The Security Hardening Guide for the NPort 5000 Series

Moxa Technical Support Team
support@moxa.com

Contents

1. Introduction 2
2. General System Information 3
2.1. Basic Information About the Device 3
2.2. Deployment of the Device 4
3. Configuration and Hardening Information 5
3.1. TCP/UDP Port Status 6
3.2. Account Management 10
3.3. Accessible IP List 12
3.4. Logging and Auditing 13
4. Patching/Upgrades 15
4.1. Patch Management Plan 15
4.2. Firmware Upgrades 15
5. Security Information and Vulnerability Feedback 17

 Released on March 26, 2021

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 (IIoT). With over 30 years of industry experience, Moxa has connected more than 57 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

1. Introduction

We at Moxa understand that more and more of Moxa's customers are concerned about the security of their network system. Naturally, these concerns also extend to individual devices. Moxa is committed to cybersecurity and endeavors to make our products as secure as possible. In support of our customers to meet certain security guidelines and frameworks, this document intends to provide guidelines on how to configure and secure the installation of Moxa's devices.

We want to reiterate that the recommended steps to securing a Moxa device, as discussed in this document, are guidelines as applications vary from one Moxa customer to another. Furthermore, these recommendations are best practices for most applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict or affecting your application, it's highly recommended to review and test the configuration thoroughly before implementing it in your production system.

2. General System InformationBasic Information About the Device

Model	Function	Operating System	Firmware Version
NPort 5000A Series	General purpose	Moxa Operating System	Version 1.6
NPort 5110	General purpose	Moxa Operating System	Version 2.10
NPort 5130/5150	General purpose	Moxa Operating System	Version 3.9
NPort 5200 Series	General purpose	Moxa Operating System	Version 2.12
NPort 5400 Series	General purpose	Moxa Operating System	Version 3.14
NPort 5600-DT Series	General purpose	Moxa Operating System	Version 2.8
NPort 5600-DTL Series	Entry level	Moxa Operating System	Version 1.6
NPort 5600 Series	Rackmount	Moxa Operating System	Version 3.10
NPort 5000AI-M12 Series	Railway	Moxa Operating System	Version 1.5
NPort IA5000 Series	Industrial automation	Moxa Operating System	Version 1.7
NPort IA5000A Series	Industrial automation	Moxa Operating System	Version 1.7

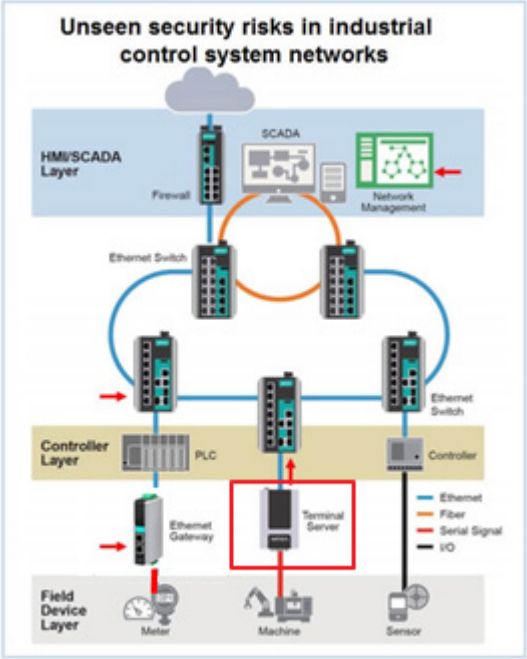
The NPort 5000 Series is a device server specifically designed to allow industrial devices to be directly accessible from the network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations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

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

It is suggested to deploy the NPort 5000 Series behind a security firewall network that has sufficient security features in place and ensures that networks are safe from internal and external threats.

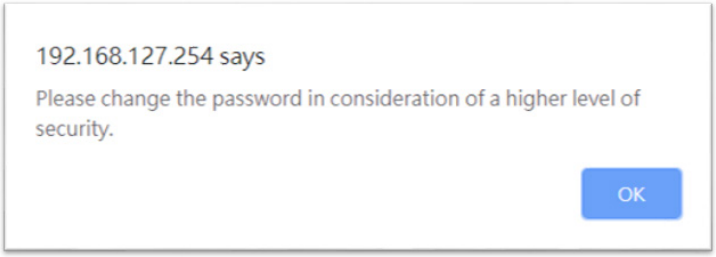
Make sure that the physical protection of the NPort devices and/or the system fulfill the requirements of basic risk management. Depending on the environment and the threat situation, the form of protection can vary significantly.



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 in order to ensure a higher level of security. A screenshot of the GUI for the web console is shown below.



3.1. TCP/UDP Port Status

Please 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.

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	DHCP client needs to acquire the system IP address from the server
SNTP	Enable/Disable	Disable	UDP	Random Port	Synchronize the time settings with the 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 the 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.)	

Operation Mode	Option	Default Settings	Type	Port Number	Remark & Description
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	

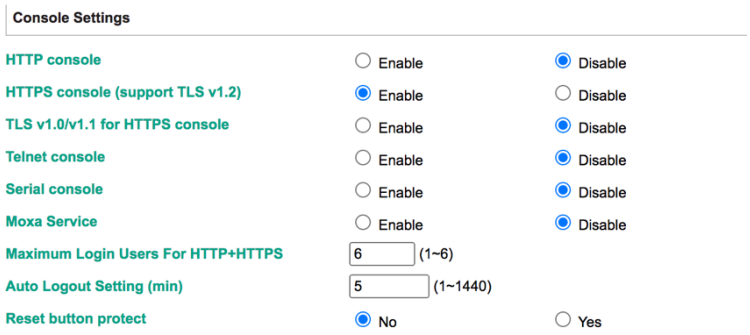
For security reasons, you can consider disabling unused services and using a higher security level of services for data communication after setting up the devices. Please refer to the table below for the suggested settings.

Service Name	Suggested Settings	Type	Port Number	Security Remark
Moxa Command (DSCI)	**Disable**	TCP	14900, 4900	Disable service that 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 the service for HTTP from plain text transmission
HTTPS Server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for NPort configuration
Telnet Server	**Disable**	TCP	23	Disable service that is not commonly used
DHCP Client	**Disable**	UDP	67, 68	Suggest to assign a system IP in static manner
SNTP Client	**Disable**	UDP	Random Port	Suggest to use the SNTP server for secure time synchronization
Remote System Log	**Enable**	UDP	Random Port	Suggest to have a system log server to store all the logs from all the devices in the network

For the console services

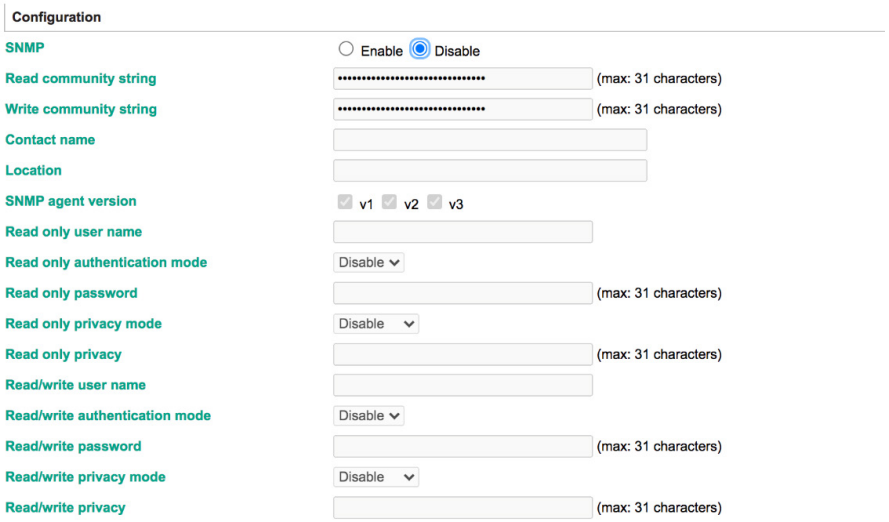
HTTP	Disable
HTTPS	Enable
Telnet	Disable
Moxa Command	Disable

Log in to the HTTP/HTTPS console and select **Basic Settings → Console Settings**. Then, you can select to enable or disable services as suggested. A screenshot of the GUI for the web console is shown below.

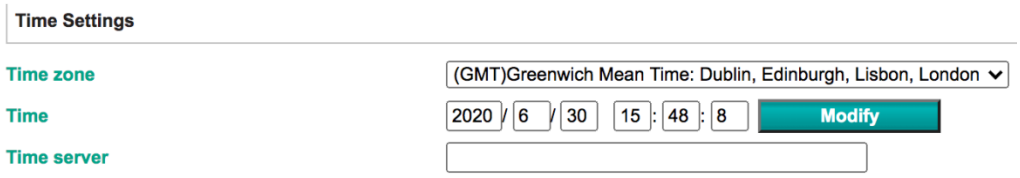


HTTPS is an encrypted communication channel. The encryption algorithm, which is lower than TLS v1.1, has severe vulnerabilities that can easily be hacked. So the device by default is using TLS v1.2 for the HTTPS console.

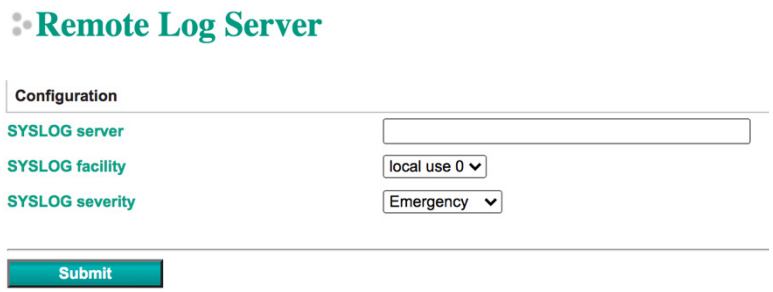
- For the SNMP agent service, log in to the HTTP/HTTPS console and select **Administration → SNMP Agent**. Then, select **Disable** for the SNMP agent service. A screenshot of the GUI for the web console is shown below.



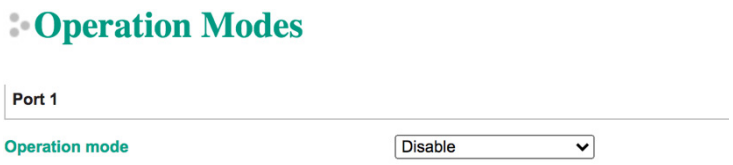
For the SNTP server, log in to the HTTP/HTTPS/SSH/Telnet console and select **Basic Settings**. Then, keep the Time server empty as **Disable** for the SNTP Server. A screenshot of the GUI for the web console is shown below.



- For the remote system log server, log in to the HTTP/HTTPS/SSH/Telnet console, select **Remote Log Server,** and keeps the SYSLOG server setting empty (disable Remote System Log Server). A screenshot of the GUI for the web console is shown below.



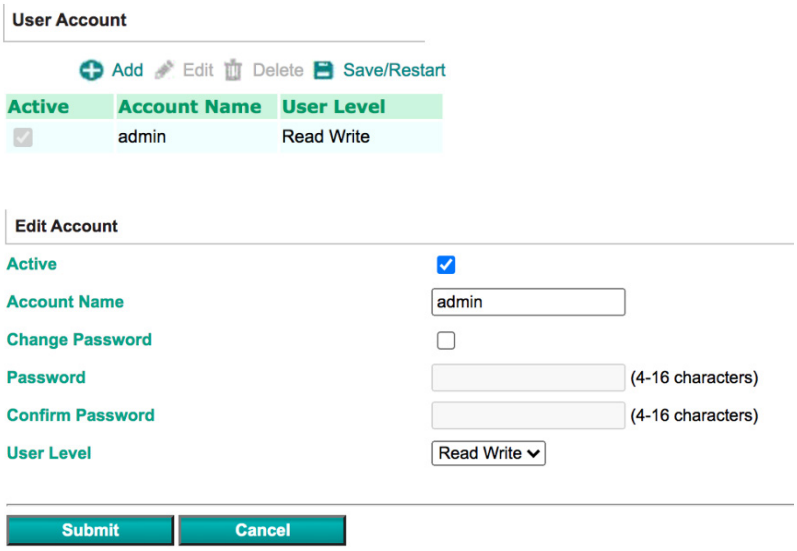
- For the operation mode services, only one can be enabled while the others need to be disabled. The specified one should be a necessary service to bring legacy devices into Ethernet-based networks. If you don't want to enable all the operation mode services, please log in to the HTTP/HTTPS/SSH/Telnet console, select **Operating Port Settings → Port # → Operation Modes**, and then select **Disable**. A screenshot of the GUI for the web console is shown below.



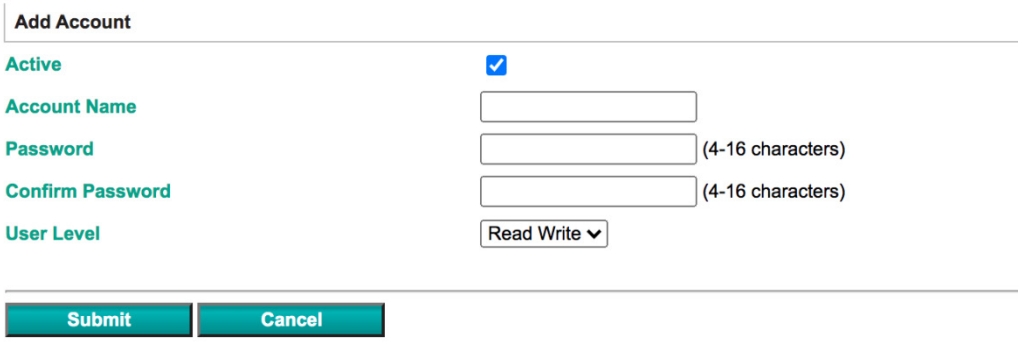
For each instruction above, click the **Submit** button to save the settings you have done, and then restart the NPort 5000 Series to make the new settings effective.

3.2. 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.



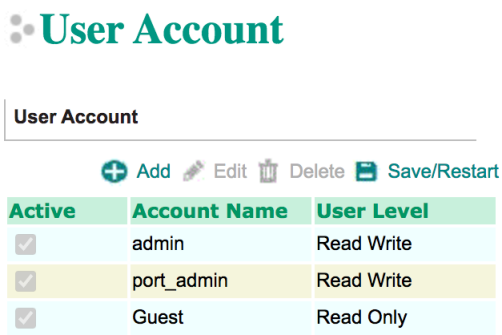
- To add new general users, please log in to the HTTP/HTTPS/Telnet console and select **Administration → Account Management → User Account**. Click **Add** in the top toolbar, then input the Account Name, Password, Confirm Password to add a new user. A screenshot of the GUI for the web console is shown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



Here, we can also **Delete** users.

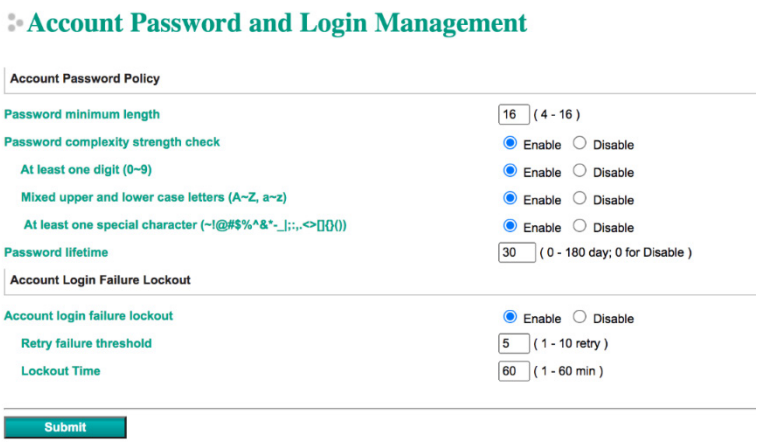
Please note that click **Save/Restart** is performed after any modification.

Note: It is suggested to manage the NPort 5000 Series in another "administration level" account instead of using the default "admin" account, as it is commonly used by embedded systems. Once the new administration level account has been created, it is suggested that the original "admin" account be monitored for security reasons to avoid a brute-force attack.

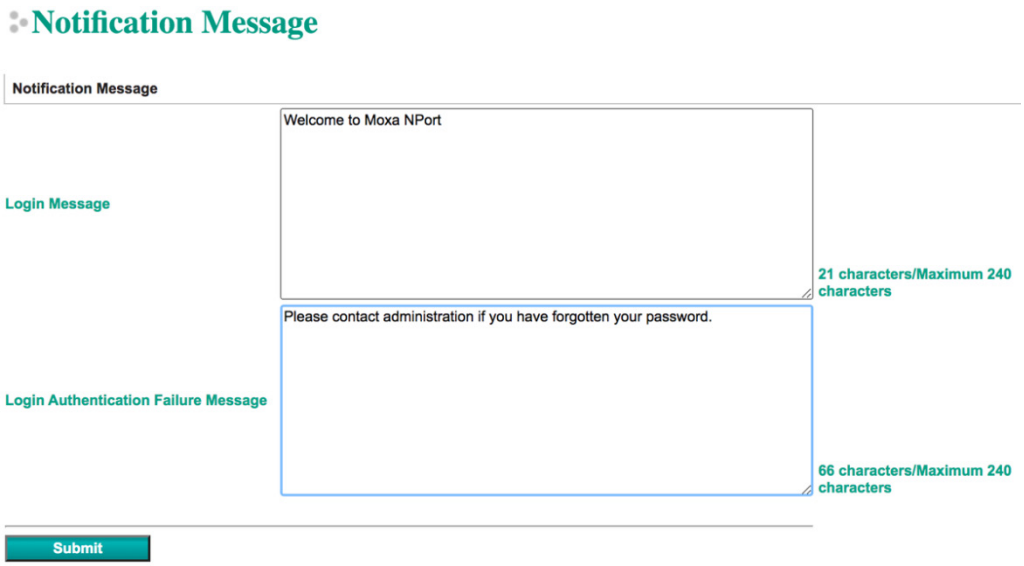


- Considering all security levels, the login password policy and failure lockout can be configured. To configure it, please log in to the HTTP/HTTPS console and select **Administration → Account Management → Password & Login Policy**. Not only can the **Account Password Policy** be configured, but the **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 that you enable the **Account login failure lockout** feature. A screenshot of the GUI for the web console is shown below.

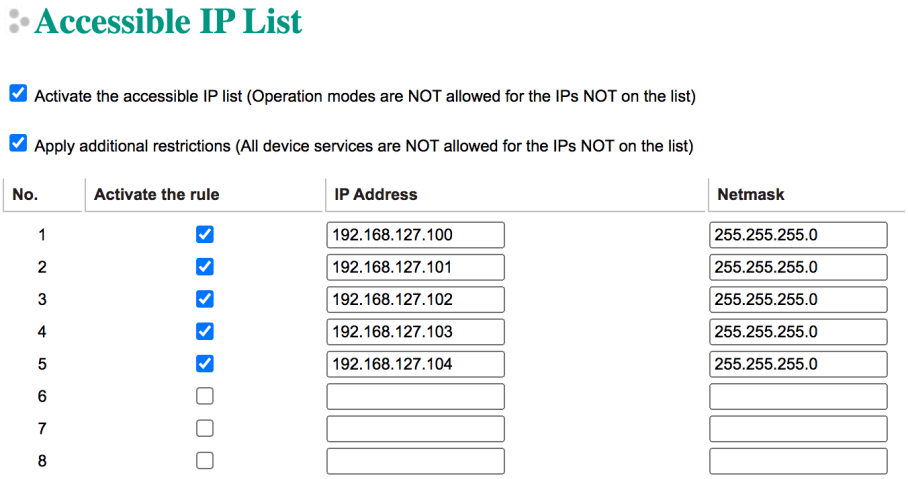


- For some system security requirements, an approved warning banner needs to be displayed to all users attempting to access the device. In addition to the warning banner, please log in to the HTTP/HTTPS console and select **Administration → Account Management → Notification Message**. Users can type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



3.3. Accessible IP List

- The NPort 5000 Series has a feature that can add or block remote host IP addresses to prevent unauthorized access. That is, 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; 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 **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 the communication peer is listed in the Accessible IP List for entering the web console.

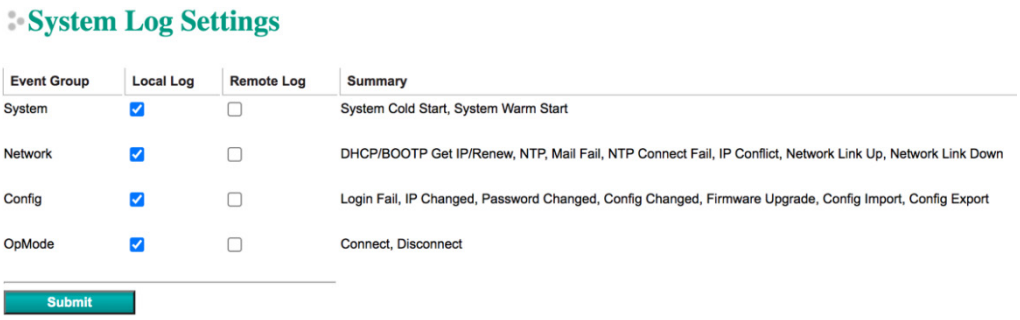
3.4. Logging and Auditing

- Please refer to table below for all the events that will be recorded by the NPort 5000 Series

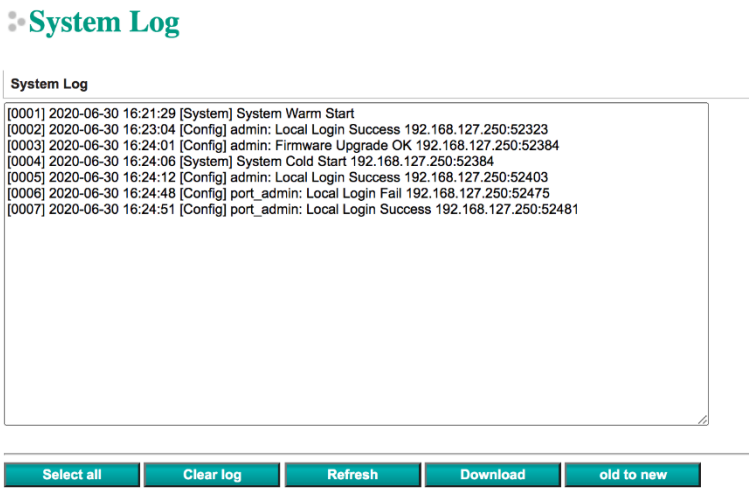
Event Group	Summary
System	System cold start, system warm start
Network	DHCP/BOOTP gets IP/renew, NTP connect failed, IP conflict, Network link down
Configuration	Login failed, IP changed, Password changed, Firmware upgraded, Certificate imported, Configuration imported or exported, Configuration changed, 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 and/or **Remote Log** for keeping the records on a server about the network. 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 .

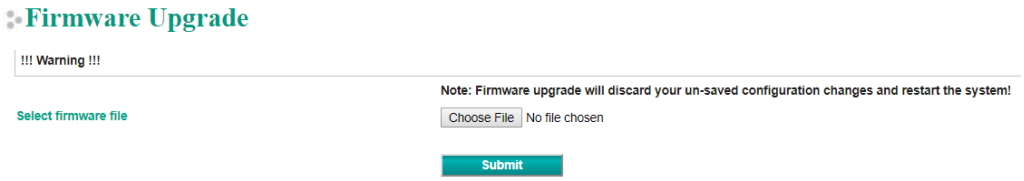
4.2. Firmware Upgrades

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

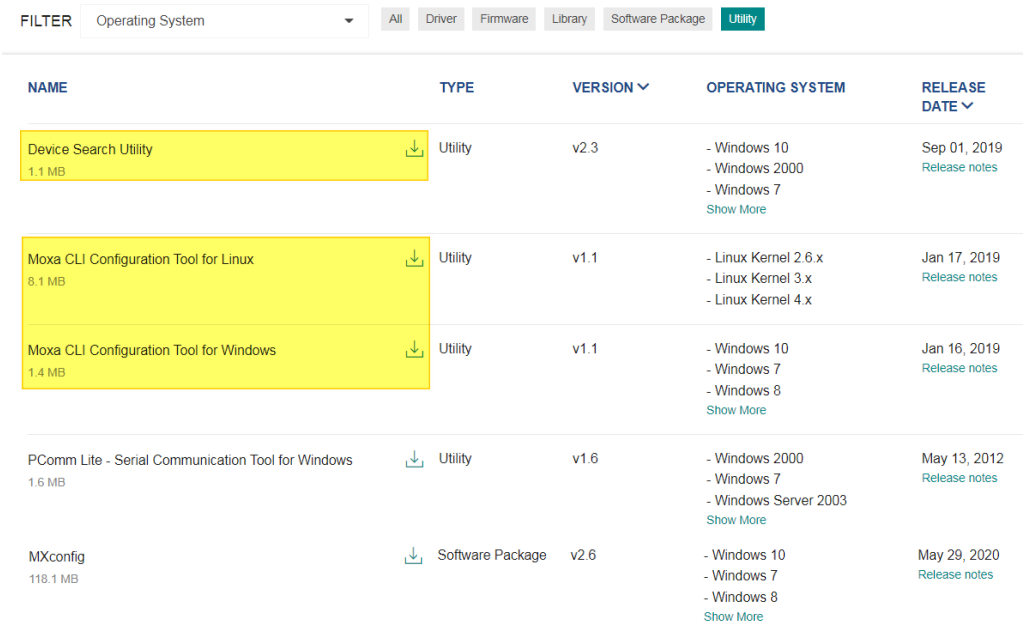
- We will release the latest firmware and software along with its released notes on our official website. The links listed below are for specified items for the NPort 5000 Series.

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

- If a user wants to upgrade the firmware of the NPort 5000 Series, 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 for 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 preform 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 Cyber Security Response Team (CSRT) 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