Moxa Technical Support Team <u>support@moxa.com</u>

Contents

| 1. | Introduction | 2 |
|------|---|----|
| 2. | General System Information | 3 |
| 2.1. | Basic Information About the Device | |
| 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 | |

Copyright © 2022 Moxa Inc.

Released on Jan 03, 2022

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 71 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 industries with reliable networks and sincere service. 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. It is 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 impacted.

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

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 | General purpose | Moxa Operating System | Version 1.6 |
| 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. It uses TLS protocols to transmit encrypted serial data over Ethernet.

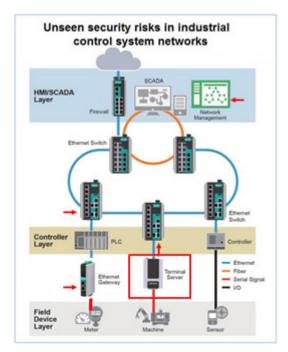
Moxa Operating System (MOS) is an embedded proprietary operating system, which is only executed in Moxa edge devices. Because the MOS operating system is not freely available, the chances of malware attacks are significantly reduced.

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

2.2. Deployment of the Device

You should deploy the NPort 5000 Series behind a security firewall network that has sufficient security features in place and 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.

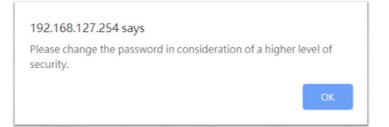


The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

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.



The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

3.1. TCP/UDP Port Status

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

| Operation Mode | Option | Default | Туре | Port Number | Remark & |
|-----------------|------------------|----------|------|------------------------|-------------------|
| | | Settings | 71 - | | Description |
| | | | | 950+ (Serial port No | |
| Real COM Mode | Enable/Disable | Enable | ТСР | 1) | |
| Real COM Mode | Linable/Disable | LIIdDie | TCF | 966+ (Serial port No | |
| | | | | 1) | |
| RFC2217 Mode | Enable/Disable | Disable | ТСР | User-defined (default: | Only available in |
| RFC2217 Mode | Lindble/Disable | Disable | ICF | 4000+Serial port No.) | certain models |
| | | | | User-defined (default: | |
| TCP Server Mode | Enable/Disable | Disable | ТСР | 4000+Serial port No.) | |
| TCF Server Mode | Linable, Disable | Disable | ICF | User-defined (default: | |
| | | | | 966+Serial port No.) | |

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

| Operation Mode | Option | Default | Туре | Port Number | Remark & |
|-----------------|-----------------|----------|------|------------------------|-------------------|
| | | Settings | 71 - | | Description |
| UDP Mode | Enable/Disable | Disable | UDP | User-defined (default: | |
| ODF Mode | Linable/Disable | DISADIE | UDF | 4000+Serial port No.) | |
| Pair Connection | Enable/Disable | Disable | ТСР | User-defined (default: | Only available in |
| Master Mode | Litable/Disable | Disable | ICP | 4000+Serial port No.) | certain models |
| Pair Connection | Epoble (Disoble | Disable | тср | User-defined (default: | Only available in |
| Slave Mode | Enable/Disable | | | 4000+Serial port No.) | certain models |
| Ethernet Modem | Epoble (Disoble | Disable | тср | User-defined (default: | |
| Mode | Enable/Disable | DISADIE | | 4000+Serial port No.) | |
| Reverse Telnet | Epoble (Disoble | | TCD | User-defined (default: | |
| Mode | Enable/Disable | Disable | ТСР | 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 Settings | Туре | Port Number | Security Remark |
|-----------------------|-----------------------|-------|--------------|--|
| Moxa Command | Disable | ТСР | 14900, 4900 | Disable service that is not commonly |
| (DSCI) | Disable | UDP | 4800 | used |
| 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 |
| | Disable | ODI | 101 | console |
| HTTP Server | Disable | тср | 80 | Disable the service for HTTP from plain |
| TITTP Server | Disable | TCF | | text transmission |
| HTTPS Server | Enable | ТСР | 443 | Encrypted data channel with trusted |
| HTTPS Server | Enable | TCP | | certificate for NPort configuration |
| Telnet Server Disable | | ТСР | 23 | Disable service that is not commonly |
| Telnet Server | Disable | ICP . | 23 | used |
| DUCD Client | Disable | | (7.6) | Suggest to assign a system IP in static |
| DHCP Client | Disable | UDP | 67, 68 | manner |
| SNTP Client | Disable | UDP | Random Port | Suggest to use the SNTP server for |
| | Disable | UDP | | secure time synchronization |
| Domoto System | | | | Suggest to have a system log server to |
| Remote System | Enable | UDP | Random Port | store all the logs from all the devices in |
| Log | | | | the network |

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

For the console services

| НТТР | 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 the SNMP, and select Disable for 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) |

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

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 Modify |
| 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

| SYSLOG server | |
|-----------------|---------------|
| SYSLOG facility | local use 0 🗸 |
| SYSLOG severity | Emergency V |

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**.

Deration Modes

| Port 1 | | |
|----------------|---------|---|
| Operation mode | Disable | • |

For each instruction above, click the **Submit** button to save your changes, and then restart the NPort 5000 Series so the new settings will take effect.

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.

| C | 🕽 Add 🥓 Edit 🏢 De | elete 🖹 Save/Rest | art | |
|------------------|-------------------|-------------------|---------------------|-------------------|
| Active | Account Name | User Level | | |
| V | admin | Read Write | | |
| | | | | |
| | | | | |
| Edit Acco | unt | | | |
| Active | | | ✓ | |
| Account Name | | | admin | |
| Change Password | | | | |
| Password | | | | (4-16 characters) |
| Confirm Password | | | | (4-16 characters) |
| User Level | | | Read Write V | |
| Jser Lever | | | Read White V | |

 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.

| Add Account | |
|------------------|-------------------|
| Active | |
| Account Name | |
| Password | (4-16 characters) |
| Confirm Password | (4-16 characters) |
| User Level | Read Write V |
| | |
| Submit Cancel | |

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.

User Account

| User Account | | | |
|---|------------------|----------------------|--|
| | 🛟 Add 🥓 Edit 🏢 D | elete 🖹 Save/Restart | |
| Active | Account Name | User Level | |
| Image: A set of the set of the | admin | Read Write | |
| V | port_admin | Read Write | |
| Image: A set of the set of the | Guest | Read Only | |

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.

- Account Password and Login Management

| Password minimum length | 16 (4 - 16) | |
|---|----------------------------------|--|
| Password complexity strength check | Enable O Disable | |
| At least one digit (0~9) | Enable O Disable | |
| Mixed upper and lower case letters (A~Z, a~z) | Enable | |
| At least one special character (~!@#\$%^&* ;:,.<>[[{()) | Enable | |
| Password lifetime | 30 (0 - 180 day; 0 for Disable) | |
| Account Login Failure Lockout | | |
| Account login failure lockout | Enable O Disable | |
| Retry failure threshold | 5 (1 - 10 retry) | |
| Lockout Time | 60 (1 - 60 min) | |

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.

Notification Message

| Notification Message | | | |
|--------------------------------------|--|---|--|
| Login Message | Welcome to Moxa NPort | | |
| Login Authentication Failure Message | Please contact administration if you have forgotten your password. | 21 characters/Maximum 240 characters | |
| Submit | | 66 characters/Maximum 240 characters | |

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.

| - Accessible IP List | | | | | | |
|----------------------|---|---|------------------|--|--|--|
| Activa | Activate the accessible IP list (Operation modes are NOT allowed for the IPs NOT on the list) | | | | | |
| Apply | additional restrictions (All de | vice services are NOT allowed for the IPs N | IOT 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; 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 |



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 | |
| Network | down | |
| | Login failed, IP changed, Password changed, Firmware upgraded, Certificate | |
| Configuration | 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.

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

| 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 | |
| Submit | | | _ | |

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.

System Log

| System Log | | | | |
|---|--|--|--|------------|
| [0002] 2020-06-30 16: [0003] 2020-06-30 16: [0004] 2020-06-30 16: [0005] 2020-06-30 16: [0006] 2020-06-30 16: | 24:01 [Config] admin: F 24:06 [System] System 24:12 [Config] admin: L 24:48 [Config] port_adr | ocal Login Success 193 Firmware Upgrade OK 1 Cold Start 192.168.127 Local Login Success 193 nin: Local Login Fail 19 | 92.168.127.250:52384 7.250:52384 2.168.127.250:52403 | 81 |
| Select all | Clear log | Refresh | Download | old to new |

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

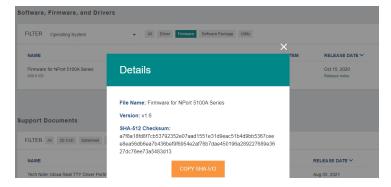
The process of firmware and/or software upgrade is instructed as below.

 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- |
| 5100A | device-servers/general-device-servers/nport-5100a-series#resources |
| 5100 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5100 | device-servers/general-device-servers/nport-5100-series#resources |
| 5200A | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5200A | device-servers/general-device-servers/nport-5200a-series#resources |
| 5200 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5200 | device-servers/general-device-servers/nport-5200-series#resources |
| 5400 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5400 | device-servers/general-device-servers/nport-5400-series#resources |
| 5600 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5000 | device-servers/general-device-servers/nport-5600-series#resources |
| 5600-DT | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 3000-01 | device-servers/general-device-servers/nport-5600-dt-series#resources |
| 5600-DTL | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 3000-DTL | device-servers/general-device-servers/nport-5600-dtl-series#resources |
| IA5000A | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| IASUUUA | device-servers/industrial-device-servers/nport-ia5000a-series#resources |
| IA5000 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 1A5000 | device-servers/industrial-device-servers/nport-ia5000-series#resources |
| 5000AI-M12 | https://www.moxa.com/en/products/industrial-edge-connectivity/serial- |
| 5000AI-M12 | device-servers/general-device-servers/nport-5000ai-m12-series#resources |

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

• 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.

| 1 | * Firmware Upgrade | | |
|---|----------------------|---|--|
| | !!! Warning !!! | | |
| | | Note: Firmware upgrade will discard your un-saved configuration changes and restart the system! | |
| | Select firmware file | Choose File No file chosen | |
| | | | |

• If a user wants to upgrade the firmware of the NPort 6000 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 preform the mass deployment.

| NAME | TYPE | VERSION V | 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 6.1 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 | لغي 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, 201 Release notes |

The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

Show More

MXconfig Joffware Package v2.6 - Windows 10 118.1 MB - Windows 7 - Windows 8 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.

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