The Security Hardening Guide for the NPort 5000 Series

Moxa Technical Support Team
support@moxa.com

Contents

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

1. Introduction

This document provides guidelines on how to configure and secure the NPort 5000 Series. The recommended steps in this document should be considered as best practices for security in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system in order to ensure that your application is not negatively impacted.

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

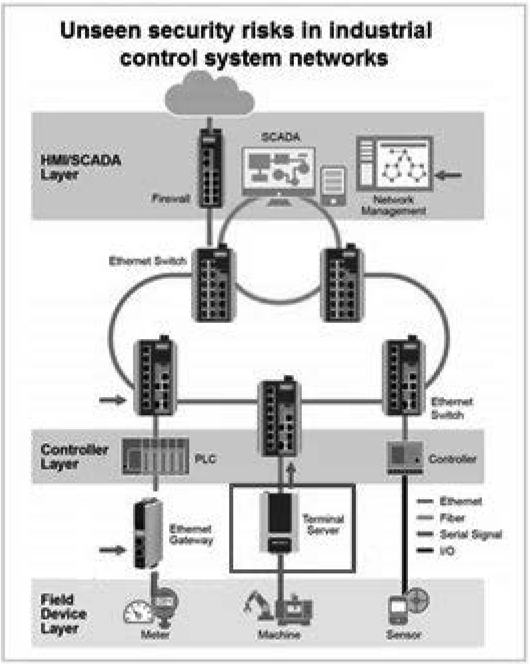
The NPort 5000 Series is a device server specifically designed to allow industrial devices to be directly accessible from the network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations 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

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.

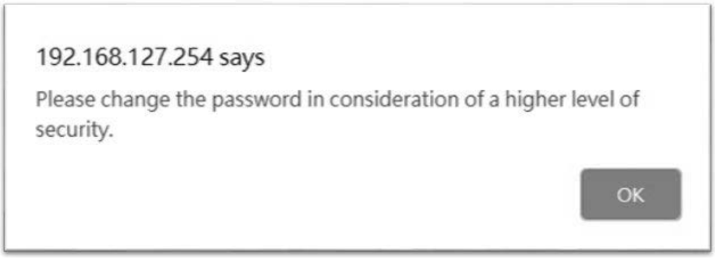
Make sure that the physical protection of the MGate devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



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.



192.168.127.254 says

Please change the password in consideration of a higher level of security.

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.

Service Name	Option	Default Setting	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 NPort 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 Setting	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 Setting	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	

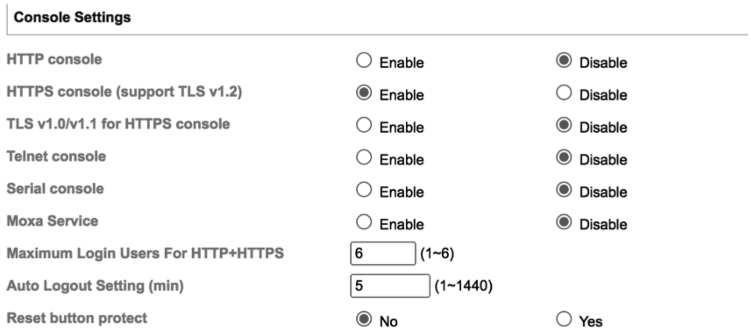
For security reasons, you should consider disabling unused services. After initial setup, use services with stronger security for data communication. Refer to the table below for the suggested settings.

Service Name	Suggested Setting	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

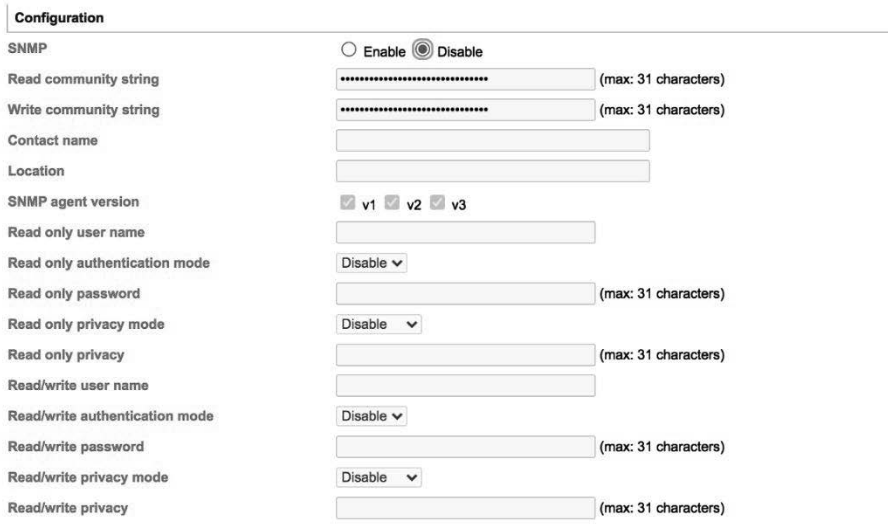
To enable or disable these services, log in to the HTTP/HTTPS console and select **Basic Settings → Console Settings**.



Console Settings

HTTP console	○ Enable	● Disable
HTTPS console (support TLS v1.2)	● Enable	○ Disable
TLS v1.0/v1.1 for HTTPS console	○ Enable	● Disable
Telnet console	○ Enable	● Disable
Serial console	○ Enable	● Disable
Moxa Service	○ Enable	● Disable
Maximum Login Users For HTTP+HTTPS	6 (1~6)	
Auto Logout Setting (min)	5 (1~1440)	
Reset button protect	● No	○ Yes

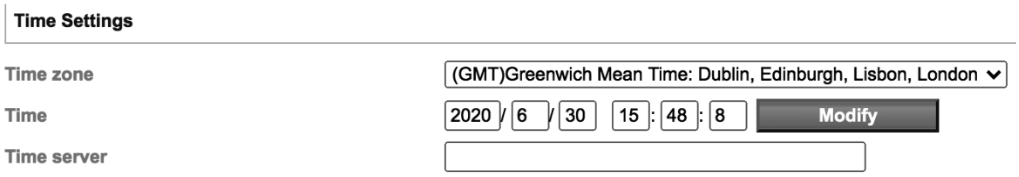
For the SNMP agent service, log in to the HTTP/HTTPS console and select **Administration → SNMP Agent**, select **Disable** for SNMP, and select **Disable** for the SNMP agent service.



Configuration

SNMP	○ Enable ● Disable
Read community string	•••••••••••••••••••••••••••••• (max: 31 characters)
Write community string	•••••••••••••••••••••••••••••• (max: 31 characters)
Contact name	
Location	
SNMP agent version	☑ v1 ☑ v2 ☑ v3
Read only user name	
Read only authentication mode	Disable
Read only password	(max: 31 characters)
Read only privacy mode	Disable
Read only privacy	(max: 31 characters)
Read/write user name	
Read/write authentication mode	Disable
Read/write password	(max: 31 characters)
Read/write privacy mode	Disable
Read/write privacy	(max: 31 characters)

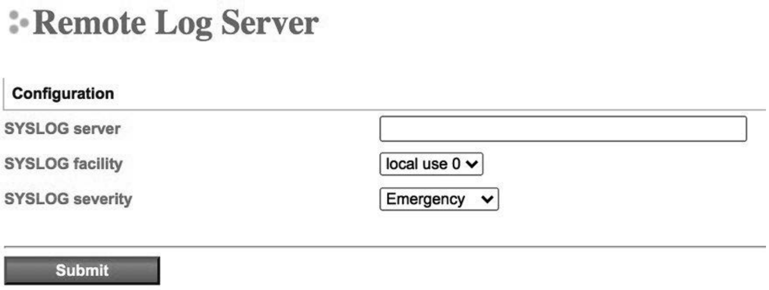
To disable the SNTP service server, log in to the HTTP/HTTPS/SSH/Telnet console and select **Basic Settings,** and keep the **Time server** setting empty. This will disable the SNTP service. Then, keep the Time server empty as **Disable** for the SNTP Server.



Time Settings

Time zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time	2020 / 6 / 30 15 : 48 : 8
Time server	

For the remote system log server, it depends on your network architecture. We recommend your network administrator to have a Log Server to receive the log messages from the device. In this case, log in to the HTTP/HTTPS/SSH/Telnet console, select **Remote Log Server**, and input the IP address of the Log Server in the **SYSLOG server** field. If your network doesn't have one, keep it empty (disable **Remote System Log Server**).

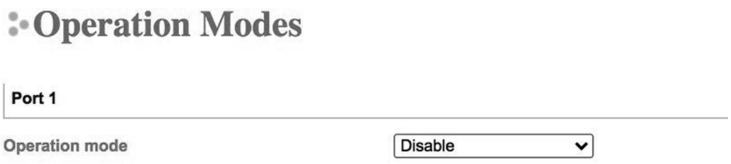


Remote Log Server

Configuration

SYSLOG server	
SYSLOG facility	local use 0
SYSLOG severity	Emergency

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 a 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**.



Operation Modes

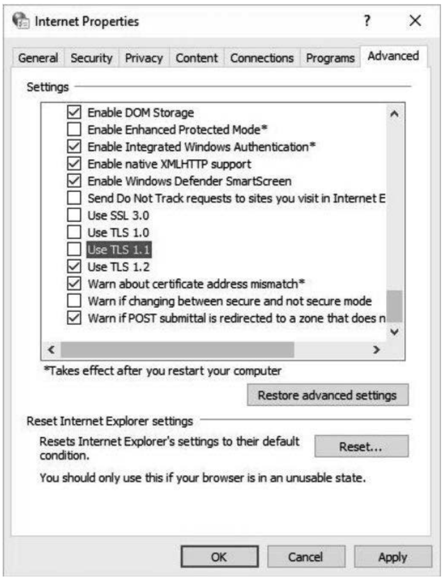
Port 1

Operation mode: 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. Make sure your browser has TLS v1.2 enabled.



Settings

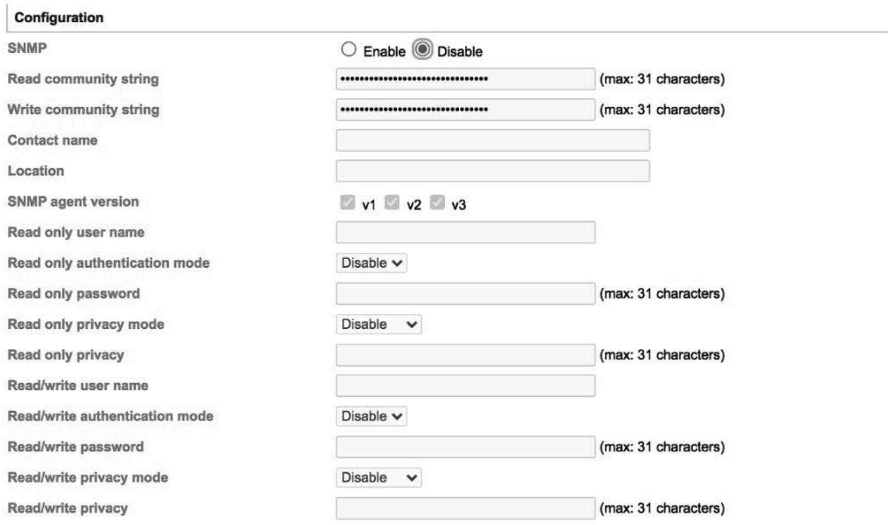
☑ Enable DOM Storage
□ Enable Enhanced Protected Mode*
☑ Enable Integrated Windows Authentication*
☑ Enable native XMLHTTP support
☑ Enable Windows Defender SmartScreen
□ Send Do Not Track requests to sites you visit in Internet E
□ Use SSL 3.0
□ Use TLS 1.0
□ Use TLS 1.1
☑ Use TLS 1.2
☑ Warn about certificate 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

Reset Internet Explorer settings

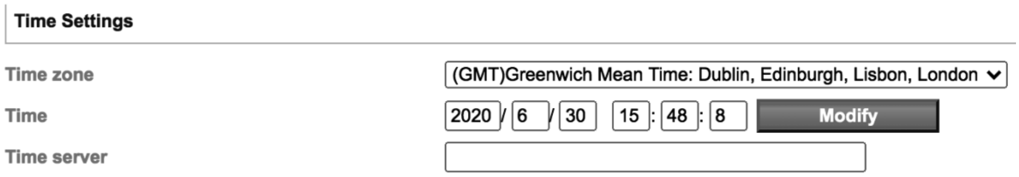
Resets Internet Explorer's settings to their default condition.

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



Configuration

SNMP	○ Enable ● Disable	
Read community string	••••••••••••••••••••••••••••••	(max: 31 characters)
Write community string	••••••••••••••••••••••••••••••	(max: 31 characters)
Contact name		
Location		
SNMP agent version	☑ v1 ☑ v2 ☑ v3	
Read only user name		
Read only authentication mode	Disable	
Read only password		(max: 31 characters)
Read only privacy mode	Disable	
Read only privacy		(max: 31 characters)
Read/write user name		
Read/write authentication mode	Disable	
Read/write password		(max: 31 characters)
Read/write privacy mode	Disable	
Read/write privacy		(max: 31 characters)



Time Settings

Time zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Time	2020 / 6 / 30 15 : 48 : 8
Time server	

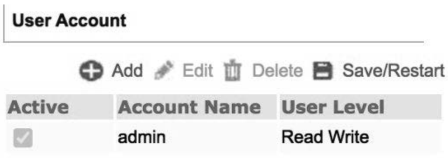
Operation Modes

Port 1

Operation mode	Disable

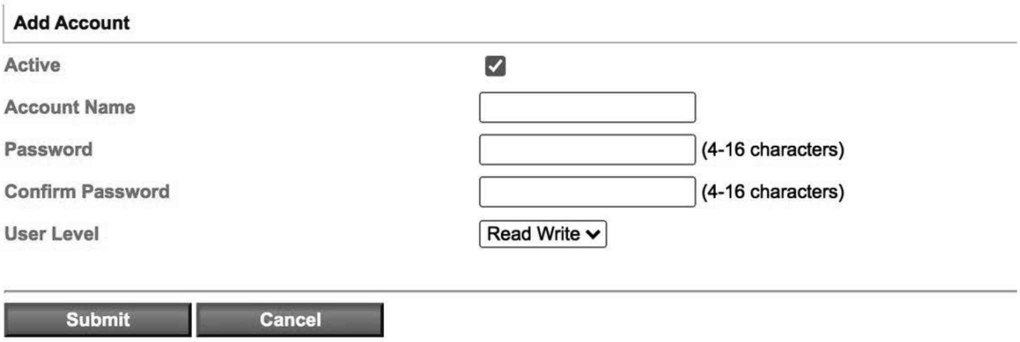
3.3. Account Management

- The NPort 5000 Series provides two different user levels, Read Write (admin) and Read Only (user). With a Read Write account, you can access and modify all settings through the web console. With a Read Only account, you can only view settings.
- The default Read Write account is **admin**, with the default password **moxa**. To manage accounts, log in to the web console and select **Administration → Account Management → User Account**.



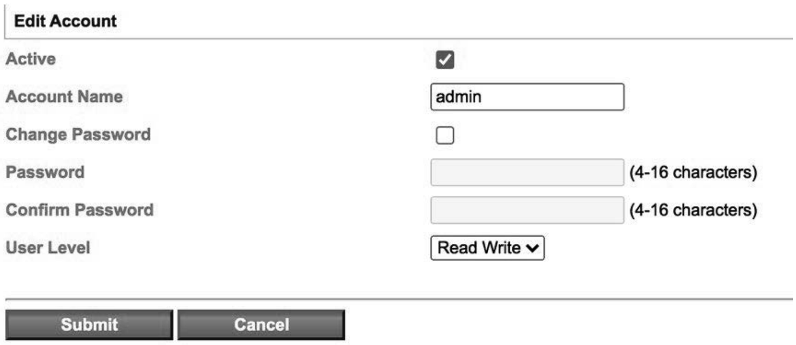
Active	Account Name	User Level
☑	admin	Read Write

- To add a new account, click **Add** in the top toolbar, then enter the Account Name, Password, Confirm Password, and select a User Level.



Active	☑
Account Name	
Password	(4-16 characters)
Confirm Password	(4-16 characters)
User Level	Read Write

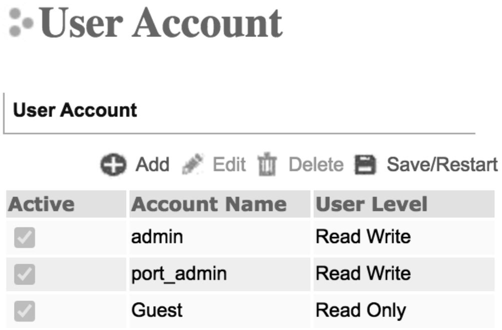
- To modify an existing account, click on the account name and select **Edit** in the top toolbar.



Active	☑
Account Name	admin
Change Password	□
Password	(4-16 characters)
Confirm Password	(4-16 characters)
User Level	Read Write

- 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, it is suggested that the original "admin" account should be monitored for security reasons to prevent brute-force attacks.

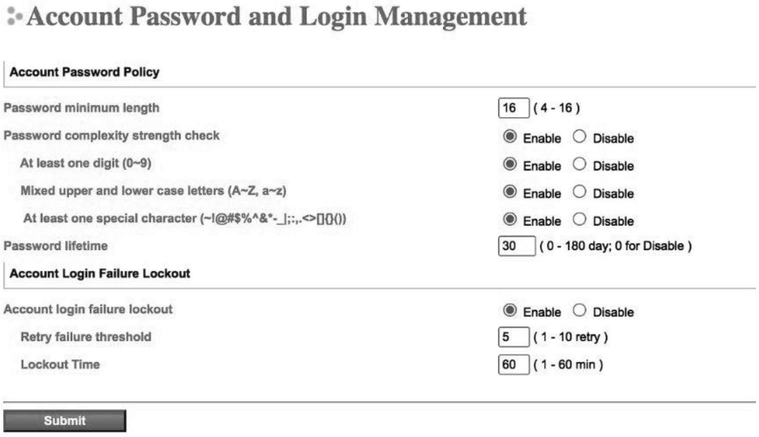


User Account

User Account

Active	Account Name	User Level
☑	admin	Read Write
☑	port_admin	Read Write
☑	Guest	Read Only

- To improve security, the login password policy and account login failure lockout can be configured. To configure them, log in to the HTTP/HTTPS console and select **Administration → Account Management → Password & Login Policy**.



Account Password and Login Management

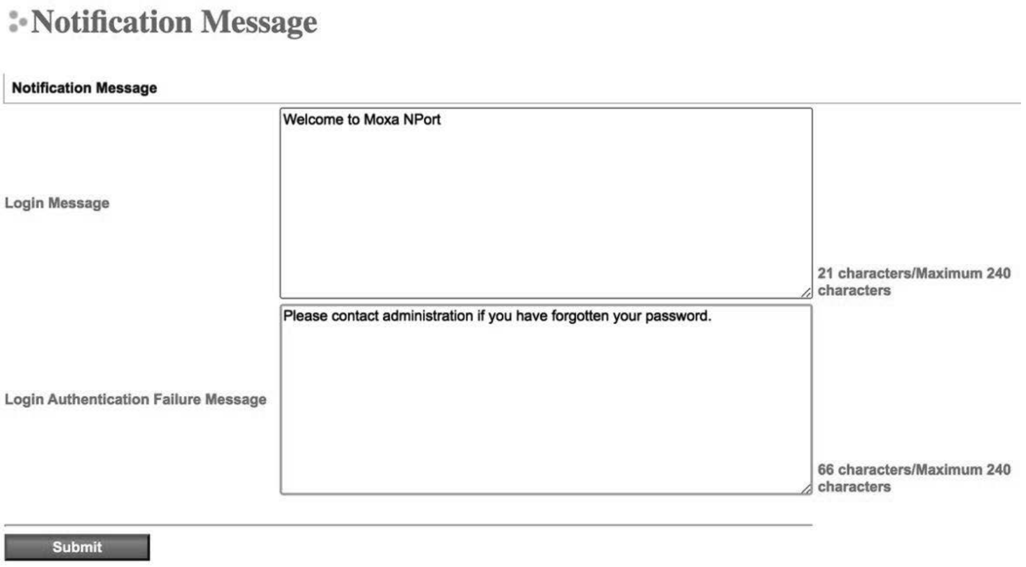
Account Password Policy

Password minimum length	16 (4 - 16)
Password complexity strength check	● Enable ○ Disable
At least one digit (0~9)	● Enable ○ Disable
Mixed upper and lower case letters (A~Z, a~z)	● Enable ○ Disable
At least one special character (~!@#$%^&*-_|;:,.<>[]{}())	● Enable ○ Disable
Password lifetime	30 (0 - 180 day; 0 for Disable)

Account Login Failure Lockout

Account login failure lockout	● Enable ○ Disable
Retry failure threshold	5 (1 - 10 retry)
Lockout Time	60 (1 - 60 min)

- You should adjust the password policy to require more complex passwords. For example, set the **Minimum length** to 16, enable all password complexity strength checks, and enable the **Password lifetime** options. Also, to avoid brute-force attack, it's suggested that you enable the **Account login failure lockout** feature.
- For some system security requirements, a warning message may need to be displayed to all users attempting to log in to the device. To add a login message, log in to the HTTP/HTTPS console and select **Administration → Account Management → Notification Message**, and enter a **Login Message** to use.



Notification Message

Notification Message

Login Message: Welcome to Moxa NPort

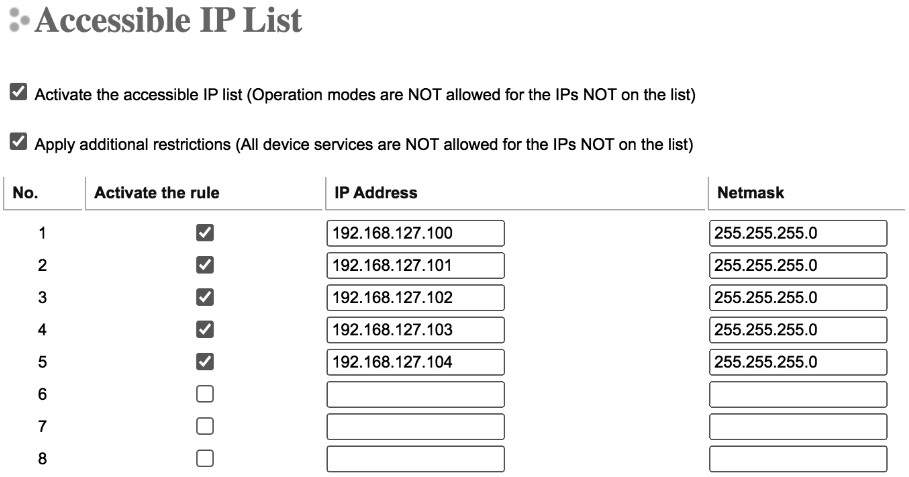
21 characters/Maximum 240 characters

Login Authentication Failure Message: Please contact administration if you have forgotten your password.

66 characters/Maximum 240 characters

3.4. Accessible IP List

- The NPort 5000 Series has a feature that can limit access to specific 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, log in to the HTTP/HTTPS console and select **Accessible IP List**.



Accessible IP List

☑ Activate the accessible IP list (Operation modes are NOT allowed for the IPs NOT on the list)

☑ Apply additional restrictions (All device services are NOT allowed for the IPs NOT on the list)

No.	Activate the rule	IP Address	Netmask
1	☑	192.168.127.100	255.255.255.0
2	☑	192.168.127.101	255.255.255.0
3	☑	192.168.127.102	255.255.255.0
4	☑	192.168.127.103	255.255.255.0
5	☑	192.168.127.104	255.255.255.0
6	□		
7	□		
8	□		

- 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 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**

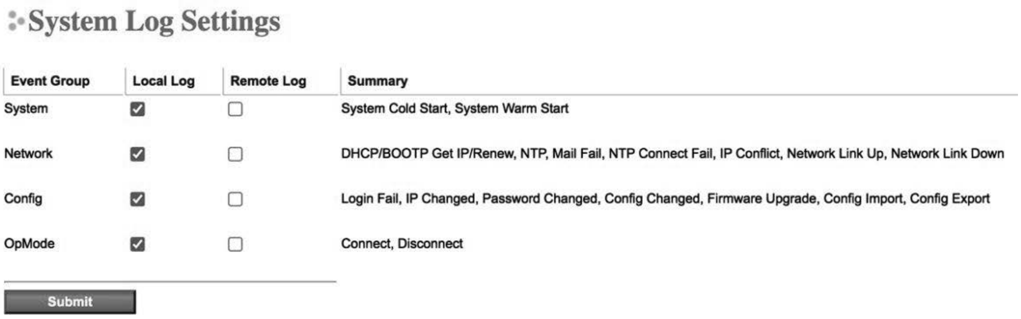
Ensure that the IP address of the PC you are using to access the web console is in the **Accessible IP List.**

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

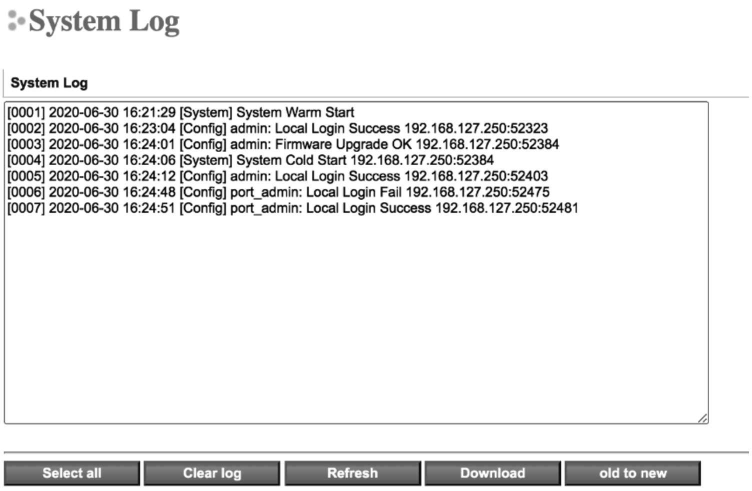
- To configure this setting, log in to the HTTP/HTTPS console and select **System Log Settings**. Then, enable the **Local Log** for recording on the NPort 5000 device and/or **Remote Log** for keeping records on a server. You should enable system log settings to record all important system events in order to monitor device status and check for security issues.



System Log Settings

Event Group	Local Log	Remote Log	Summary
System	☑	□	System Cold Start, System Warm Start
Network	☑	□	DHCP/BOOTP Get IP/Renew, NTP, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Up, Network Link Down
Config	☑	□	Login Fail, IP Changed, Password Changed, Config Changed, Firmware Upgrade, Config Import, Config Export
OpMode	☑	□	Connect, Disconnect

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



System Log

System Log

```
[0001] 2020-06-30 16:21:29 [System] System Warm Start
[0002] 2020-06-30 16:23:04 [Config] admin: Local Login Success 192.168.127.250:52323
[0003] 2020-06-30 16:24:01 [Config] admin: Firmware Upgrade OK 192.168.127.250:52384
[0004] 2020-06-30 16:24:06 [System] System Cold Start 192.168.127.250:52384
[0005] 2020-06-30 16:24:12 [Config] admin: Local Login Success 192.168.127.250:52403
[0006] 2020-06-30 16:24:48 [Config] port_admin: Local Login Fail 192.168.127.250:52475
[0007] 2020-06-30 16:24:51 [Config] port_admin: Local Login Success 192.168.127.250:52481
```

4. Patching/Upgrades

4.1. Patch Management Plan

With regards to patch management, Moxa releases version enhancements annually with detailed release notes.

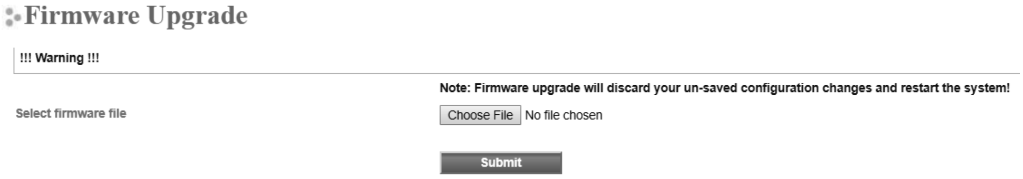
4.2. Firmware Upgrades

The process for upgrading firmware is as follows:

- Download the latest firmware for your MGate device from the Moxa website:

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

- Log in to the HTTPS console and select **System Management → Maintenance → Firmware Upgrade**. Click the **Choose File** button to select the proper firmware and click **Submit** to upgrade the firmware.



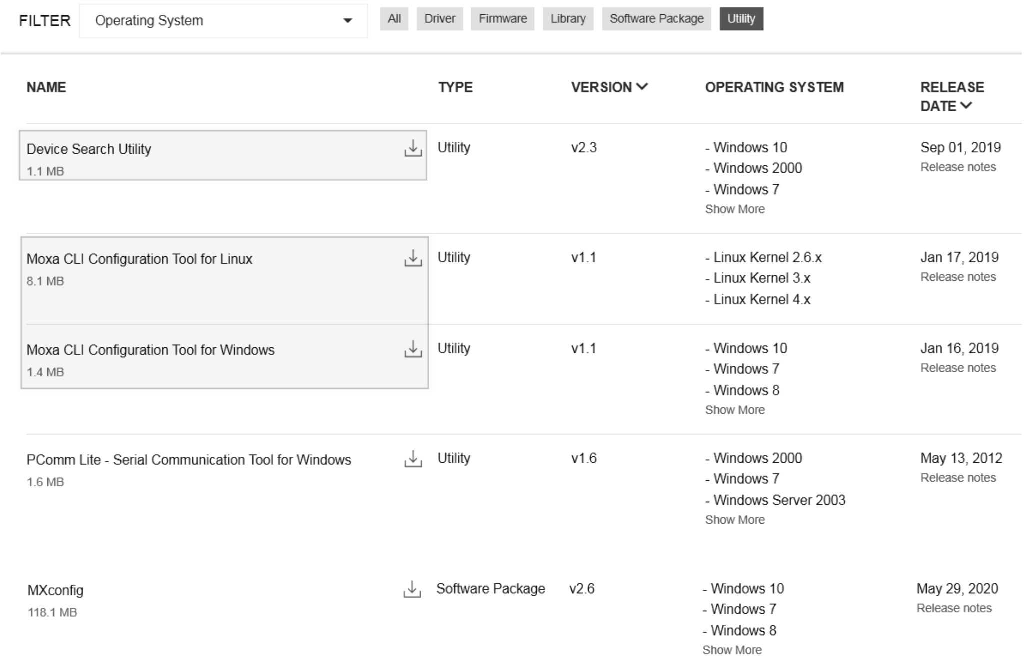
Firmware Upgrade

!!! Warning !!!

Note: Firmware upgrade will discard your un-saved configuration changes and restart the system!

Select firmware file — No file chosen

- If you want to upgrade the firmware for multiple units, download the Device Search Utility (DSU) or MXconfig for a GUI interface, or the Moxa CLI Configuration Tool for a CLI interface.



NAME	TYPE	VERSION	OPERATING SYSTEM	RELEASE DATE
Device Search Utility 1.1 MB	Utility	v2.3	- Windows 10 - Windows 2000 - Windows 7 Show More	Sep 01, 2019 Release notes
Moxa CLI Configuration Tool for Linux 8.1 MB	Utility	v1.1	- Linux Kernel 2.6.x - Linux Kernel 3.x - Linux Kernel 4.x	Jan 17, 2019 Release notes
Moxa CLI Configuration Tool for Windows 1.4 MB	Utility	v1.1	- Windows 10 - Windows 7 - Windows 8 Show More	Jan 16, 2019 Release notes
PComm Lite - Serial Communication Tool for Windows 1.6 MB	Utility	v1.6	- Windows 2000 - Windows 7 - Windows Server 2003 Show More	May 13, 2012 Release notes
MXconfig 118.1 MB	Software Package	v2.6	- Windows 10 - Windows 7 - Windows 8 Show More	May 29, 2020 Release notes

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.

You can find the latest Moxa security information here:
https://www.moxa.com/en/support/product-support/security-advisory