The Security Hardening Guide for the NPort 6000-G2 Series

Moxa Technical Support Team

support@moxa.com

Contents

 Released on Dec 11, 2024

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

1 Introduction

The NPort 6000-G2 Series configuration and security guidelines are detailed in this document. 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 to ensure that your application is not negatively affected.

2 General System Information

2.1 Basic Information About the Device

Model	Function	Operating System	Firmware Version
NPort 6000-G2 Series	Device server	Zephyr RTOS	Version 1.0

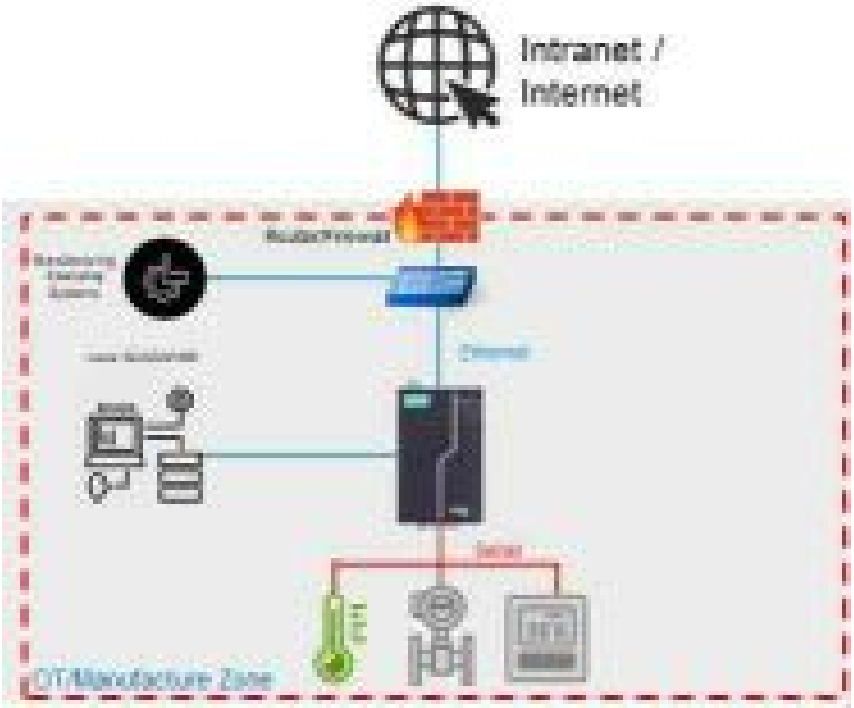
The NPort 6000-G2 Series is a device server specifically designed to allow industrial devices to be accessible directly from a network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location or even the Internet. Different configurations and features are available for specific applications, such as Real COM drivers and TCP operation modes, to name a few. The series uses TLS protocols to transmit encrypted serial data over Ethernet.

Zephyr RTOS is a full-featured OS with an architecture that is developed with security in mind. The governance and its members have a responsibility to ensure that all aspects of the code are developed securely and conform to the expectations of the next generation RTOS of Moxa.

2.2 Deployment of the Device

Deploy the NPort 6000-G2 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

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



2.3 Security Threats

The security threats that can harm NPort 6000-G2 Series are:

1. **Attacks over the network**

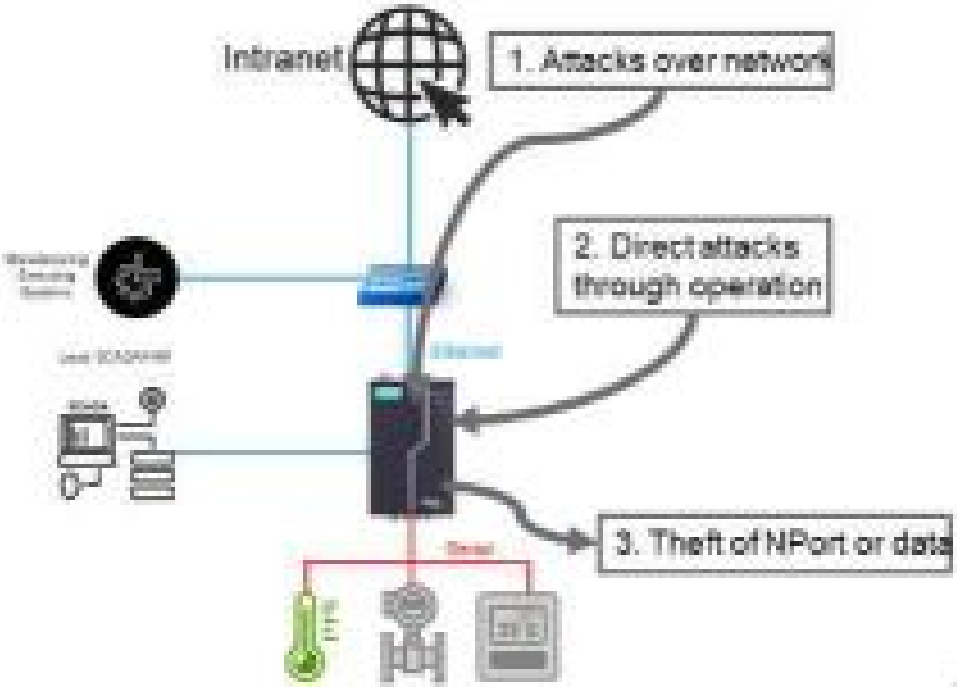
   Threats from individuals with no rights to the NPort 6000-G2 Series via networks such as intranets.

2. **Direct attacks through operation**

   Threats where individuals with no rights to the NPort 6000-G2 Series directly operate a device to affect the system and steal important data.

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

   Threats where an NPort 6000-G2 Series or data is stolen, and important data is analyzed.



2.4 Security Measures

To fend off security threats, we arranged security measures applied in security guides for the general business network environment and identified a set of security measures for the NPort 6000-G2 Series. We classify the security measures into three security types. The following table describes the security measures and the threats that each measure handles.

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

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

To defend against the theft of the NPort or data, we recommend you use the NPort 6000-G2 Series within a secure local network, as mentioned above. We also suggest that you enable the Allowlist function (for more details, refer to chapter 3.3) to only allow the necessary hosts/IPs to access the device and Secure Connection function (for more details, refer to chapter 3.1) to encode the data and protect the data from a stolen.

3 Configuration and Hardening Information

For security reasons, there is no default account name or password. When accessing the NPort 6000-G2 for the first time, you will be reminded to create an account name and password before logging in via the Device Search Utility (DSU) or the web console.

Device Search Utility V3.0 or later

Web console

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-G2 Series and other devices.

Service Name	Option	Default Settings	Type	Port Number	Description
Moxa server	Enable/ Disable	Enable	TCP	443	For Moxa utility communication
			UDP	5353	
WINS	Enable/ Disable	Disable	UDP	137	Processing WINS (Client) data
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
RIPD_PORT	Enable/ Disable	Disable	UDP	520, 521	Processing RIP routing data
HTTPS server	Enable/ Disable	Enable	TCP	443	Secured web 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 get 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	Disable (Changed to Enable after user set username/password)	TCP	949+ (Serial port No.) 965+ (Serial port No.)
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: 965+Serial Port No.)
UDP Mode	Enable/ Disable	Disable	UDP	User-defined (default: 4000+Serial Port No.)
Pair Connection Slave Mode	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)
Reverse Terminal-Telnet	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)
Reverse Terminal-SSH	Enable/ Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.)
Disabled Mode	Enable/ Disable	Disable	N/A	N/A

For security reasons, the NPort 6000-G2 Series only enables limited services to ensure the security of the device itself. It will only enable the Moxa services, HTTPS, and serial console for the user to configure the device and the Real COM mode for the COM-based Control application users. If this is not the case, you may modify or disable the above services.

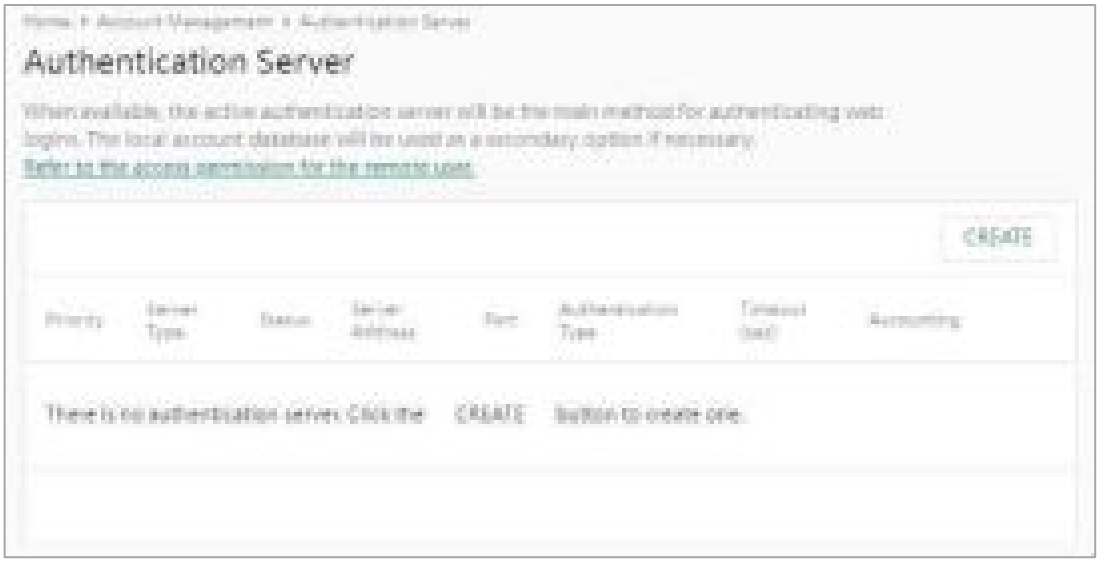
To integrate the NPort 6000-G2 Series to your network topology and secure applications, consider enabling the services below with proper settings to enhance the security architecture of the network and to protect the network with depth of defense.

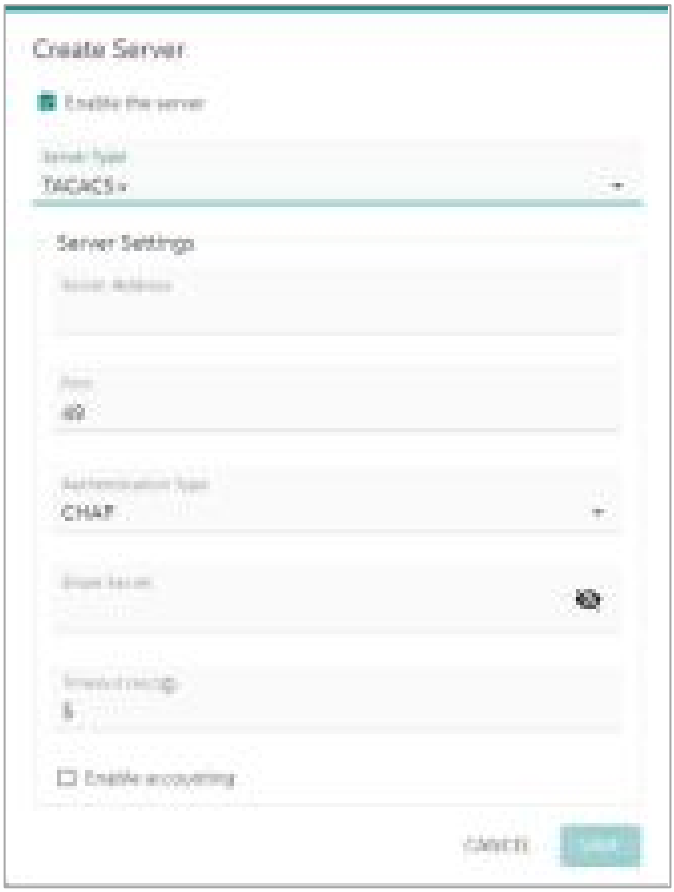
Service Name	Type	Port Number	Security Remark
SNMP agent	UDP	161	The Simple Network Management Protocol is a popular tool for remote device monitoring and management. If needed, turn on SNMPv3 to encrypt the communication data.
RADIUS	UDP	User Define (1645 as default or 1812)	If you are using the central account management feature (has a RADIUS server), enable this service.
TACACS+	TCP	49	If you are using the central account management feature (has a TACACS+ server), enable this service. Select either RADIUS or TACACS+ to be the central account management service and disable the other one.
DHCP Client	UDP	67, 68	If you have a DHCP Server to assign an IP automatically, enable this service for easy management.
SNTP Client	UDP	Random port	For log tracing, the time synchronization is important.
Remote System Log	UDP	Random port	Central log management may be important in some applications. Enable the remote system log service to store all the logs of the NPort 6000-G2 to a remote log server.

To enable or disable these services, log in to the HTTPS console and select **Security > Services**.

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

For the RADIUS and TACACS+ server, log in to the HTTPS console and select **Account Management > Authentication Server**. Then, click the **CREATE** button to add the RADIUS or TACACS+ server and complete relative settings with the **Enable the server** checked.

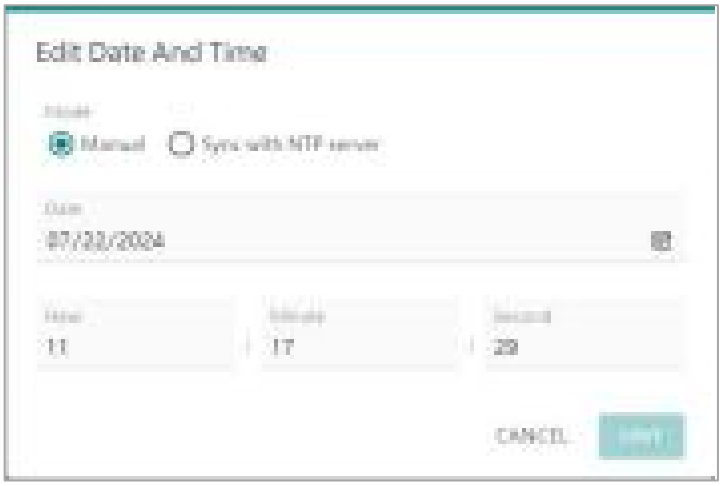




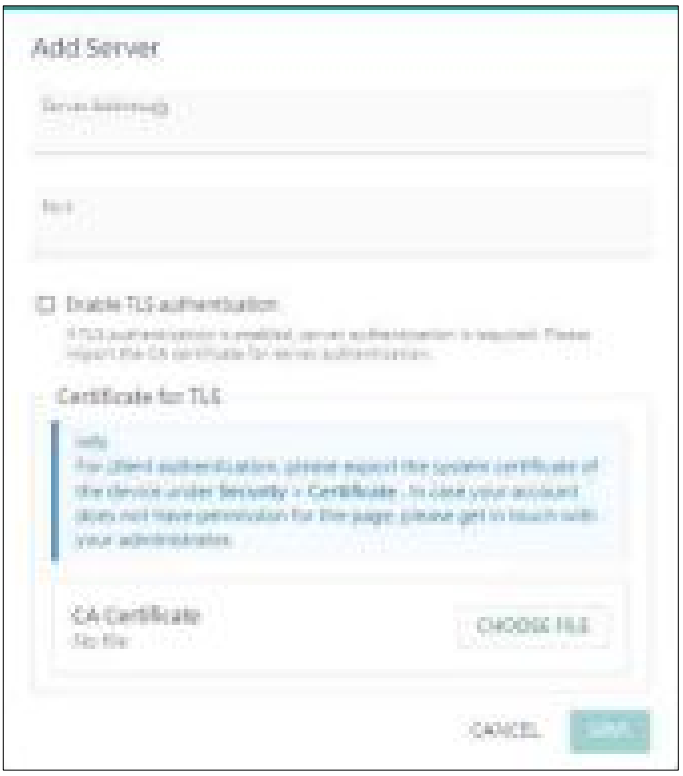
If you want to enable DHCP Client, log in to the HTTPS console, select **Network Settings > IP Address,** and select Get IP From **DHCP**.

If you want to enable SNTP Client, log in the HTTPS console, select **System Settings > General**, and select the **Date & Time** tab.

Click the **EDIT** button and select **Sync with NTP server**. Then, click the **SAVE** button to enable it.



For the remote system log server, log in to the HTTPS console, select **System Settings > Notification**, click the **EDIT** button next to Syslog, and add the server in the server field.



You may also **Enable TLS authentication**. The NPort 6000-G2 will then authenticate whether the remote syslog server is the correct one or not. This function will require you to import the CA Certificate by clicking the **CHOOSE FILE** button.

The operation mode services depend on your serial device's Ethernet network connection method. For example, if your host PC uses legacy software to open a COM port to communicate with the serial device, then the NPort will enable the Real COM mode for this application. If you don't want the NPort to provide such a service, log in to the HTTPS console, select **Serial Port Settings > Operation Modes > Port # > CONFIGURE**, and then select **No Operation**.

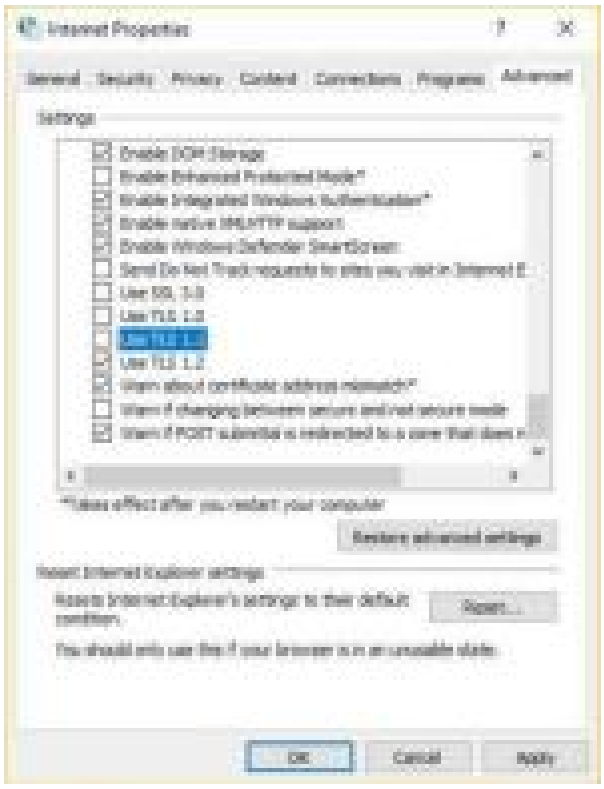
If you are concerned about serial data being transmitted or received with plaintext over the Ethernet network, enable the TLS encryption to encode the serial data. Log in the HTTPS console and select **Serial Port Settings > Secure Connection**.

Select the target serial ports and click the **CONFIGURE** button to select the Encrypted **connection** option to enable the TLS encryption function.

Selecting the **Encrypted and authenticated connection** will also trigger the NPort 6000-G2 to authenticate whether the remote device/host is the correct one or not. This function will require you to import the CA Certificate by switching to the **Remote Device Certificate** tab and clicking the **UPLOAD** button.

3.2 HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. Because TLS v1.1 and lower versions have severe, easily exploitable vulnerabilities, the NPort 6000-G2 Series uses TLS v1.2 for HTTPS to secure data transmissions. Make sure your browser has TLS v1.2 enabled.



To use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority or export the "NPort self-signed" certificate to the browser.

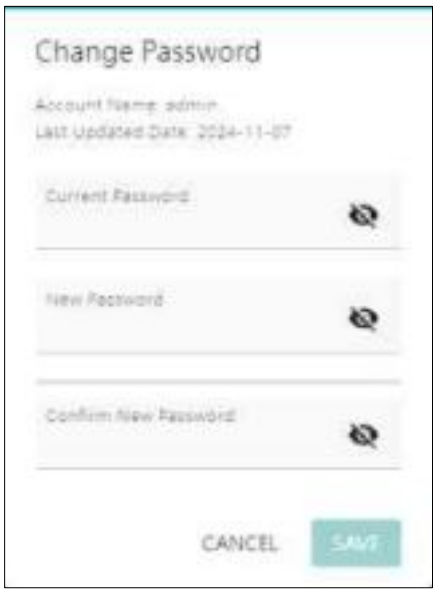
Log in to the HTTPS console and select **Security > Certificate**. Click the **MANAGE** button to **Import user certificate**.

- Behavior of the System Certificate on an NPort 6000-G2 device
  - NPort devices will auto-generate a self-signed SSL certificate when the IP address is changed or you can click the **Regenerate system certificate** option to generate a new one manually. 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 NPort device's self-signed certificate is encoded based on the Elliptic Curve Cryptography (ECC) 256-bit algorithm, which should be compatible with most applications. Some applications may need a longer or stronger key, requiring importing a third-party certificate. Note that longer keys will mean browsing the web console will be slower because of the increased complexity of encrypting and decrypting communicated data.
- Importing the third-party trusted SSL certificate:

  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. 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. Note that NPort devices only accept certificates using a "**.pem**" format. The NPort 6000-G2 Series supports the algorithms below:
    - RSA-1024, RSA-2048, RSA-3072, RSA-4096
    - ECC-256, ECC-384, ECC-521
- 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/)

3.3 Account Management

- The NPort 6000-G2 Series provides two different user groups, Administrator, and Operator. With an Administrator account, you can access and change all settings through the web console. With an Operator account, you can change and monitor most of the settings, except **Security** and **Account Management**.
- 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 **Account Management > Accounts**. To change the password of an existing account, click on the account name's option icon. Input the old password and the new password twice (at least 8 characters) to change the password.

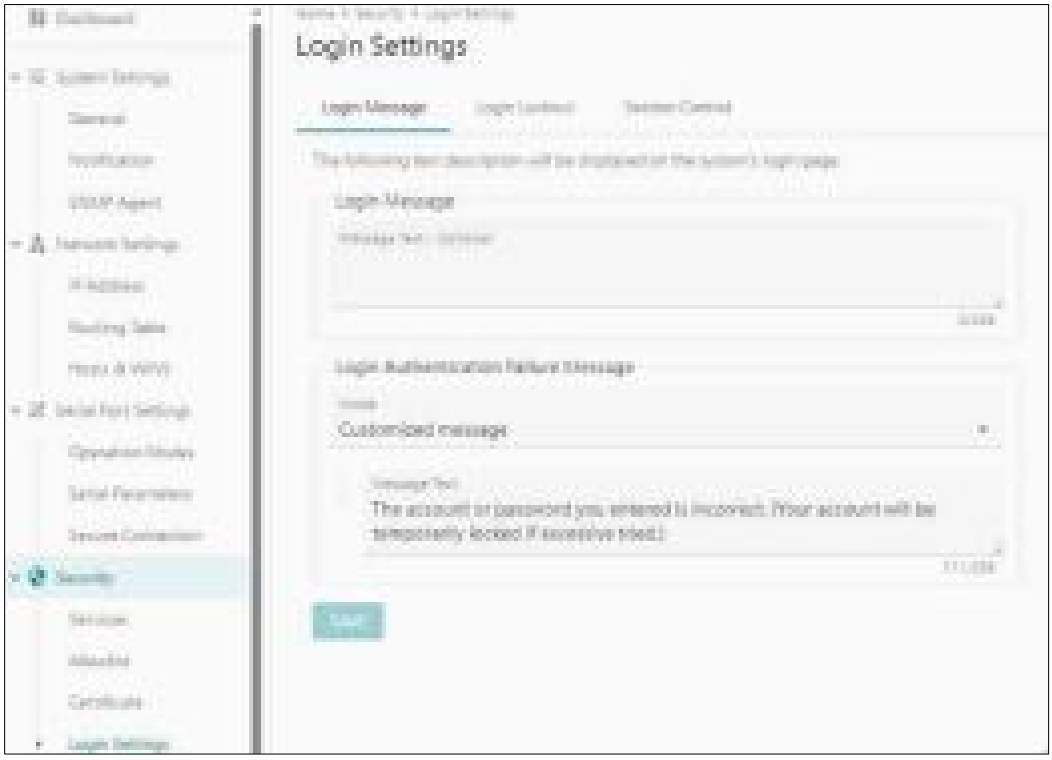


- To add new accounts, select **Account Management > Accounts > CREAT**. A window will pop up for you to input account information and assign a password to the user. Also, the Administrator(s) shall assign a proper **Group** to users to limit their privileges of using the NPort 6000-G2. To add/delete/edit the **Group** privileges, go to the **Groups** section in the menu. The **Password** rules can be set up in **Password Policy** section.

- Configure the login password policy and account login failure lockout to improve security. To configure them, log in to the HTTPS console and select **Account management > Password Policy**.

Adjust the password policy to require more complex passwords. For example, set the **Min. Password Length** to 16, enable all **Password Strength Policy** checks, and enable the **Password lifetime** options. Also, to avoid a brute-force attack, we suggest that you **Enable login failure lockout** feature. Select **Security > Login Settings > Login Lockout** to enable the function.

- For some system security requirements, a warning message may be shown to every user who logs in. To add a login message, select **Security > Login Settings > Login Message**, and enter the messages to be delivered.



3.4 Allowlist

- An allowlist is a list of IP addresses or domains that are provided privileged access. Enabling this function limits the number of IP addresses that can access the device server, which can prevent unauthorized access from an untrusted network.

- You can add a specific address or range of addresses by using a combination of an IP address and a subnet mask:
  - **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 **Allowlist** toggle button is closed.

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 **Allowlist**.

3.5 Logging and Auditing

- The local syslog function is enabled to record the events that happened on the NPort 6000-G2 device. Under the Security category, the severity of events—Notice, Warning and Error—will be saved on the local flash memory by default. The events can be recorded for up to 10,000 items.
- These are five categories of events:

Category	Description
System	The events related to the NPort itself, like firmware ready.
Network	The events related to the Ethernet interface, for example, the Ethernet link up.
Security	The events which may be considered security related; the administrator may need to figure out why it happened. For example, a login fail event.
Maintenance	The events which usually happen during the maintenance process, for example, firmware upgrades.
Serial	The events related to the serial interface(s), for example, Port connect.

- There are four severities of the events:

Priority	Severity	Description
1	Error	Events that indicate problems, but in a category that may or may not require immediate attention.
2	Warning	Events that provide forewarning of potential problems and indicate that some further actions could result in a critical error.
3	Notice	Events that are not error conditions but may require special handling.
4	Informational	Confirmation that the program works as expected.

- To enable what events shall be recorded, log in to the HTTPS console and select **Diagnostics > System Log> Log Settings > EDIT > Events Settings**. Select the events you would like to save in the system log.

- To view events in the system log, select **Diagnostics > System Log > Log View**.

- To enable the remote log server, select **System Settings > Notification**. Click the **EDIT** button next to **Syslog**, and add the server in the server field.

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:

- 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-G2/6200-G2 Series:

    https://www.moxa.com/en/support/search?psid=137659
- 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.

- Log in to the HTTPS console and select **Maintenance > Firmware Upgrade**. Click the **Choose File** button to select the proper firmware and click **UPLOAD** to upgrade the firmware.

  - Manual for the NPort 6000-G2 Series:
    https://www.moxa.com/en/support/search?psid=137659

5 Decommission

Since the NPort is the primary device for transferring serial data to Ethernet devices, decommissioning an NPort device requires arranging annual maintenance to replace the old unit with a new one. Follow these steps to complete the process:

1. Export the configuration file from the old NPort and import it to the new unit. This will save you from having to configure the new unit manually.
2. Stop the communication and replace the old unit.
3. Re-start communication and check if everything works fine. If yes, proceed to step d to decommission the old unit. If no, you may need assistance to troubleshoot the issue.
4. Keep the old unit powered on and press the Reset button for 5 seconds to restore the settings to factory default.
5. After the device reboots and all user settings are removed or overwritten, you may scrap it.

If you enable the function Reset button "Only enable with 60 seconds after booting". You will need to push the Reset button within 60 seconds after booting to enable the Reset function.

---

6 Security Information and Vulnerability Feedback

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security has become one of the top priorities. The Moxa Product Security Incident Response Team (PSIRT) is taking a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

Follow the updated Moxa security information from the link below:
https://www.moxa.com/en/support/product-support/security-advisory