The Security Hardening Guide for the NPort S9000 Series

Moxa Technical Support Team

support@moxa.com

Contents

Released on Mar 31, 2026

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.

1 Introduction

The NPort S9450I/S9650I Series configuration and security guidelines are detailed in this document. Consider the recommended steps in this document as best practices for security in most applications. We highly recommend that you review and test the configurations thoroughly before implementing them in your production system to ensure that your application is not negatively affected.

2 General System Information

2.1 Basic Information About the Device

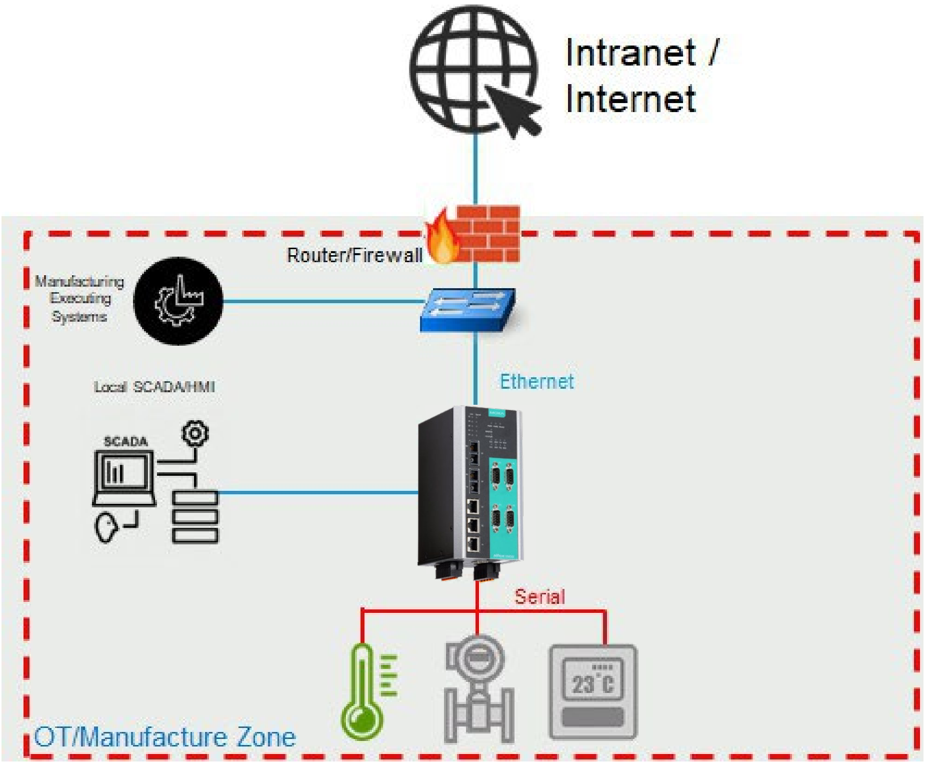
Model	Function	Firmware Version
NPort S9450I Series	Device server	Version 1.4
NPort S9650I Series	Device server	Version 1.4

The NPort S9450I/S9650I Series is a device server specifically designed to allow industrial devices to be accessible directly from a network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations and features are available for specific applications, such as Real COM drivers and TCP operation modes, to name a few.

2.2 Deployment of the Device

Deploy the NPort S9450I/S9650I Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

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



2.3 Security Threats

The security threats that can harm NPort S9450I/S9650I Series are:

1. **Attacks over the network**

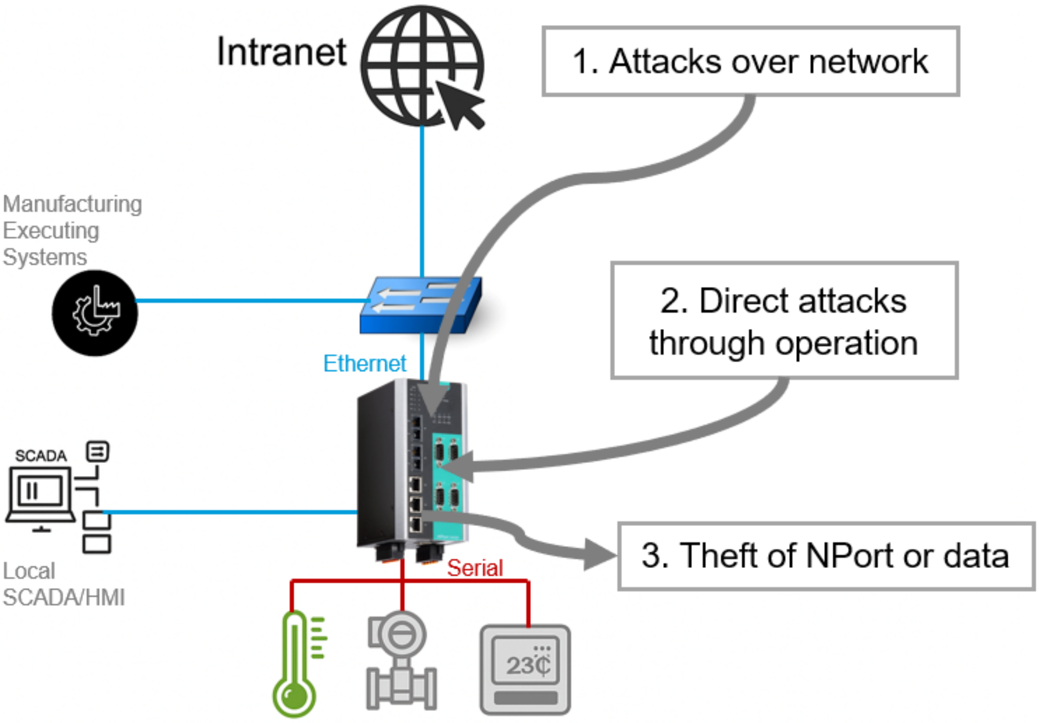
   Threats from individuals with no rights to the NPort S9450I/S9650I via networks such as intranets.

2. **Direct attacks through operation**

   Threats where individuals with no rights to the NPort S9450I/S9650I directly operate a device to affect the system and steal important data.

3. **Theft of the NPort or data**

   Threats where the NPort S9450I/S9650I or data is stolen, enabling critical data to be analyzed and used.


Intranet
1. Attacks over network
Manufacturing Executing Systems
2. Direct attacks through operation
Ethernet
SCADA
Local SCADA/HMI
Serial
3. Theft of NPort or data
23°C

2.4 Security Measures

To fend off security threats, we arranged security measures applied in security guides for the general business network environment and identified a set of security measures for the NPort S9450I/S9650I Series. We classify the security measures into three security types.

The following table describes the security measures and the threats that each measure handles.

Responsibility	Security Layer	Security Measure	Risk Addressed	Threat Handled		
				1	2	3
Asset owner	Policy and procedure	Establish policies and procedures to guide employees in their roles and responsibilities for the safe use of security-sensitive assets.	Vulnerabilities created because of a lack of security policies or employees' lack of awareness of procedures.	Yes	Yes	No
Asset owner	Perimeter security	Physical security	Physical modification, manipulation, theft, removal, or destruction of an asset.	No	Yes	Yes
Asset owner/ system integrator	Network security	Network firewall	Unauthorized and malicious communication from an untrusted network.	Yes	No	No
		Network IDS/IPS	Network attacks from various sources, such as port scanning and DDOS.	Yes	No	No
		VPN	Man-in-the-middle attacks during configuration and protocol communication.	Yes	No	No
System integrator/ Device vendor	Device security	IP-based access control	Unauthorized users/nodes to access the device.	Yes	Yes	No

Responsibility	Security Layer	Security Measure	Risk Addressed	Threat Handled		
				1	2	3
		Stopping unused services	Network attacks on weak points of the device.	Yes	No	No
		Role-based access control	Unauthorized users accessing the device or employees' incorrect operation.	Yes	Yes	No
		Applying the audit policy	Lack of records for following or improving policies/ procedures.	Yes	Yes	No
		Applying the password policy	Brute-force attack	Yes	Yes	No
		Applying the account lockout policy	Brute-force attack.	Yes	Yes	No

Note

1. Attacks over the network.
2. Direct attacks through the operation.
3. Theft of the NPort or data.

To defend against the theft of the NPort or data, we recommend you use the NPort S9450I/S9650I Series within a secure local network, as mentioned above. We also suggest that you enable the Accessible IP List function (refer to Chapter 3.5 for more details) to only allow the necessary hosts/IPs to access the device.

2.5 Defense-in-depth Strategy

The defense-in-depth strategy is a security approach to protect systems from various types of attacks by using multiple independent defense mechanisms. This strategy involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

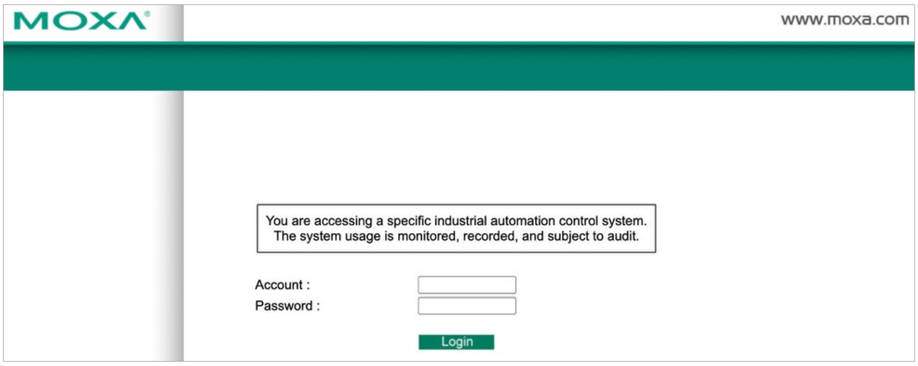
It is important to understand that no single protection measure can guarantee complete security. That's why the defense-in-depth approach makes it difficult for attackers to exploit one weakness to attack the product or the network.

By implementing a defense-in-depth approach, attackers must overcome multiple security layers undetected, making breaches increasingly difficult. Refer to the following table for measures you can leverage to create a defense-in-depth security environment at the edge device level based on the NPort S9450I/S9650I Series.

Security Function	Description	Type	Implementation
Account management	Reduces human error by enforcing access privileges	Administrative control	Role-based access control; refer to Chapter 3.4.
Syslog logging	Logs operations and anomalies	Administrative control	Supports local and remote logs; refer to Chapter 3.6
Web/CLI login authentication	Prevents unauthorized user access to the device	Administrative control	Role-based access control; refer to Chapter 3.4.
Device certificate and authentication	Prevent man-in-the-middle (MITM) attacks	Logical/technical control	Supports TLS v1.2, SNMPv3; refer to Chapter 3.3.
Accessible IP List	Limit specific remote host IP addresses from logging in to prevent unauthorized access to the gateway	Logical/technical control	Allowlist table to manage device access; refer to Chapter 3.5.
Physical security	Prevents unauthorized physical access	Physical control	Install the device in cabinets with strict access control and surveillance

3 Configuration and Hardening Information

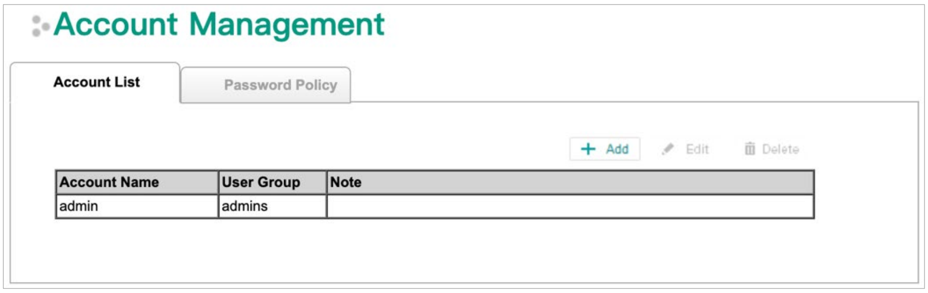
On the first page of the web console, type **admin** for the default account name and **moxa** for the default password to log in to the device.



You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.

Account :
Password :

The device will remind you that you’re using the default username and default password to access the device. We strongly recommend that you change the default username and password via **System Management > Maintenance > Account Management**.



Account Name	User Group	Note
admin	admins	

You may select **Add** to create a new user or check the account admin, select **Edit** to change the existing account.

After you create a new account that belongs to the admins group, you can delete the default “admin” account.

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 S9450I/S9650I Series and other devices.

Service Name	Option	Default Settings	Type	Port Number	Description
Moxa service	Enable/ Disable	Enable	TCP	4900	For Moxa utility communication
			UDP	4800	
WINS	Enable/ Disable	Disable	UDP	137	Processing WINS (Client) data
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
HTTPS server	Enable/ Disable	Enable	TCP	443	Secured web console
RADIUS	Enable/ Disable	Disable	UDP	User-defined (1645 as default or 1812)	Authentication server
TACACS+	Enable/ Disable	Disable	TCP	49	Authentication server
DHCP client	Enable/ Disable	Disable	UDP	68	The DHCP client needs to get the system's IP address from the server
SNTP	Enable/ Disable	Disable	UDP	Random port	Synchronize time settings with a time server
Remote System Log	Enable/ Disable	Disable	UDP	Random port	Send the event log to a remote log server
MMS	Enable/ Disable	Enable	TCP	102	Real-time managing the device server

Operation Mode	Option	Default Settings	Type	Port Number
Real COM mode	Enable/ Disable	Disable (Changed to Enable after user set username/password)	TCP	949+ (Serial port 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.)

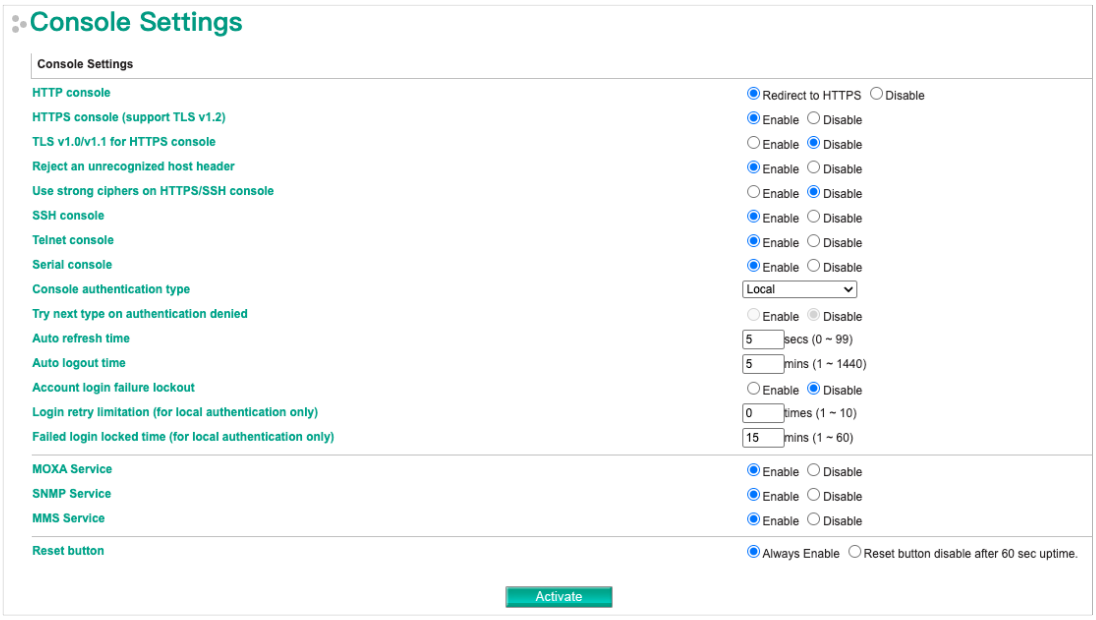
Operation Mode	Option	Default Settings	Type	Port Number
DNP3 mode	Enable/ Disable	Disable	TCP	User-defined (default: 20,000)
Modbus mode	Enable/ Disable	Disable	TCP	User-defined (default: 502)
Disabled mode	Enable/ Disable	Disable	N/A	N/A

For security reasons, the NPort S9450I/S9650I Series only enables limited services to ensure the security of the device itself. It will only enable the Moxa services, HTTPS, and serial console for the user to configure the device and the Real COM mode for the COM-based Control application users. If this is not the case, you may modify or disable the above services.

To integrate the NPort S9450I/S9650I Series into your network topology and secure applications, consider enabling the services below with proper settings to enhance the security architecture of the network and to protect the network with depth of defense.

Service Name	Type	Port Number	Security Remark
SNMP agent	UDP	161	The Simple Network Management Protocol is a popular tool for remote device monitoring and management. If needed, turn on SNMPv3 to encrypt the communication data.
RADIUS	UDP	User Define (1645 as default or 1812)	If you are using the central account management feature (has a RADIUS server), enable this service.
TACACS+	TCP	49	If you are using the central account management feature (has a TACACS+ server), enable this service. Select either RADIUS or TACACS+ to be the central account management service and disable the other one.
DHCP Client	UDP	67, 68	If you have a DHCP server to assign an IP automatically, enable this service for easy management.
SNTP Client	UDP	Random port	For log tracing, time synchronization is important.
Remote System Log	UDP	Random port	Central log management may be important in some applications. Enable the remote system log service to store all the logs of the NPort S9450I/S9650I to a remote log server.
MMS	TCP	102	The MMS protocol is one of the IEC 61850 protocols for remote device monitoring and management. With security concerns, turn off the protocol and use SNMPv3 as an alternative.

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

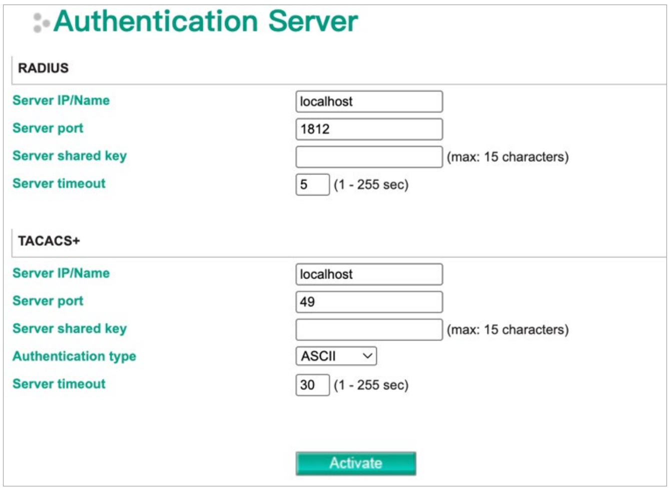


Console Settings

Console Settings	
HTTP console	● Redirect to HTTPS ○ Disable
HTTPS console (support TLS v1.2)	● Enable ○ Disable
TLS v1.0/v1.1 for HTTPS console	○ Enable ● Disable
Reject an unrecognized host header	● Enable ○ Disable
Use strong ciphers on HTTPS/SSH console	○ Enable ● Disable
SSH console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
Serial console	● Enable ○ Disable
Console authentication type	Local
Try next type on authentication denied	○ Enable ● Disable
Auto refresh time	5 secs (0 ~ 99)
Auto logout time	5 mins (1 ~ 1440)
Account login failure lockout	○ Enable ● Disable
Login retry limitation (for local authentication only)	0 times (1 ~ 10)
Failed login locked time (for local authentication only)	15 mins (1 ~ 60)
MOXA Service	● Enable ○ Disable
SNMP Service	● Enable ○ Disable
MMS Service	● Enable ○ Disable
Reset button	● Always Enable ○ Reset button disable after 60 sec uptime.

Activate

For the RADIUS and TACACS+ servers, log in to the HTTPS console and select **System Management > Misc. Network Settings > Authentication Server**. Then, input the Server IP/Name to add the RADIUS or TACACS+ server and complete the relative settings by selecting the **Activate** button.



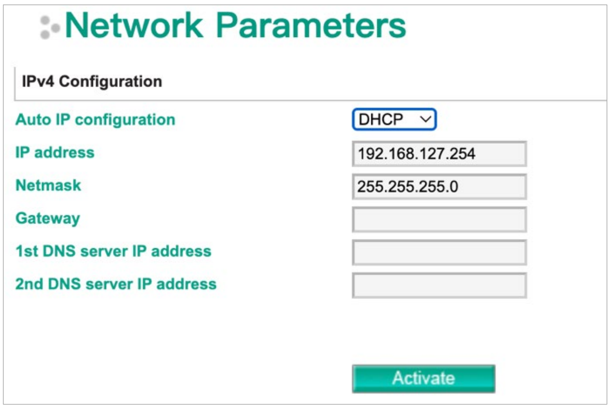
Authentication Server

RADIUS	
Server IP/Name	localhost
Server port	1812
Server shared key	(max: 15 characters)
Server timeout	5 (1 - 255 sec)

TACACS+	
Server IP/Name	localhost
Server port	49
Server shared key	(max: 15 characters)
Authentication type	ASCII
Server timeout	30 (1 - 255 sec)

Activate

If you want to enable DHCP Client, log in to the HTTPS console, select **Basic Settings > Network Parameters** and then Auto IP configuration from **DHCP**.

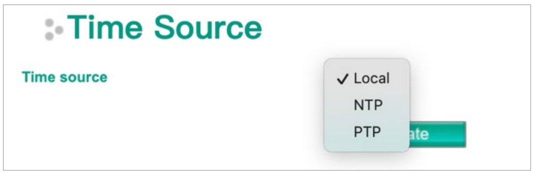


Network Parameters

IPv4 Configuration

Auto IP configuration	DHCP
IP address	192.168.127.254
Netmask	255.255.255.0
Gateway	
1st DNS server IP address	
2nd DNS server IP address	

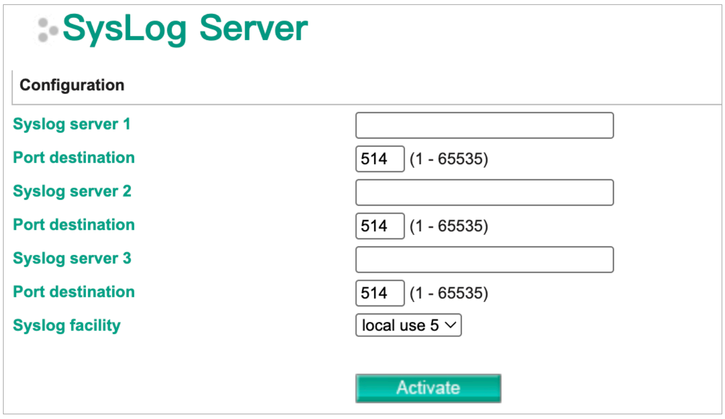
If you want to enable SNTP Client or PTP Client, log in to the HTTPS console, select **Basic Settings > Time Settings > Time Source**, and then NTP or PTP.



Time Source

Time source: ✓ Local

For the remote system log server, log in to the HTTPS console, select **System Management > Misc. Network Settings > SysLog Server**, type the remote log server IP or name and select the **Activate** button to enable the service.



SysLog Server

Configuration

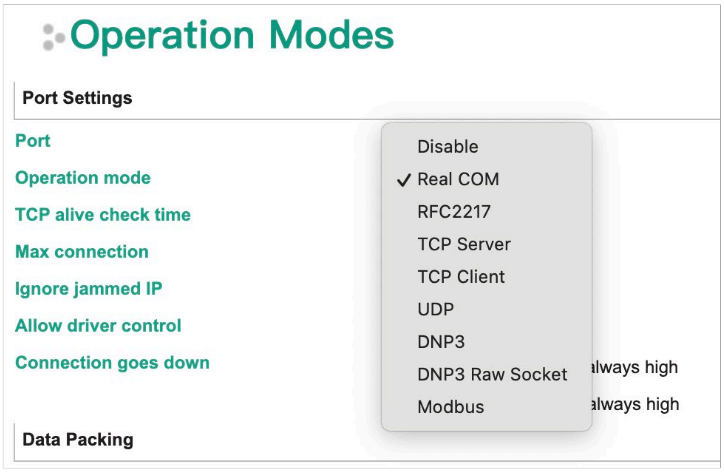
Syslog server 1	
Port destination	514 (1 - 65535)
Syslog server 2	
Port destination	514 (1 - 65535)
Syslog server 3	
Port destination	514 (1 - 65535)
Syslog facility	local use 5

3.2 Serial Ports and Recommended Services

The serial protocols used to communicate between the NPort S9450I/S9650I Series and other devices are listed in the following table:

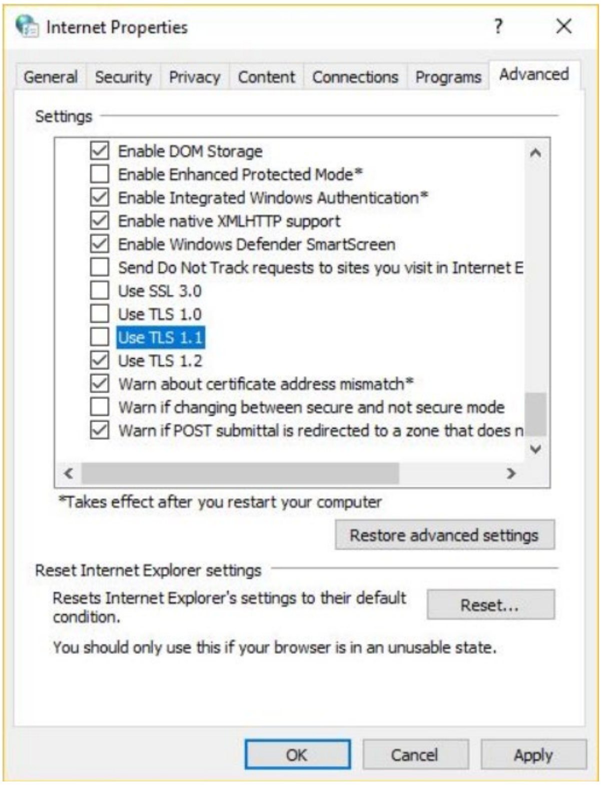
Service Name	Option	Default Settings	Type	Description
Proprietary serial	N/A	Real COM mode	RS-232/422/485	User-designed data frame for proprietary serial protocol

The operation mode services depend on your serial device’s Ethernet network connection method. For example, if your host PC uses legacy software to open a COM port to communicate with the serial device, then the NPort will enable the Real COM mode for this application. If you don't want the NPort to provide such a service, log in to the HTTPS console, select **Serial Settings > Operation Modes > Port # > Operation mode**, and then **Disable**.



3.3 HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. Because TLS v1.1 and lower versions have severe, easily exploitable vulnerabilities, the NPort S9450I/S9650I Series uses TLS v1.2 for HTTPS to secure data transmissions. Make sure your browser has TLS v1.2 enabled.



☑ Enable DOM Storage
☐ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
☐ Send Do Not Track requests to sites you visit in Internet E
☐ Use SSL 3.0
☐ Use TLS 1.0
☐ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate address mismatch*
☐ Warn if changing between secure and not secure mode
☑ Warn if POST submittal is redirected to a zone that does n

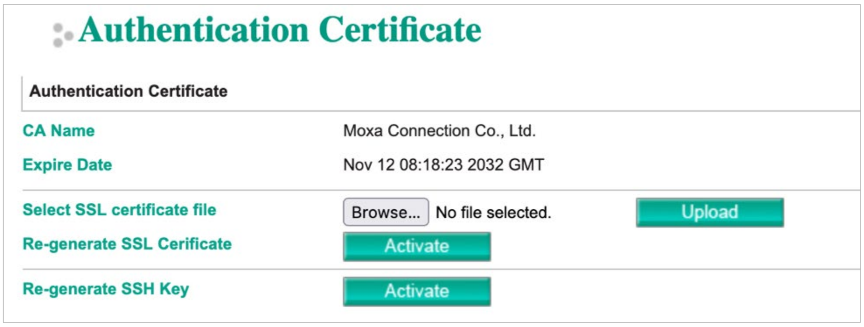
*Takes effect after you restart your computer

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority or export the "NPort self-signed" certificate to the browser.

Log in to the HTTPS console and select **System Management > Maintenance > Authentication Certificate**. Select **Browse...** to choose the certificate to import. Then, select the **Upload** button to import it.



Authentication Certificate

CA Name	Moxa Connection Co., Ltd.
Expire Date	Nov 12 08:18:23 2032 GMT
Select SSL certificate file	No file selected.
Re-generate SSL Cerificate	
Re-generate SSH Key	

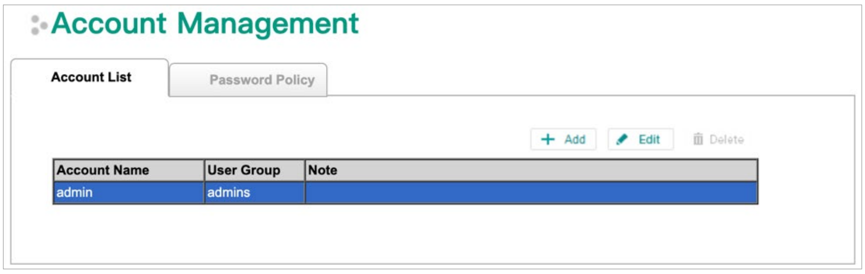
- Behavior of the System Certificate on an NPort S9450I/S9650I device
    - NPort devices will auto-generate a self-signed SSL certificate when the IP address is changed or you can select the **Activate** button for the **Re-generate SSL certificate** option to generate a new one manually. It is recommended that you import SSL certificates certified by a trusted third-party Certificate Authority (CA) or by an organization's CA.
    - The NPort device’s self-signed certificate is encoded based on the Rivest-Shamir-Adleman asymmetric encryption algorithm (RSA-1024 algorithm), which should be compatible with most applications. Some applications may need a longer or stronger key, requiring importing a third-party certificate. Note that longer keys will mean browsing the web console will be slower because of the increased complexity of encrypting and decrypting communicated data.
- Importing the third-party trusted SSL certificate:

  To generate the SSL certificate through a third party, here are the 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. The NPort S9450I/S9650I Series supports the algorithms below:
        - RSA-1024, RSA-2048
- 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/)
    - Comodo Cybersecurity (https://www.comodo.com/)
    - GoDaddy (https://www.godaddy.com/)
    - Verisign (https://www.verisign.com/)

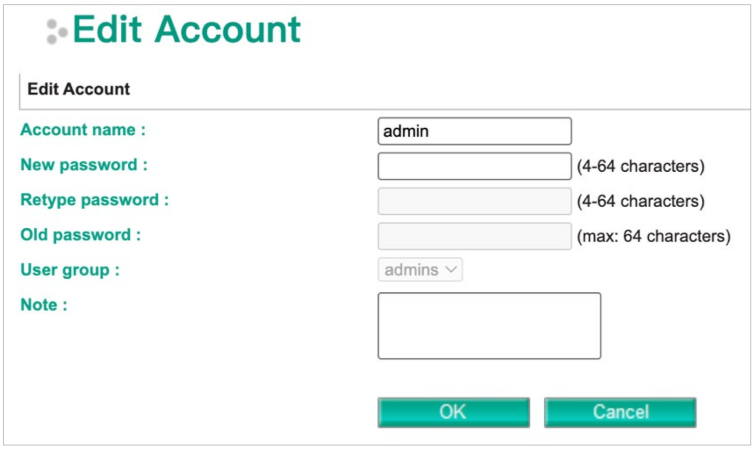
3.4 Account Management

The NPort S9450I/S9650I Series provides three different user groups: admins, users, and guests. With an admin account, you can access and change all settings through the web console. With a user account, you can monitor most of the settings. With a guest account, you cannot access the web console of the S9450I/S9650I, but you can bypass the device server and issue a request to the remote server to access the local network.

We strongly recommend that you change the default password after you log in to the device for the first time. Select **System Management > Maintenance > Account Management** and check the account “admin” and select the **Edit** button to change the password.



Account Name	User Group	Note
admin	admins	



Account name : admin

New password : (4-64 characters)

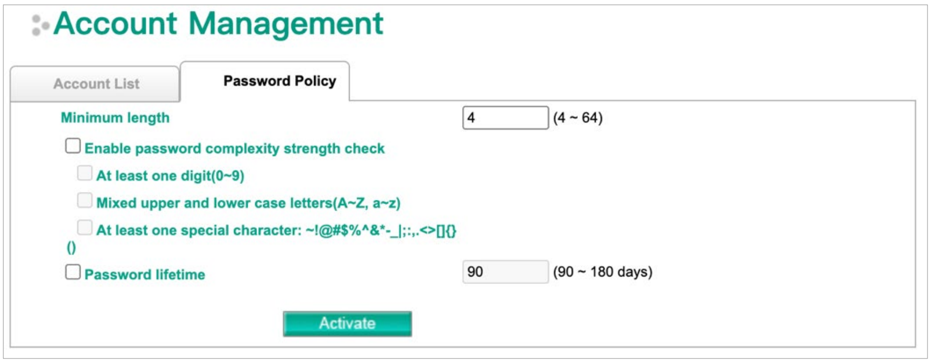
Retype password : (4-64 characters)

Old password : (max: 64 characters)

User group : admins

Note :

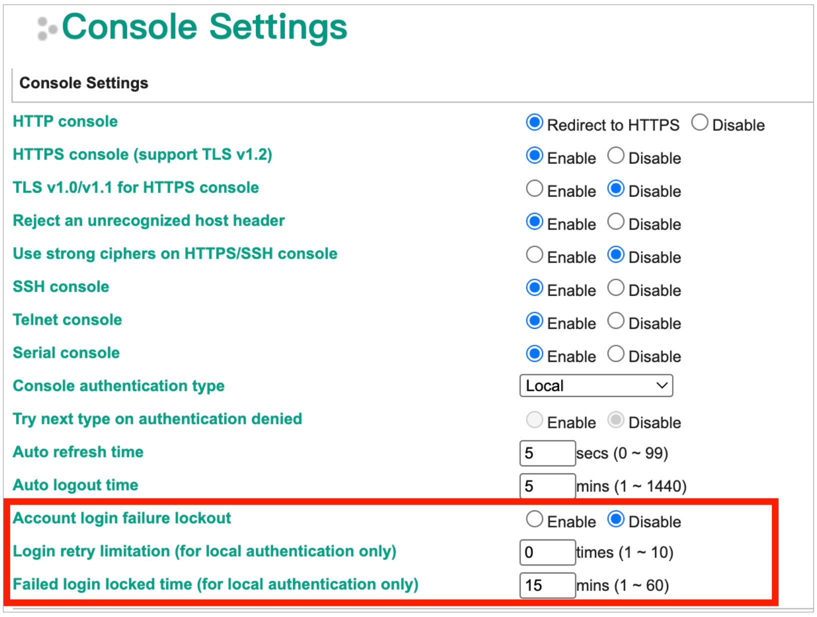
To add new accounts, select the **Add** button and input the account information, and assign a password to the user. Also, the administrator(s) shall assign a proper **User Group** to users to limit their privileges of using the NPort S8000/S9450I/S9650I. The password rules can be set up in **the Password Policy** section.



Account Management

Minimum length	4	(4 ~ 64)
□ Enable password complexity strength check		
□ At least one digit(0~9)		
□ Mixed upper and lower case letters(A~Z, a~z)		
□ At least one special character: ~!@#$%^&*-_|;:,.<>[]{}()		
□ Password lifetime	90	(90 ~ 180 days)

Configure the **login password policy** and **account login failure lockout** to improve security. To configure the login failure lockout function, log in to the HTTPS console and select **System Management > Maintenance > Console Settings**.



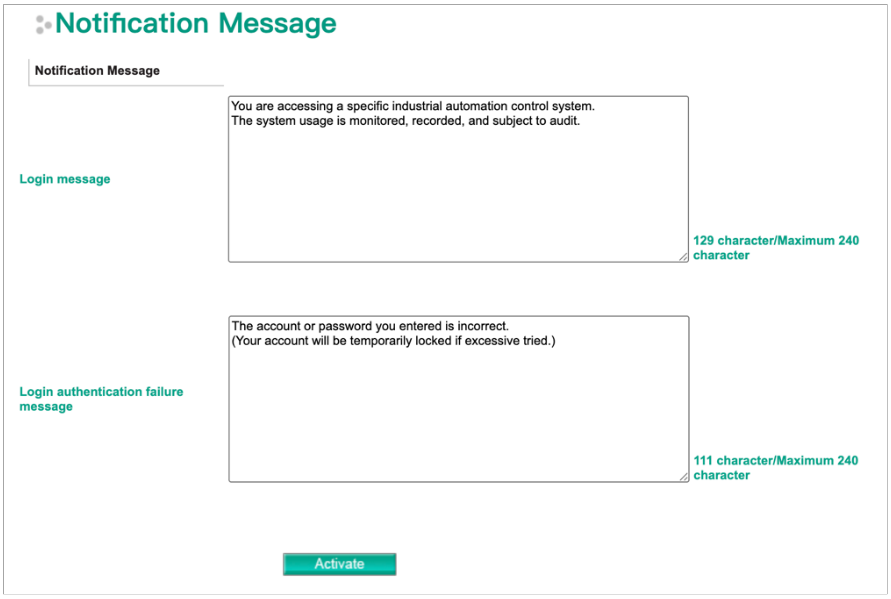
Console Settings

Console Settings

HTTP console	● Redirect to HTTPS ○ Disable
HTTPS console (support TLS v1.2)	● Enable ○ Disable
TLS v1.0/v1.1 for HTTPS console	○ Enable ● Disable
Reject an unrecognized host header	● Enable ○ Disable
Use strong ciphers on HTTPS/SSH console	○ Enable ● Disable
SSH console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
Serial console	● Enable ○ Disable
Console authentication type	Local
Try next type on authentication denied	○ Enable ● Disable
Auto refresh time	5 secs (0 ~ 99)
Auto logout time	5 mins (1 ~ 1440)
Account login failure lockout	○ Enable ● Disable
Login retry limitation (for local authentication only)	0 times (1 ~ 10)
Failed login locked time (for local authentication only)	15 mins (1 ~ 60)

Enable the **Account login failure lockout** and select the number of login attempts users can make before lockout, and the duration of their rejection from the NPort S9450I/S9650I Series.

For some system security requirements, the system may show a warning message to every user who logs in. To add a login message, select **System Management > Maintenance > Notification Message**, and enter the messages to be delivered.



Notification Message

Notification Message

Login message: You are accessing a specific industrial automation control system.
The system usage is monitored, recorded, and subject to audit.

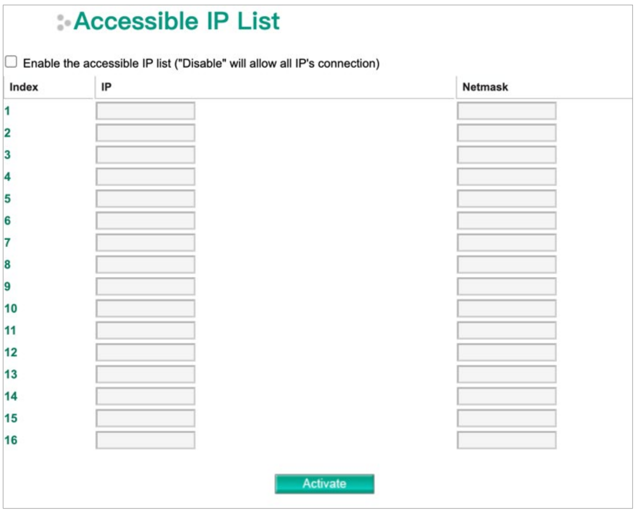
129 character/Maximum 240 character

Login authentication failure message: The account or password you entered is incorrect.
(Your account will be temporarily locked if excessive tried.)

111 character/Maximum 240 character

3.5 Accessible IP List

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



Accessible IP List

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

Index	IP	Netmask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

- Add a specific address or range of addresses by using a combination of an IP address and a subnet mask:
  - **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 the **Allowlist** toggle button is closed.

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**.

3.6 Logging and Auditing

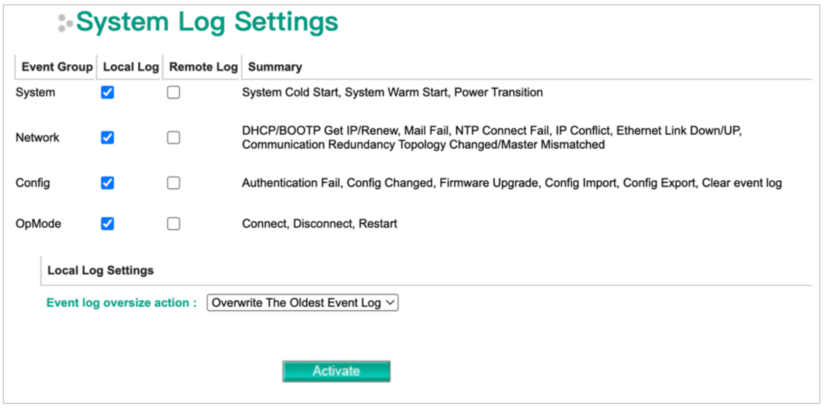
The local syslog function is enabled to record events that happened on the NPort S9450I/S9650I device. The events can be recorded for up to 1,000 items.

These are the events that the NPort S9450I/S9650I Series will record:

Category	Description
System	The events related to the NPort itself, like device cold start or warm start.
Network	The events related to the Ethernet interface, for example, the Ethernet link is down.
Configuration	The events that usually happen during the maintenance process, for example, firmware upgrades.
OpMode	The events related to the serial interface(s), for example, port connection.

To configure this setting, log in to the HTTPS console and select **System Management > Auto Warning Settings > System Log Settings**. Select the events you would like to save in the system log.

When the local logs reach 1,000 items, you may select **Overwrite The Oldest Event Log** or **Stop Recording Event Log** for the device server to handle the new event.



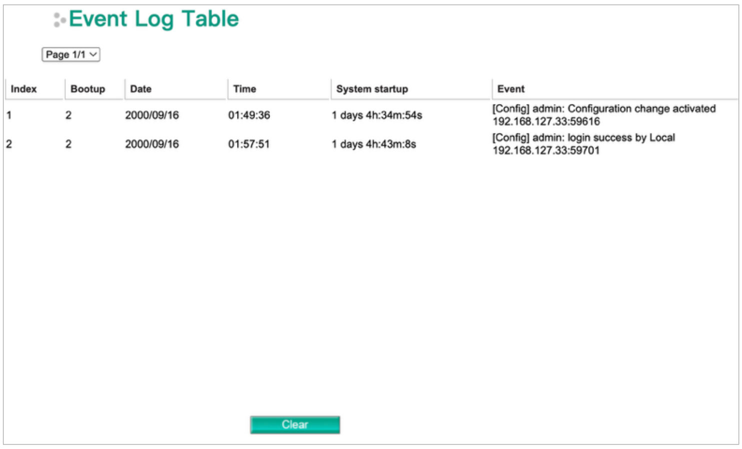
System Log Settings

Event Group	Local Log	Remote Log	Summary
System	☑	☐	System Cold Start, System Warm Start, Power Transition
Network	☑	☐	DHCP/BOOTP Get IP/Renew, Mail Fail, NTP Connect Fail, IP Conflict, Ethernet Link Down/UP, Communication Redundancy Topology Changed/Master Mismatched
Config	☑	☐	Authentication Fail, Config Changed, Firmware Upgrade, Config Import, Config Export, Clear event log
OpMode	☑	☐	Connect, Disconnect, Restart

Local Log Settings

Event log oversize action : Overwrite The Oldest Event Log

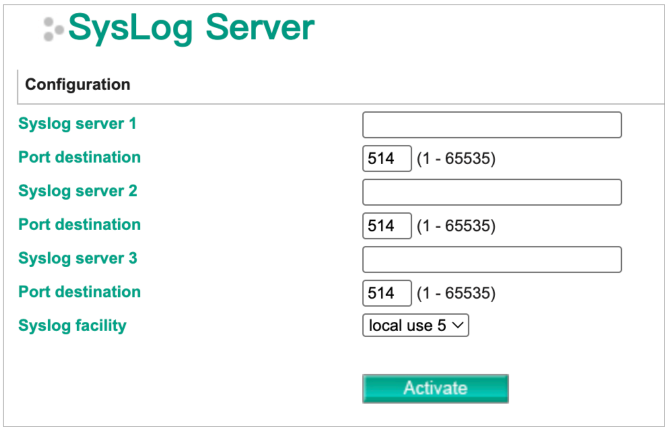
To view events in the system log, select **System Monitoring > System Status > Event Log**.



Event Log Table

Index	Bootup	Date	Time	System startup	Event
1	2	2000/09/16	01:49:36	1 days 4h:34m:54s	[Config] admin: Configuration change activated 192.168.127.33:59616
2	2	2000/09/16	01:57:51	1 days 4h:43m:8s	[Config] admin: login success by Local 192.168.127.33:59701

To enable the remote log server, select **System Management > Misc. Network Settings > SysLog Server**. There are three remote syslog servers that can be configured, and you can select the syslog facility of each event sent by the NPort S9450I/S9650I.



SysLog Server

Configuration

Syslog server 1	
Port destination	514 (1 - 65535)
Syslog server 2	
Port destination	514 (1 - 65535)
Syslog server 3	
Port destination	514 (1 - 65535)
Syslog facility	local use 5

4 Patching/Upgrades

4.1 Patch Management

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

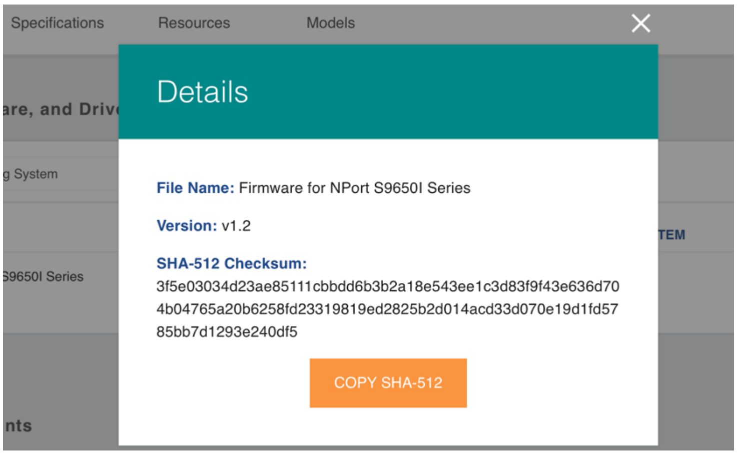
4.2 Firmware Upgrades

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 for the NPort S9450I Series:

    https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/combo-device-servers/nport-s9450i-series#resources
  - ➢ Firmware for the NPort S9650I Series:

    https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/combo-device-servers/nport-s9650i-series#resources
- 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.

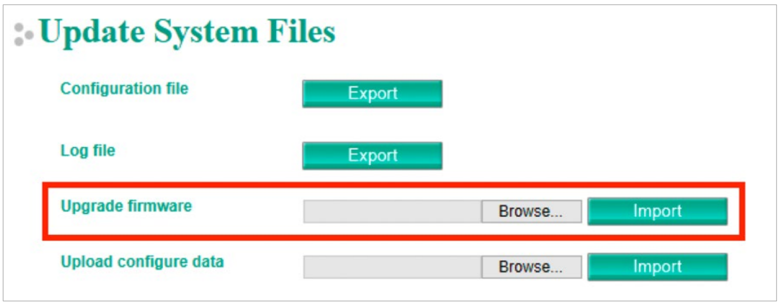


File Name: Firmware for NPort S9650I Series

Version: v1.2

SHA-512 Checksum:
3f5e03034d23ae85111cbbdd6b3b2a18e543ee1c3d83f9f43e636d70
4b04765a20b6258fd23319819ed2825b2d014acd33d070e19d1fd57
85bb7d1293e240df5

- Log in to the HTTPS console and select **System Management > System File Update > Update System Files**. Select the **Browse** button to choose the proper firmware and select **Import** to upgrade the firmware.



- Manual for the NPort S9450I Series:
  https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/combo-device-servers/nport-s9450i-series#resources
- Manual for the NPort S9650I Series:
  https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/combo-device-servers/nport-s9650i-series#resources

4.3 Recommendation to Secure the Environment

Besides using devices that support security functions, network managers can follow several recommendations to protect the entire network and devices.

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

- Testing tools are available for checking the cybersecurity environment. Some may provide limited free use, for example, Nessus. These tools help identify probable security leaks in the environment.
- You must operate the device inside a secure network, and a firewall or router must protect it to block attacks via the Internet.
- Control/restrict access to the serial console (depending on the model deployed), and physical access to the device itself.
- Avoid using insecure services such as SNMPv1 or v2c. We recommend disabling them completely.
- Limit the number of simultaneous web server sessions allowed. We recommend changing the passwords periodically.
- Back up the configuration files periodically.
- Audit the devices periodically to ensure that they comply with these recommendations and/or any internal security policies.
- If there is a need to return the unit to Moxa, ensure that you back up the configuration on it.

Note DISCLAIMER:
The information above and this guide (the "information") are for your reference only. We do not guarantee a cyberthreat-free environment. These guidelines are intended to increase the security level to defend against cyber-intrusions and is not guaranteed to meet your specific requirements. We provide the abovementioned information "as-is" and do not warrant its accuracy, completeness, or performance, whether express, implied, or otherwise.

5 Decommission

Since the NPort is the primary device for transferring serial data to Ethernet devices, decommissioning an NPort device requires arranging annual maintenance to replace the old unit with a new one. Follow these steps to complete the process:

1. Export the configuration file from the old NPort and import it to the new unit. This will save you from having to configure the new unit manually.
2. Stop communication and replace the old unit.
3. Restart communication and check if everything works fine. If yes, proceed to step d to decommission the old unit. If not, you may need assistance to troubleshoot the issue.
4. Keep the old unit powered on and press the Reset button for 5 seconds to restore the settings to factory default.
5. After the device reboots and all user settings are removed or overwritten, you may scrap it.

Note If you enable the function Reset button "Only enable with 60 seconds after booting". You will need to push the Reset button within 60 seconds after booting to enable the Reset function.

6 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.

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