The Security Hardening Guide for the MGate MB3000-G2 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 4
2.3 Security Threats 5
2.4 Security Measures 6
3 Configuration and Hardening Information 8
3.1 TCP/UDP Ports and Recommended Services 9
3.2 Serial Ports and Recommended Services 13
3.3 HTTPS and SSL Certificates 14
3.4 Account Management 16
3.5 Allowlist 19
3.6 Logging and Auditing 20
3.7 DoS Defense 22
4 Patching/Upgrades 23
4.1 Patch Management 23
4.2 Firmware Upgrades 23
4.3 Testing the Security Environment 24
5 Decommission 25
6 Security Information and Vulnerability Feedback 25

 Released on Sep 9, 2025

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 over 35 years of industry experience, Moxa has connected more than 111 million devices worldwide and has a distribution and service network that reaches customers in more than 91 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

The MGate MB3000-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 or monitoring 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
MGate MB3170-G2 Series MGate MB3270-G2 Series MGate MB3470-G2 Series	Modbus gateway	Zephyr RTOS	Version 1.0

The MGate MB3000-G2 Series Modbus protocol gateways are specifically designed to allow direct network access to industrial devices. Thus, legacy Modbus serial devices can be transformed into Ethernet devices, enabling them to be monitored and controlled from any network location and even via the Internet.

Zephyr RTOS is a full-featured OS with an architecture that has security in mind. The open-source project governance model of this ensures that all aspects of the code are developed securely and conform to the expectations of the next generation RTOS of Moxa.

To harden the security of the operating system, the following open-source HTTPS libraries are included and undergo regular cybersecurity enhancement reviews.

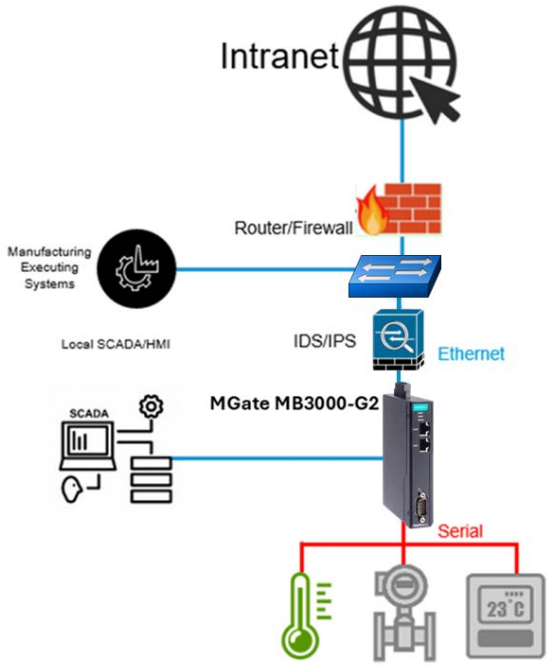
- Zephyr RTOS: mbed TLS v3.6.3

2.2 Deployment of the Device

Deploy the MGate MB3000-G2 Series behind a secure firewall and/or IDS/IPS network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

Customers who buy products from Moxa or Moxa resellers should be aware that Moxa might have already launched a newer firmware version with enhanced security features. We strongly recommend checking Moxa's support website for newer firmware. Upgrade the firmware to the newest to benefit from the latest security features/upgrades.

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



2.3 Security Threats

The security threats that can harm MGate MB3000-G2 Series are:

1. **Attacks over the network**

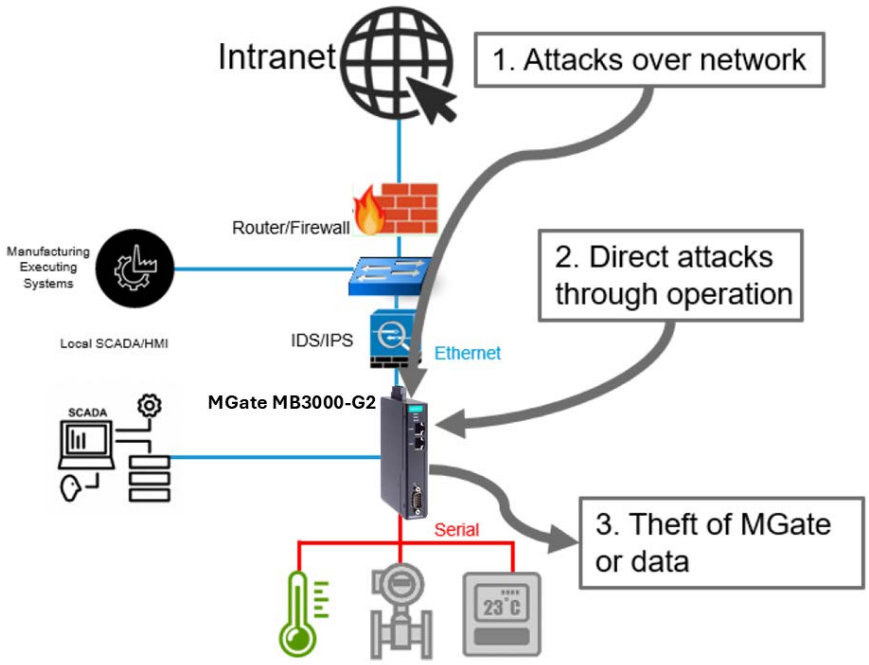
   Threats from individuals with no rights to the MGate MB3000-G2 Series via networks such as intranets.

2. **Direct attacks through operation**

   Threats where individuals with no rights to the MGate MB3000-G2 Series directly operate a device to affect the system and steal critical data.

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

   Threats where an MGate MB3000-G2 Series or data from it is stolen, enabling critical data to be analyzed and used.



2.4 Security Measures

To fend off security threats, we have identified a set of security measures for the MGate MB3000-G2 Series for the general business network environment. The security measures are classified into three security types. The following table details the security measures and the threats that each measure handles.

Security Layer	Security Measure	Subcategory	Threats Handled Yes/No			Responsibility
			1	2	3	
Policy and Procedure	Establish policies and procedures to guide employees on their role and responsibilities for safe use of security sensitive assets.	Vulnerabilities created because of lack of security policies or employees' lack of awareness of procedures	Yes	Yes	Yes	Asset owner
Perimeter Security	Physical security	Physical modification, manipulation, theft, removal, or destruction of asset	No	Yes	Yes	Asset owner
Network Security	Network firewall	Unauthorized and malicious communications from untrusted network	Yes	No	No	Asset owner
	Network IDS/IPS	Network attacks from various sources, such as port scanning and DDOS.	Yes	No	No	
	VPN	Man-in-the-middle attacks during configuration and protocol communication	Yes	No	No	
Device Security	Access control	–	Yes	Yes	No	Built into the MGate
	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	

Security Layer	Security Measure	Subcategory	Threats Handled Yes/No			Responsibility
			1	2	3	
		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	

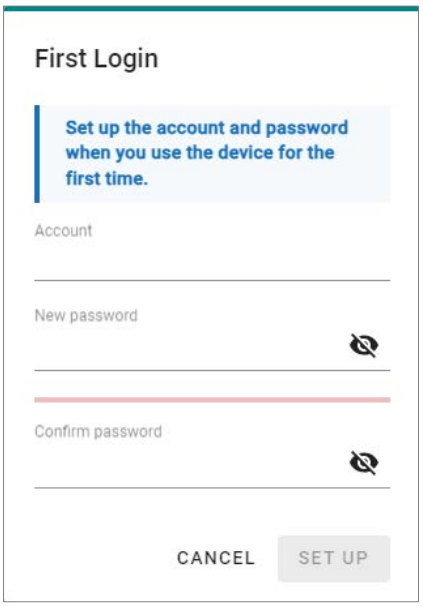
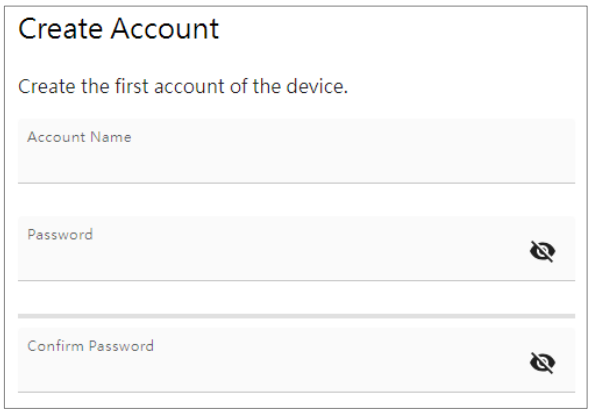
Note
1. Attacks over the network.
2. Direct attacks through the operation.
3. Theft of the MGate or data.

To defend against the theft of the MGate or data, we recommend you use the MGate MB3000-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 3.5) to only allow the necessary hosts/IPs to access the device and Secure Connection function (for more details, refer to chapter 3.3) to encode the data and protect the data from being stolen.

3 Configuration and Hardening Information

For security reasons, there is no default account name and password. When accessing the MGate MB3000-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.

The following screenshot is of the Device Search Utility v3.0 or later and 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 MGate MB3000-G2 Series and other devices.

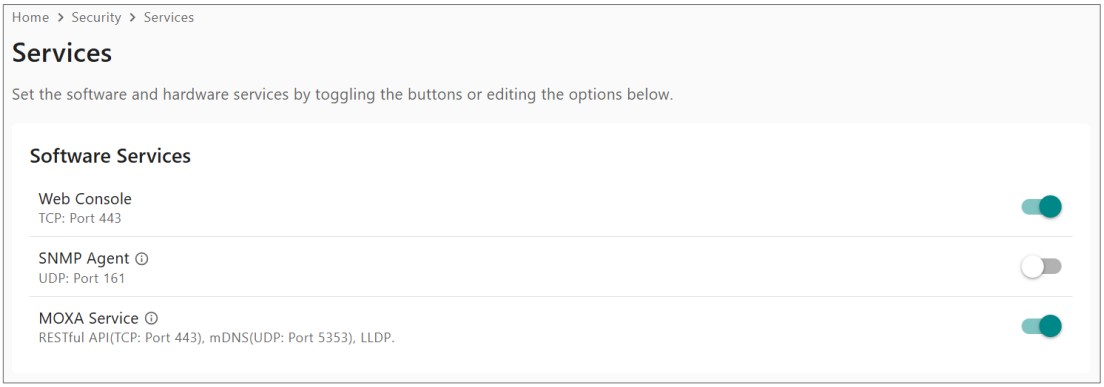
Service Name	Option	Default Settings	Type	Port Number	Description
Moxa service	Enable/ Disable	Enable	TCP	443	For Moxa utility communication
			UDP	5353	
Modbus TCP client/server	Enable/ Disable	Enable (Can be disabled after you disable Modbus TCP in Topology settings)	TCP	502, 7502	502 for Modbus communication; 7502 for priority Modbus communication
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
HTTPS server	Enable/ Disable	Enable	TCP	443	Secured web console
email	Enable/ Disable	Disable	UDP/ TCP	25	Sending system/ configuration event notifications
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 (syslog)	Enable/ Disable	Disable	UDP	Random port	Send the event log to a remote log server
Real COM (only supported in the MGate MB3x70-G2 Series)	Enable/ Disable	Disable (Can be enabled after you enable Real COM in Topology settings)	UDP/ TCP	950 to 953 966 to 969	Create a virtual serial COM port that communicates over TCP/IP

For security reasons, the MGate MB3000-G2 Series only enables limited services to ensure the security of the device itself. It will only enable the Moxa services and HTTPS for the user to configure the device. If this is not the case, you may modify or disable the above services.

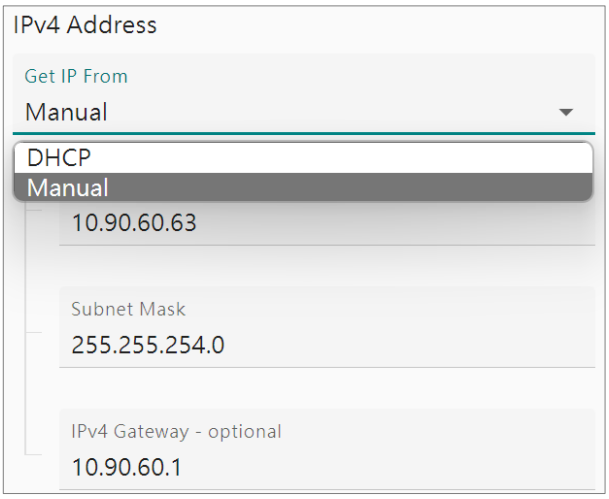
To integrate the MGate MB3000-G2 Series into your network topology and secure your applications, use the following services with proper settings to enhance the security architecture of the network and provide defense-in-depth protection.

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.
DHCP Client	UDP	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, time synchronization is important.
Remote System Log (syslog)	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 MGate MB3000-G2 to a remote log server.

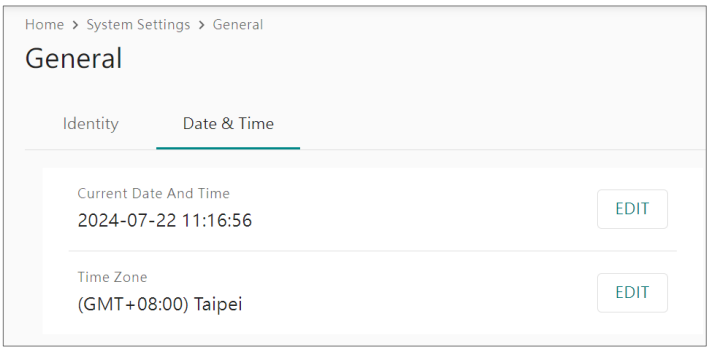
To configure the security services, log in to the Web console and select **Security > Services**.



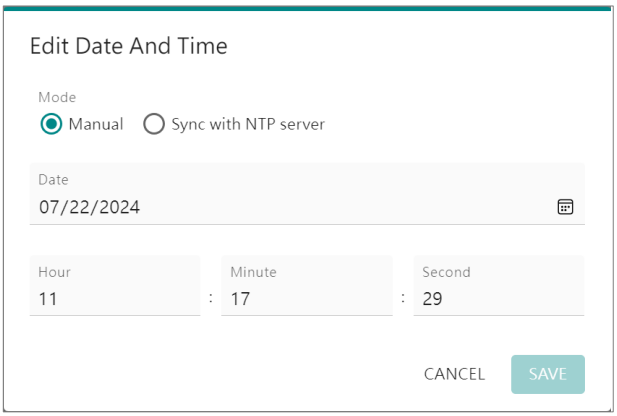
If you want to configure DHCP Client, log in to the Web console, select **Network Settings > IP Address,** and select **Get IP From DHCP**.



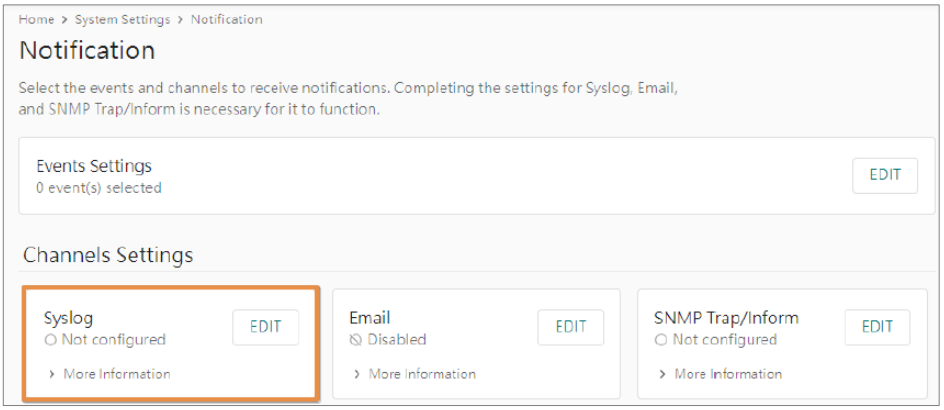
If you want to configure SNTP Client, log in to the HTTPS console, select **System Settings > General**, and select the **Date & Time** tab.

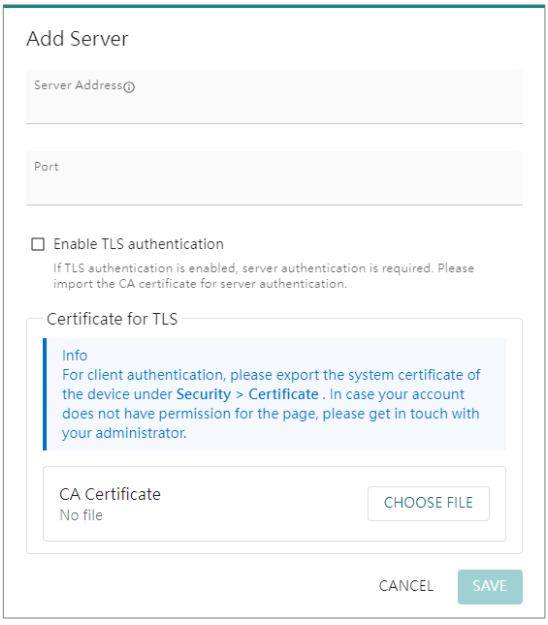


Click the **EDIT** button and select **Sync with NTP server**. Then, click the **SAVE** button to enable it.



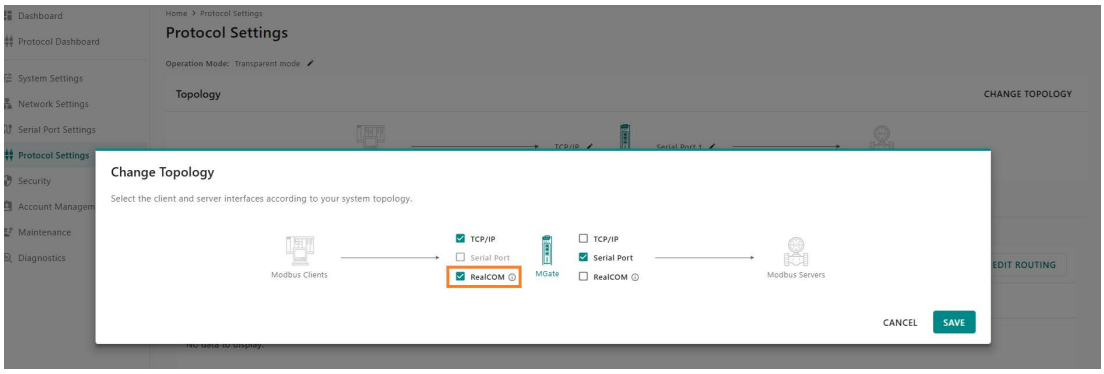
For the remote system log server, log in to the HTTPS console, select **System Settings > Notification**, click the **EDIT** button next to Syslog, and add the server in the server field.





You may also **Enable TLS authentication**. The MGate MB3000-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.

To enable Real COM service in MGate MB3x70-G2 series, log in to the HTTPS console and select **Protocol Settings > CHANGE TOPOLOGY** and select Real COM.



3.2 Serial Ports and Recommended Services

A list of all serial protocols used to communicate between the MGate 3000-G2 Series and other devices are in the following table:

Service Name	Option	Default Settings	Type	Description
Modbus RTU/ASCII	N/A	Enable	RS-232/422/485	Modbus serial protocol
Proprietary Serial	N/A	Enable	RS-232/422/485	User-configurable data frame for proprietary serial protocol

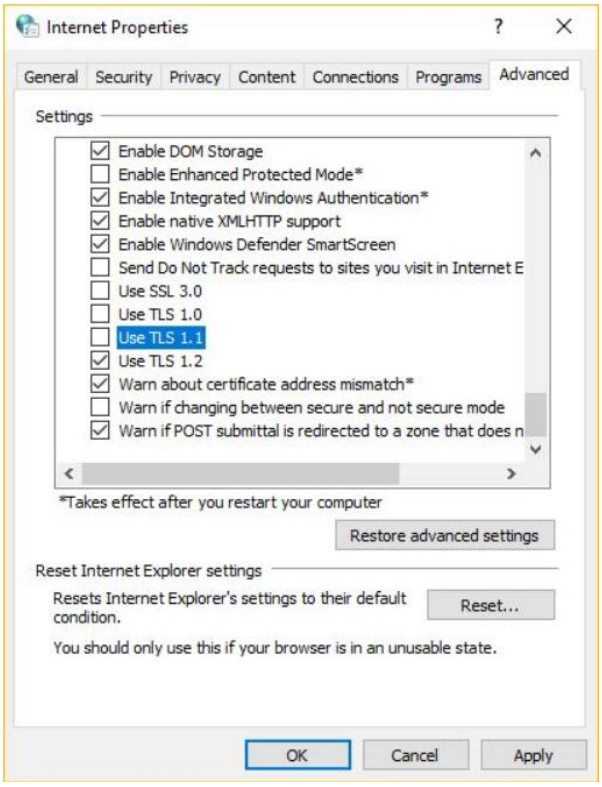
For security reasons, consider disabling unused services. The serial settings suggested in the following table depends on the product model and user preferences. Ensure that serial connections and cables are under physical protection. Proprietary serial uses user-configurable data frames. Hence, application security requirements and risks associated with user-defined data frames must be addressed at the system level.

Service Name	Suggested Settings	Type	Security Remark
Modbus RTU/ASCII	Enable	RS-232/422/485	Serial connections and cables are under physical protection
Proprietary Serial	Enable	RS-232/422/485	Serial connections and cables are under physical protection

Note For each instruction above, click the **Submit** button to save your changes, then restart the MGate device so the new settings can take effect.

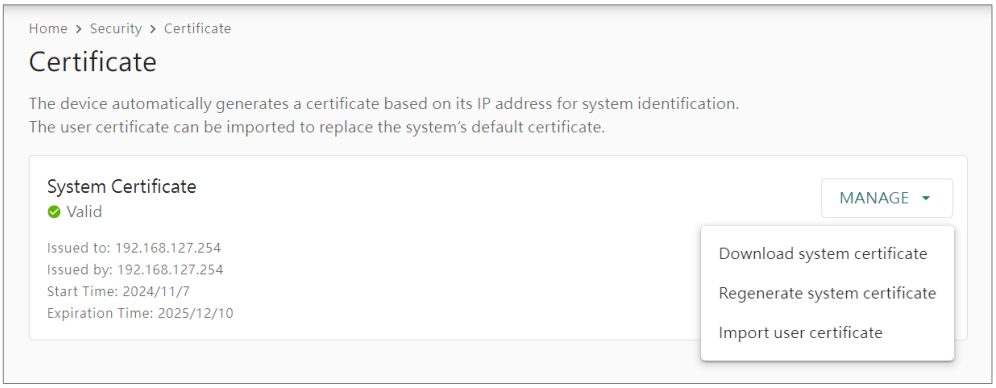
3.3 HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. Because TLS v1.1 and lower versions have severe, easily exploitable vulnerabilities, the MGate MB3000-G2 Series uses TLS v1.2 for HTTPS to secure data transmissions. Ensure that your browser is TLS v1.2 enabled and is set to update to the newest version.



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

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

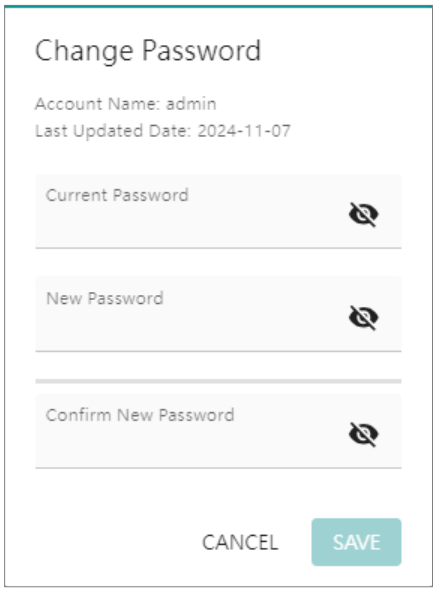


- Behavior of the System Certificate on an MGate MB3000-G2 device
  - MGate devices will auto-generate a self-signed SSL certificate when the IP address is changed or you can click the **Regenerate system certificate** option to generate a new one manually. We recommend importing SSL certificates that are issued by a trusted third-party Certificate Authority (CA) or by the organization's CA.
  - The MGate 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:

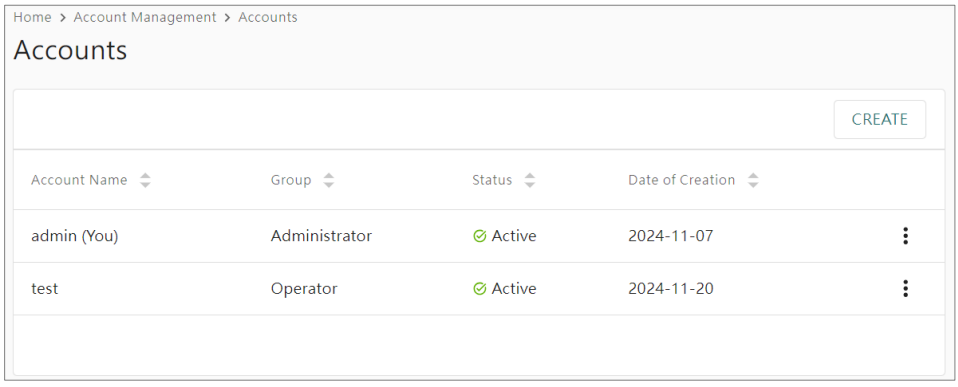
  To generate the SSL certificate through the third party, here are the steps:
  - Step 1. Create a certification authority (Root CA), such as Microsoft AD Certificate Service (https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/)
  - Step 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 MGate device. Note that MGate devices only accept certificates using a "**.pem**" format. The MGate MB3000-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/)

3.4 Account Management

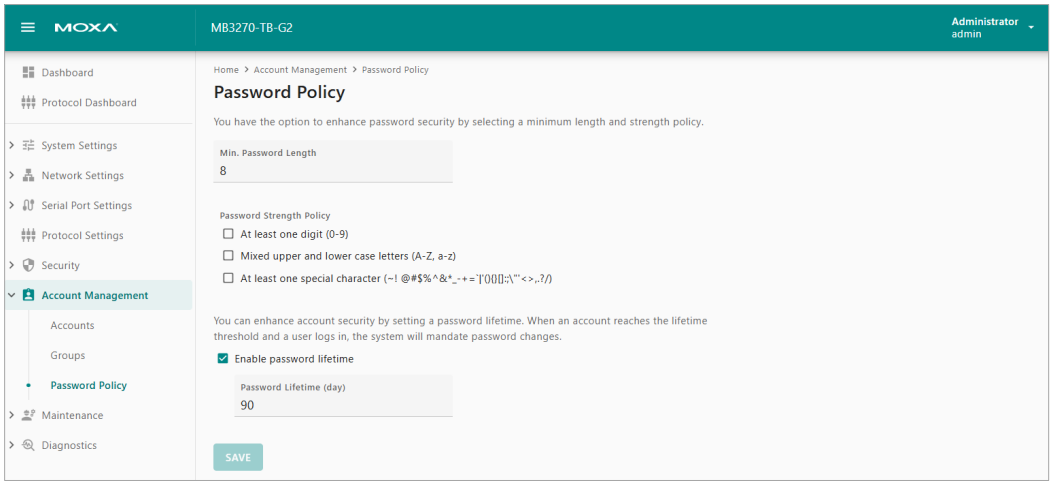
- The MGate MB3000-G2 Series provides two different user groups, Administrator, and Operator. With an Administrator account, you can access and change all settings through the web console. With an Operator account, you can change and monitor most of the settings, except **Security** and **Account Management**.
- Set the Administrator's account and password when 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.



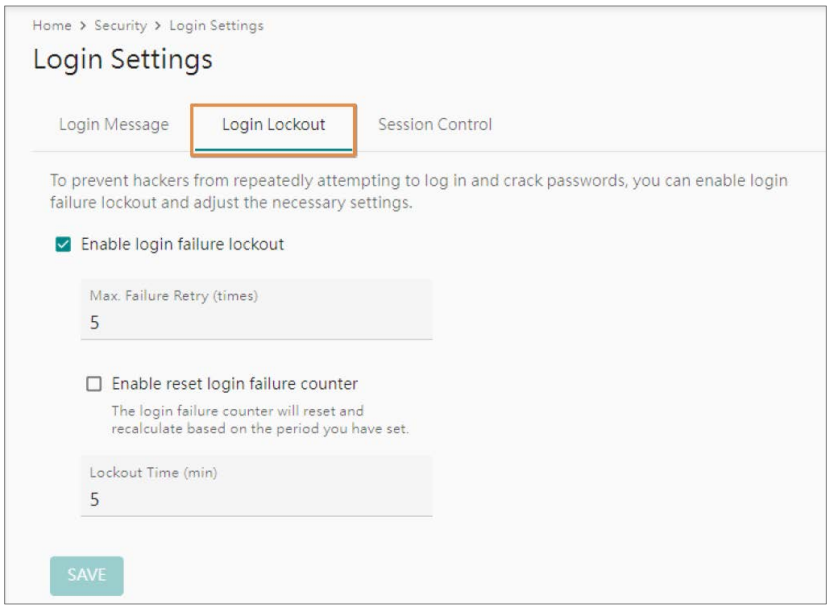
- To add new accounts, select **Account Management > Accounts > CREAT**. A window will pop up for you to input account information and assign a password to the user. Also, the Administrator(s) shall assign a proper **Group** to users to limit their privileges of using the MGate MB3000-G2. To add/delete/edit the **Group** privileges, go to the **Groups** section in the menu. The **Password** rules can be set up in **Password Policy** section.



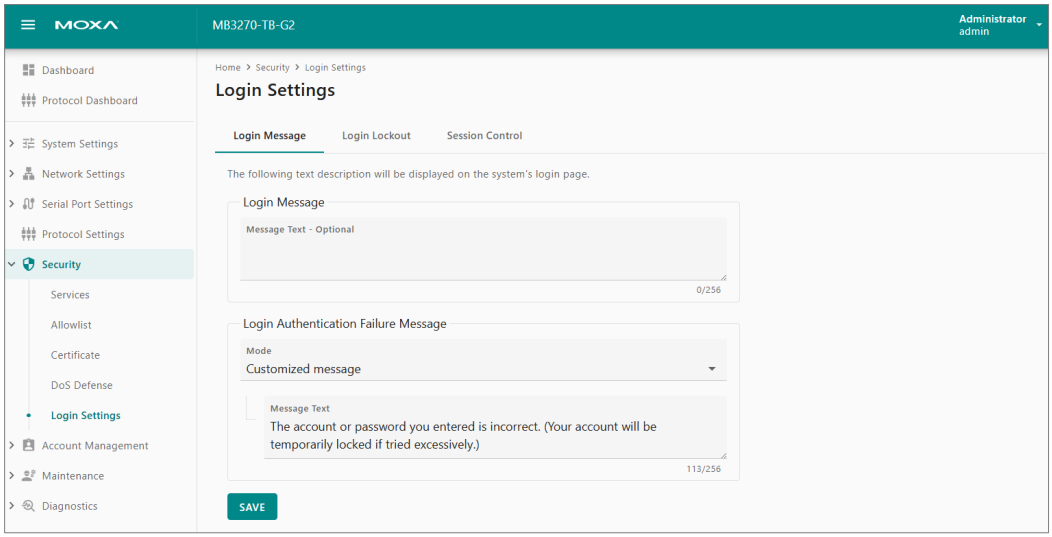
- Configure the login password policy and account login failure lockout to improve security. To configure them, log in to the HTTPS console and select **Account management > Password Policy**.



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.

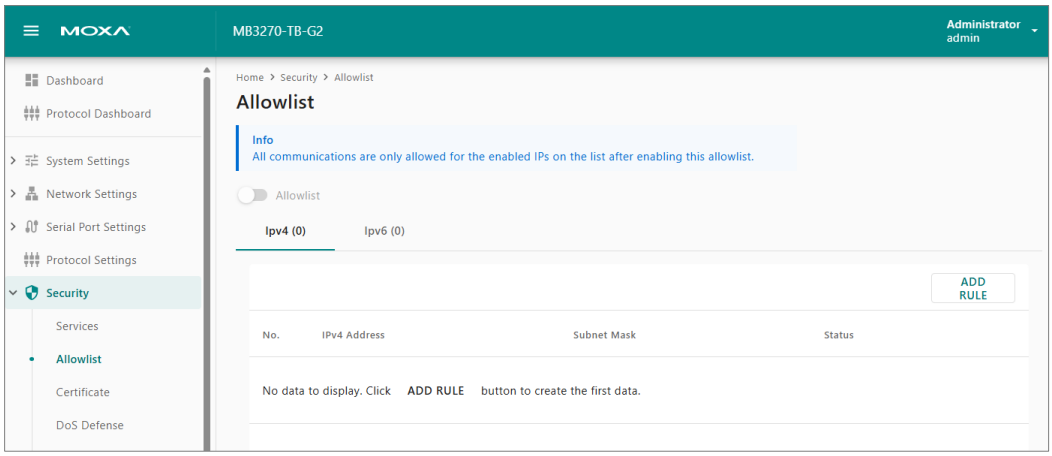


- To highlight critical system-security requirements, a warning message may be shown to every user who logs in. To add messages to be shown at login, select **Security > Login Settings > Login Message**, and enter the messages.



3.5 Allowlist

- An allowlist is a list of IP addresses or domains that have 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:** Ensure 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**.

3.6 Logging and Auditing

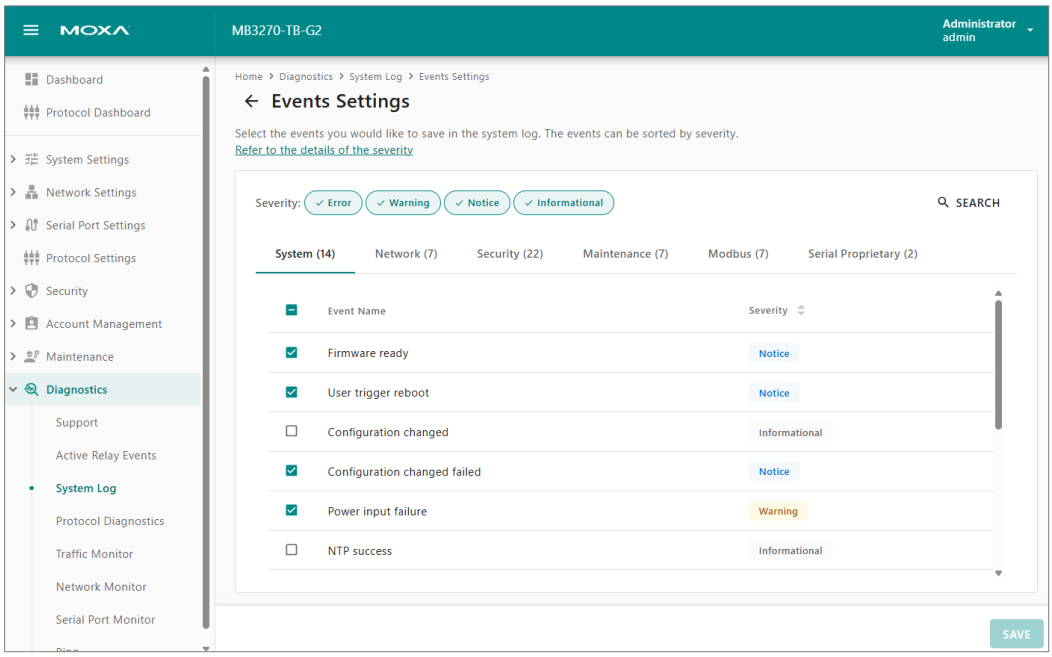
- The local syslog function is enabled to record the events that happened on the MGate MB3000-G2 device. Under the Security category, the severity of events—Notice, Warning and Error—will be saved on the local flash memory by default. Up to 10,000 events can be recorded.
- These are six categories of events:

Category	Description
System	Events related to the MGate itself, like firmware ready.
Network	Events related to the Ethernet interface. For example, the Ethernet link up.
Security	Events related to security—the administrator may need to figure out why certain events happened. For example, a login fail event.
Maintenance	Events that usually happen during the maintenance process. For example, firmware upgrades.
Modbus	Events related to Modbus protocol communication. For example, a Modbus exception occurred.
Proprietary Serial	Events related to proprietary serial communication. For example, a serial device is offline.

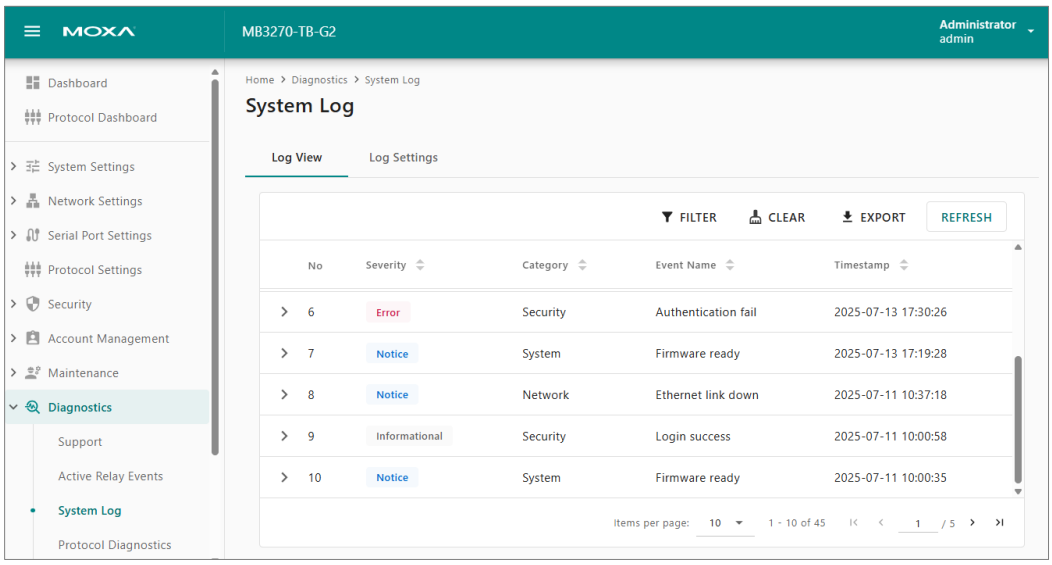
- There are four severities of the events:

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 indicating 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.

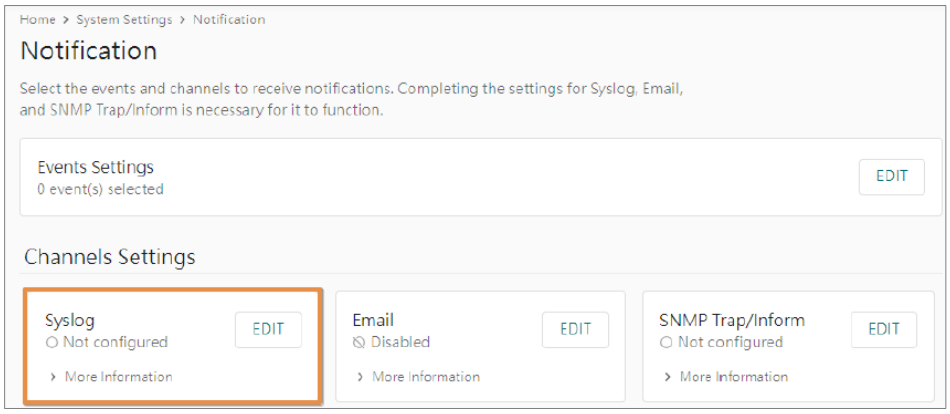
- To enable what events must be recorded, log in to the HTTPS console and select **Diagnostics > System Log> Log Settings > EDIT > Events Settings**. Select the events you would like to save in the system log.



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

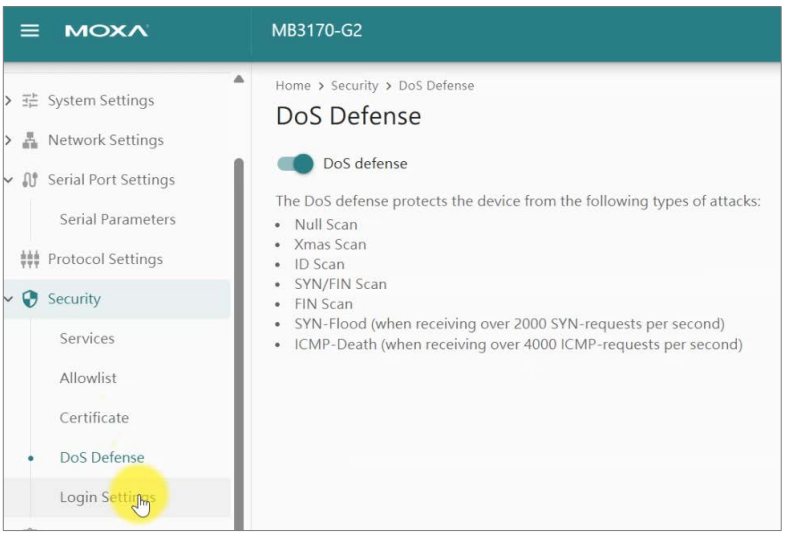


- To enable the remote log server, select **System Settings > Notification**. Click the **EDIT** button next to **Syslog** and add the server in the server field.



3.7 DoS Defense

Enable DoS Defense to protect against the following denial-of-service (DoS) attacks.



4 Patching/Upgrades

4.1 Patch Management

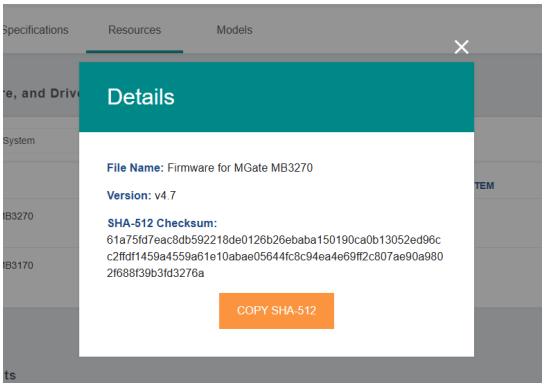
Regarding patch management, Moxa releases version enhancements annually, with detailed release notes.

4.2 Firmware Upgrades

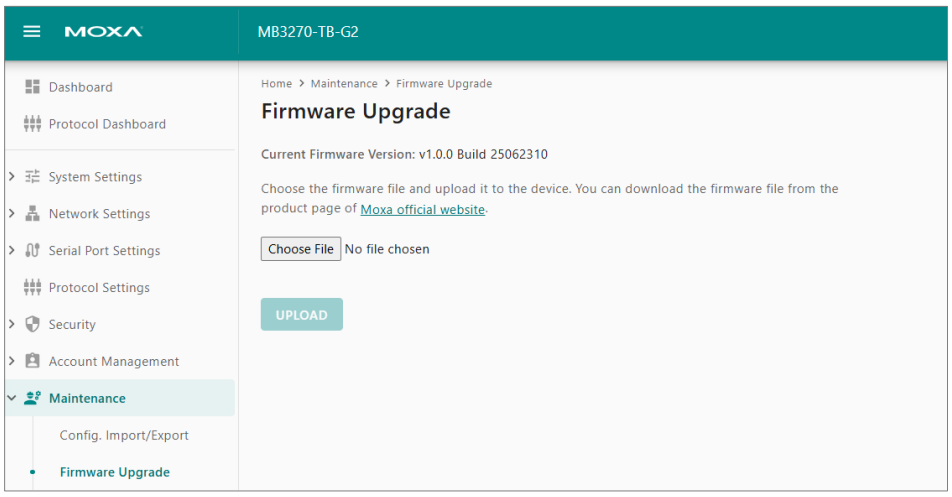
The process for upgrading firmware is:

- Download the latest firmware and software, along with its release notes and hash values for your MGate device from the Moxa website:
  - Firmware of MGate MB3170-G2/MB3270-G2/MB3470-G2 Series:

    https://www.moxa.com/en
- If you want to upgrade the firmware of the MGate MB3000-G2 Series, download the firmware from Moxa's website first. 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.



4.3 Testing the Security Environment

Besides using devices that support security functions, network managers can follow several recommendations/best practices to protect their network and devices.

To prevent unauthorized access to a device, follow these recommendations:

- Testing tools are available checking cybersecurity environment. Some may provide limited free use, for example, Nessus. These tools help identify probable security leaks in the environment.
- The device must be operated inside a secure network, protected by a firewall or router that blocks attacks via the Internet.
- Control/restrict access to the serial console (depends on the model deployed), and physical access to the device itself.
- Avoid using insecure services such as SNMPv1 or v2c. We recommend disabling them completely.
- Limit the number of simultaneous web server sessions allowed. We recommend changing the passwords periodically.
- Back up the configuration files periodically.
- Audit the devices periodically to ensure that they comply with these recommendations and/or any internal security policies.
- If there is a need to return the unit to Moxa, ensure that you back up the configuration and data on it.

Note DISCLAIMER:
The information above and this guide (the "information") are for your reference only. We do not guarantee a cyberthreat-free environment. These guidelines are to increase the security level to defend against cyber intrusions and is not guaranteed to meet your specific requirements. The abovementioned information is provided "as-is", and we make no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

5 Decommission

Since the MGate is the primary device for converting Modbus serial devices to Modbus TCP devices, decommissioning an MGate 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 MGate and import it to the new unit. This will save you from having to configure the new unit manually.
2. Stop 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 not, 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.

Note 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 manage security risks better.

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