The Security Hardening Guide for the NPort 6000-G2 Series

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

Contents

1	Introduction					
2	General System Information					
	2.1	Basic Information About the Device				
	2.2	Deployment of the Device				
	2.3	Security Threats				
	2.4	Security Measures	5			
3	Conf	6				
	3.1	TCP/UDP Ports and Recommended Services				
	3.2	HTTPS and SSL Certificates				
	3.3	Account Management	17			
	3.4	Allowlist	20			
	3.5	Logging and Auditing				
4	Patching/Upgrades					
	4.1	Patch Management	23			
	4.2	Firmware Upgrades	23			
5	Deco	ommission	25			
6	Security Information and Vulnerability Feedback					

Copyright © 2024 Moxa Inc.

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.

	Subseterer	Threat Handled			
Security measure	Subcategory	1	2	3	
Access control	-	Yes	Yes	No	
Stopping unused services	-	Yes	No	No	
	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	
Changing IT	Applying AutoRun restrictions	No	Yes	No	
settings	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

Set up the when you of first time.	account and p use the device	assword for the
Account		
New password		Ø
Confirm passwor	d	Ø
	CANCEL	SET UP

Web console

Create Account	
Create the first account of the device.	
Account Name	
Password	Ø
Confirm Password	ø

Copyright © 2024 Moxa Inc.

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	Туре	Port Number	Description
Moxa server	Enable/	Fnable	ТСР	443	For Moxa utility
	Disable	Enable	UDP	5353	communication
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	ТСР	443	Secured web console
RADIUS	Enable/ Disable	Disable	UDP	User-defined (1645 as default or 1812)	Authentication server
TACACS+	Enable/ Disable	Disable	ТСР	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

The Security Hardening Guide for the NPort 6000-G2 Series

Operation Mode	Option	Default Settings	Туре	Port Number
Real COM Mode	Enable/ Disable	Disable (Changed to Enable after user set username/password)	ТСР	949+ (Serial port No.) 965+ (Serial port No.)
RFC2217 Mode	Enable/ Disable	Disable	ТСР	User-defined (default: 4000+Serial port No.)
TCP Server Mode	Enable/ Disable	Disable	ТСР	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	ТСР	User-defined (default: 4000+Serial Port No.)
Reverse Terminal- Telnet	Enable/ Disable	Disable	ТСР	User-defined (default: 4000+Serial Port No.)
Reverse Terminal- SSH	Enable/ Disable	Disable	ТСР	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	Туре	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+	ТСР	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.

Home > Ac	count Manag	ement > Aut	hentication Se	erver			
Authe	nticatio	on Serve	er				
When avail logins. The Refer to the	lable, the ac local accou e access per	tive authent int database rmission for	ication serve will be used the remote u	er will be th I as a secon <u>user.</u>	e main method for dary option if nece	authenticating ssary.	j web
							CREATE
Priority	Server Type	Status	Server Address	Port	Authentication Type	Timeout (sec)	Accounting
There is	no authenti	cation serve	er. Click the	CREATE	button to create	one.	

Create Server		
Server Type TACACS +		•
Server Settings		
Server Address		
Port 49		
Authentication Type CHAP		•
Share Secret		ø
Timeout (sec) 5		
Enable accounting		
	CANCEL	SAVE

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

IPv4 Address	
Get IP From	
Manual	•
DHCP	
Manual	
10.90.60.63	
Subnet Mask	
255.255.254.0	
IPv4 Gateway - optional	
10.90.60.1	

Copyright © 2024 Moxa Inc.

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

Home	Home > System Settings > General								
General									
	Identity	Date & Time							
			-						
	Current Date	e And Time							
	2024-07-	22 11:16:56		EDIT					
	T								
	(GMT+08	·00) Taipei		EDIT					
	(01011100	.00) taipei							

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

Edit Date And Time				
Mode Manual OS	Sync with NTP server			
Date 07/22/2024		Ē		
Hour 11	Minute : 17	Second 29		
		CANCEL SAVE		

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.

Home > System Settings > Notification				
Notification				
Select the events and channels to receive no and SNMP Trap/Inform is necessary for it to	tifications. Completing the s function.	settings for Syslog	, Email,	
Events Settings 0 event(s) selected				EDIT
Channels Settings				
Syslog O Not configured > More Information	Email © Disabled → More Information	EDIT	SNMP Trap/Inform O Not configured More Information	EDIT

Server Address()	
Port	
Enable TLS authentication	
If TLS authentication is enabled, serve import the CA certificate for server as	er authentication is required. Please uthentication.
Certificate for TLS	
A DATE OF THE OWNER	
Info For client authentication, please the device under Security > Cen does not have permission for th your administrator.	e export the system certificate of rtificate . In case your account ne page, please get in touch with
Info For client authentication, please the device under Security > Cer does not have permission for th your administrator. CA Certificate No file	e export the system certificate of rtificate . In case your account he page, please get in touch with CHOOSE FILE

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**.

Select One	•
No Operation	
COM-based Control	
Socket	
Pair Connection	
Connect Console	
Connect Modem	

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.



If you set the port(s) as an encrypted and upload the remote device certificate for a	authenticated connect authentication.	tion,
TCP Connection Type		
 Unencrypted connection 		
O Encrypted connection		
O Encrypted and authenticated connection		
	CANCEL	SAVE

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.

- 55	Dashboard	Home > Serial Port Settings > Se	ecure Connection				
		Secure Connectio	'n				
> ==	System Settings	Secure connection supports R	ure connection supports Real COM, Reverse Real COM, TCP Server, TCP Client, and Pair				
> #	Network Settings	Connection modes in TCP con Refer to the cipher suites for a	nnection modes in TCP connection. Configure the TCP connection type as needed. :fer to the cipher suites for an encrypted connection.				
~ ល	Serial Port Settings						
	Operation Modes	TCP Connection Type	Remote Device Certificate				
	Serial Parameters	The port(s) with encrypted	and authenticated connections will verif	y the uploaded certificates.			
•	Secure Connection				Γ	UPLOAD	
> 🕲	Security						
> 🖻	Account Management	File Name	Issued to	Issued by	Status		
>	Maintenance	No certificate to display.	No certificate to display. Click UPLOAD button to unload the certificate.				
> ®	Diagnostics						

Moxa Tech Note

The Security Hardening Guide for the NPort 6000-G2 Series

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.

Conoral	Convibu	Driveren	Contant	Connections	Dragrama	Advan	red
General	Security	Privacy	Content	Connections	Programs	Advan	ceu
Setting	s						-
	Enable Enable Enable Enable Enable Enable Send I Use S: Use Ti	E DOM Sto Enhance Integrat Native Xi Windows Do Not Tra SL 3.0 LS 1.0	orage ed Protecte ed Window MLHTTP su s Defender ack reques	d Mode* vs Authenticatio pport SmartScreen ts to sites you	on* visit in Inter	net E	
	Use TI Use TI Warn Warn Warn	LS 1.1 LS 1.2 about cer if changin if POST su	tificate ado g between Jbmittal is r	dress mismatch secure and no edirected to a	* t secure mo zone that de	de oes n	
	Use TI Use TI Warn Warn Warn	S 1.1 S 1.2 about cer if changin if POST su	tificate ado g between ubmittal is r	dress mismatch secure and no redirected to a	* it secure mo zone that d	de oes n	
< *Ta	Use TI Use TI Warn Warn Warn	IS 1.1 IS 1.2 about cer if changin if POST su	tificate ado g between ubmittal is r	dress mismatch secure and no redirected to a	* t secure mo zone that d	de oes n >	
< *⊺a	Use Ti Use Ti Warn Warn Warn Warn	LS 1.1 LS 1.2 about cer if changin if POST su after you	tificate add g between ubmittal is r restart you	dress mismatch secure and no redirected to a ur computer	* it secure mo zone that do	de oes n >	
< *Ta	Use TI Use TI Warn Warn Warn kes effect a	S 1.1 S 1.2 about cer if changin if POST su after you	tificate add g between ubmittal is r restart you	dress mismatch secure and no edirected to a ur computer Restore	* it secure mo zone that do advanced s	de oes n >	
*Ta Reset 1 Rese conc You	Use TI Use TI Warn Warn Warn Warn Warn kes effect a internet Ex internet Ex internet ition.	LS 1.1 LS 1.2 about cer if changin if POST su after you plorer set t Explorer use this i	tificate add g between Jbmittal is r restart you tings tings tings tis settings	dress mismatch secure and no edirected to a ur computer Restore to their default wser is in an un	* t secure mo zone that d advanced s C Res usable state	de oes n > settings et e.	

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 (<u>https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installingcertificate-authority-on-windows-server-2012-r2/</u>)
- Step 2. Find a tool to issue a certificate signing request (CSR) file. Get one from a third-party CA company such as DigiCert (<u>https://www.digicert.com/easycsr/openssl.htm</u>).
- 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 (<u>https://en.wikipedia.org/wiki/Certificate_authority</u>):
 - IdenTrust (<u>https://www.identrust.com/</u>)
 - DigiCert (<u>https://www.digicert.com/</u>)
 - Comodo Cybersecurity (<u>https://www.comodo.com/</u>)
 - GoDaddy (<u>https://www.godaddy.com/</u>)
 - Verisign (<u>https://www.verisign.com/</u>)

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.

Change Password	
Account Name: admin Last Updated Date: 2024-11-07	
Current Password	Ø
New Password	ø
Confirm New Password	Ø
CANCEL	SAVE

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.

Home > Account Management	> Accounts			
Accounts				
				CREATE
Account Name 🍦	Group 🔷	Status 🌲	Date of Creation 🌲	
admin (You)	Administrator	⊘ Active	2024-11-07	:
test	Operator	⊘ Active	2024-11-20	:

Copyright © 2024 Moxa Inc.

Moxa Tech Note

 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.

	Dashboard	Home > Account Management > Password Policy
i† ==	System Settings Network Settings	You have the option to enhance password security by selecting a minimum length and strength policy.
> N	Serial Port Settings	Min. Password Length 8
> 🖗	Security	
~ 🖻	Account Management	Password Strength Policy
	Accounts	 Mixed upper and lower case letters (A-Z, a-z)
	Groups	At least one special character (~! @#\$%^&*+=` '0}[:;\``'<>,.?/)
•	Password Policy Authentication Server	You can enhance account security by setting a password lifetime. When an account reaches the lifetime threshold and a user logs in, the system will mandate password changes.
> 0	* Maintenance	Enable password lifetime
> @) Diagnostics	Password Lifetime (day) 90
		SAVE

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.

Home > Security > Log	gin Settings	
Login Setting	gs	
Login Message	Login Lockout	Session Control
To prevent hackers failure lockout and	from repeatedly attem adjust the necessary s	ipting to log in and crack passwords, you can enable login ettings.
🗹 Enable login fa	ilure lockout	
Max. Failure Re 5	try (times)	
Enable resi The login fa recalculate b	et login failure counter ilure counter will reset an based on the period you h	d nave set.
Lockout Time (5	min)	
SAVE		

Copyright © 2024 Moxa Inc.

Moxa Tech Note

 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.

	Dashboard	Home's Security's Login Settings
· 主	System Settings	Login Settings
	General	Login Message Login Lockout Session Control
	Notification	The following text description will be displayed on the system's login page.
	SNMP Agent	Login Message
- #	Network Settings	Message Text - Optional
	IP Address	
	Routing Table	0/256
	Hosts & WINS	Login Authentication Failure Message
ល	Serial Port Settings	Mode
	Operation Modes	
	Serial Parameters	Message Text The account or password you entered is incorrect. (Your account will be
	Secure Connection	temporarily locked if excessive tried.)
0	Security	111/256
	Services	SAVE
	Allowlist	
	Certificate	
	Login Settings	

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.

	Dashboard	Home > Security > Allowlist	
		Allowlist	
> =	🗄 System Settings	Info	
> 4	Network Settings	All communications are only allowed for the enabled IPs on the list after enabling this allowlist.	
> (🕅 Serial Port Settings	Allowlist	
~ 🤇	Security	IPv4 (0) IPv6 (0)	
	Services		
	Allowlist		ADD RULE
	Certificate	No. IPv4 Address Subnet Mask Status	
	Login Settings		
~ 6	Account Management	No data to display. Click ADD RULE button to create the first data.	
	Accounts		

- 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 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.
	The events which may be considered security related; the
Security	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,
Maintenance	for example, firmware upgrades.
Sorial	The events related to the serial interface(s), for example, Port
Jenai	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.

System Log

Joseff Log				
Log View Log Se	tings			
Log Settings			EDIT 👻	
Current Log Capacity: 3% Log Capacity Policy: Overwrite the oldest log			Events Settings	
			Log Capacity Settings	

Moxa Tech Note

The Security Hardening Guide for the NPort 6000-G2 Series

		Home > Diagnostics > System Log > Events Settings						
	Groups	← Events Settings						
	Password Policy	Select the events you would like to save in the system log. The events can be sorted by severity. Refer to the details of the severity. Severity: ✓ Error ✓ Votice ✓ Informational						
	Authentication Server							
~ <u>+</u>	Maintenance							
	Config. Import/Export							
	Firmware Upgrade	System (16) Network (7) Security (23) Maintenance (8) Serial (8)						
	Reset to Default							
	Restart	Event Name Severity 🖨	Î					
~ @	Diagnostics	Firmware ready Notice						
	Support	Detect SD card Informational						
•	System Log	SD card removed Warning						
	Operation Mode Statistic:							
	Network Monitor	No SD card inserted Error						
	Ping							
	Traffic Monitor		SAVE					

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

	Groups	Home > Diag	nostics > System Log			
	Password Policy	Log Viev	v Log Settings			
0.00	Authentication Server	- cog rici	- Log Settings			
	Config. Import/Export				Y FILTER 👗 CLEAR	▲ EXPORT REFRESH
	Firmware Upgrade	N	o Severity 🜲	Category 🌲	Event Name 🌲	Timestamp 💠
	Reset to Default	> 1	Informational	Security	Login success	2024-11-21 10:13:18
	Restart	> 2	Notice	Network	Ethernet link down	2024-11-21 10:11:27
~ @	Support	> 3	Informational	Security	Login success	2024-11-21 10:07:58
	System Log	> 4	Informational	Security	Login success	2024-11-21 10:05:02
	Operation Mode Statistic:	> 5	Informational	Security	Login success	2024-11-21 10:04:50
	Network Monitor	> 6	Notice	Network	Ethernet link down	2024-11-20 19:46:54
	Ping			ltems per	page: 10 👻 1 - 10 of 13	3 K K 1 / 14 > >1
	Traffic Monitor 🚽					

• 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.

Home > System Settings > No	otification				
Notification					
Select the events and chann and SNMP Trap/Inform is n	nels to receive not ecessary for it to f	ifications. Completing the s unction.	ettings for Syslog	Email,	
Events Settings 0 event(s) selected					EDIT
Channels Settings					
Syslog ○ Not configured → More Information	EDIT	Email © Disabled > More Information	EDIT	SNMP Trap/Inform O Not configured > More Information	EDIT

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.

Specifications	Resources Models	×
vare, and Driv	Details	
ing System	File Name: Firmware for NPort 6000-G2 Series	
	Version: v1.0.0	тем
t 6000-G2 Series	SHA-512 Checksum: 07fb0aec9389528a856dfc166e7a02c3ece263a6f9112d481150dfd 040ec8f929d141f4453491dcc4c9413517d821a30f6d26a227a0987	5 ′c
	032b14070ae1cdb7	
ents		

• 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.

≡	ΜΟΧΛ	NPort 6250-G2
	Dashboard	Home > Maintenance > Firmware Upgrade Firmware Upgrade
> ==	System Settings	Current Firmware Version: v1.0.0 Build 24091909
> 볿	Network Settings	Choose the firmware file and upload it to the device. You can download the firmware file from the
> ល	Serial Port Settings	product page of <u>Moxa official website</u> -
> 🖗	Security	Choose File No file chosen
> 🖻	Account Management	
> 🚅	Maintenance	UPLOAD
> -2	Diagnostics	

> 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