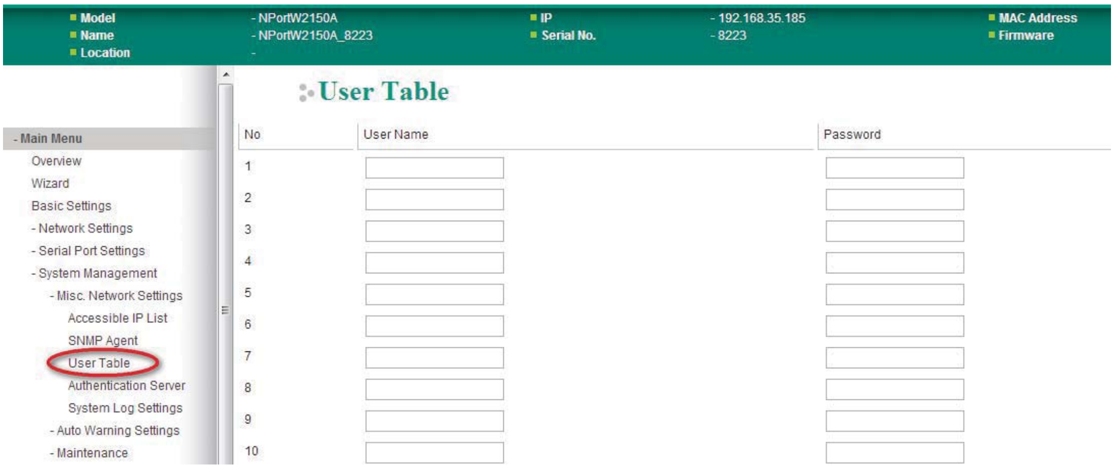
Read/Write Privacy mode

Default	Disable
Options	Disable, DES, AES
Description	This field specifies whether 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



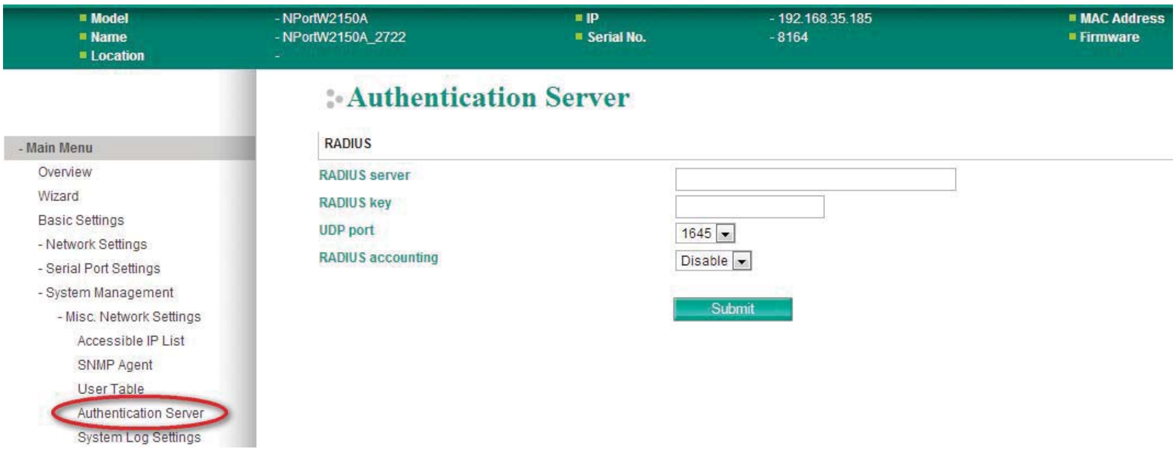
Model	- NPortW2150A	IP	- 192.168.35.185	MAC Address	
Name	- NPortW2150A_8223	Serial No.	- 8223	Firmware	
Location	-				

User Table

No	User Name	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

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



Model	- NPortW2150A	IP	- 192.168.35.185	MAC Address	
Name	- NPortW2150A_2722	Serial No.	- 8164	Firmware	
Location	-				

Authentication Server

RADIUS

RADIUS server:

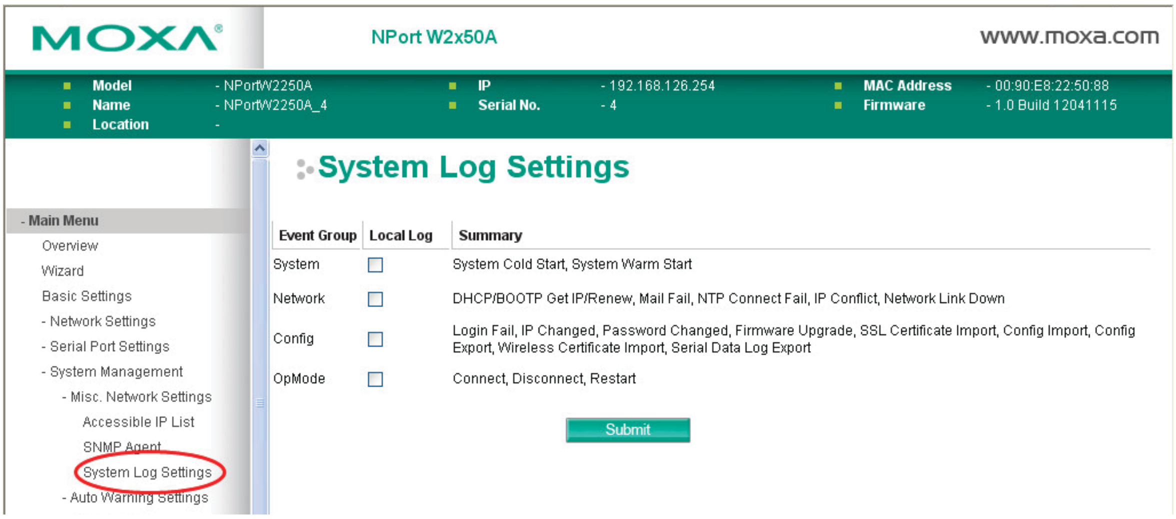
RADIUS key:

UDP port: 1645

RADIUS accounting: Disable

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): Please select which UDP port your RADIUS server is using to communicate. The device supports UDP port 1645 or 1812.
RADIUS accounting: Use this field to enable or disable RADIUS accounting.

System Log Settings



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

System Log Settings

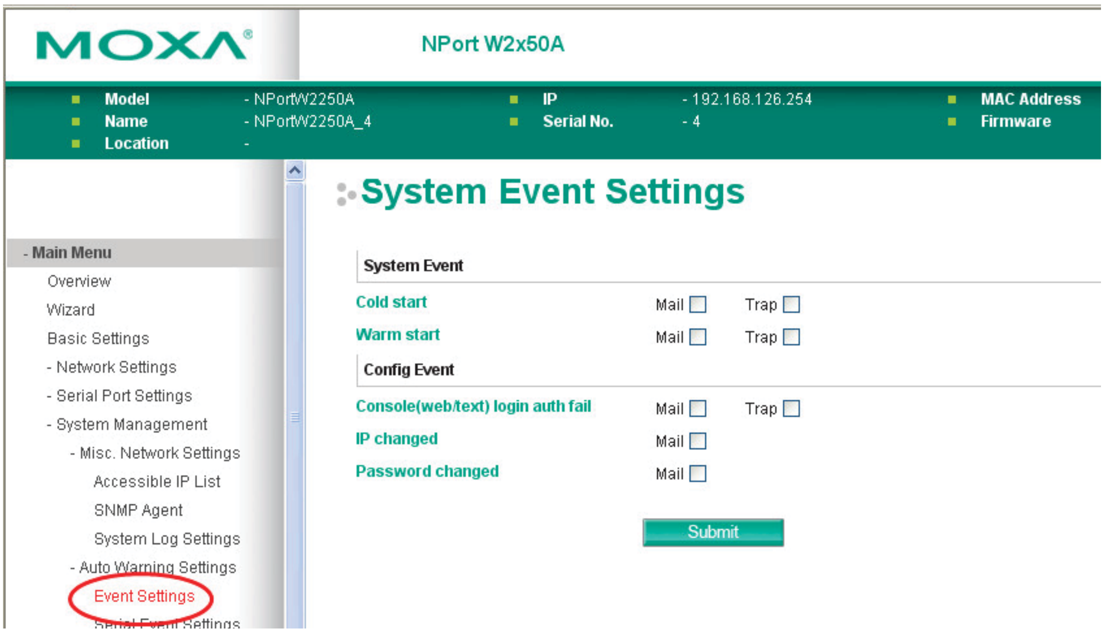
Event Group	Local Log	Summary
System	□	System Cold Start, System Warm Start
Network	□	DHCP/BOOTP Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down
Config	□	Login Fail, IP Changed, Password Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export, Wireless Certificate Import, Serial Data Log Export
OpMode	□	Connect, Disconnect, Restart

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
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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

System Event Settings

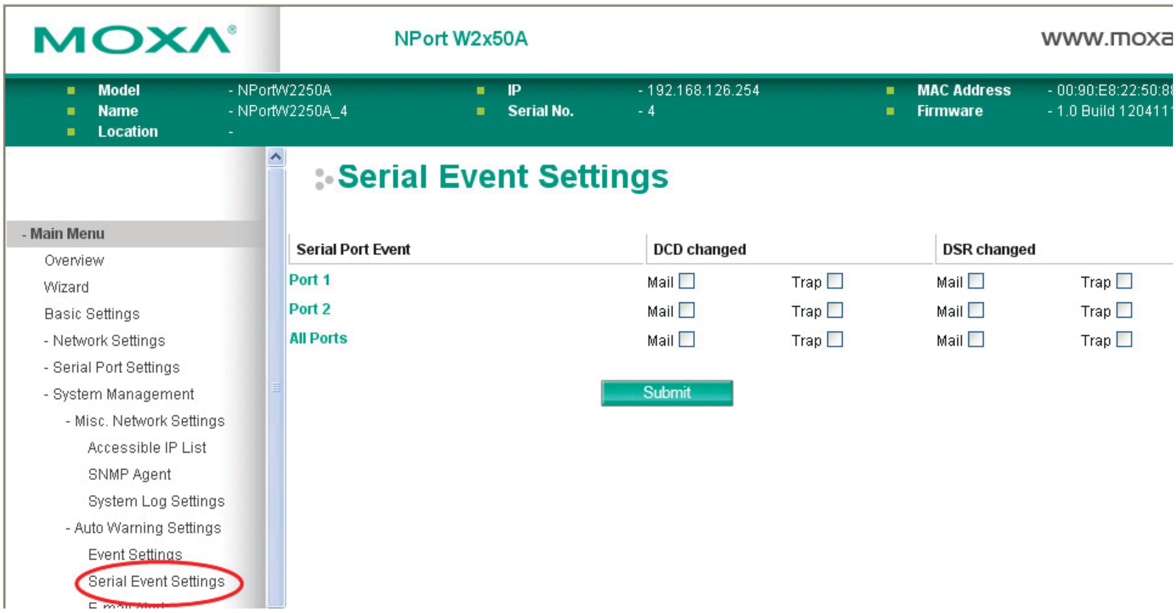
System Event
Cold start Mail □ Trap □
Warm start Mail □ Trap □

Config Event
Console(web/text) login auth fail Mail □ Trap □
IP changed Mail □
Password changed Mail □

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.
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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:8
Firmware - 1.0 Build 120411

Serial Event Settings

Serial Port Event	DCD changed		DSR changed	
Port 1	Mail □	Trap □	Mail □	Trap □
Port 2	Mail □	Trap □	Mail □	Trap □
All Ports	Mail □	Trap □	Mail □	Trap □

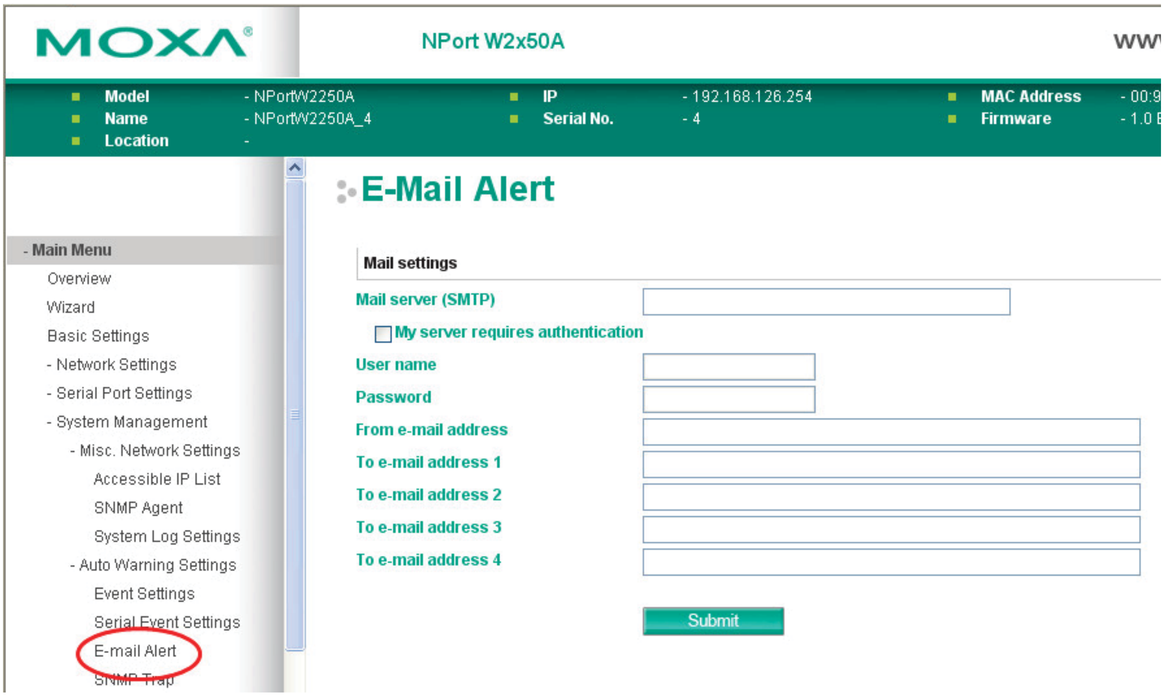
The **Serial Event Settings** page is located under **Auto Warning Settings** in the **System Management** folder. This is where you specify how the NPort will notify you of DCD and DSR events for each serial port. **Mail** refers to sending an e-mail to a specified address. **Trap** refers to sending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

E-mail Alert



Model	- NPortW2250A	IP	- 192.168.126.254	MAC Address	- 00:9
Name	- NPortW2250A_4	Serial No.	- 4	Firmware	- 1.0 E
Location	-				

E-Mail Alert

Mail settings

Mail server (SMTP)

□ My server requires authentication

User name

Password

From e-mail address

To e-mail address 1

To e-mail address 2

To e-mail address 3

To e-mail address 4

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.

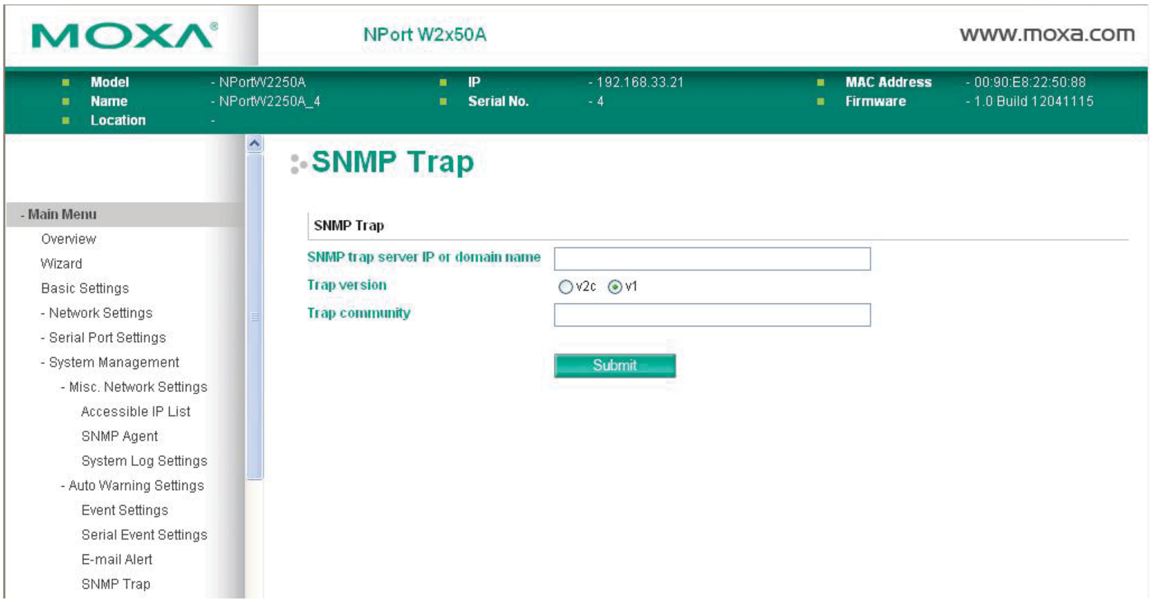
From e-mail address

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.33.21
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

SNMP Trap

SNMP Trap
SNMP trap server IP or domain name
Trap version ○ v2c ● v1
Trap community

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

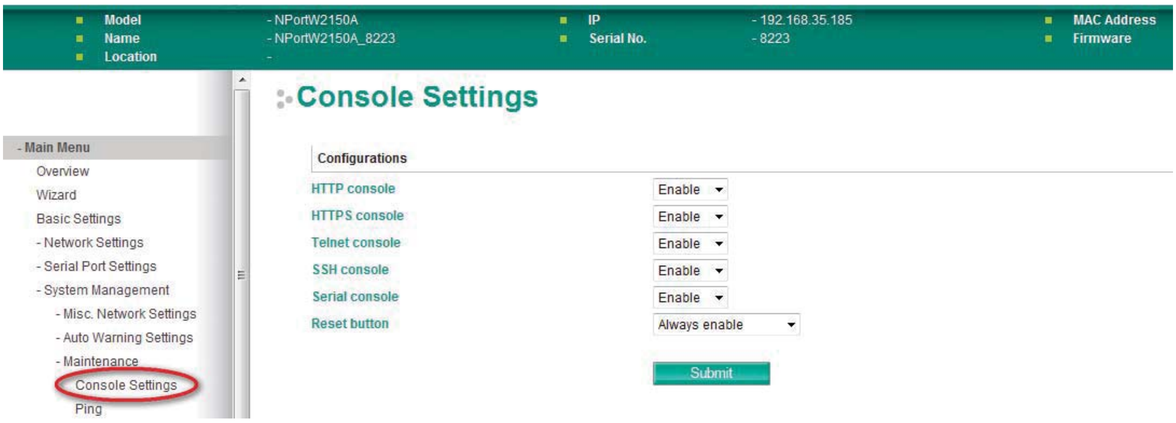
Default	v1
Options	v1, v2c
Description	This field specifies the SNMP trap version to use.

Trap Community

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

Maintenance

Console Settings



Model - NPortW2150A
Name - NPortW2150A_8223
Location -
IP - 192.168.35.185
Serial No. - 8223
MAC Address
Firmware

Console Settings

Configurations

HTTP console	Enable
HTTPS console	Enable
Telnet console	Enable
SSH console	Enable
Serial console	Enable
Reset button	Always enable

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.

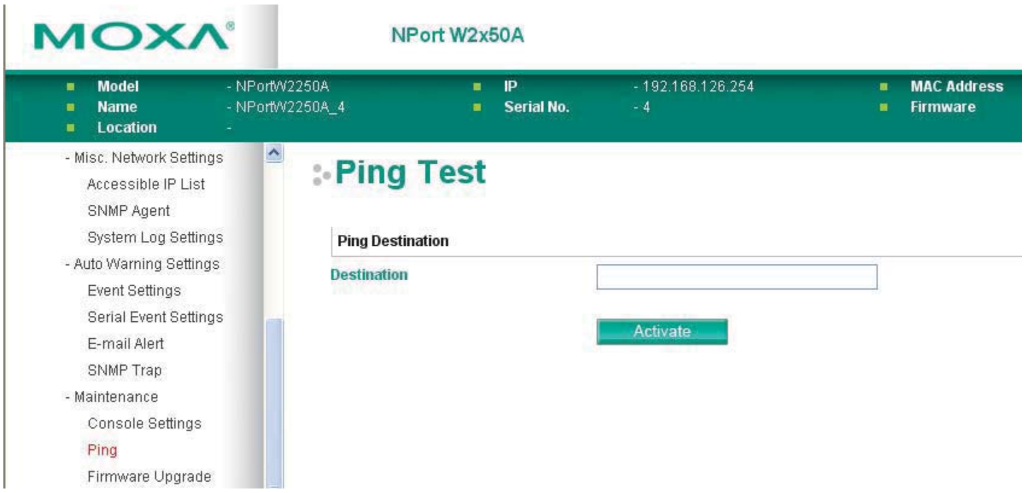
Serial Console

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

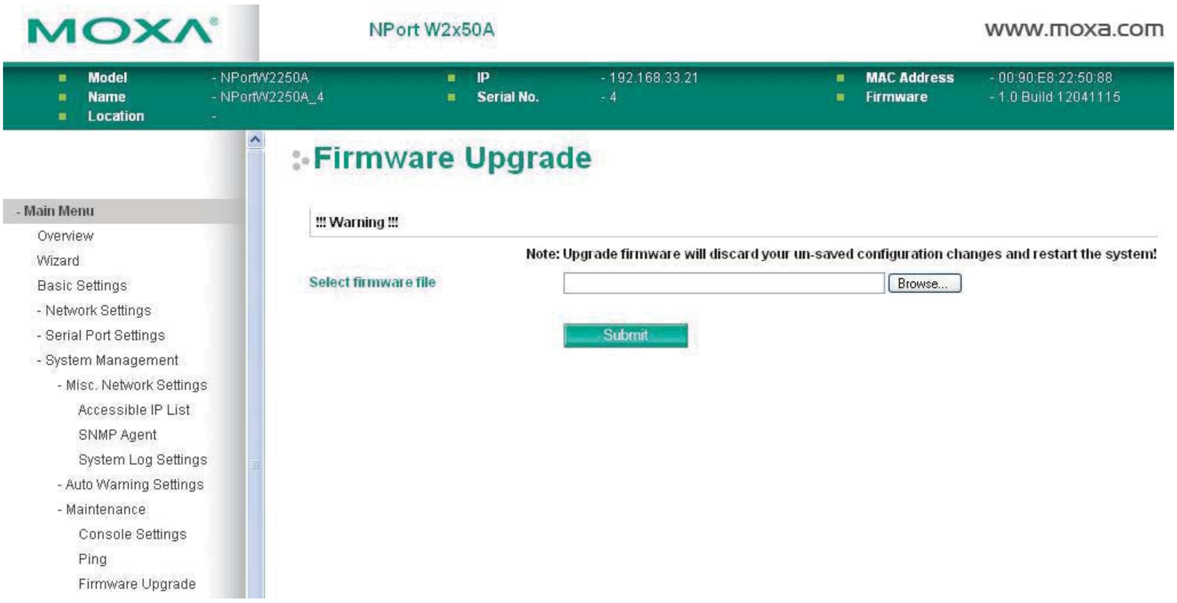
Ping Test

Ping Destination

Destination

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.33.21
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

Firmware Upgrade

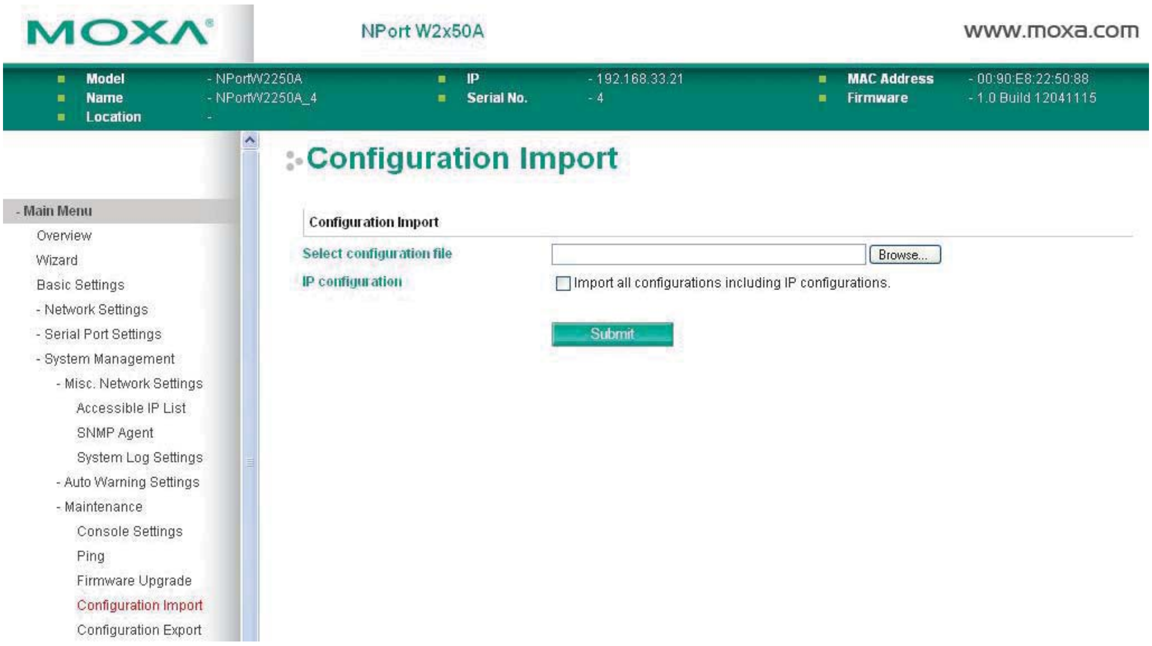
!!! Warning !!!

Note: Upgrade firmware will discard your un-saved configuration changes and restart the system!

Select firmware file

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.

Configuration Import



NPort W2x50A

www.moxa.com

Model - NPortW2250A

Name - NPortW2250A_4

Location -

IP - 192.168.33.21

Serial No. - 4

MAC Address - 00:90:E8:22:50:88

Firmware - 1.0 Build 12041115

Configuration Import

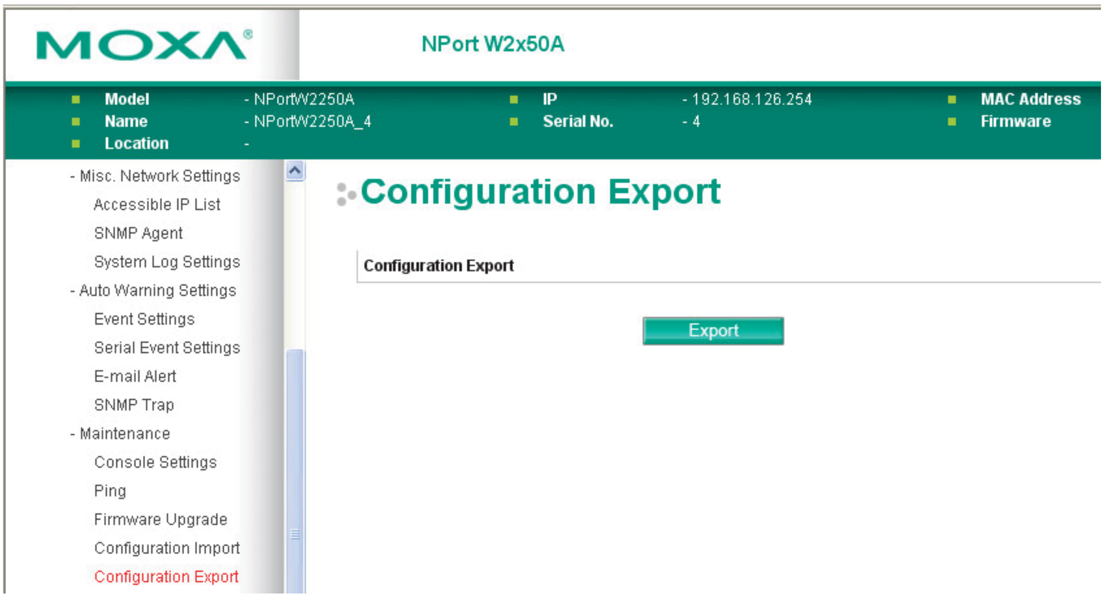
Configuration Import

Select configuration file

IP configuration ☐ Import all configurations including IP configurations.

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



NPort W2x50A

Model - NPortW2250A

Name - NPortW2250A_4

Location -

IP - 192.168.126.254

Serial No. - 4

MAC Address

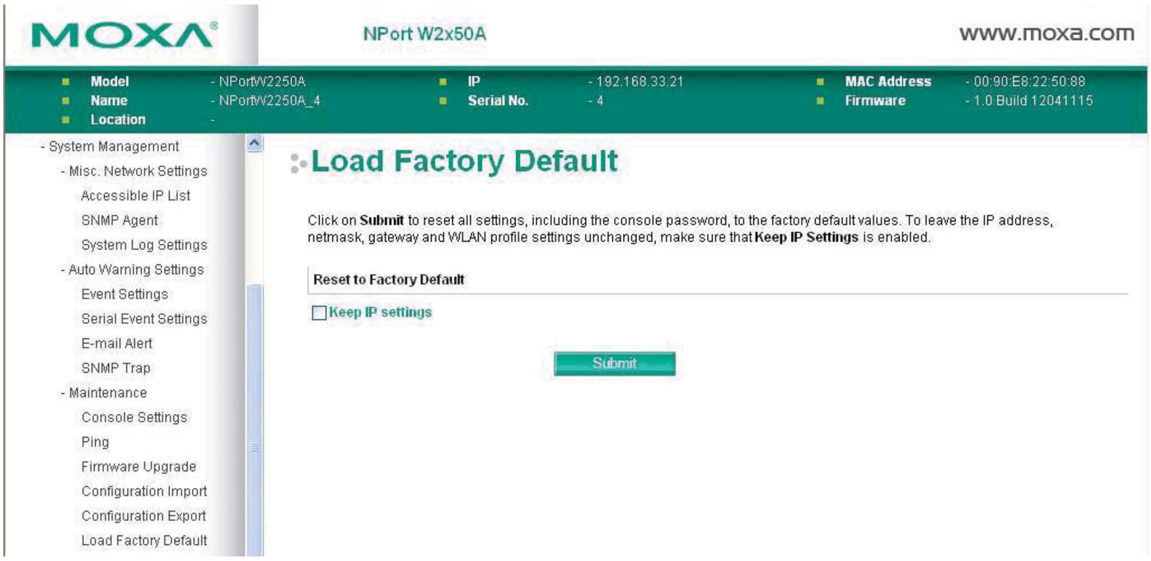
Firmware

Configuration Export

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 **[Download]** to begin the process. A window should appear asking you to open or save the configuration text file.

Load Factory Default



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.33.21
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

Load Factory Default

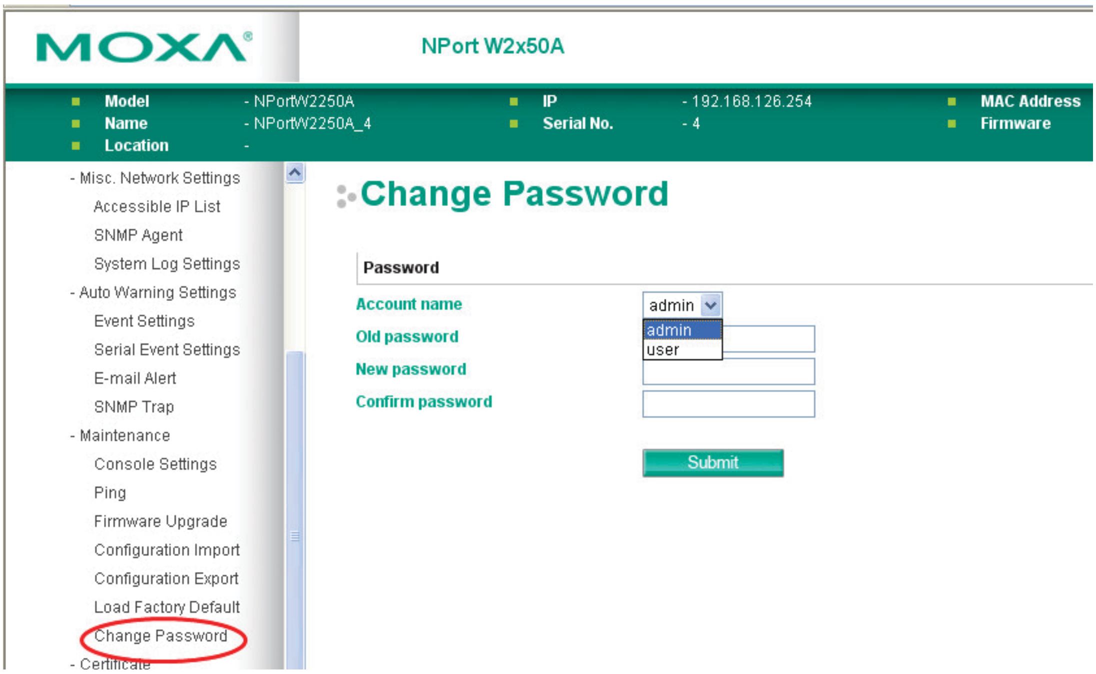
Click on **Submit** to reset all settings, including the console password, to the factory default values. To leave the IP address, netmask, gateway and WLAN profile settings unchanged, make sure that **Keep IP Settings** is enabled.

Reset to Factory Default

□ Keep IP settings

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

Change Password

Password

Account name	admin
Old password	
New password	
Confirm 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. 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.

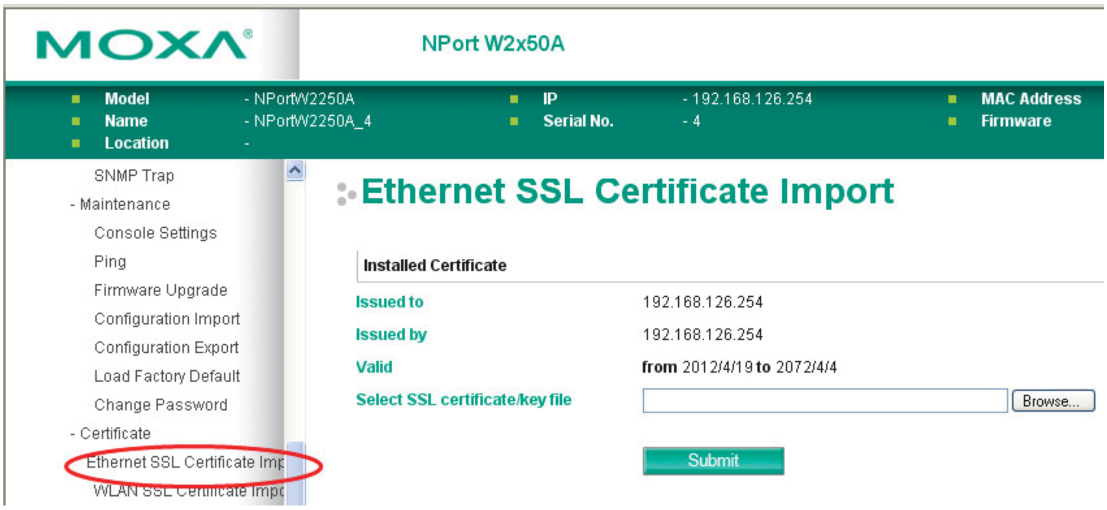
ATTENTION

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.

Certificate

Ethernet SSL Certificate Import



Ethernet SSL Certificate Import

Installed Certificate

Issued to 192.168.126.254

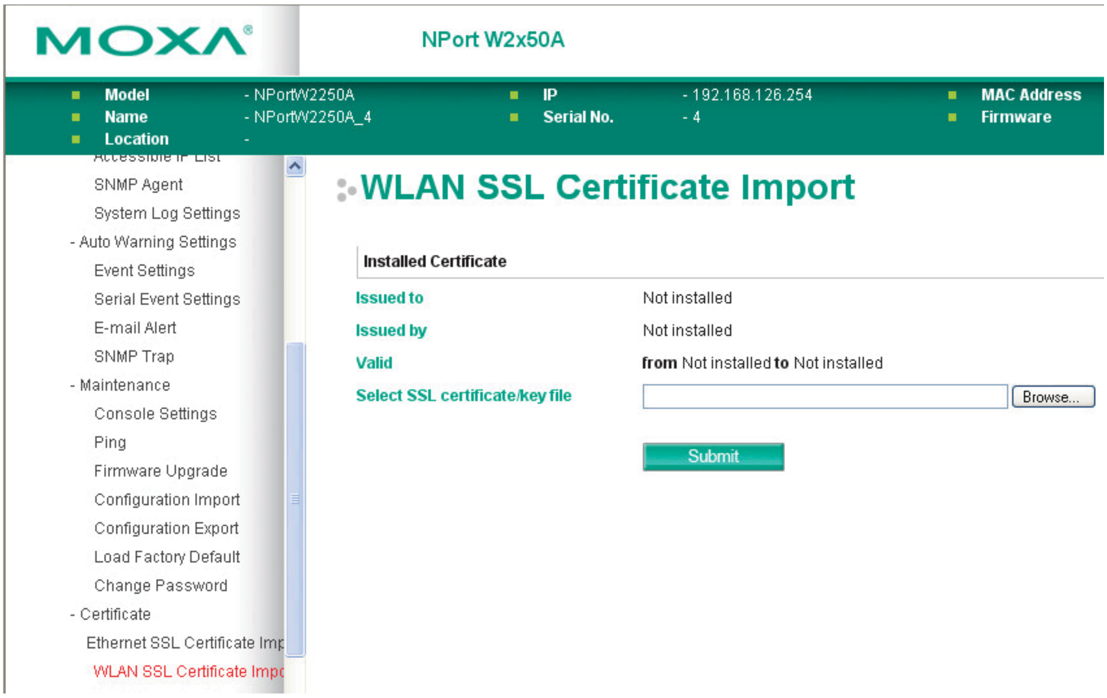
Issued by 192.168.126.254

Valid from 2012/4/19 to 2072/4/4

Select SSL certificate/key file

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. The NPort only supports the PEM format of the certificate so far. If your file is in another format, for example DER or PFX, please convert it to PEM first.

WLAN SSL Certificate Import



Model	- NPortW2250A	IP	- 192.168.126.254	MAC Address	
Name	- NPortW2250A_4	Serial No.	- 4	Firmware	
Location	-				

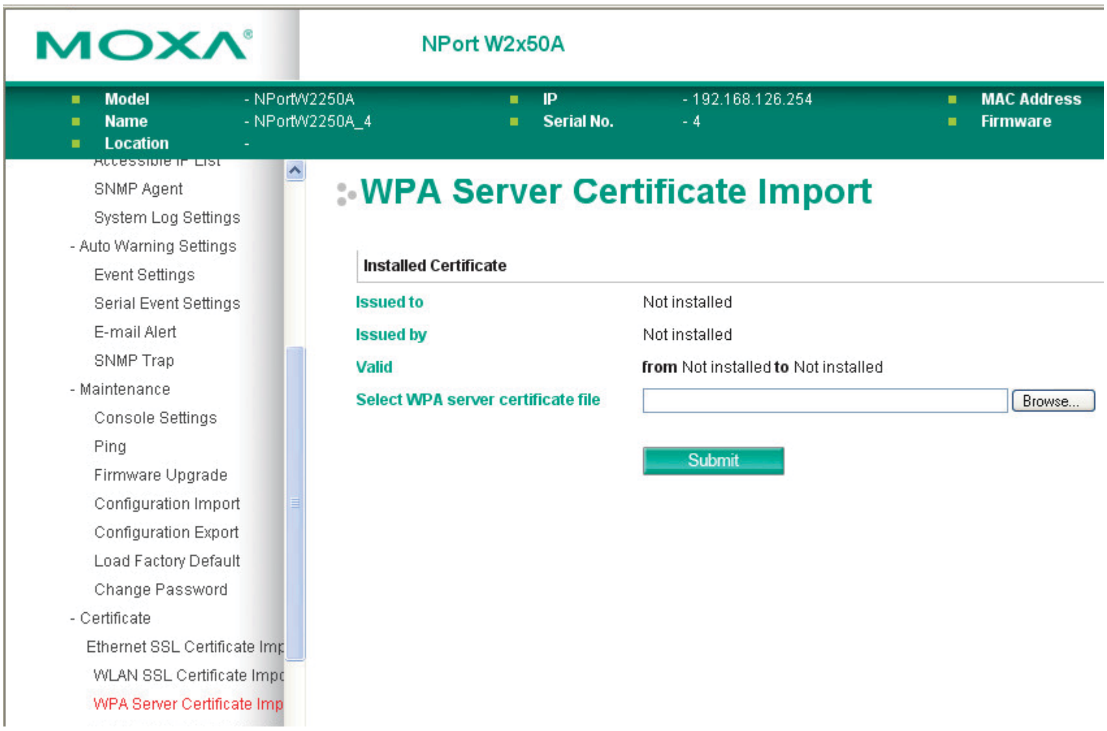
WLAN SSL Certificate Import

Installed Certificate

Issued to	Not installed
Issued by	Not installed
Valid	from Not installed to Not installed
Select SSL certificate/key file	

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



Model	- NPortW2250A	IP	- 192.168.126.254	MAC Address	
Name	- NPortW2250A_4	Serial No.	- 4	Firmware	
Location	-				

WPA Server Certificate Import

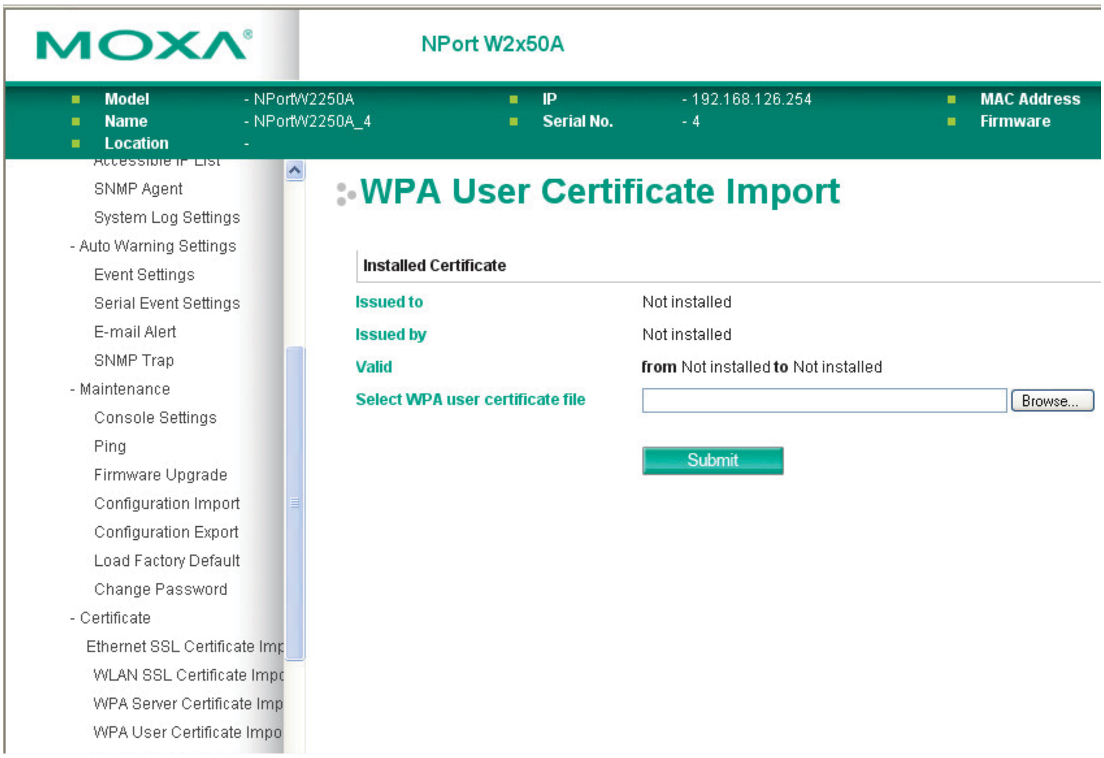
Installed Certificate

Issued to	Not installed
Issued by	Not installed
Valid	from Not installed to Not installed
Select WPA server certificate file	

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

WPA User Certificate Import

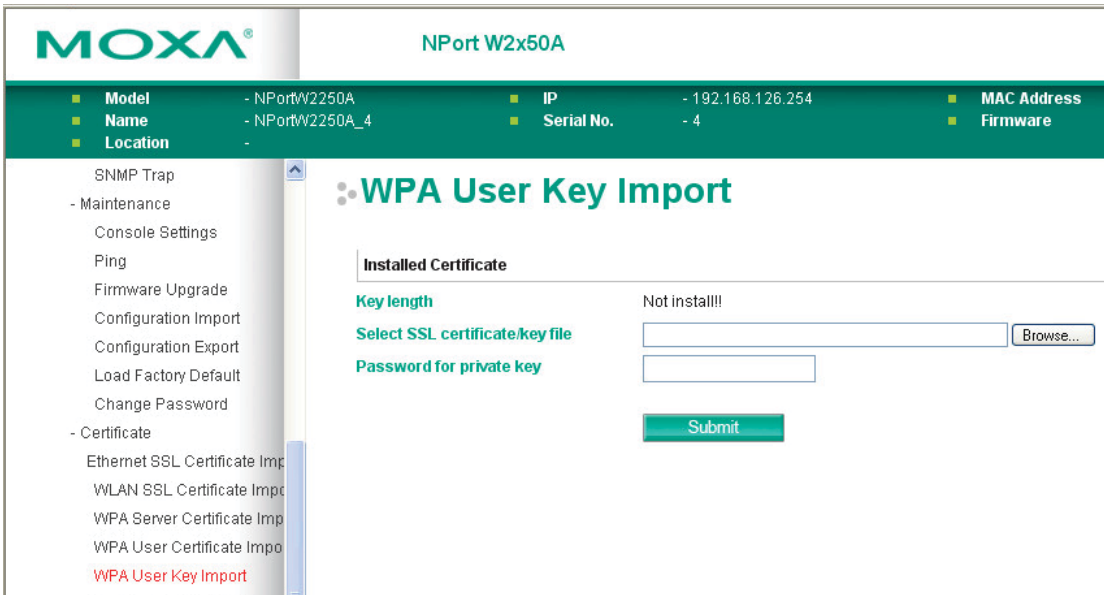
Installed Certificate

Issued to: Not installed
Issued by: Not installed
Valid: from Not installed to Not installed
Select WPA user certificate file:

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

WPA User Key Import

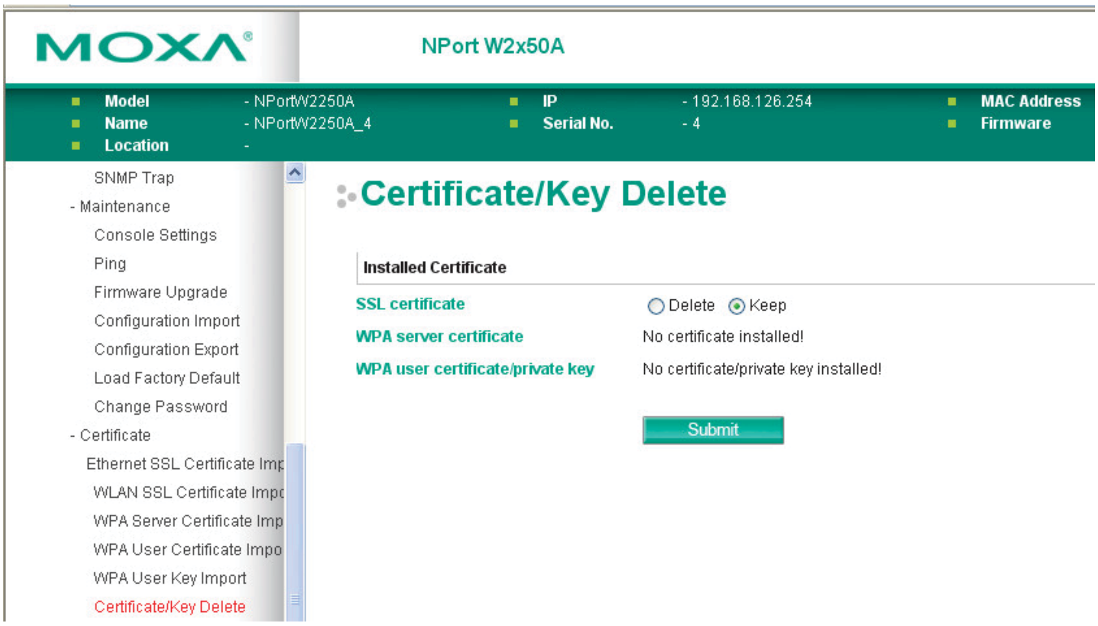
Installed Certificate

Key length: Not install!!
Select SSL certificate/key file:
Password for private key:

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

Certificate/Key Delete

Installed Certificate

SSL certificate	○ Delete ● Keep
WPA server certificate	No certificate installed!
WPA user certificate/private key	No certificate/private key installed!

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.

10

Web Console: System Monitoring

The following topics are covered in this chapter:

- ❒ **Overview**
- ❒ **System Monitoring**
  - ➢ Serial Status
  - ➢ System Status

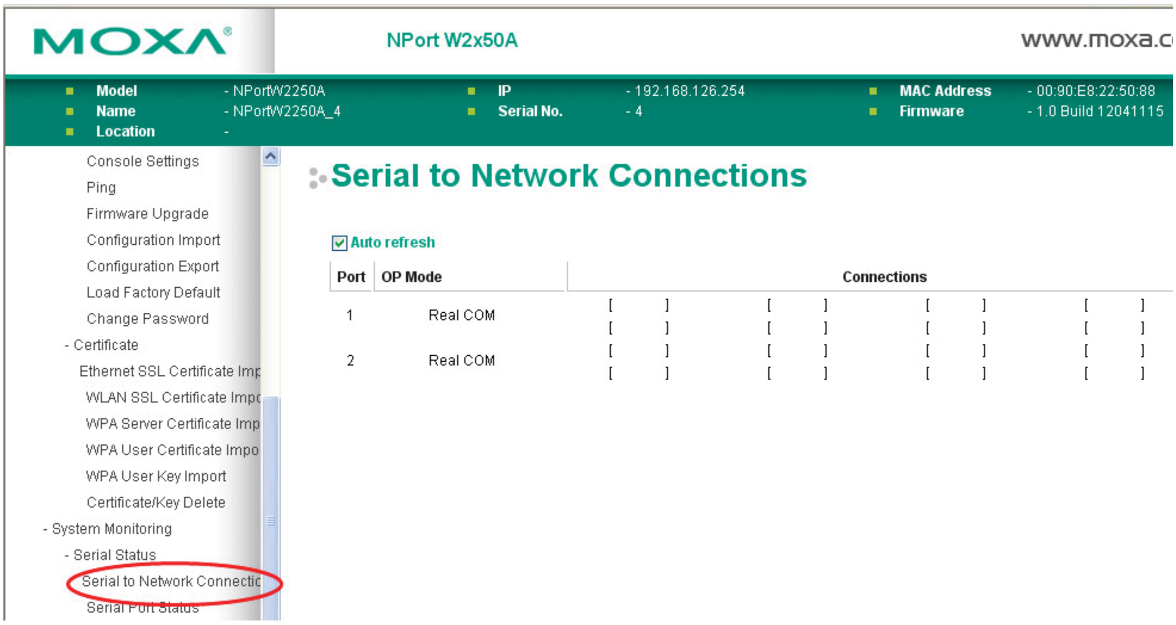
Overview

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

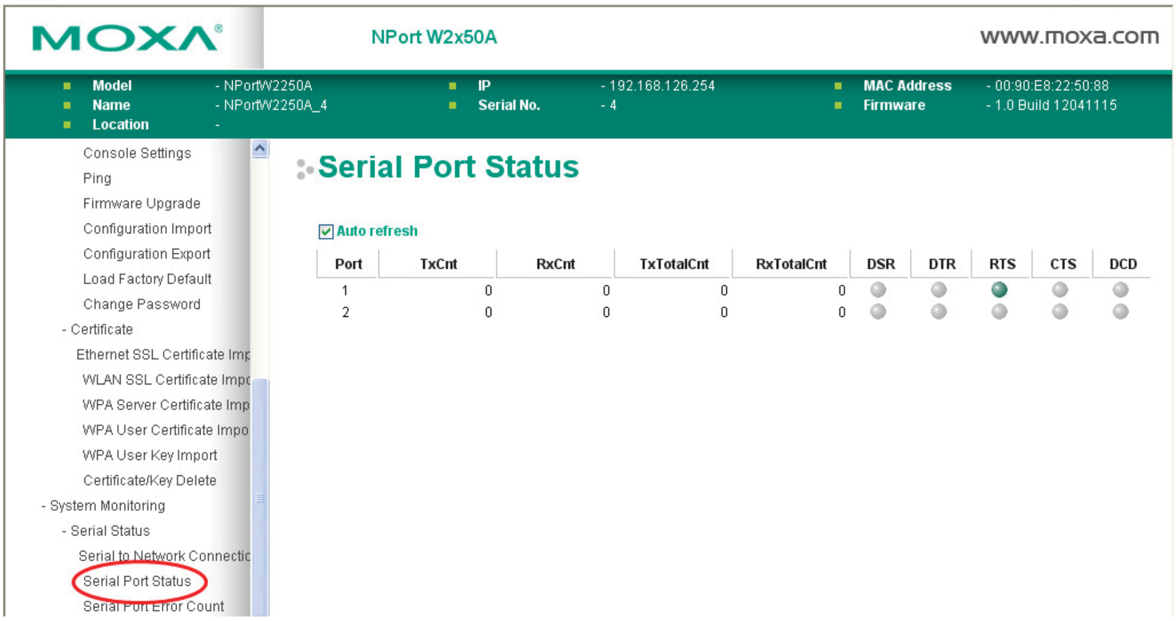
Serial to Network Connections

☑ Auto refresh

Port	OP Mode	Connections			
1	Real COM	[ ] [ ]	[ ] [ ]	[ ] [ ]	[ ] [ ]
2	Real COM	[ ] [ ]	[ ] [ ]	[ ] [ ]	[ ] [ ]

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

Serial Port Status

☑ Auto refresh

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD
1	0	0	0	0	○	○	●	○	○
2	0	0	0	0	○	○	○	○	○

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.

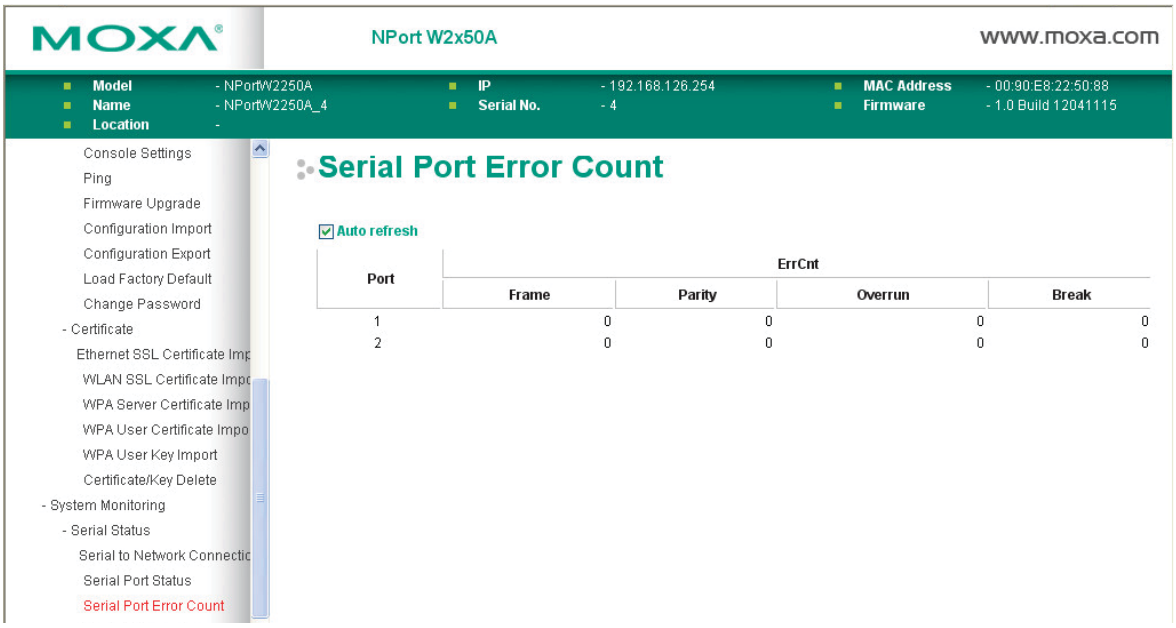
TxCnt: number of Tx packets (to device) for the current connection

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

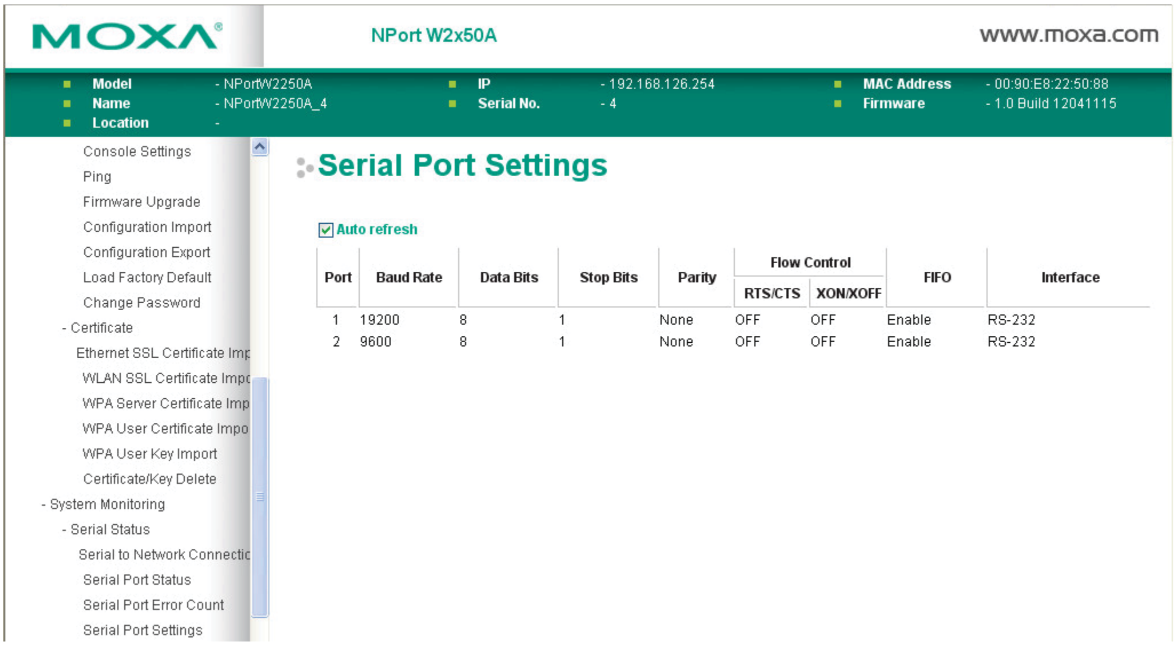
Serial Port Error Count

☑ Auto refresh

Port	ErrCnt			
	Frame	Parity	Overrun	Break
1	0	0	0	0
2	0	0	0	0

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

Serial Port Settings

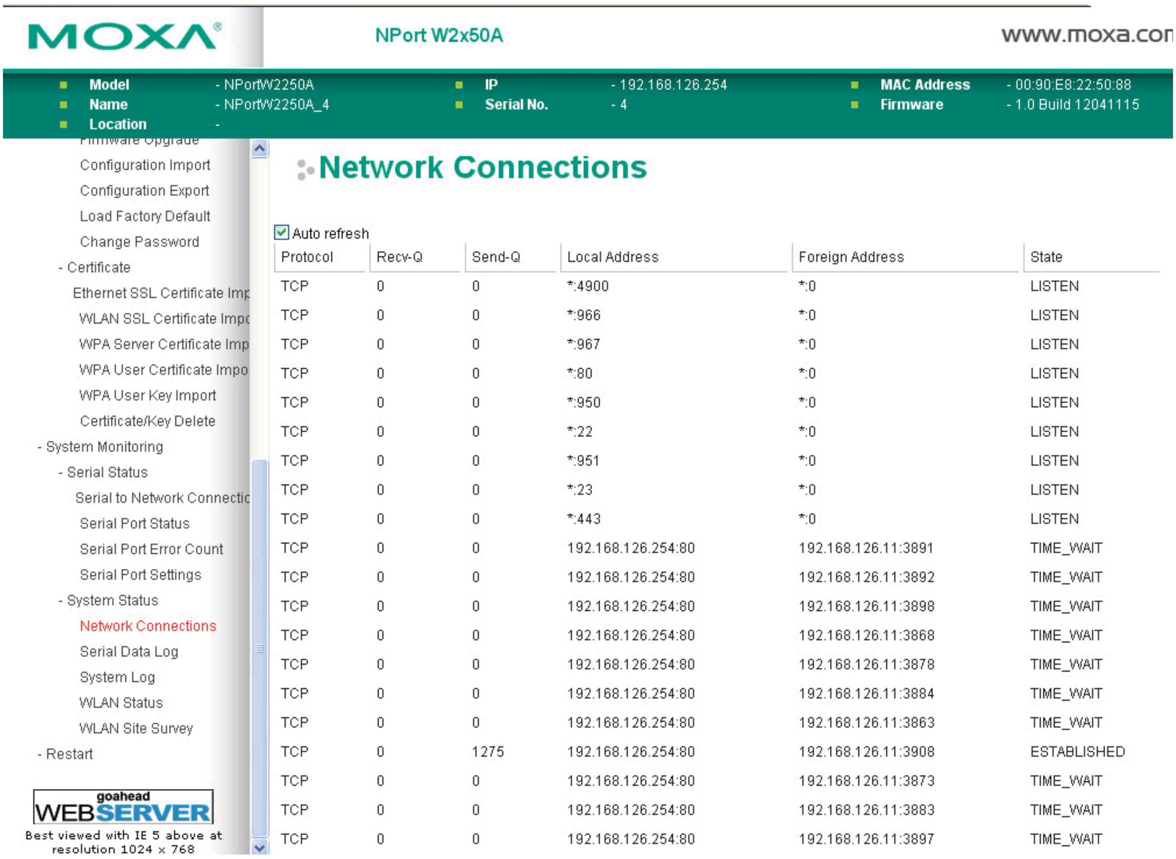
☑ Auto refresh

Port	Baud Rate	Data Bits	Stop Bits	Parity	Flow Control		FIFO	Interface
					RTS/CTS	XON/XOFF		
1	19200	8	1	None	OFF	OFF	Enable	RS-232
2	9600	8	1	None	OFF	OFF	Enable	RS-232

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

Network Connections

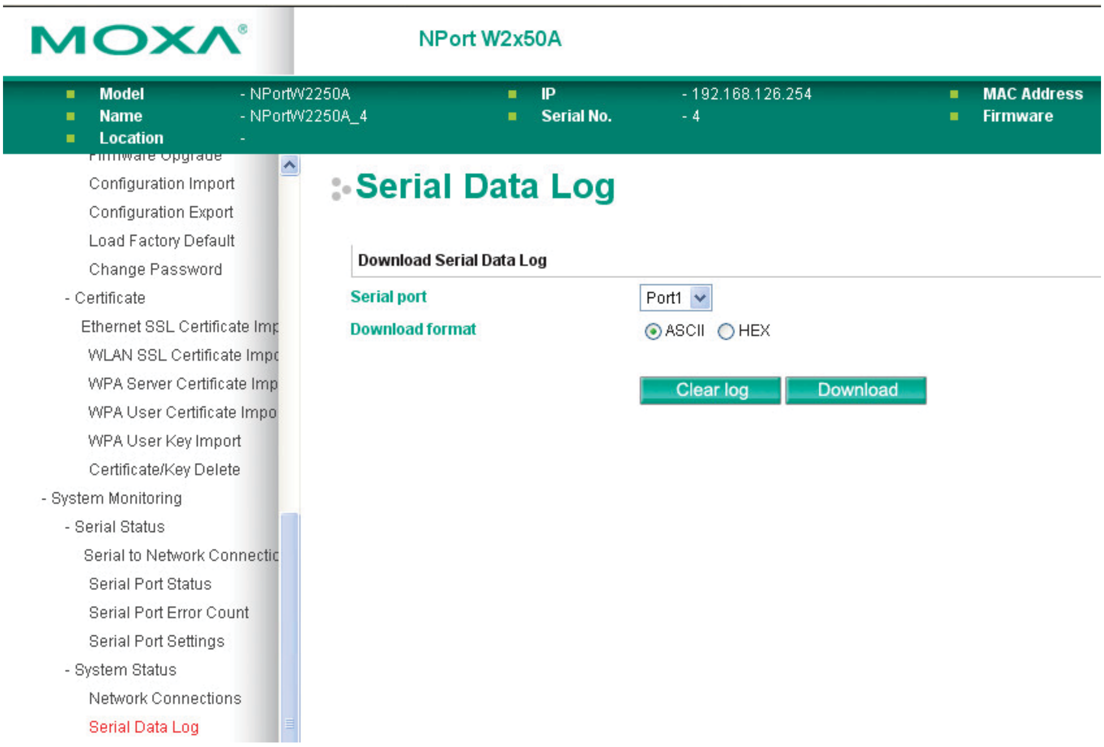
☑ Auto refresh

Protocol	Recv-Q	Send-Q	Local Address	Foreign Address	State
TCP	0	0	*:4900	*:0	LISTEN
TCP	0	0	*:966	*:0	LISTEN
TCP	0	0	*:967	*:0	LISTEN
TCP	0	0	*:80	*:0	LISTEN
TCP	0	0	*:950	*:0	LISTEN
TCP	0	0	*:22	*:0	LISTEN
TCP	0	0	*:951	*:0	LISTEN
TCP	0	0	*:23	*:0	LISTEN
TCP	0	0	*:443	*:0	LISTEN
TCP	0	0	192.168.126.254:80	192.168.126.11:3891	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3892	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3898	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3868	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3878	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3884	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3863	TIME_WAIT
TCP	0	1275	192.168.126.254:80	192.168.126.11:3908	ESTABLISHED
TCP	0	0	192.168.126.254:80	192.168.126.11:3873	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3883	TIME_WAIT
TCP	0	0	192.168.126.254:80	192.168.126.11:3897	TIME_WAIT

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.



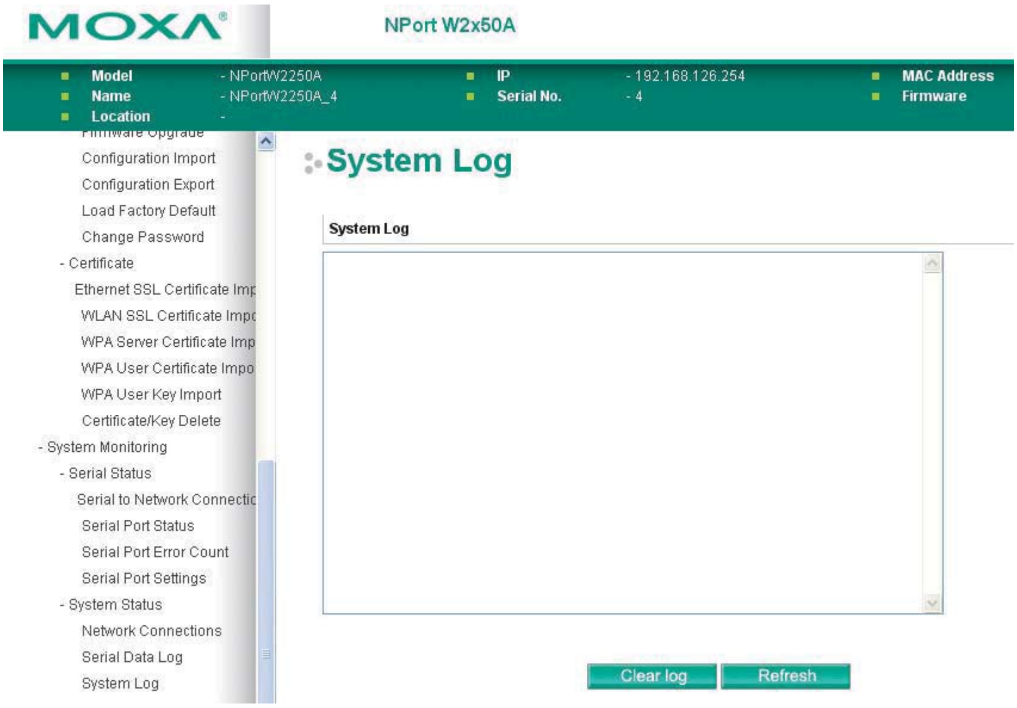
Serial port: Port1

Download format: ● ASCII ○ HEX

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.

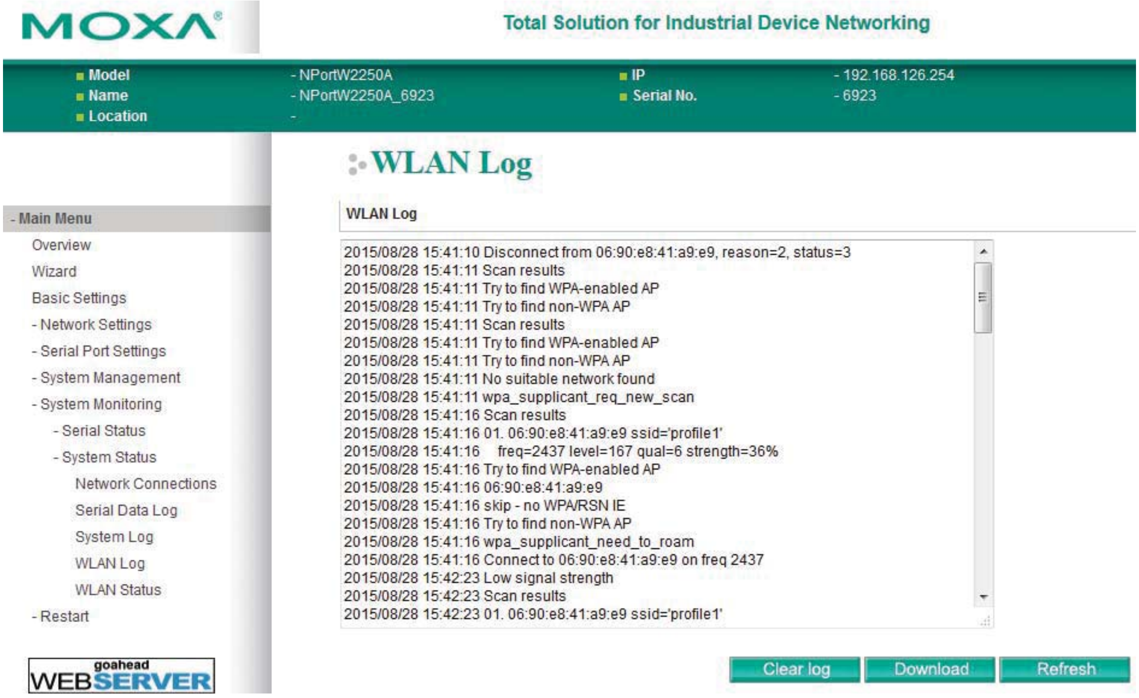
System Log



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address
Firmware

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 (This function is supported by firmware V1.10 or above)

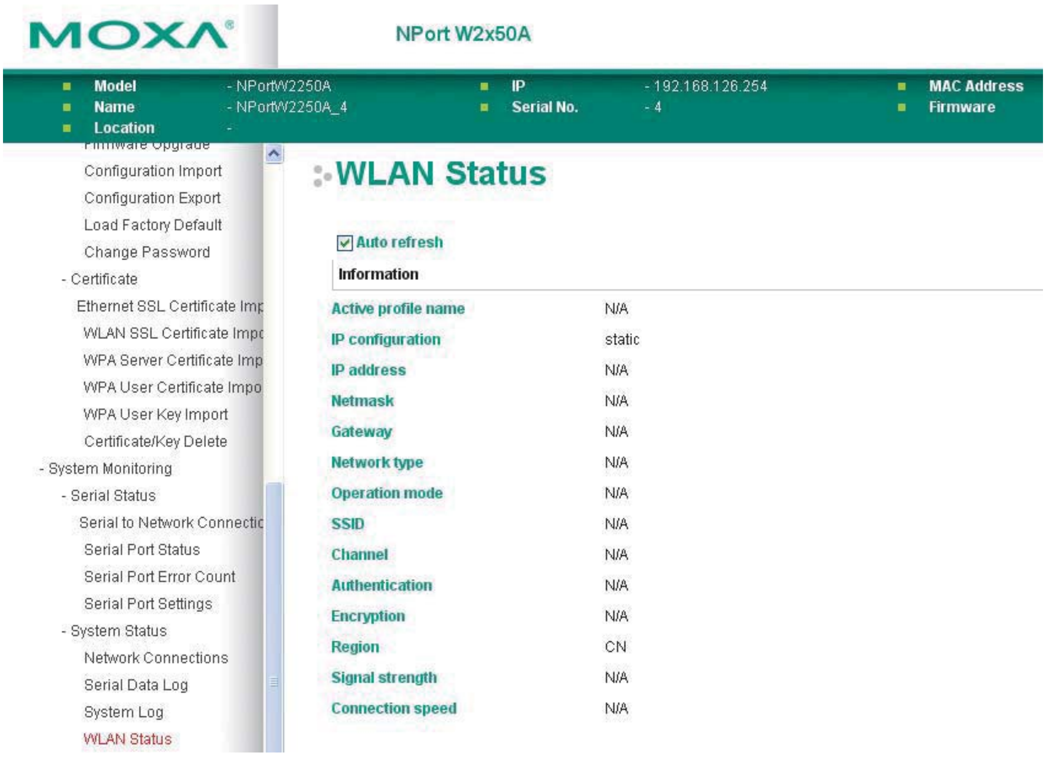


Model - NPortW2250A
Name - NPortW2250A_6923
Location -
IP - 192.168.126.254
Serial No. - 6923

```
2015/08/28 15:41:10 Disconnect from 06:90:e8:41:a9:e9, reason=2, status=3
2015/08/28 15:41:11 Scan results
2015/08/28 15:41:11 Try to find WPA-enabled AP
2015/08/28 15:41:11 Try to find non-WPA AP
2015/08/28 15:41:11 Scan results
2015/08/28 15:41:11 Try to find WPA-enabled AP
2015/08/28 15:41:11 Try to find non-WPA AP
2015/08/28 15:41:11 No suitable network found
2015/08/28 15:41:11 wpa_supplicant_req_new_scan
2015/08/28 15:41:16 Scan results
2015/08/28 15:41:16 01. 06:90:e8:41:a9:e9 ssid='profile1'
2015/08/28 15:41:16     freq=2437 level=167 qual=6 strength=36%
2015/08/28 15:41:16 Try to find WPA-enabled AP
2015/08/28 15:41:16 06:90:e8:41:a9:e9
2015/08/28 15:41:16 skip - no WPA/RSN IE
2015/08/28 15:41:16 Try to find non-WPA AP
2015/08/28 15:41:16 wpa_supplicant_need_to_roam
2015/08/28 15:41:16 Connect to 06:90:e8:41:a9:e9 on freq 2437
2015/08/28 15:42:23 Low signal strength
2015/08/28 15:42:23 Scan results
2015/08/28 15:42:23 01. 06:90:e8:41:a9:e9 ssid='profile1'
```

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



WLAN Status

☑ Auto refresh

Information

Active profile name	N/A
IP configuration	static
IP address	N/A
Netmask	N/A
Gateway	N/A
Network type	N/A
Operation mode	N/A
SSID	N/A
Channel	N/A
Authentication	N/A
Encryption	N/A
Region	CN
Signal strength	N/A
Connection speed	N/A

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.

11

Web Console: Restart

The following topics are covered in this chapter:

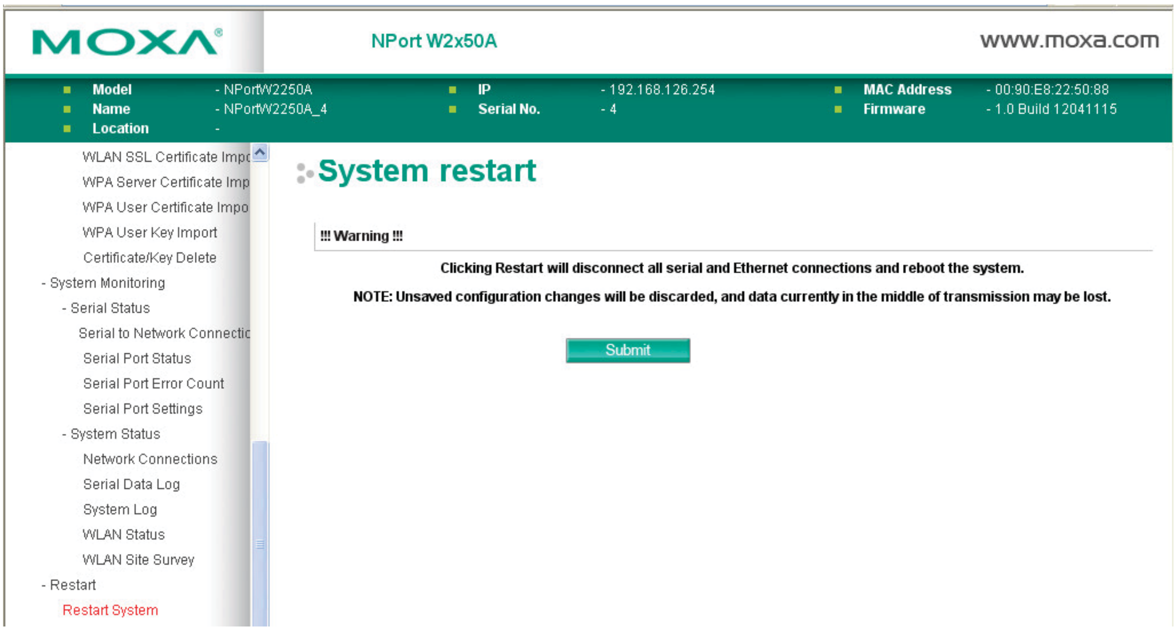
- ❒ **Overview**
- ❒ **Restart**
  - ➢ Restart System
  - ➢ Restart Ports

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



Model - NPortW2250A
Name - NPortW2250A_4
Location -
IP - 192.168.126.254
Serial No. - 4
MAC Address - 00:90:E8:22:50:88
Firmware - 1.0 Build 12041115

System restart

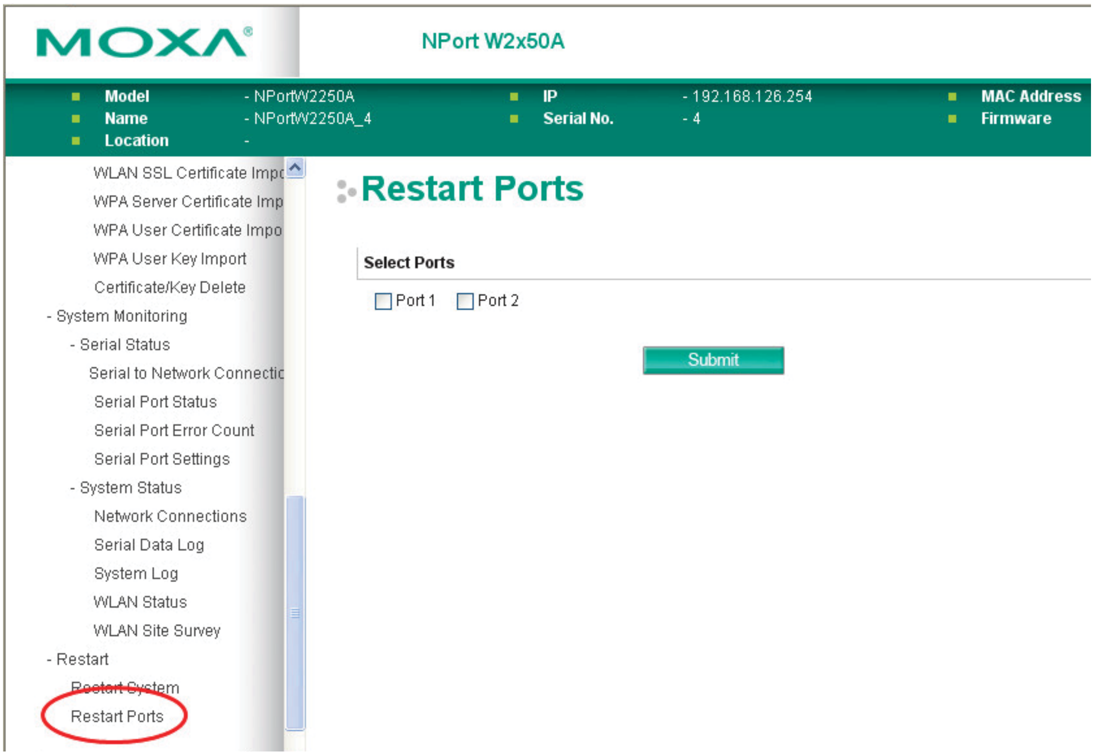
!!! Warning !!!

Clicking Restart will disconnect all serial and Ethernet connections and reboot the system.

NOTE: Unsaved configuration changes will be discarded, and data currently in the middle of transmission may be lost.

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



NPort W2x50A

- Model - NPortW2250A
- Name - NPortW2250A_4
- Location -
- IP - 192.168.126.254
- Serial No. - 4
- MAC Address
- Firmware

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.

12

Android API Instructions

The following topics are covered in this chapter:

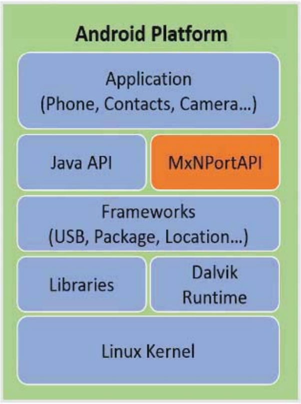
- ❒ **Overview**
  - ➢ How to Start MxNPortAPI
- ❒ **MxNPortAPI Function Groups**
- ❒ **Example Program**

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.

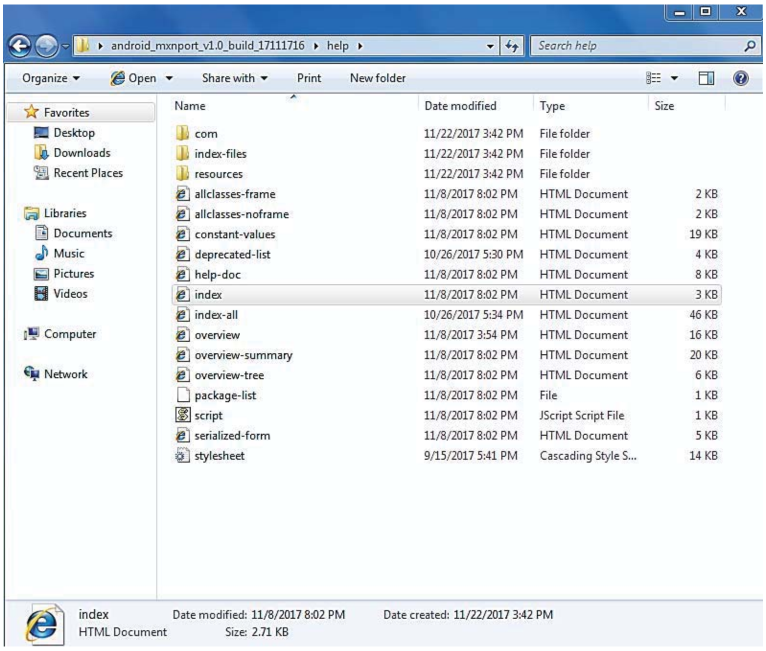


How to Start MxNPortAPI

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).

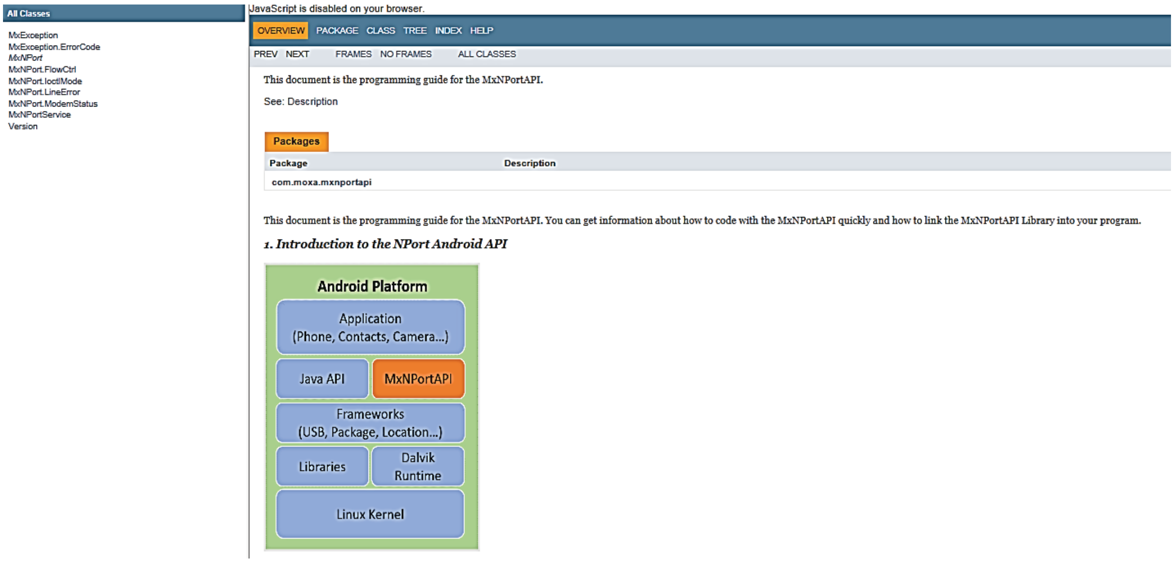
To start your application program, please unzip the MxNPortAPI file and refer to the index (.html) under the Help directory.



Name	Date modified	Type	Size
com	11/22/2017 3:42 PM	File folder	
index-files	11/22/2017 3:42 PM	File folder	
resources	11/22/2017 3:42 PM	File folder	
allclasses-frame	11/8/2017 8:02 PM	HTML Document	2 KB
allclasses-noframe	11/8/2017 8:02 PM	HTML Document	2 KB
constant-values	11/8/2017 8:02 PM	HTML Document	19 KB
deprecated-list	10/26/2017 5:30 PM	HTML Document	4 KB
help-doc	11/8/2017 8:02 PM	HTML Document	8 KB
index	11/8/2017 8:02 PM	HTML Document	3 KB
index-all	10/26/2017 5:34 PM	HTML Document	46 KB
overview	11/8/2017 3:54 PM	HTML Document	16 KB
overview-summary	11/8/2017 8:02 PM	HTML Document	20 KB
overview-tree	11/8/2017 8:02 PM	HTML Document	6 KB
package-list	11/8/2017 8:02 PM	File	1 KB
script	11/8/2017 8:02 PM	JScript Script File	1 KB
serialized-form	11/8/2017 8:02 PM	HTML Document	5 KB
stylesheet	9/15/2017 5:41 PM	Cascading Style S...	14 KB

index
HTML Document
Date modified: 11/8/2017 8:02 PM
Size: 2.71 KB
Date created: 11/22/2017 3:42 PM

For more details about the installation, please refer to the Overview section.



JavaScript is disabled on your browser.

This document is the programming guide for the MxNPortAPI.

See: Description

Packages

Package	Description
com.moxa.mxnportapi	

This document is the programming guide for the MxNPortAPI. You can get information about how to code with the MxNPortAPI quickly and how to link the MxNPortAPI Library into your program.

1. Introduction to the NPort Android API

MxNPortAPI Function Groups

The supported functions in this API are listed below:

Port Control	Input/Output	Port Status Inquiry	Miscellaneous
open close setIoctlMode setFlowCtrl setBaud setRTS setDTR flush	read write	getBaud getFlowCtrl getIoctlMode getLineStatus getModemStatus getOQueue	setBreak

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
SysObjectID
SysUpTime
SysContact
SysName
SysLocation
SysServices

Interfaces MIB

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

IP MIB

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

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
rs232AsyncPortEntry
rs232AsyncPortIndex
rs232AsyncPortBits
rs232AsyncPortStopBits
rs232AsyncPortParity

The Input Signal Table

rs232InSigTable
rs232InSigEntry
rs232InSigPortIndex
rs232InSigName
rs232InSigState

The Output Signal Table

rs232OutSigTable
rs232OutSigEntry
rs232OutSigPortIndex
rs232OutSigName
rs232OutSigState

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

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 provided 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 a 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-W2X50A "

Information for the OEMs and Integrators

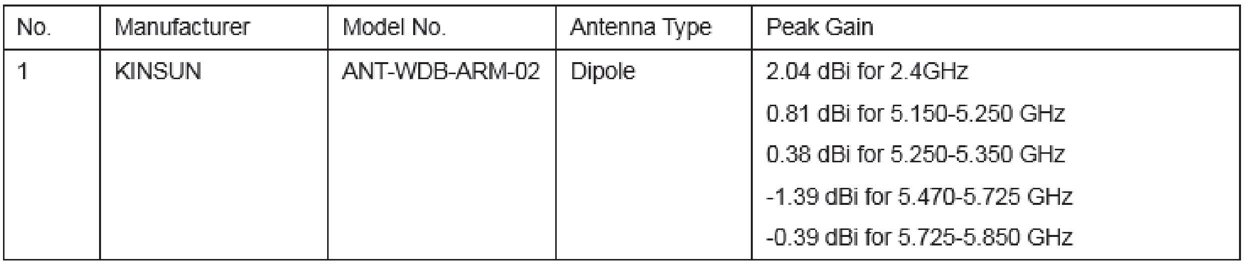
The following statement must be included with all versions of this document supplied to an

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 FCCID: SLE-W2X50A 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	Dipole	2.04 dBi for 2.4GHz 0.81 dBi for 5.150-5.250 GHz 0.38 dBi for 5.250-5.350 GHz -1.39 dBi for 5.470-5.725 GHz -0.39 dBi for 5.725-5.850 GHz

E

FCC Warning Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

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 party responsible for compliance could void the user's authority to operate the equipment. The operation frequency of the device is in the 5150-5250 MHz band and is for indoor use only.

Prohibition of Co-location

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Safety Information

To maintain compliance with FCC's RF exposure guidelines, when installing and/or operating this equipment, you should maintain a minimum distance of 20 cm between the transmitter and your body. Use only the supplied antenna. Unauthorized antennae, modifications, or attachments could damage the transmitter and may violate FCC regulations.