

The Security Hardening Guide for the NPort 6000 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 | 3 |
| 3. Configuration and Hardening Information | 4 |
| 3.1. TCP/UDP Ports and Recommended Services..... | 5 |
| 3.2. HTTPS and SSL Certificates | 10 |
| 3.3. Account Management | 13 |
| 3.4. Accessible IP List..... | 16 |
| 3.5. Logging and Auditing | 17 |
| 4. Patching/Upgrades..... | 18 |
| 4.1. Patch Management | 18 |
| 4.2. Firmware Upgrades | 18 |
| 5. Security Information and Vulnerability Feedback | 20 |

Copyright © 2021 Moxa Inc.

Released on November 16, 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

This document provides guidelines on how to configure and secure the NPort 6000 Series. You should consider the recommended steps in this document as best practices for security in most applications. We highly recommend that you review and test the configurations thoroughly before implementing them in your production system in order to ensure that your application is not negatively affected.

2. General System Information Basic Information About the Device

| Model | Function | Operating System | Firmware Version |
|-------------------|---------------|-----------------------|------------------|
| NPort 6000 Series | Device server | Moxa Operating System | Version 2.0 |

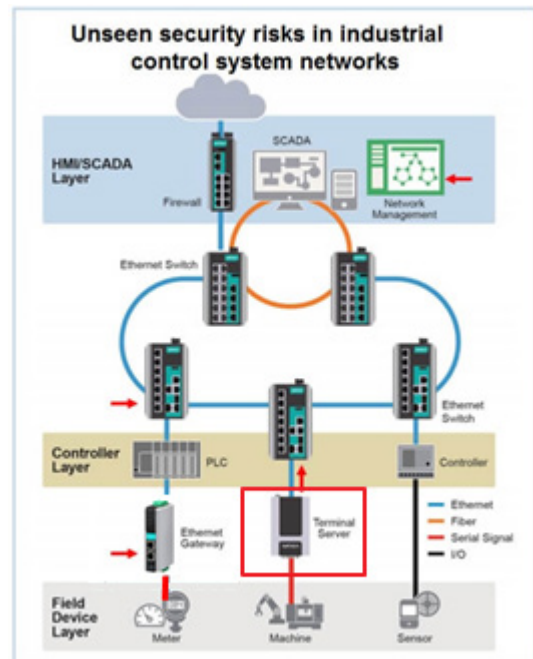
The NPort 6000 Series is a device server specifically designed to allow industrial devices to be accessible directly from a network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations and features are available for specific applications, such as protocol conversion, Real COM drivers, and TCP operation modes, to name a few. The series uses TLS protocols to transmit encrypted serial data over Ethernet.

Moxa Operating System (MOS) is an embedded proprietary operating system that is only used 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 6000 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

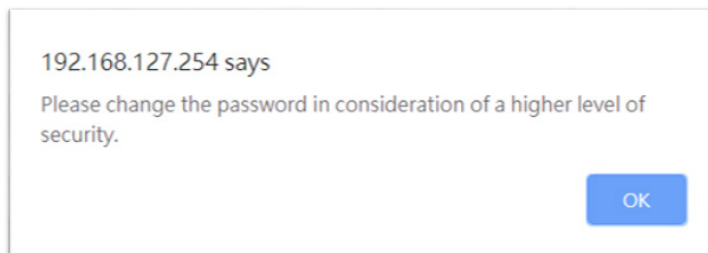
Make sure that the physical protection of the NPort devices and/or the system fulfill meet the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



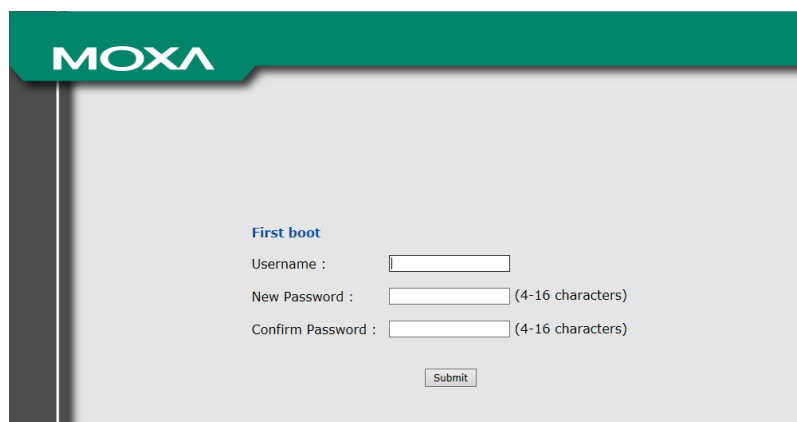
3. Configuration and Hardening Information

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.



From firmware version 2.0, there is no default username or password. You should immediately create a username and password before logging in for the first time to enhance the security of your device.



Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

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 6000 Series and other devices.

| Service Name | Option | Default Settings | Type | Port Number | 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 |
| RIPD_PORT | Enable/Disable | Disable | UDP | 520, 521 | Processing RIP routing data |
| HTTP server | Redirect to HTTPS/Disable | Disable | TCP | 80 | Web console |
| HTTPS server | Enable/Disable | Enable | TCP | 443 | Secured web console |
| SSH | Enable/Disable | Enable | TCP | 22 | SSH console |
| Telnet server | Enable/Disable | Disable | TCP | 23 | Telnet console |
| RADIUS | Enable/Disable | Disable | UDP | User-defined (1645 as default or 1812) | Authentication server |
| TACACS+ | Enable/Disable | Disable | TCP | 49 | Authentication server |
| DHCP client | Enable/Disable | Disable | UDP | 68 | The DHCP client needs to acquire the system IP address from the server |
| SNTP | Enable/Disable | Disable | UDP | Random port | Synchronize time settings with a time server |
| Remote System Log | Enable/Disable | Disable | UDP | Random port | Send the event log to a remote log server |

| Operation Mode | Option | Default Settings | Type | Port Number |
|-----------------|----------------|------------------|------|---|
| 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.) |
| 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.) |

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

| Operation Mode | Option | Default Settings | Type | Port Number |
|----------------------------|----------------|------------------|------|--|
| Pair Connection Slave Mode | Enable/Disable | Disable | TCP | User-defined (default: 4000+Serial Port No.) |
| 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.) |
| Reverse SSH Mode | Enable/Disable | Disable | TCP | User-defined (default: 4000+Serial Port No.) |
| Printer RAW Mode | Enable/Disable | Disable | TCP | 2048+(Group No. -1) |
| Printer LPD Mode | Enable/Disable | Disable | TCP | 515 |
| Disabled Mode | Enable/Disable | Disable | N/A | N/A |

For security reasons, consider disabling 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 | We suggest you manage the NPort via HTTPS console |
| RIPD_PORT | Disable | UDP | 520, 521 | Since the NPort is not a router or layer 3 switch, you may not need this service |
| HTTP Server | Disable | TCP | 80 | Disable HTTP to prevent plain text transmission |
| HTTPS Server | Enable | TCP | 443 | Encrypted data channel with a trusted certificate for NPort configurations |
| SSH | Enable | TCP | 22 | If you prefer the console mode to configure the device, you can enable the SSH service. If you prefer the GUI, then disable it. |
| Telnet Server | Disable | TCP | 23 | Disable service that is not commonly used |

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

| Service Name | Suggested Settings | Type | Port Number | Security Remark |
|-------------------|--------------------|------|---------------------------------------|---|
| RADIUS | Enable | UDP | User Define (1645 as default or 1812) | If you are using central account management feature (has a RADIUS server), you may enable this service. |
| TACACS+ | Enable | TCP | 49 | If you are using the central account management feature (has a TACACS+ server), you may enable this service. Select either RADIUS or TACACS+ to be the central account management service, and disable the other one. |
| DHCP Client | Disable | UDP | 67, 68 | Assign an IP address manually for the device |
| SNTP Client | Disable | UDP | Random Port | We suggest you use the SNTP server for secure time synchronization |
| Remote System Log | Enable | UDP | Random port | We suggest using a system log server to store all the logs from all the devices in the network |

For console services, we recommend:

| | |
|--------------|---------|
| 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](#)

[HTTPS console \(support TLS v1.2\)](#)

[TLS v1.0/v1.1 for HTTPS console](#)

[Telnet console](#)

[SSH console](#)

[Moxa Service](#)

Redirect to HTTPS Disable

Enable Disable

Enable Disable

Enable Disable

Enable Disable

Enable Disable

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

To disable the SNMP agent service, log in to the HTTPS console and select **System Management** → **SNMP Agent**, then select **Disable** for SNMP.

SNMP Agent Settings

Configuration

| | |
|--------------------------------|--|
| SNMP | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Read community string | <input type="text" value="....."/> (max: 31 characters) |
| Write community string | <input type="text" value="....."/> (max: 31 characters) |
| Contact name | <input type="text"/> |
| Location | <input type="text"/> |
| SNMP agent version | <input checked="" type="checkbox"/> v1 <input checked="" type="checkbox"/> v2 <input checked="" type="checkbox"/> v3 |
| Read only user name | <input type="text"/> |
| Read only authentication mode | Disable ▾ |
| Read only password | <input type="text" value="....."/> (8-31 characters) |
| Read only privacy mode | Disable ▾ |
| Read only privacy | <input type="text" value="....."/> (8-31 characters) |
| Read/write user name | <input type="text"/> |
| Read/write authentication mode | Disable ▾ |
| Read/write password | <input type="text" value="....."/> (8-31 characters) |
| Read/write privacy mode | Disable ▾ |
| Read/write privacy | <input type="text" value="....."/> (8-31 characters) |

Submit

For the RADIUS server, log in to the HTTPS/SSH/Telnet console and select **System Management** → **Mics. Network Settings** → **Authentication Server**. Then, keep the IP setting empty as **Disable** for the RADIUS server.

Authentication Server

RADIUS

| | |
|-------------------|---|
| RADIUS server | <input type="text"/> |
| RADIUS key | <input type="text"/> |
| UDP port | 1645 ▾ |
| RADIUS accounting | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |

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

Time Settings

| | |
|----------------------|---|
| Time zone | (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▾ |
| Local time (24-hour) | 2020 / 9 / 18 3 : 46 : 1 Modify |
| Time server | <input type="text"/> |

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

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 | <input type="text"/> |
| 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

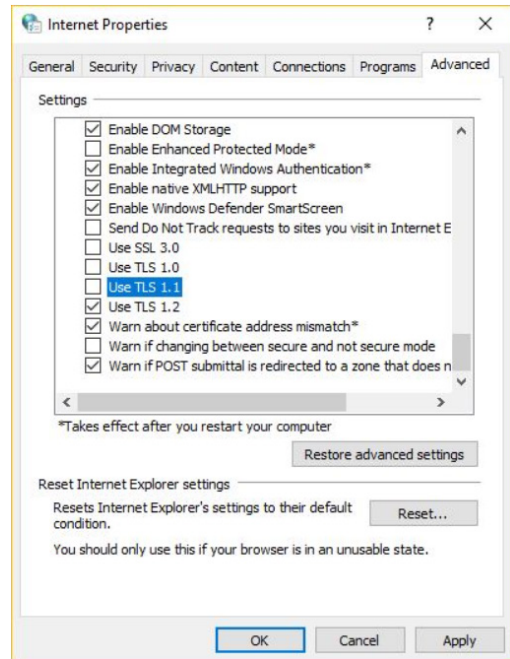
Port 1

| | |
|------------------------------------|--|
| Application | Disable ▾ |
| Apply the above settings to | <input checked="" type="checkbox"/> P1 <input type="checkbox"/> P2 <input type="checkbox"/> All ports |

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 6000 Series uses TLS v1.2 for HTTPS to ensure data transmissions are secured. Make sure your browser has TLS v1.2 enabled.



In order to use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority.

Log in to the HTTP/HTTPS console and select **System Management → Certificate**. You can generate an up-to-date valid certificate by importing a third-party trusted SSL certificate or generating the “NPort self-signed” certificate.

- Behavior of SSL certificate on an NPort 6000 device
 - NPort devices can auto-generate a self-signed SSL certificate. It is recommended that you import SSL certificates that are certified by a trusted third-party Certificate Authority (CA) or by an organization's CA.
 - The length of the NPort device’s self-signed private keys is 1,024 bits, which should be compatible with most applications. Some applications may need a longer key, such as 2,048 bits, which would require importing a third-party certificate. Please note that longer keys will mean browsing the web console will be slower due to the increased complexity of encrypting and decrypting communicated data.

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- For the NPort self-signed certificate:

If a certificate has expired, you can regenerate the NPort self-signed certificate with the following steps.

- Step 1. **Delete** the current SSL certificate issued by the NPort device.
- Step 2. **Enable** the NTP server and set up the time zone and local time.
- Step 3. After restarting the device, the NPort self-signed certificate will be regenerated with a new expiration date.

- Importing the third party trusted SSL certificate:

By importing the third-party trusted SSL certificate, the security level can be enhanced. A snapshot of the GUI for the web console is shown below. To generate the SSL certificate through the third party, here are the steps:

- Step 1. Create a certification authority (Root CA), such as Microsoft AD Certificate Service (<https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/>)
- Step 2. Find a tool to issue a certificate signing request (CSR) file. You can get one from a third-party CA company such as DigiCert (<https://www.digicert.com/easy-csr/openssl.htm>).
- Step 3. Submit the CSR file to a public certification authority to get a signed certificate.
- Step 4. Import the certificate to the NPort device. Please note that NPort devices only accept certificates using a **".pem"** format.

Note: The maximum supported key length of the NPort devices is 2,048 bits.

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- Some well-known third-party CA (Certificate Authority) companies for your reference (https://en.wikipedia.org/wiki/Certificate_authority):
 - IdenTrust (<https://www.identrust.com/>)
 - DigiCert (<https://www.digicert.com/>)
 - Comodo Cybersecurity (<https://www.comodo.com/>)
 - GoDaddy (<https://www.godaddy.com/>)
 - Verisign (<https://www.verisign.com/>)

Certificate

Certificate Settings

| | |
|-----------|---------------------------|
| Issued to | 10.144.8.226 |
| Issued by | 10.144.8.226 |
| Valid | from 2000/3/4 to 2020/3/4 |

Select SSL certificate file No file chosen

Delete SSL certificate file

MOXA Total Solution for Industrial Device Networking

| | | | | | |
|-------|------------------|------------|-------------------|-------------|------------------------|
| Model | - MGate MB3270 | IP | - 192.168.127.200 | MAC Address | - 00:90:E8:44:F0:E2 |
| Name | - MG-MB3270_3348 | Serial No. | - 3348 | Firmware | - 4.1.5 Build 19100215 |

Certificate Settings OK!

Your changes have been saved.

Click Restart to reboot the server. Your changes will take effect when the server restarts.

If you would like to make additional changes, remember to save your configuration before restarting the server.

Main Menu

- Overview
- Basic Settings
- Network Settings
- Serial Settings
- Protocol Settings
- System Management
 - Accessible IP List
 - System Log Settings
 - Auto Warning Settings
 - E-mail Alert
 - SNMP Trap
 - SNMP Agent
 - Misc. Settings
 - Maintenance
 - Certificate
- System Monitoring
 - System Log
 - Relay State
 - Save/Restart
 - Log Out

3.3. Account Management

- The NPort 6000 Series provides two different user levels, administrator and user. With a Read Write account, you can access and change all settings through the web console. With a user account, you can only view settings.
- The default administrator account is **admin**, and the default password is **moxa**. Starting from firmware version 2.0, you need to set the administrator's account and password before you log in the first time. To manage accounts, log in to the web console and select **Administration → Account Management → User Account**. To change the password of an existing account, click on the account name and select **Edit** in the top toolbar. Input the old password in the **Password** field and the new password in **Confirm Password** field to change the password.
- Through the administration account, admin, log in to NPort 6000 Series and perform the configuration settings. To change the default password (moxa), log in to the HTTPS/SSH/Telnet console and select **System Management → Account Management → User Account**. For the **Password** part, input the old password and the new password twice (at least 4 characters) to change the password.

Change Password

| | |
|------------------------|--|
| Password | |
| Old password | <input type="text"/> |
| New password | <input type="text"/> |
| Confirm password | <input type="text"/> |
| User Management | |
| User Name | <input type="text"/> |
| User Old password | <input type="text"/> |
| User New password | <input type="text"/> |
| User Confirm password | <input type="text"/> |
| Action | <input checked="" type="radio"/> Change <input type="radio"/> Add <input type="radio"/> Delete |

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- To add new general users, log in to the HTTPS/SSH/Telnet console and select **System Management → Maintenance → Change Password**. At the **User Management** part, input the username, old password, and the new password twice to **Add** a new user, **Change** the password, or **Delete** an old user.

User Account

Add Account

Active

Account Name

Password

Confirm Password

Group administrator ▼

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.

Access Permission

Access Permission

[+](#) Add
 [✎](#) Edit
 [🗑](#) Delete
 [💾](#) Save

| Group Name | Overview | Network Config | Serial Config | System Config | Administration | Log, Monitoring and Warning | Common Settings |
|---------------|-----------|----------------|---------------|---------------|----------------|-----------------------------|-----------------|
| administrator | Read Only | Read Write | Read Write | Read Write | Read Write | Read Write | Read Write |
| guest | Read Only | No Display | No Display | No Display | No Display | No Display | No Display |
| port_admin | Read Only | No Display | Read Write | Read Write | No Display | Read Write | Read Write |

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- 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 **System Management → Misc. Settings → Login Password Policy**.

Account Password and Login Management

Account Password Policy

| | |
|--|---|
| Password minimum length | <input type="text" value="16"/> (4 - 16) |
| Password complexity strength check | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| At least one digit (0~9) | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Mixed upper and lower case letters (A~Z, a~z) | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| At least one special character (~!@#\$\$%^&*~_!;:,.<>[]{}()) | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Password lifetime | <input type="text" value="1"/> (0 - 180 day; 0 for Disable) |

Account Login Failure Lockout

| | |
|-------------------------------|---|
| Account login failure lockout | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Retry failure threshold | <input type="text" value="5"/> (1 - 10 retry) |
| Lockout Time | <input type="text" value="5"/> (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 HTTPS console and select **System Management → Misc. Settings → Notification Message**, and enter a **Login Message** to use.

Notification Message

Notification Message

| | | |
|--------------------------------------|--|--------------------------------------|
| Notification Message | <input type="text" value="Welcome to Moxa NPort"/> | |
| Login Message | <input type="text" value="Please contact administration if you have forgotten the password."/> | 21 characters/Maximum 240 characters |
| Login Authentication Failure Message | <input type="text" value=""/> | 65 characters/Maximum 240 characters |

3.4. Accessible IP List

- The NPort 6000 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 6000 Series. To configure it, log in to the HTTPS console and select **System Management** → **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. | Active | IP Address | Netmask/Prefix |
|-----|--------------------------|----------------------|----------------------|
| 1 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 2 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 3 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 4 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 5 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| 6 | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |

- 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 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 6000 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, Authentication Fail, Restart |

- To configure this setting, log in to the HTTPS console and select **System Management → System Log Settings**. Then, enable the **Local Log** for recording on the NPort 6000 device and/or **Syslog** for keeping records on a server. You should enable system log settings to record all important system events to monitor device status and check for security issues.

System Log Settings

| Event Group | Local Log | Remote Log | Summary |
|-------------|-------------------------------------|--------------------------|--|
| System | <input checked="" type="checkbox"/> | <input type="checkbox"/> | System Cold Start, System Warm Start |
| Network | <input checked="" type="checkbox"/> | <input type="checkbox"/> | DHCP/BOOTP/PPPoE Get IP/Renew, NTP, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down |
| Config | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Login Fail, IP Changed, Password Changed, Config Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export |
| OpMode | <input checked="" type="checkbox"/> | <input type="checkbox"/> | Connect, Disconnect, Authentication Fail, Restart |

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

System Log

| System Log |
|---|
| 2014/02/07 12:36:25 [System] System Warm Start |
| 2014/02/07 12:36:28 [Network] DHCP/BOOTP/PPPoE Get IP/Renew |
| 2014/02/07 12:36:36 [Network] Get IP Fail (IPv6) |
| 2014/02/10 04:40:32 [System] System Cold Start |
| 2014/02/10 04:40:43 [Network] Get IP Fail (IPv6) |
| 2014/02/10 05:18:18 [Network] DHCP/BOOTP/PPPoE Get IP/Renew |
| 2014/02/20 09:10:33 [System] System Cold Start |
| 2014/02/20 09:10:44 [Network] Get IP Fail (IPv6) |
| 2014/02/24 04:50:09 [System] System Cold Start |
| 2014/02/24 04:50:20 [Network] Get IP Fail (IPv6) |
| 2014/02/24 13:54:11 [Network] DHCP/BOOTP/PPPoE Get IP/Renew |
| 2014/03/10 07:18:33 [System] System Cold Start |
| 2014/03/10 07:18:49 [Network] Get IP Fail (IPv6) |
| 2014/03/10 09:54:20 [Config] Config Changed |
| 2014/03/10 09:54:35 [System] System Warm Start |
| 2014/03/10 09:54:46 [Network] Get IP Fail (IPv6) |
| 2014/03/10 09:56:15 [Config] Config Changed |
| 2014/03/10 09:56:18 [Config] IP Changed |
| 2014/03/10 09:56:30 [System] System Warm Start |

4. Patching/Upgrades

4.1. Patch Management

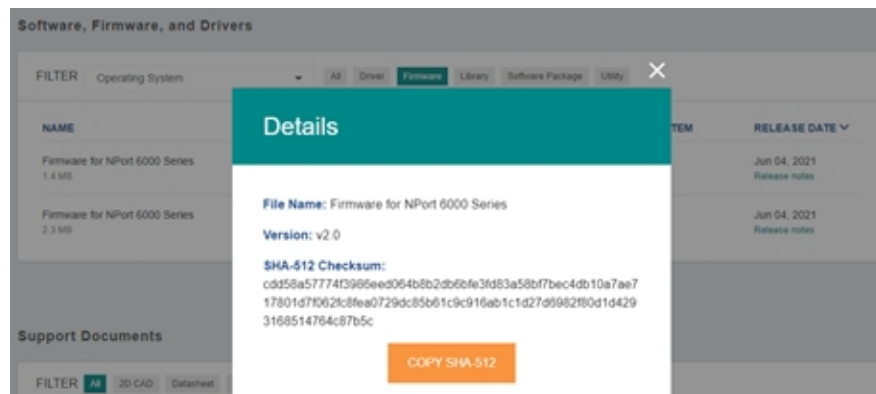
Regarding patch management, Moxa releases version enhancements annually with detailed release notes.

4.2. Firmware Upgrades

The process for upgrading firmware is as follows:

- Download the latest firmware and software along with its release notes and hash values for your NPort device from the Moxa website:
 - Firmware of NPort 6100/6200 Series:
<https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/terminal-servers/nport-6100-6200-series#resources>
 - Firmware of NPort 6400/6600 Series:
<https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/terminal-servers/nport-6400-6600-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.



Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- 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

Note: Due to memory limitations, the firmware structure of the NPort 6000 Series is being fine-tuned. As a result, we cannot upgrade the firmware of NPort 6450 to v2.0 from v1.21 via the web console. To upgrade the firmware, use DSU or MCC Tool (Moxa CLI Configuration Tool).

- 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.

FILTER

| NAME | TYPE | VERSION | OPERATING SYSTEM | RELEASE DATE |
|---|------------------|---------|---|---|
| Moxa CLI Configuration Tool for Linux 8.1 MB | Utility | v1.2 | - Linux Kernel 2.6.x - Linux Kernel 3.x - Linux Kernel 4.x | Mar 31, 2021 Release notes |
| Moxa CLI Configuration Tool for Windows 2.1 MB | Utility | v1.2 | - Windows 10 - Windows 7 - Windows 8 Show More | Mar 31, 2021 Release notes |
| Device Search Utility 1.1 MB | Utility | v2.4 | - Windows 10 - Windows 2000 - Windows 7 Show More | Mar 31, 2021 Release notes |
| PCComm 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 |

- If you need instructions on using the Moxa CLI Configuration Tool, download the manual.

Moxa Tech Note The Security Hardening Guide for the NPort 6000 Series

- Manual for the NPort 6100/6200 Series:
<https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/terminal-servers/nport-6100-6200-series#resources>
- Manual for the NPort 6400/6600 Series:
<https://www.moxa.com/en/products/industrial-edge-connectivity/serial-device-servers/terminal-servers/nport-6400-6600-series#resources>

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>