The Security Hardening Guide for the NPort W2x50A-W4 Series

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Jul 22, 2025

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa

Tel: 1-714-528-6777
Fax: 1-714-528-6778

1 Introduction

This document provides guidelines on configuring and securing the NPort W2x50A-W4 Series. Consider the recommendations in this document as best practices for securing the device in most applications. We highly recommend thoroughly reviewing and testing the configurations before implementing them in your production system to ensure your applications remain unaffected.

2 General System Information

2.1 Basic Information About the Device

Model	Function	Firmware Version
NPort W2150A-W4	Device server	Version 1.5
NPort W2250A-W4	Device server	Version 1.5
NPort W2150A-W4-T	Device server	Version 1.5
NPort W2250A-W4-T	Device server	Version 1.5

2.2 Deployment of the Device

Deploy the NPort W2x50A-W4 Series behind a secure firewall or/and housed in a locked cabinet to ensure continuous protection from internal and external threats. Those who purchase from Moxa or its resellers should check for updated firmware offering enhanced security. Check Moxa's support website for newer firmware. If so, we recommend upgrading the firmware to the newest. Make sure that the physical protection of the NPort W2x50A-W4 devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.

2.3 Security Threats and Measures

The security threats that can harm NPort W2x50A-W4 Series are:

Threat 1: Attacks over the network

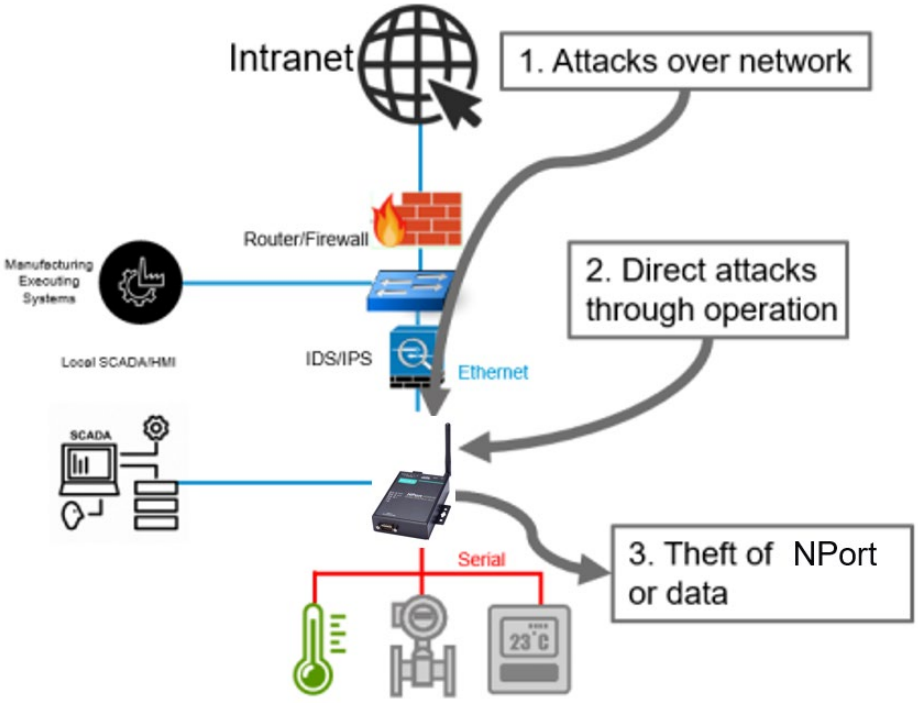
Threats from individuals with no rights to the NPort W2x50A-W4 Series via networks such as intranets.

Threat 2: Direct attacks through operation

Threats involving unauthorized individuals physically accessing the NPort W2x50A-W4 Series to manipulate the system or steal sensitive data.

Threat 3: Theft of the NPort or data

Someone steals NPort W2x50A-W4 Series devices or data and analyzes the important data.



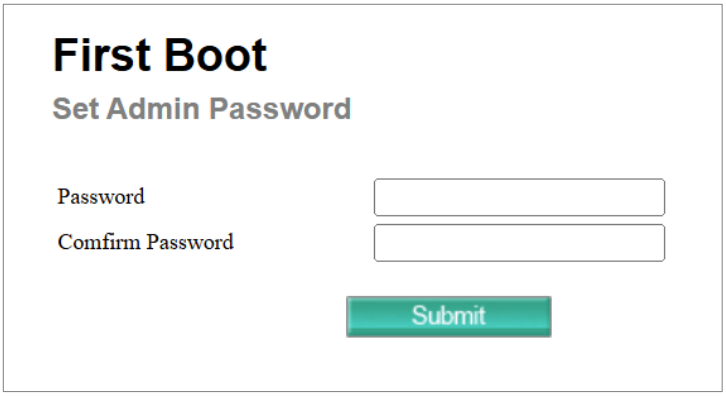
To protect against security threats, we implemented a secure network environment and defined security measures for the NPort W2x50A-W4 Series. This table shows which security measures address specific threats. To protect the NPort W2x50A-W4 and its data from theft, we advise using the NPort W2x50A-W4 Series on a secure local network. We recommend enabling the firewall function to restrict access.

Security Layer	Security Measure	Threat Mitigated/Handled				Responsibility
		Description	1	2	3	
Policy and Procedure	Establish policies and procedures to guide employees in their role and responsibilities for safe use of security sensitive assets	Vulnerabilities created because of employees' lack of security policies and awareness of procedures	Yes	Yes	Yes	Asset Owner
Perimeter Security	Physical security	Physical modification, manipulation, theft, removal, or destruction of asset	No	Yes	Yes	Asset Owner
Network Security	Network firewall	Unauthorized and malicious communications from untrusted network	Yes	Yes	Yes	Asset Owner
	Network IDS/IPS	Network attacks from various sources, such as DoS.	Yes	No	No	Asset Owner
Device Security	Account management	Unauthorized operation of the NPort	Yes	Yes	No	Provided by the NPort
	Service management	Potential cyberattacks	Yes	Yes	No	Provided by the NPort
	Accessible IP List	Unauthorized operation of NPort	Yes	Yes	No	Provided by the NPort
	Login Policy	Trial-and-error attack attempting to crack login credentials or unauthorized operation of the device	Yes	Yes	No	Provided by the NPort

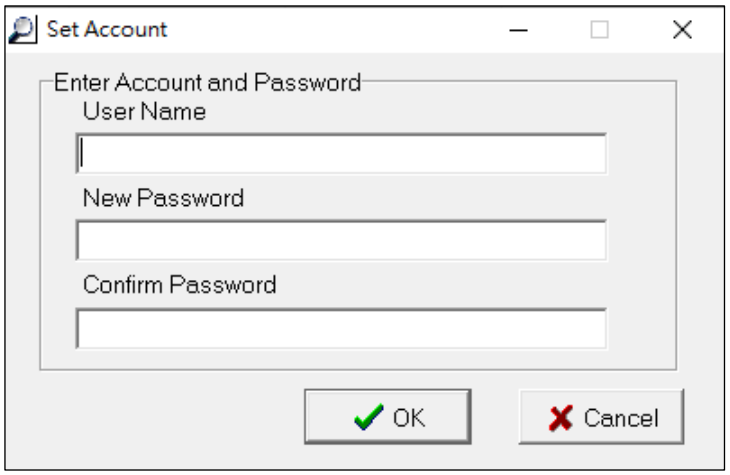
3 Configuration and Hardening Information

For security reasons, there is no default password. Upon first accessing the NPort W2x50A-W4, you must create a password for the default username **admin** using the Device Search Utility (DSU) or the web console before logging in.

Web console



Device Search Utility



3.1 TCP/UDP Ports and Recommended Services

Refer to the table below for all the ports, protocols, and services that are used to communicate between the NPort W2x50A-W4 Series and other devices.

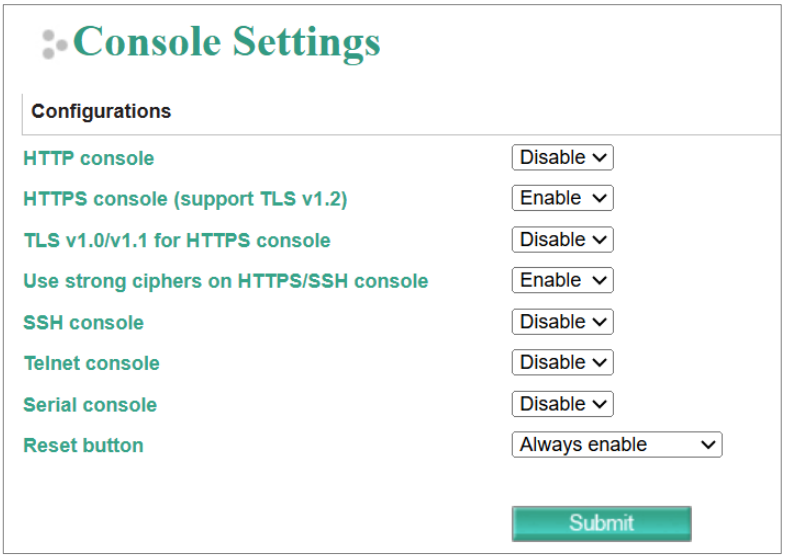
Service Name	Option	Default Settings	Type	Port Number	Description
Moxa service	Enable	Enable	TCP	4900	For Moxa utility communication
			UDP	4800	
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
HTTP server	Enable/ Disable	Disable	TCP	80	Web console
HTTPS server	Enable/ Disable	Enable	TCP	443	Web console
SSH server	Enable/ Disable	Disable	TCP	22	SSH console
Telnet server	Enable/ Disable	Disable	TCP	23	Telnet console
SNTP	Enable/ Disable	Disable	UDP	Random port	Synchronize time settings with a time server

Operation Mode	Option	Default Settings	Type	Port Number
Real COM Mode	Enable/ Disable	Enable	TCP	949+ (Serial port No.) 965+ (Serial port No.)
RFC2217 Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)
TCP Server Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.) User-defined (default: 965+Serial Port No.)
UDP Mode	Enable/ Disable	Disable	UDP	User-defined (default: 4000+Serial Port No.)
Pair Connection Slave Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)
Ethernet Modem Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)
Reverse Terminal Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)

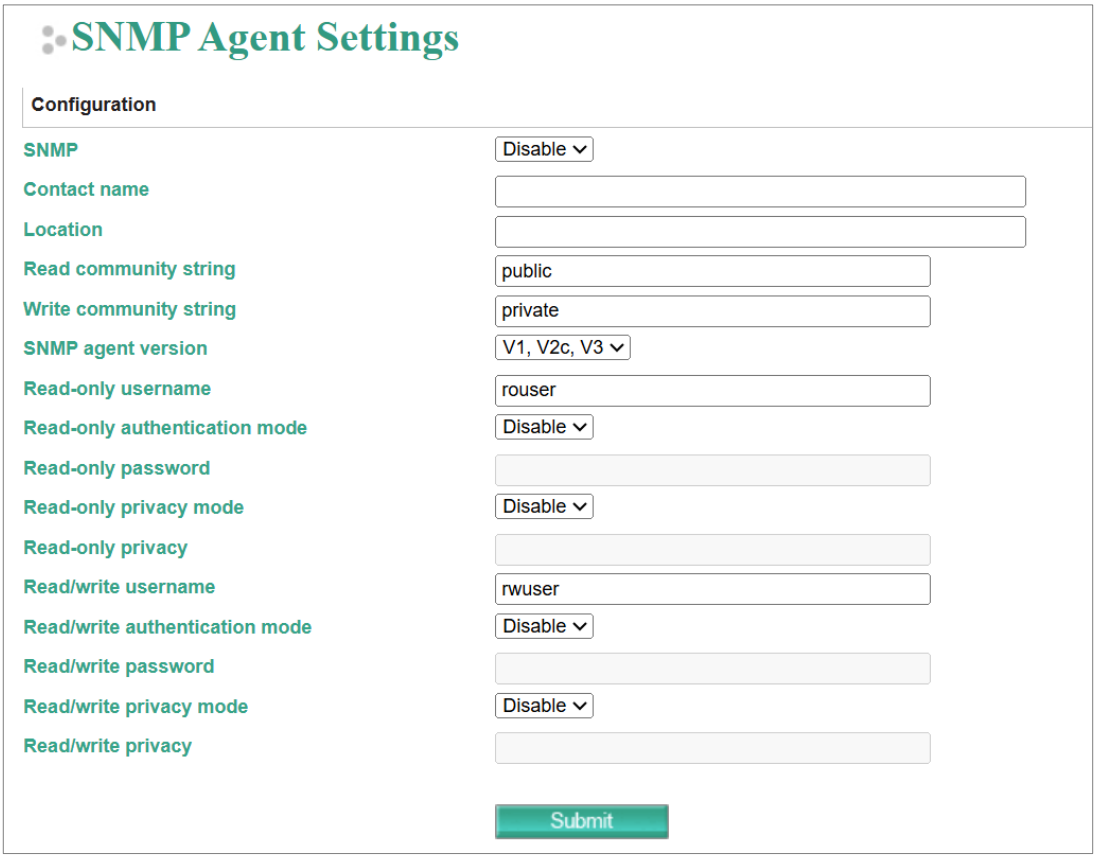
For security reasons, consider disabling unused services. After the initial setup, use services with stronger security for data communication. Refer to the table below for the suggested settings.

Service Name	Suggested Settings	Type	Port Number	Description
SNMP agent	Disable	UDP	161	We suggest you manage the NPort via HTTPS console
HTTP server	Disable	TCP	80	Disable HTTP to prevent plain text transmission
HTTPS server	Enabled	TCP	443	Encrypted data channel with a trusted certificate for NPort configuration
SSH server	Disabled	TCP	22	Disable the service if you don't need remote access to the device for configuration.
Telnet server	Disabled	TCP	23	Disable this service as it is not commonly used
SNTP	Disabled	UDP	Random port	We suggest you use the SNTP server for secure time synchronization

To enable or disable these services, log in to the HTTP/HTTPS console and select **System Management > Maintenance > Console Settings**.

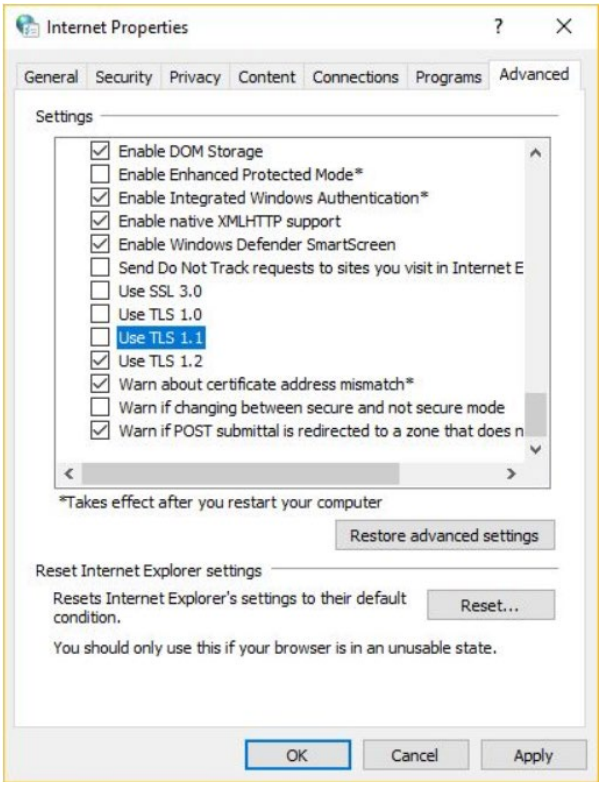


To enable or disable the SNMP agent service, log in to the HTTPS console and select **System Management > Misc. Network Settings > SNMP Agent**, then select Disable for SNMP.



3.2 HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. Since TLS v1.1 or lower has severe vulnerabilities that can easily be hacked, the NPort W2x50A-W4 Series uses TLS v1.2 for HTTPS to ensure data transmissions are secured. Make sure your browser has TLS v1.2 enabled.



To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority.

Log in to the HTTP/HTTPS console and select **System Management > Certificate**. Generate an up-to-date valid certificate by importing a third-party trusted SSL certificate or generating the "NPort self-signed" certificate.

- Behavior of the System Certificate on an NPort W2x50A-W4 device
  - NPort devices can auto-generate a self-signed SSL certificate. We recommend importing SSL certificates that are certified by a trusted third-party Certificate Authority (CA) or by an organization's CA.
  - The length of the NPort device's self-signed private keys is 1,024 bits, which should be compatible with most applications. Some applications may need a longer key, such as 2,048 bits, requiring importing a third-party certificate. Note that longer keys mean browsing the web console will be slower because of the increased complexity of encrypting and decrypting communicated data.

- For the NPort self-signed certificate:

  If a certificate has expired, regenerate the NPort self-signed certificate with the following steps.

  - Step 1. Select **System Management > Certificate > Certificate/Key Deletion**. Delete the current SSL certificate issued by the NPort device.
  - Step 2. Enable the NTP server and set up the time zone and local time.
  - Step 3. After restarting the device, the NPort self-signed certificate will be regenerated with a new expiration date.

- Importing the third-party trusted SSL certificate:

  By importing the third-party trusted SSL certificate, the security level can be enhanced. A snapshot of the GUI for the web console is shown below. To generate the SSL certificate through the third party, follow these steps:

  - Step 1. Create a certification authority (Root CA), such as Microsoft AD Certificate Service (https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/)
  - Step 2. Find a tool to issue a certificate signing request (CSR) file. Get one from a third-party CA company such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).
  - Step 3. Submit the CSR file to a public certification authority to get a signed certificate.
  - Step 4. Import the certificate to the NPort device. Note that NPort devices only accept certificates using a "**.pem**" format.

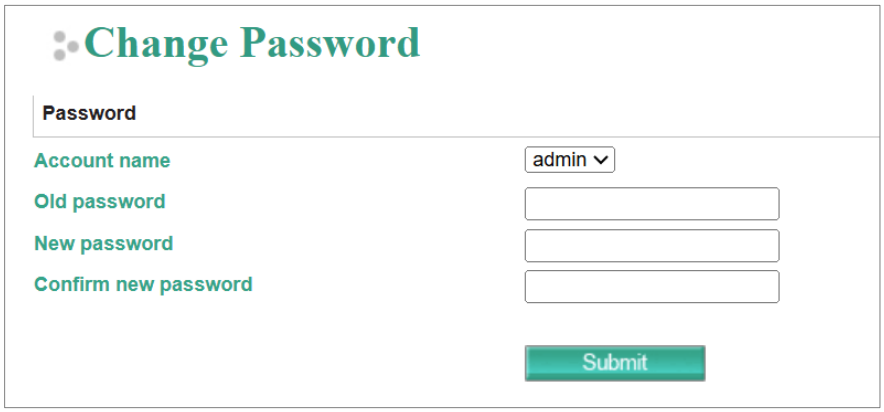
- Some well-known third-party CA (Certificate Authority) companies for your reference (https://en.wikipedia.org/wiki/Certificate_authority):

  - IdenTrust (https://www.identrust.com/)
  - DigiCert (https://www.digicert.com/)
  - Sectigo (Comodo Cybersecurity) (https://www.comodo.com/)
  - GoDaddy (https://www.godaddy.com/)
  - Verisign (https://www.verisign.com/)


Certificate/Key Deletion
Installed Certificate
SSL certificate
Delete
Keep
WPA server certificate
No certificate installed!
WPA user certificate/private key
No certificate/private key installed!
Submit

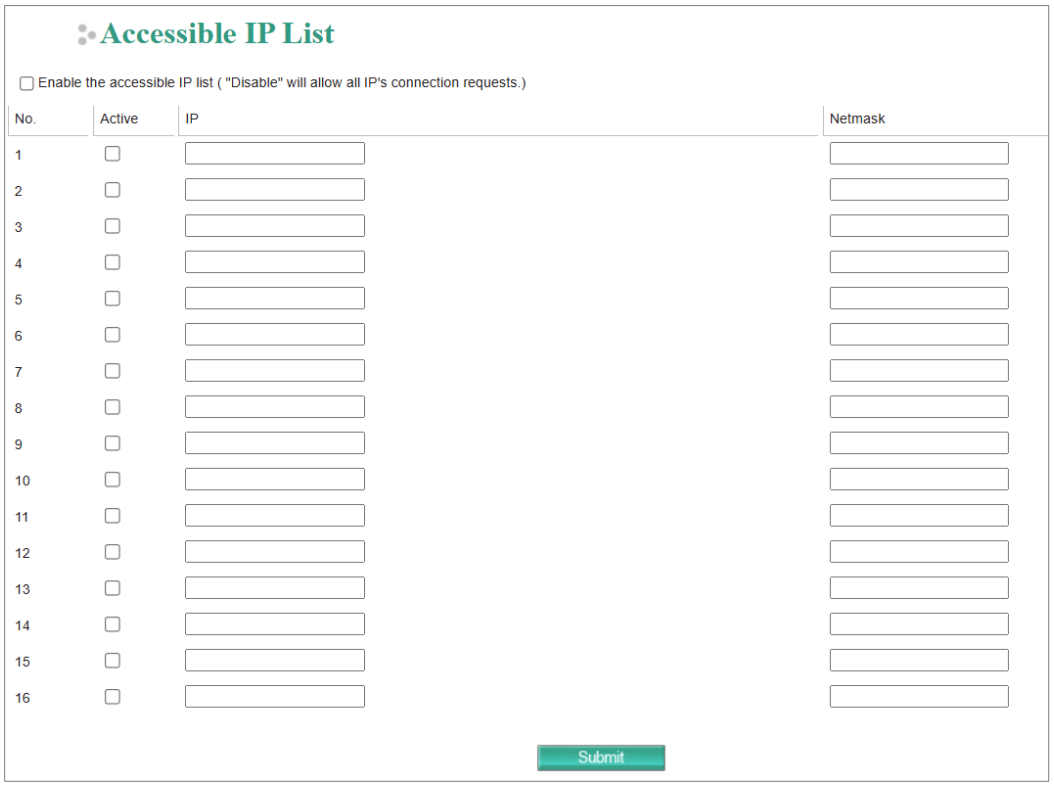
3.3 Account Management

- The NPort W2x50A-W4 Series provides two different user levels, administrator and user. With a Read Write account, you can access and change all settings through the web console. With a user account, you can only view settings.
- For firmware version 1.4 and earlier, the default administrator account is admin, and the default password is moxa. Starting from firmware version 1.5, you need to set the administrator's password before you log in the first time. To manage accounts, log in to the web console and select **System Management > Maintenance > Change Password**. To change the password of an existing account, select the account name in the top toolbar. Input the old password in the Password field and the new password in Confirm Password field to change the password.



3.4 Accessible IP List

- The W2x50A-W4 Series has a feature that limits access to specific remote host IP addresses to prevent unauthorized access. If a host's IP address is not in the accessible IP table, then the host may not access the serial ports of W2x50A-W4 Series. To configure it, log in to the HTTPS console and select **System Management > Misc. Network Settings > Accessible IP List**.



- You may add a specific address or range of addresses by using a combination of an IP address and a netmask:
  - **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:** Leave the Enable checkbox for the Accessible IP List unchecked.

The following table shows additional configuration examples.

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	Enable
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
192.168.1.1 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

● WARNING

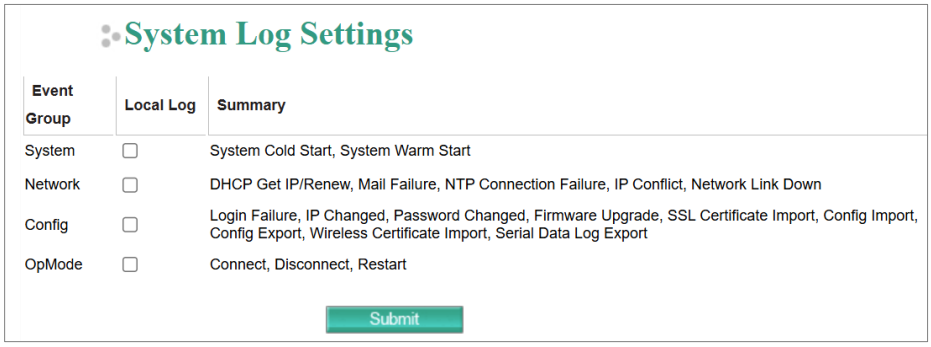
Ensure that the IP address of the PC you are using to access the web console is on the **Accessible IP List**.

3.5 Logging and Auditing

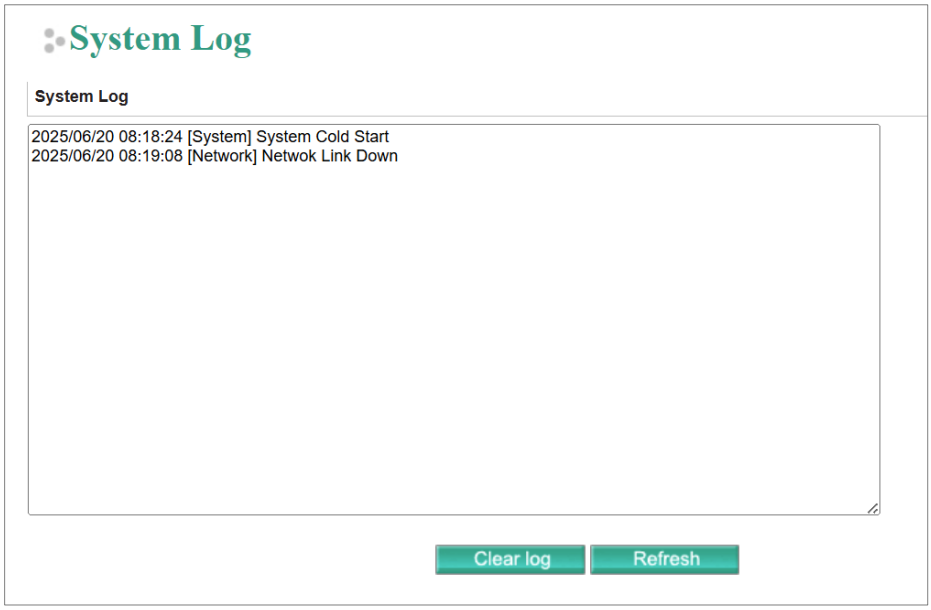
- These are the events that the W2x50A-W4 Series will record:

Event Group	Summary
System	System Cold Start, System Warm Start
Network	DHCP, Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down
Configuration	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

- To configure these settings, log in to the HTTPS console and select **System Management > Misc. Network Setting > System Log Settings**. Then, enable the **Local Log** for recording on the W2x50A-W4 device. Enable system log settings to record all important system events to monitor device status and check for security issues.



- To view events in the system log, log in to the HTTP/HTTPS console and select **System Monitoring > System status > System Log**.



3.6 Testing the Security Environment

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

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

1. Testing tools for cybersecurity environment checks are available. Some may provide limited free use, for example, Nessus. These tools help identify potential security leaks in the environment.
2. The device should be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
3. Control access to the serial console as with any physical access to the device.
4. Avoid using insecure services such as Telnet and TFTP; the best way is to disable them completely.
5. Limit the number of simultaneous web servers and Telnet sessions allowed. Periodically, change the passwords.
6. Backup the configuration files periodically and compare the configurations to make sure the devices work properly.
7. Audit the devices periodically to make sure they comply with these recommendations and/or any internal security policies.
8. If you need to return the unit to Moxa, disable encryption and back up the current configuration beforehand.

4 Patching/Upgrades

4.1 Patch Management

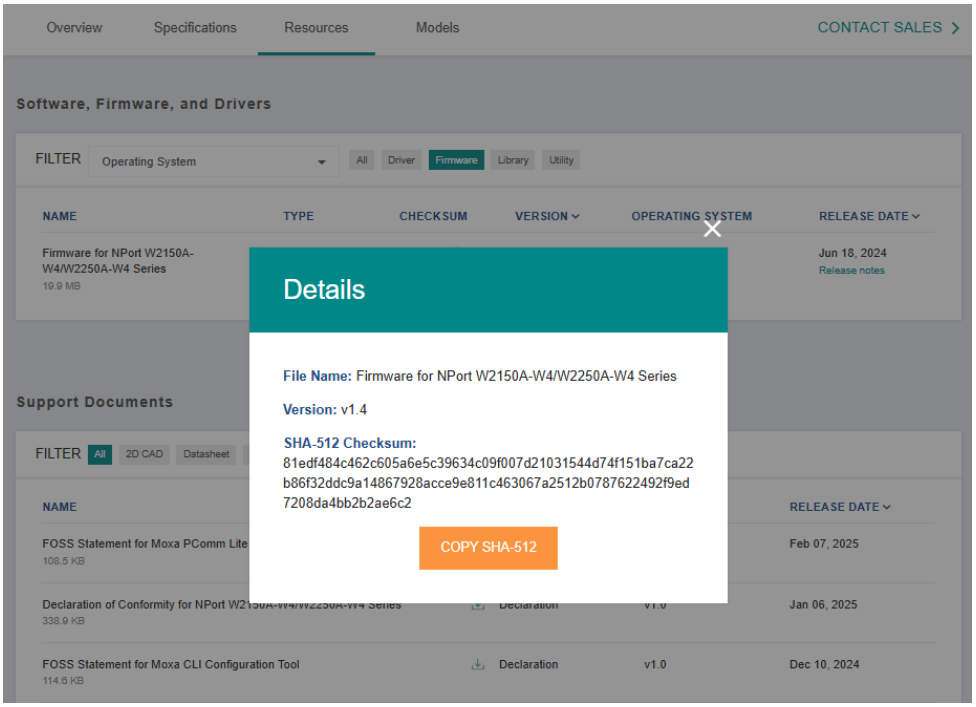
Regarding patch management, Moxa releases version enhancements annually, with detailed release notes.

4.2 Firmware Upgrades

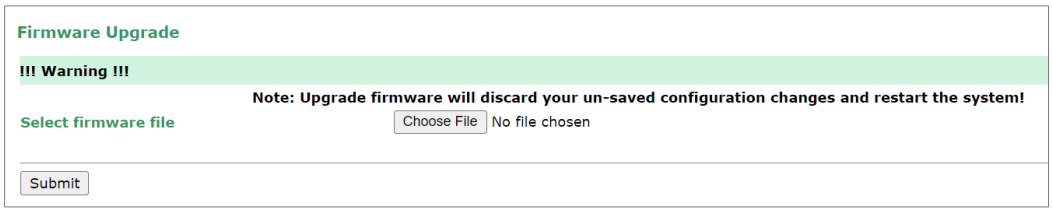
The process for upgrading firmware is:

- Download the latest firmware and software, along with its release notes and hash values for your NPort device from the Moxa website:
  - Firmware of NPort W2x50A-W4 Series:

    NPort W2150A-W4/W2250A-W4 Series - Wireless Device Servers | MOXA
- Moxa's website provides the SHA-512 hash value for you to double-check if the firmware is identical to the one on the website.



- Log in to the HTTPS console and select **System Management > Maintenance > Firmware Upgrade**. Select first the **Choose File** button to select the proper firmware and then **Submit** to upgrade the firmware.



5 Security Information and Vulnerability Feedback

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Product Security Incident Response Team (PSIRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

Please follow the updated Moxa security information from the link below:
https://www.moxa.com/en/support/product-support/security-advisory