

The Security Hardening Guide for the CN2600 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 Update..... 5
 - 3.2 HTTPS and SSL Certificates 10
 - 3.3 Accessible IP List..... 13
 - 3.4 Logging and Auditing 14
- 4 Patching/Upgrades 15
 - 4.1 Patch Management 15
 - 4.2 Firmware Upgrades 15
- 5 Security Information and Vulnerability Feedback..... 16

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.

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 CN2600 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 to ensure that your application is not negatively affected.

2 General System Information

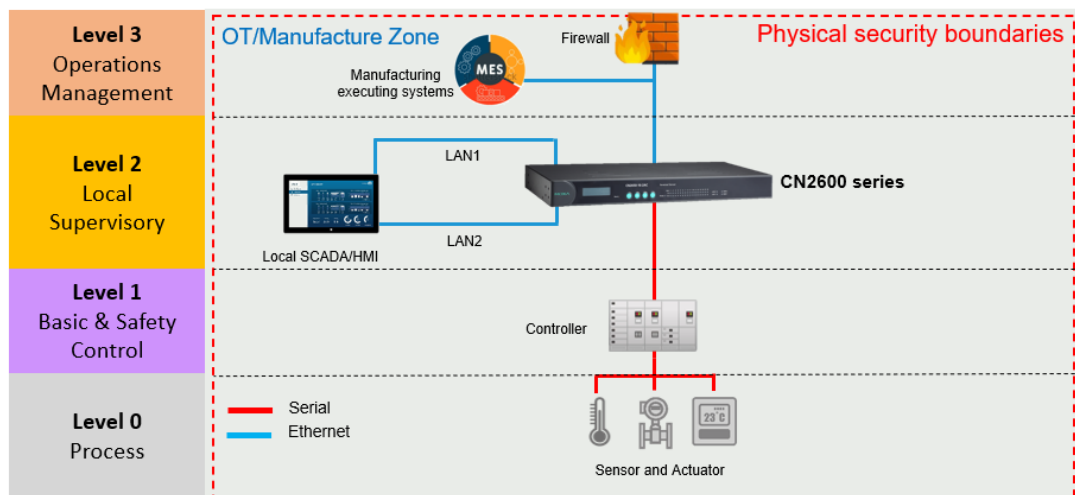
2.1 Basic Information About the Device

Model	Function	Operating system	Firmware version
CN2600 Series	Device server	Moxa Operating System	Version 4.6

The CN2600 Series is a device server that allows industrial devices to be accessed directly from a network. Thus, legacy devices can be transformed into Ethernet devices, which then can be monitored and controlled from any network location. 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.

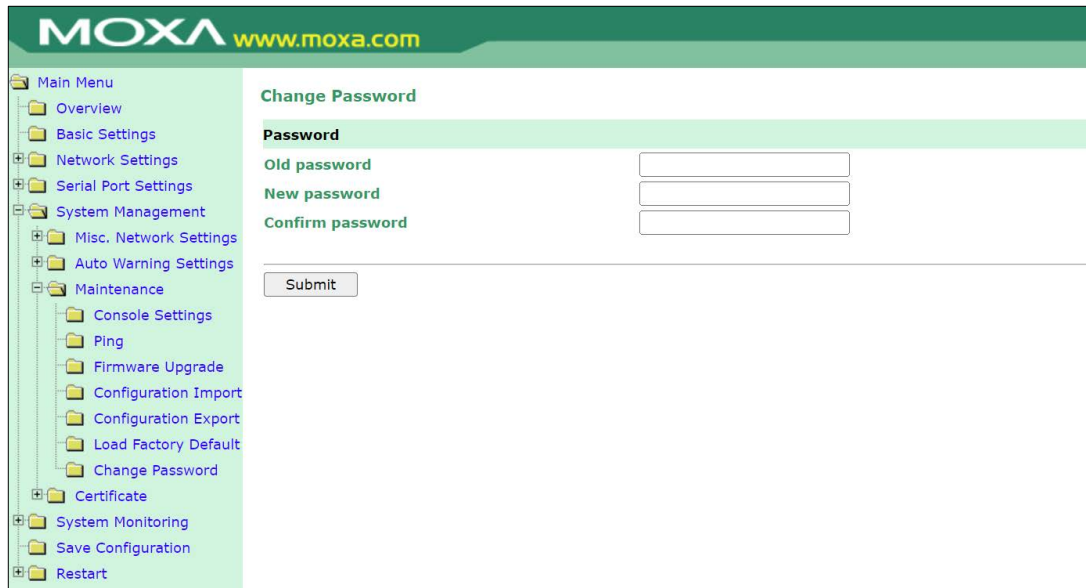
2.2 Deployment of the Device

The Dual-LAN cards feature of the CN2600 Series, with two independent MAC addresses and IP addresses, primarily aims to provide network redundancy. If one connection fails, the PC host can still communicate with the serial devices over the alternative LAN connection. We recommend using this feature only within internal networks. You should also deploy the CN2600 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 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

The CN2600 Series does not have a default password for security reasons, so we strongly advise setting up password protection. To set up password protection, log in to the HTTPS console and select **System Management > Maintenance > Change Password**. Leave **Old password** blank and enter your desired password under both **New password** and **Confirm password**.



3.1 TCP/UDP Ports and Recommended Services Update

Refer to the table below for all the ports, protocols, and services that are used to communicate between the CN2600 Series and other devices. For security reasons, consider disabling unused services. After the initial setup, use services with stronger security for data communication. Please also refer to the table below for the suggested settings.

Service Name	Default Setting	Suggested Settings	Type	Port Number	Description	Security Remark
Moxa Command (DSCI)	Enable	Disable	TCP	14900, 4900	For Moxa utility communication	Disable this service as it is not commonly used
			UDP	4800		
DNS_wins	Enable	Enable	UDP	137, 949	Processing DNS and WINS (Client) data	A necessary service to get IP; cannot be disabled
SNMP agent	Enable	Disable	UDP	161	SNMP handling routine	We suggest you manage the NPort via HTTPS console
RIPD_PORT	Disable	Disable	UDP	520	Processing RIP routing data	Since the NPort is not a router or layer 3 switch, you may not need this service
HTTP server	Enable	Disable	TCP	80	Web console	Disable HTTP to prevent plain text transmission
HTTPS server	Enable	Enable	TCP	443	Secured web console	Encrypted data channel with a trusted certificate for NPort configurations
SSH	Enable	Enable	TCP	22	SSH console	If you prefer the console mode to configure the device, you can enable the SSH service. If you prefer the GUI, then disable it.

Service Name	Default Setting	Suggested Settings	Type	Port Number	Description	Security Remark
Telnet server	Enable	Diabile	TCP	23	Telnet console	Disable service that is not commonly used
RADIUS	Disable	Enable	UDP	1645 as default or 1812	Authentication Server	If you are using central account management feature (has a RADIUS server), you may enable this service
DHCP client	Disable	Disable	UDP	68	The DHCP client needs to acquire the system IP address from the server	Assign an IP address manually for the device
SNTP	Disable	Disable	UDP	Random port	Synchronize time settings with a time server	We suggest you use the SNTP server for secure time synchronization

Operation Mode	Option	Default Setting	Type	Port Number
Real COM Mode	Enable/Disable	Enable	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.)
Redundant COM	Enable/Disable	Disable	TCP	949+ (Serial port No.) 965+ (Serial port No.)
DRDAS Real COM Mode	Enable/Disable	Disable	TCP	949+ (Serial port No.) 965+ (Serial port No.)
DRDAS TCP Server Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial Port No.) User-defined (default: 965+Serial Port No.)

Operation Mode	Option	Default Setting	Type	Port Number
Terminal Mode	Enable/Disable	Disable	TCP	User-defined (default: 23)
Reverse Terminal Mode	Enable/Disable	Disable	TCP	User-defined (default: 4000+Serial port No.)

For console services, we recommend:

HTTP	Disable
HTTPS	Enable
TLS v1.0/v1.1 for HTTPS console	Disable
Telnet console	Disable

The HTTP protocol transmits data in plain text, making it susceptible to interception and manipulation, while HTTPS adds a layer of encryption on top of HTTP using TLS. This encryption safeguards the transmitted data from interception and manipulation. Therefore, we recommend disabling HTTP and using HTTPS.

As TLS v1.0/v1.1 possesses certain vulnerabilities and weaknesses that could be exploited by malicious actors for attacks or sensitive information theft, it is recommended to disable **TLS v1.0/v1.1 for HTTPS console** to ensure secure data transmission.

Telnet is also a plaintext protocol that transmits all sensitive information in plain text, making it susceptible to eavesdropping and interception attacks. Hence, we recommend using SSH console instead of Telnet console.

To enable or disable these services, log in to the HTTP/HTTPS console and select **System Management > Maintenance > 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

SSH console Enable Disable

Reset button Always Enable Disable after 60 sec

LCM read-only protection Writable Read-only

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

SNMP Agent Settings

Configuration

SNMP Enable Disable

Read community string

Write community string

Contact name

Location

SNMP agent version v1 v2 v3

Read only user name

Read only authentication mode

Read only password

Read only privacy mode

Read only privacy

Read/write user name

Read/write authentication mode

Read/write password

Read/write privacy mode

Read/write privacy

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

Configuration

RADIUS server IP

RADIUS key

UDP port

RADIUS accounting Enable 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.

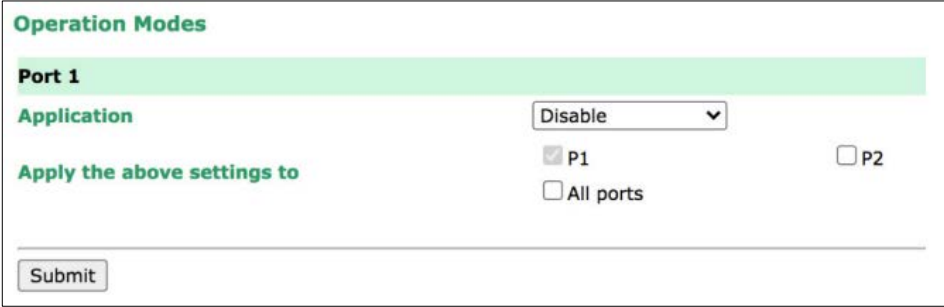
Time Settings

Time zone (24-hour)

Local time / / : :

Time server

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 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

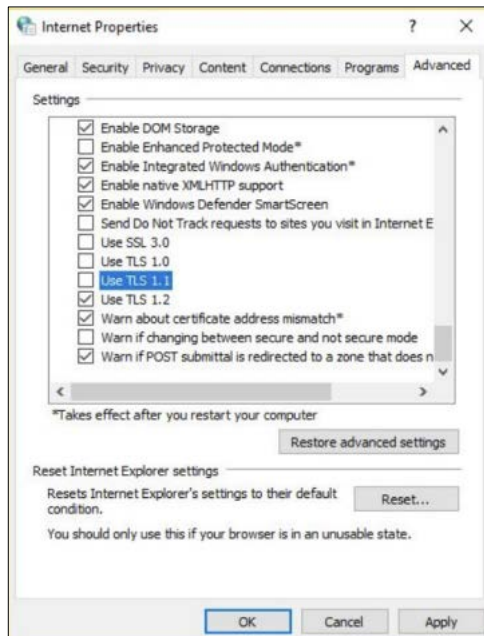
P1 P2

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. Since TLS v1.1 or lower has severe vulnerabilities that can easily be hacked, the CN2600 Series uses TLS v1.2 for HTTPS to ensure data transmissions are secured. 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.

Log in to the HTTP/HTTPS console and select **System Management > Certificate**. 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 CN2600 device
 - NPort devices can auto-generate a self-signed SSL certificate. We recommend importing 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 because of the increased complexity of encrypting and decrypting communicated data.

- For the NPort self-signed certificate:

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

- Step 1. Select **System Management > Certificate > Certificate/Key Delete**. 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, follow these 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. 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.

- 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/>)
 - Sectigo (Comodo Cybersecurity) (<https://www.comodo.com/>)
 - GoDaddy (<https://www.godaddy.com/>)
 - Verisign (<https://www.verisign.com/>)

Ethernet SSL Certificate Import

Installed Certificate

Issued to	192.168.127.254
Issued by	192.168.127.254
Valid	from 2024/5/21 to 2044/5/21

Select SSL certificate/key file No file chosen

MOXA Total Solution for Industrial Device Networking

Model	MG-ME3270	IP	192.168.127.200	MAC Address	00 90 E8 44 F0 E2
Name	MG-ME3270_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 Accessible IP List

- The CN2600 Series has a feature that limits access to specific remote host IP addresses to prevent unauthorized access. If a host’s IP address is **not** in the accessible IP table, then the host will **not** be allowed to access the serial ports of CN2600 Series. To configure it, log in to the HTTPS console and select **System Management > Misc. Network Settings > Accessible IP List**.

Accessible IP List

Enable the accessible IP list ("Disable" will allow all IP's connection request.)

No	Active	IP Address	Netmask
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"/>
7	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
8	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
9	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
10	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
11	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
12	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
13	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
14	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
15	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
16	<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

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

3.4 Logging and Auditing

- These are the events that will be recorded by the CN2600 Series:

Event Group	Summary
System	System Cold Start, System Warm Start, Power Down
Network	DHCP/BOOTP/PPPoE Get IP/Renew, NTP, Mail Fail, NTP Connect Fail, IP Conflict, Network Link Down
Configuration	Login Fail, IP Changed, Password Changed, Config Changed, Firmware Upgrade, SSL Certificate Import, Config Import, Config Export
OpMode	Connect, Disconnect, Authentication Fail, Restart

- To configure this setting, log in to the HTTPS console and select **System Management > Misc. Network Settings > System Log Settings**. Then, enable the **Local Log** for recording on the CN2600 device. Enable system log settings to record important system events to monitor device status and check for security issues.

System Log Settings

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

System Log

System Log

2024/05/21 11:16:50 [System] System Warm Start

2024/05/21 11:16:50 [System] Power 2 Down

4 Patching/Upgrades

4.1 Patch Management

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

4.2 Firmware Upgrades

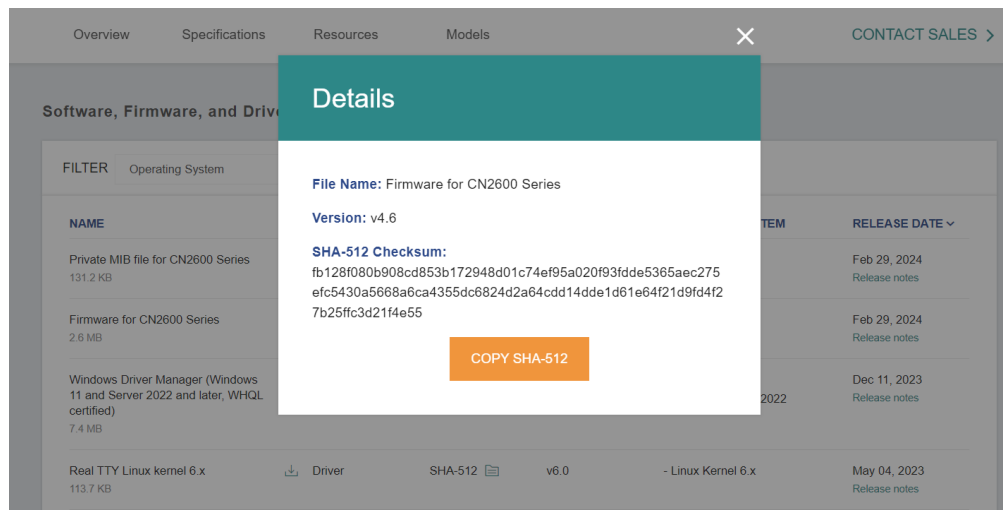
The process for upgrading firmware is:

- Download the latest firmware and software along with its release notes and hash values for your NPort device from the Moxa website:

➤ Firmware CN2600 Series:

[CN2600 Series - Software & Documentation | MOXA](#)

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 **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: Upgrade firmware will discard your un-saved configuration changes and restart the system!

Select firmware file No file chosen

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>