The Security Hardening Guide for the NPort 5000 Series

Moxa Technical Support Team

support@moxa.com

Contents

 Released on May 24, 2023

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 how to configure and secure the NPort 5000 Series. You should consider the recommended steps in this document as best practices for security in most applications. We highly recommended 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	Operating System	Firmware Version
NPort 5000A Series	General purpose	Moxa Operating System	Version 1.6 and later
NPort 5110	General purpose	Moxa Operating System	Version 2.10 and later
NPort 5130/5150	General purpose	Moxa Operating System	Version 3.9 and later
NPort 5200 Series	General purpose	Moxa Operating System	Version 2.12 and later
NPort 5400 Series	General purpose	Moxa Operating System	Version 3.14 and later
NPort 5600-DT Series	General purpose	Moxa Operating System	Version 2.8 and later
NPort 5600-DTL Series	Entry level	Moxa Operating System	Version 1.6 and later
NPort 5600 Series	Rackmount	Moxa Operating System	Version 3.10 and later
NPort 5000AI-M12 Series	Railway	Moxa Operating System	Version 1.5 and later
NPort IA5000 Series	Industrial automation	Moxa Operating System	Version 1.7 and later
NPort IA5000A Series	Industrial automation	Moxa Operating System	Version 1.7 and later

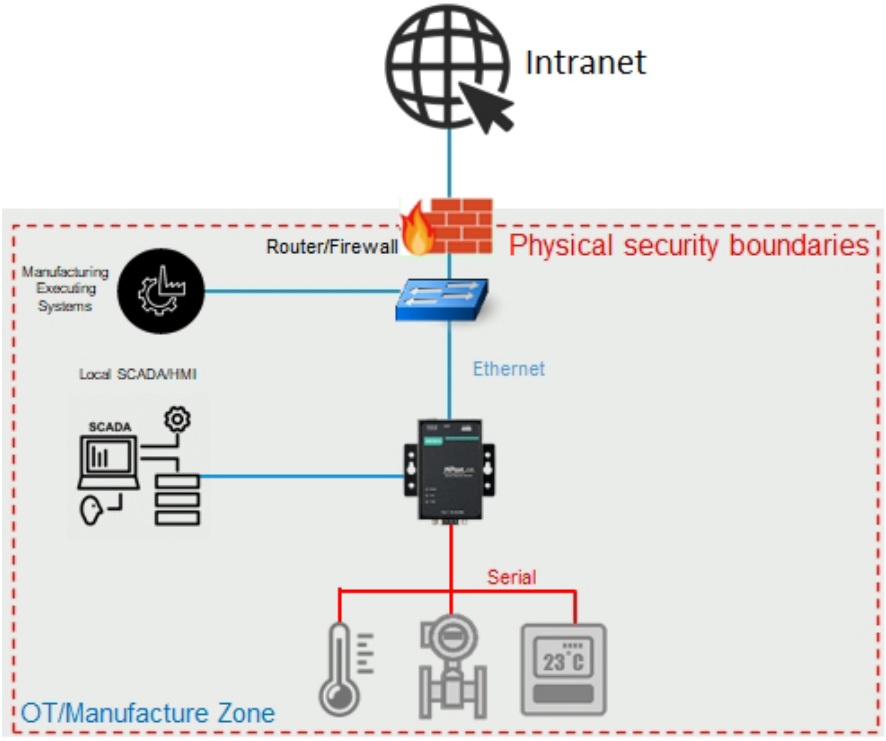
The NPort 5000 Series is a device server specifically designed to allow industrial devices to be accessible directly from the network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations and features are available for specific applications, such as protocol conversion, Real COM drivers, and TCP operation modes, to name a few. It uses TLS protocols to transmit encrypted serial data over Ethernet.

Moxa Operating System (MOS) is an embedded proprietary operating system, which is only executed in Moxa edge devices. Because the MOS operating system is not freely available, the chances of malware attacks are significantly reduced.

2.2 Deployment of the Device

You should deploy the NPort 5000 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 5000 Series are:

1. **Attacks over the network**

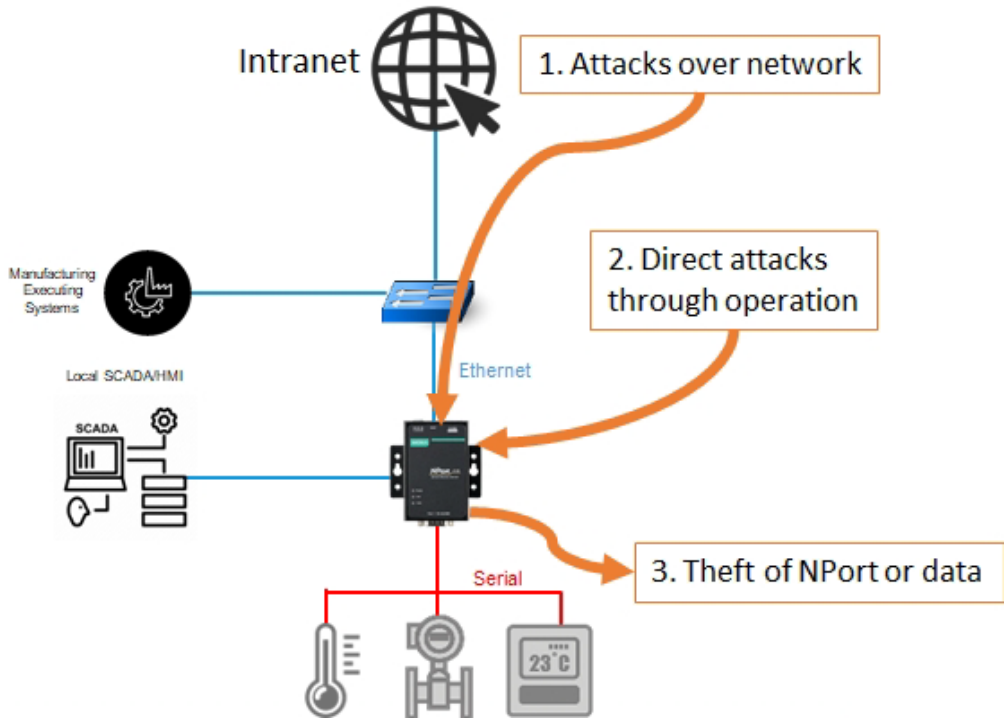
   Threats from individuals with no rights to the NPort 5000 Series via networks such as intranets.

2. **Direct attacks through operation**

   Threats where individuals with no rights to the NPort 5000 Series directly operate a device to affect the system and steal important data.

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

   Threats where an NPort 5000 Series or data is stolen, and important data is analyzed.



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 5000 Series. We classify the security measures into three security types. The following table describes the security measures and the threats that each measure handles.

Security Measure	Subcategory	Threat Handled		
		1	2	3
Access Control	–	Yes	Yes	No
Stopping unused services	–	Yes	No	No
Changing IT environment settings	Disabling the built-in Administrator account or changing its username	Yes	Yes	No
	IT firewall tuning	Yes	No	No
	Hiding the last logon username	Yes	Yes	No
	Applying the software restriction policies	Yes	Yes	No
	Applying AutoRun restrictions	No	Yes	No
	Applying the StorageDevicePolicies function	No	Yes	Yes
	Disabling USB storage devices	No	Yes	Yes
	Disabling NetBIOS over TCP/IP	Yes	No	No
	Applying the password policy	Yes	Yes	No
	Applying the audit policy	Yes	Yes	No
	Applying the account lockout policy	Yes	Yes	No

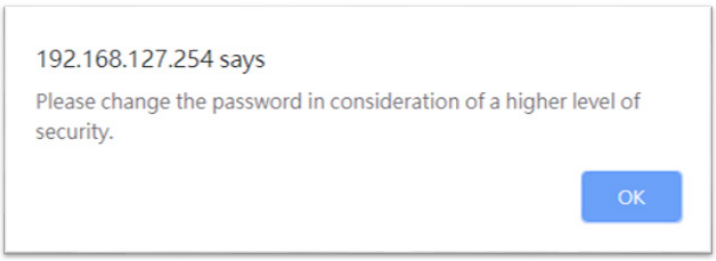
Note
1. Attacks over the network.
2. Direct attacks through the operation.
3. Theft of the NPort or data.

To defend against the theft of the NPort or data, we recommend you to use the NPort 5000 Series within a secure local network, as mentioned above. We also suggest that you enable the Accessible IP List function (for more details, please refer to chapter 3.3) to only allow the necessary hosts/IPs to access the device and protect the device from attacks of unknown clients.

3 Configuration and Hardening Information

For security reasons, account and password protection is enabled by default, so you must provide the correct account and password to unlock the device before entering the web console of the gateway.

The default account and password are **admin** and **moxa** (both in lowercase letters), respectively. Once you are successfully logged in, a pop-up notification will appear to remind you to change the password to ensure a higher level of security.



The NPort 5110, NPort 5130/5150, and NPort 5200 Series only have password protection. The default password is **moxa**.

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 5000 Series and other devices. Depending on different applications and market positions, some NPort 5000 models may not support all the services listed here.

Service Name	Option	Default Settings	Type	Port Number	Remark & Description
Moxa Command (DSCI)	Enable/Disable	Enable	TCP	14900, 4900	For Moxa utility communication
			UDP	4800	
DNS_wins	Enable	Enable	UDP	53, 137, 949	Processing DNS and WINS (Client) data
SNMP agent	Enable/Disable	Enable	UDP	161	SNMP handling routine
HTTP server	Enable/Disable	Enable	TCP	80	Web console
HTTPS server	Enable/Disable	Enable	TCP	443	Secured web console
Telnet server	Enable/Disable	Disable	TCP	23	Telnet console
DHCP client	Enable/Disable	Disable	UDP	68	The DHCP client needs to acquire the system IP address from the server
SNTP	Enable/Disable	Disable	UDP	Random Port	Synchronize time settings with a time server This function is not available for the 5100/5100A/5200/ 5200A Series.
Remote System Log	Enable/Disable	Disable	UDP	Random Port	Send the event log to a remote log server

Operation Mode	Option	Default Settings	Type	Port Number	Remark & Description
Real COM Mode	Enable/Disable	Enable	TCP	950+ (Serial port No. - 1) 966+ (Serial port No. - 1)	
RFC2217 Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)	Only available in certain models
TCP Server Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.) User-defined (default: 966+Serial port No.)	
UDP Mode	Enable/Disable	Disable	UDP	User-defined (default: 4000+Serial port No.)	
Pair Connection Master Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)	Only available in certain models
Pair Connection Slave Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)	Only available in certain models
Ethernet Modem Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)	
Reverse Telnet Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)	
Disabled Mode	Enable/Disable	Disable	N/A	N/A	

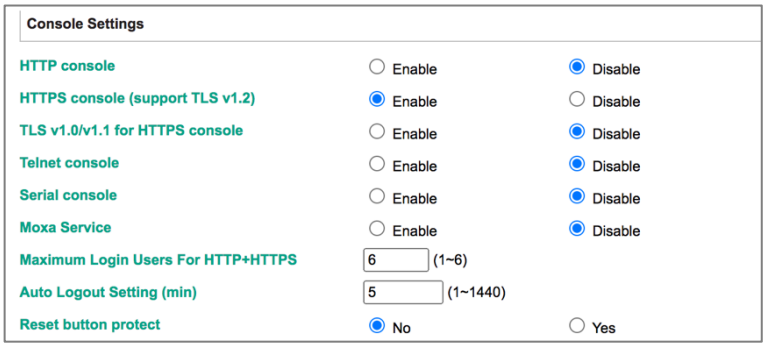
For security reasons, disable unused services. After the initial setup, use services with stronger security for data communication. Refer to the table below for the suggested settings.

Service Name	Suggested Settings	Type	Port Number	Security Remark
Moxa Command (DSCI)	**Disable**	TCP	14900, 4900	Disable this service as it is not commonly used
		UDP	4800	
DNS_wins	**Enable**	UDP	53, 137, 949	A necessary service to get IP; cannot be disabled
SNMP	**Disable**	UDP	161	Suggest to manage NPort via HTTPS console
HTTP Server	**Disable**	TCP	80	Disable HTTP to prevent plain text transmission
HTTPS Server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for NPort configuration
Telnet Server	**Disable**	TCP	23	Disable this service as it is not commonly used
DHCP Client	**Disable**	UDP	67, 68	Assign an IP address manually for the device
SNTP Client	**Disable**	UDP	Random Port	Suggest to use the SNTP server for secure time synchronization
Remote System Log	**Enable**	UDP	Random Port	Suggest using a system log server to store all the logs from all the devices in the network

For console services, we recommend the following:

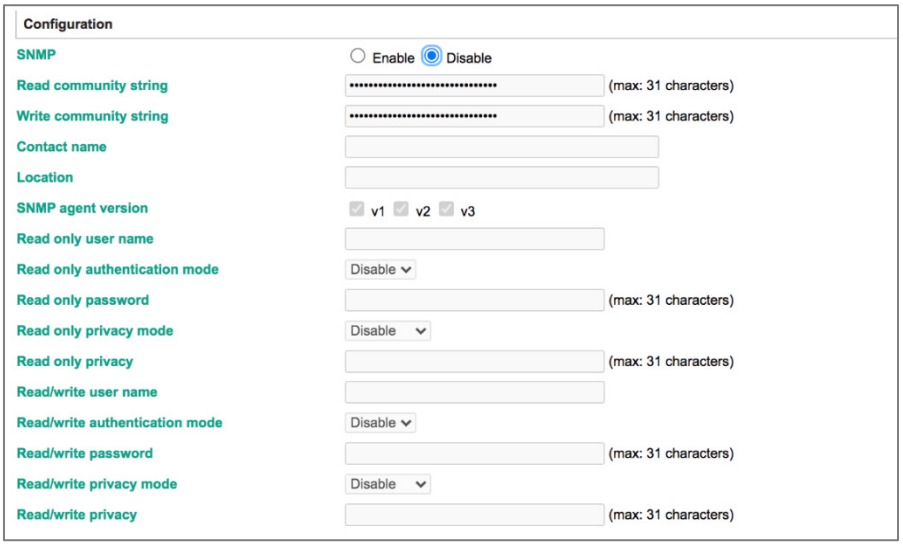
HTTP	Disable
HTTPS	Enable
Telnet	Disable
Moxa Command	Disable

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



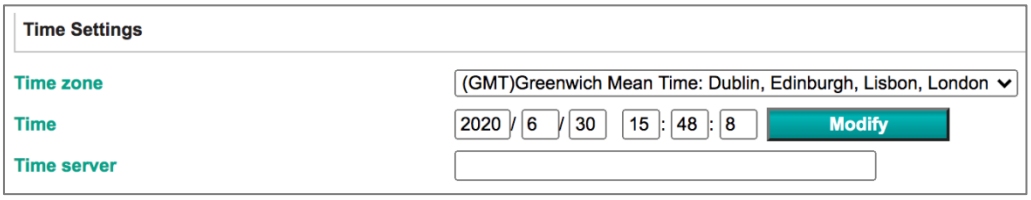
The NPort 5110, NPort 5130/5150, and NPort 5200 Series can only enable or disable the Web console (HTTP console), Telnet console, or Reset button protection.

- To disable the SNMP agent service, For the SNMP agent service, log in to the HTTP/HTTPS console and select **Administration > SNMP Agent**, then select **Disable** for SNMP., then. Then, select **Disable** for the SNMP agent service.



The NPort 5110, NPort 5130/5150, and NPort 5200 Series only support SNMP v1 and v2.

To disable the the SNTP service server, log in to the HTTP/HTTPS/Telnet console and select **Basic Settings,** and keep the **Time server** setting empty. This will disable the SNTP service.. Then, keep the Time server empty as **Disable** for the SNTP Server.

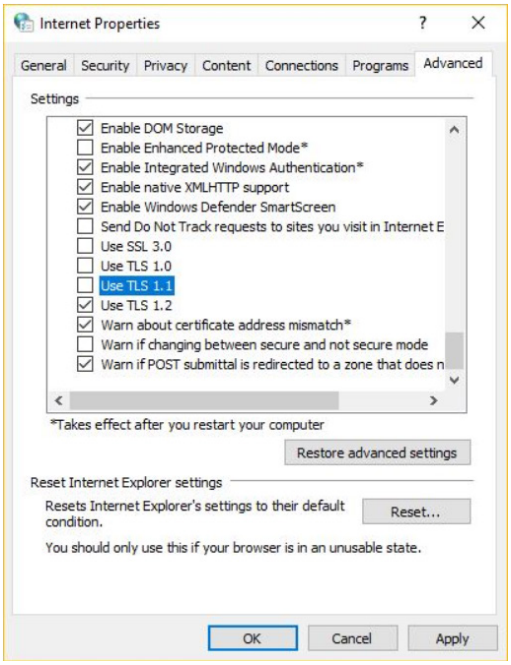


- For the operation mode services, it depends on how you bring your serial device to the Ethernet network. For example, if your host PC uses legacy software to open a COM port to communicate with the serial device, then the NPort will enable the Real COM mode for this application. If you don't want the NPort to provide such a service, log in to the HTTP/HTTPS/SSH/Telnet console, **select Serial Port Settings > Port # > Operation Modes**, and then select **Disable**.

Note For each instruction above, click the **Submit** button to save your changes, then restart the NPort device so the new settings will take effect.

3.2 HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. As TLS v1.1 or lower has severe vulnerabilities that can easily be hacked, the NPort 5000 Series uses TLS v1.2 for HTTPS to ensure data transmissions are secured. (The NPort 5100/5200 Series does not support HTTPS, which is the exception.) Make sure your browser has TLS v1.2 enabled.

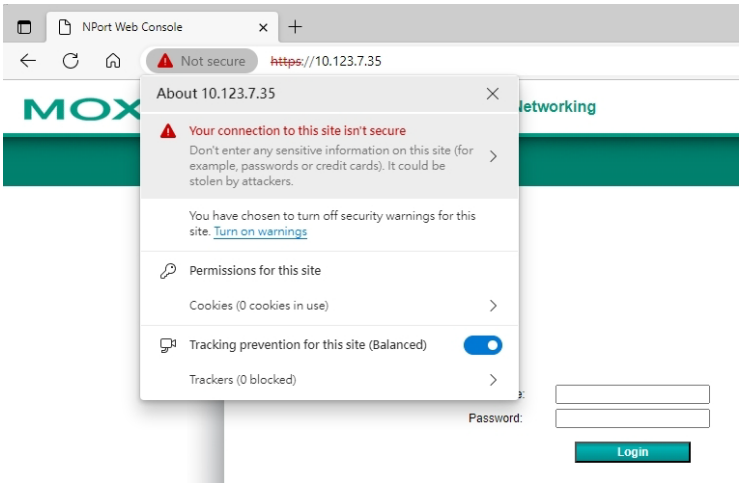


To use the HTTPS console without a certificate warning appearing, you need to import the self-signed certificate from the NPort 5000 Series.

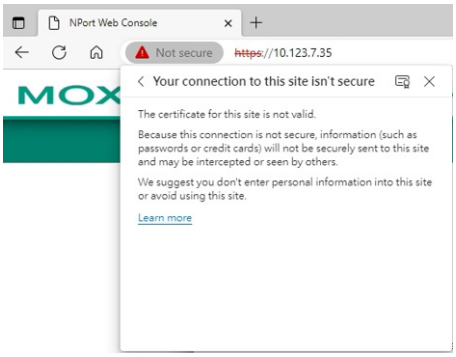
Log in to the HTTPS console and follow the steps below. You can export the self-signed certificate. Then, import it to the host's browser to recognize the NPort's certificate as a trusted one.

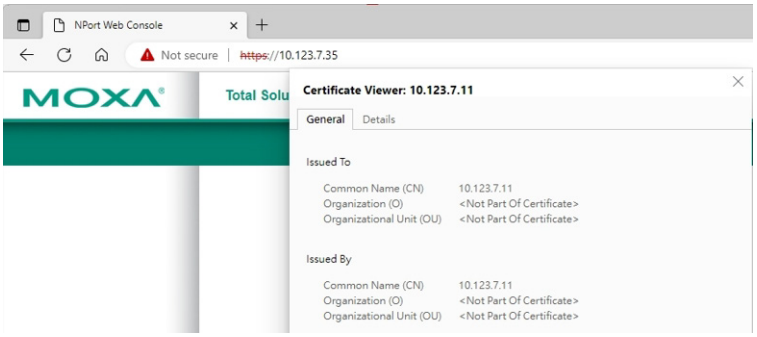
Step 1: Execute the browser and input **https://NPort's IP address** to access the web console of an NPort device.

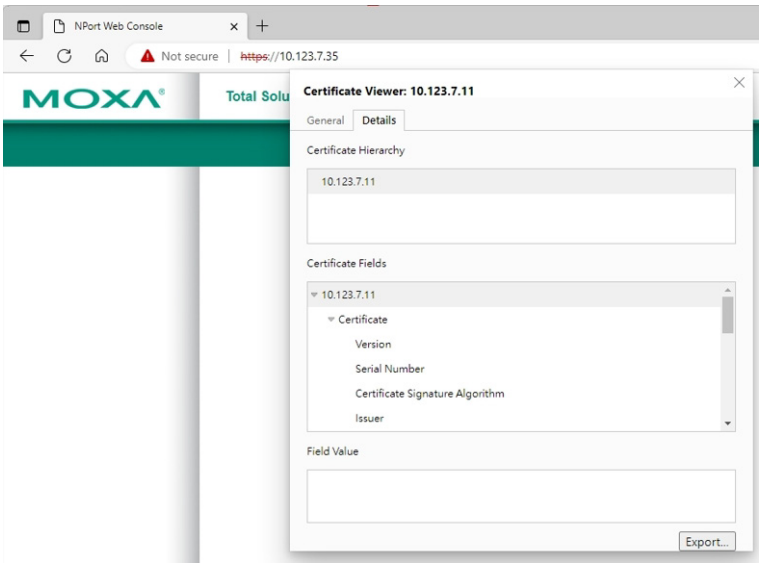
Step 2: You may find a **Not secure** icon before the IP address, click the **Not secure** icon, and the browser may prompt out some options. Select **Your connection to this site isn't secure**.



Step 3: Click **Learn more.** Then, you will find more information about the self-signed certificate of the NPort device. Switch to the **Details** tab to find an **Export** button. Click **Export** to export the self-signed certificate.



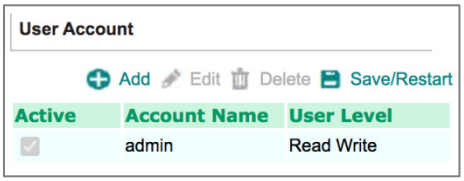


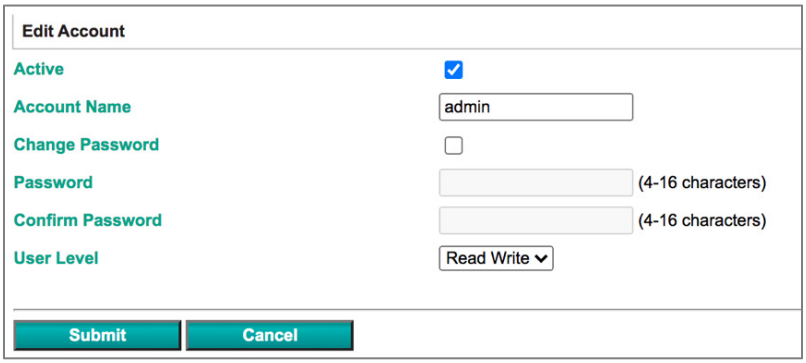


Step 4: Import the self-signed certificate to your browser. The "Not secure" warning will not show again.

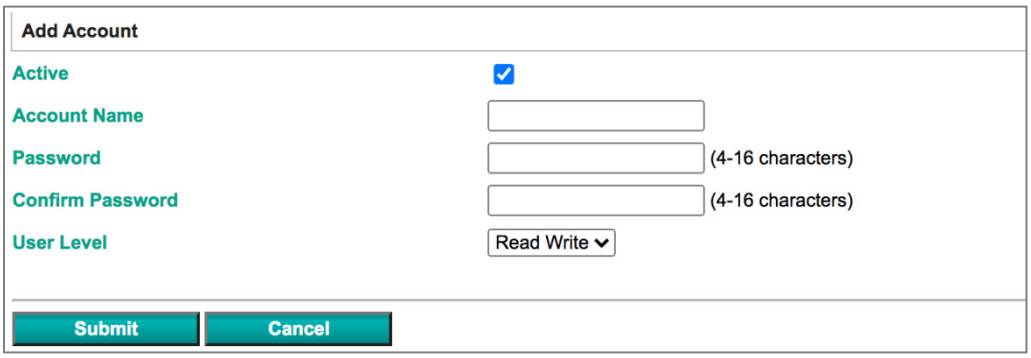
3.3 Account Management

- Through the administration account, admin, log in to NPort 5000 Series and perform configuration settings. To change the default password (moxa), please log in to the HTTP/HTTPS/Telnet console and select **Administration > Account Management > User Account**. Click on the 'admin' account row and select 'Edit' in the top toolbar. Input the old password in the **Password** field and the new password in **Confirm Password** field (at least 4 characters) to change the password. A screenshot of the GUI for the web console is shown below.



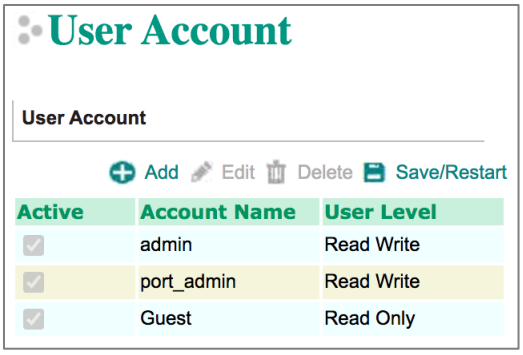


- To add new general users, please log in to the HTTP/HTTPS/Telnet console and select **Administration > Account Management > User Account**. Click **Add** in the top toolbar, then input the Account Name, Password, Confirm Password to add a new user. A snapshot of the GUI for the web console is shown below.



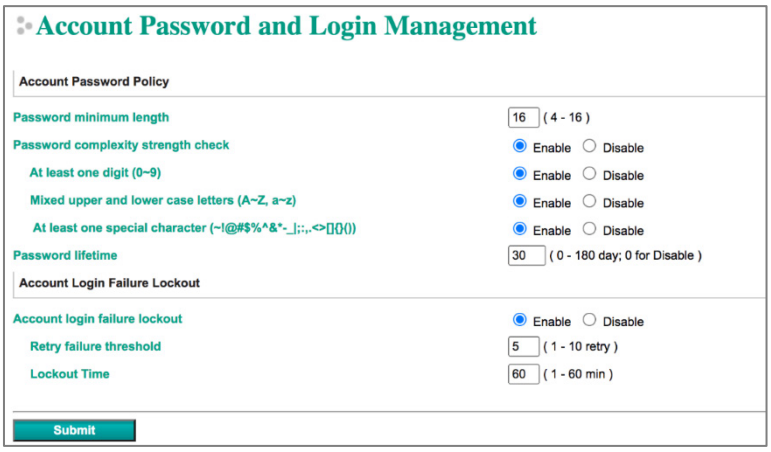
- To delete an account, click on the account name and select **Delete** in the top toolbar.
- After making any changes, click **Save/Restart** in the top toolbar.

Note We suggest you manage your device with another "administrator level" account instead of using the default "admin" account, as it is commonly used by embedded systems. Once the new administrator level account has been created, the original "admin" account should be monitored for security reasons to prevent brute-force attacks.

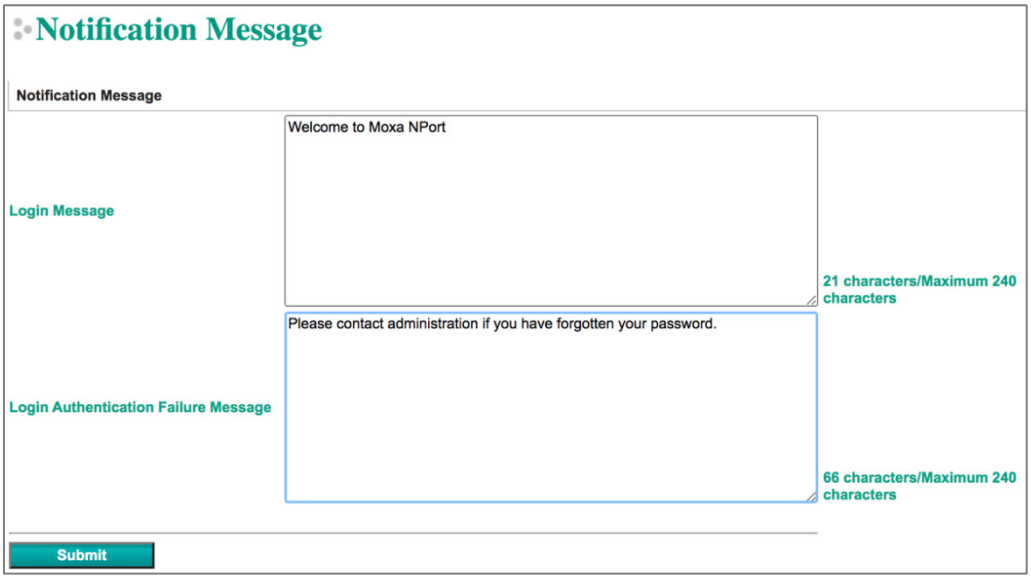


- Considering all security levels, the login password policy and failure lockout can be configured. To configure it, please log in to the HTTP/HTTPS console and select **Administration > Account Management > Password & Login Policy**. Not only can the **Account Password Policy** be configured, but the **Account Login Failure Lockout** can be further enabled to increase the security level of the account management.

  It is suggested to set the password policy at a higher complexity. For example, set the **Password minimum length** at 16, enable all password complexity strength checks, and enable the **Password lifetime** checking mechanism. Also, to avoid a brute-force attack, it's suggested to enable the **Account login failure lockout** feature. A screenshot of the GUI for the web console is shown below.



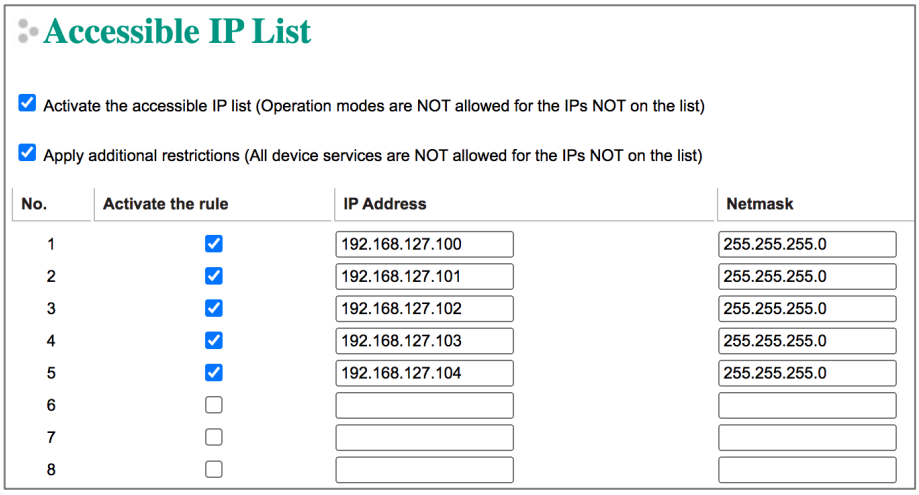
- For some system security requirements, an approved warning banner needs to be displayed to all users attempting to access the device. Besides the warning banner, please log in to the HTTP/HTTPS console and select **Administration > Account Management > Notification Message**. Users can type in the warning message in the **Login Message** field at all access points.



The NPort 5110, NPort 5130/5150, and NPort 5200 Series do not support Account Management function.

3.4 Accessible IP List

The NPort 5000 Series has a feature that can add or block remote host IP addresses to prevent unauthorized access. If a host's IP address is in the accessible IP table, then the host will be allowed to access the NPort 5000 Series. To configure it, please log in to the HTTP/HTTPS console and select **Accessible IP List**.



You may add a specific address or range of addresses by using a combination of an IP address and a netmask as follows:

- **To allow access to a specific IP address:** Enter the IP address in the corresponding field, then 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 **Enable** checkbox for the Accessible IP List is not checked.

Additional configuration examples are shown in the following table:

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 in the Accessible IP List.

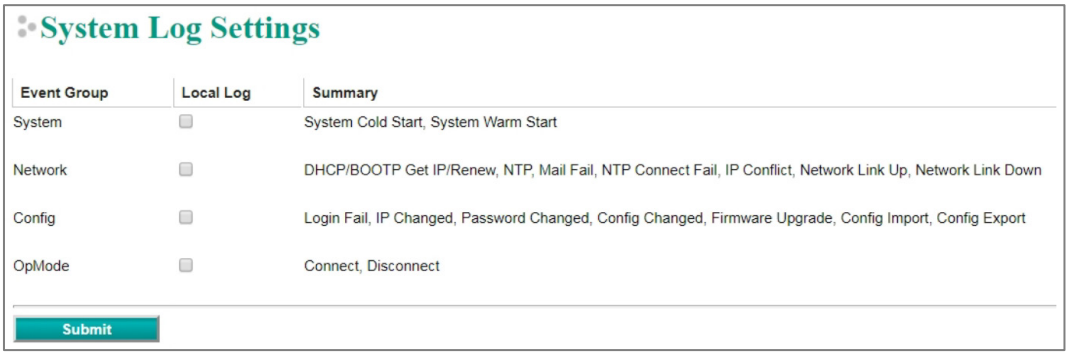
The NPort 5110, NPort 5130/5150, and NPort 5200 Series only support Activate the accessible IP list (Operation modes are NOT allowed for the IPs that are not on the list).

3.5 Logging and Auditing

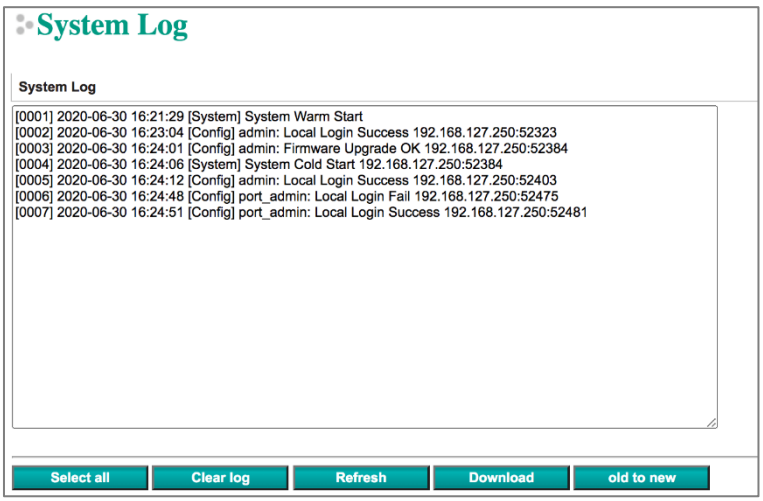
- These are the events that will be recorded by the NPort 5000 Series:

Event Group	Summary
System	System cold start, system warm start
Network	DHCP/BOOTP gets IP/renew, NTP connect failed, IP conflict, Network link down
Configuration	Login failed, IP changed, Password changed, Firmware upgraded, Certificate imported, Configuration imported or exported, Configuration changed, Clear event logged
OpMode	Connect, Disconnect

- To configure this setting, log in to the HTTP/HTTPS console and select **System Log Settings**. Then, enable the **Local Log** for recording on the NPort 5000 device. It is suggested to enable the system log settings to record all important system events in order to monitor any security issue with the device status. A screenshot of the GUI for the web console is shown below.



- To review the above events, log in to HTTP/HTTPS console, select **Monitor > System Log**. A screenshot of the GUI for the web console is shown below.



4 Patching/Upgrades

4.1 Patch Management Plan

With regard to patch management, Moxa in general releases version enhancement with thorough release notes annually. If any security vulnerability issue is identified, Moxa will release a beta fix within 30 days.

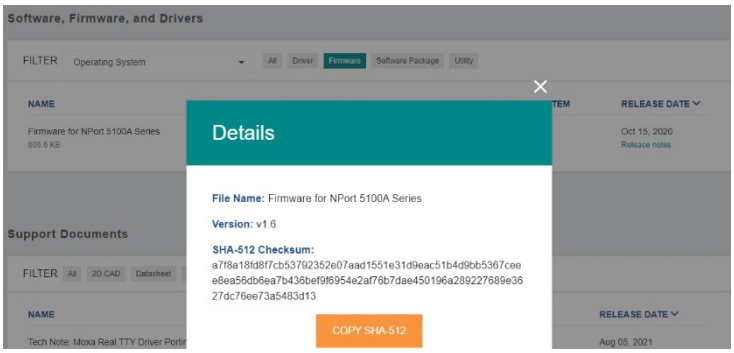
4.2 Firmware Upgrades

The process of firmware and/or software upgrade is instructed as below.

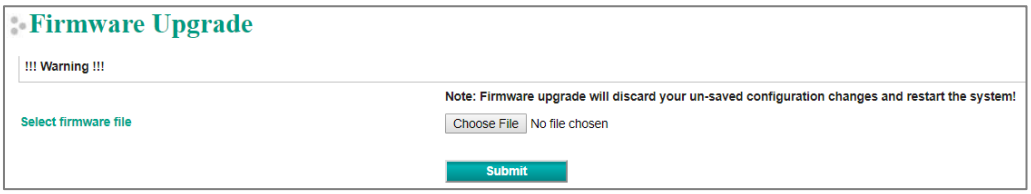
- We will release the latest firmware and software, along with its released notes on our official website. The links listed below are for specified items for the NPort 5000 Series.

NPort Series	URL
5100A	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5100a-series#resources
5100	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5100-series#resources
5200A	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5200a-series#resources
5200	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5200-series#resources
5400	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5400-series#resources
5600	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5600-series#resources
5600-DT	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5600-dt-series#resources
5600-DTL	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5600-dtl-series#resources
IA5000A	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/industrial-device-servers/nport-ia5000a-series#resources
IA5000	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/industrial-device-servers/nport-ia5000-series#resources
5000AI-M12	https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/general-device-servers/nport-5000ai-m12-series#resources

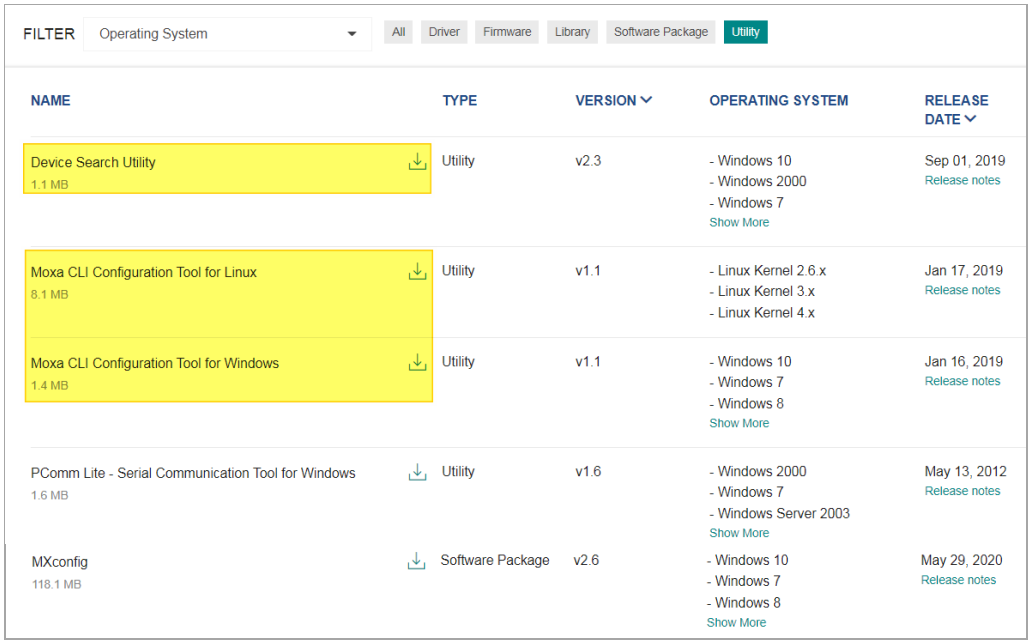
- Moxa's website provides the SHA-512 hash value for you to double-check if the firmware is identical to the one on the website.



- When a user wants to upgrade the firmware of the NPort 5000 Series, please download the firmware from the website first. Then log in to HTTP/HTTPS console and select **Upgrade Firmware**. Click the **Choose File** button to select the proper firmware and click **Submit** to upgrade the firmware.



- If a user wants to upgrade the firmware of the NPort 5000 Series with multiple units , please download the utility Device Search Utility (DSU) or MXconfig for a GUI interface, or the Moxa CLI Configuration Tool for a CLI interface to perform the mass deployment.



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