The Security Hardening Guide for the MGate MB3000 Series

Moxa Technical Support Team
support@moxa.com

Contents

Released on March 26, 2021

About Moxa
Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things (IIoT). With over 30 years of industry experience, Moxa has connected more than 57 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industries with reliable networks and sincere service. Information about Moxa's solutions is available at www.moxa.com.

How to Contact Moxa
Tel: +886-2-8919-1230

1. Introduction

This document provides guidelines on how to configure and secure the MGate MB3000 Series. The recommended steps in this document should be considered as best practices for security in most applications. It is highly recommended that you review and test the configurations thoroughly before implementing them in your production system in order to ensure that your application is not negatively impacted.

2. General System InformationBasic Information About the Device

Model	Function	Operating System	Firmware Version
MGate MB3170/3270 Series	Gateway	Moxa Operating System	Version 4.2
MGate MB3660 Series	Gateway	Moxa Operating System	Version 2.5
MGate MB3280	Gateway	Moxa Operating System	Version 4.1
MGate MB3480	Gateway	Moxa Operating System	Version 3.2

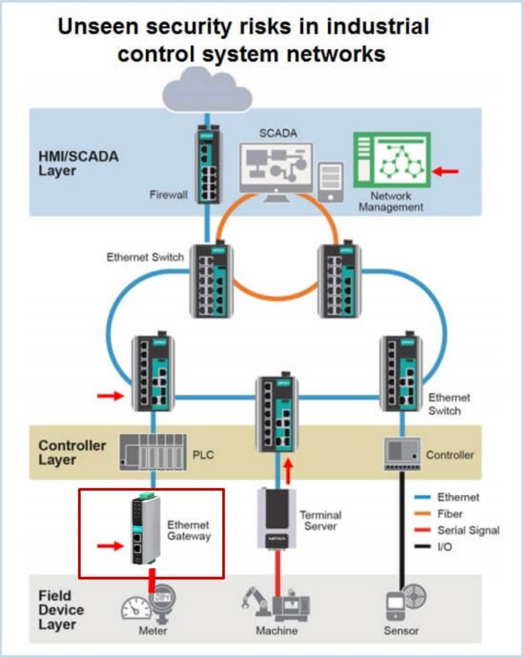
The MGate MB3170/3270/3660/3280/3480 Series consists of Modbus protocol gateways are specifically designed to allow industrial devices to be directly accessed from a network. Thus, legacy Modbus serial devices can be transformed into Ethernet ones, which can be monitored and controlled from any network location or even the Internet.

Moxa Operating System (MOS) is an embedded proprietary operating system, which is only executed in Moxa edge devices. Because the MOS operating system is not freely available, the chances of malware attacks are significantly reduced. To harden the security of this proprietary operating system, the open-source HTTPS library, mbed TLS v2.7.5, is also included and periodically reviewed for cybersecurity enhancement.

2.2. Deployment of the Device

You should deploy the MGate MB3170/3270/3660/3280/3480 Series behind a secure firewall network that has sufficient security features in place to ensure that networks are safe from internal and external threats.

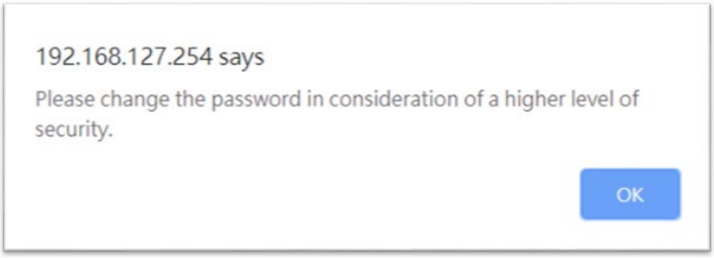
Make sure that the physical protection of the MGate devices and/or the system meets the security needs of your application. Depending on the environment and the threat situation, the form of protection can vary significantly.



3. Configuration and Hardening Information

For security reasons, account and password protection is enabled by default, so you must provide the correct account and password to unlock the device before entering the web console of the gateway.

The default account and password are **admin** and **moxa** (both in lowercase letters), respectively. Once you are successfully logged in, a pop-up notification will remind you to change the password to ensure a higher level of security



192.168.127.254 says

Please change the password in consideration of a higher level of security.

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 MB3170/3270/3660/3280/3480 Series and other devices.

Service Name	Option	Default Setting	Type	Port Number	Description
DSCI (Moxa Command)	Enable/Disable	Enable	TCP	4900	For Moxa utility communication
			UDP	4800	
DNS client	Enable/Disable	Disable	UDP	53	Processing DNS and WINS (Client) data
SNMP agent	Enable/Disable	Enable	UDP	161	SNMP handling routine
HTTP server	Enable/Disable	Enable	TCP	80	Web console
HTTPS server	Enable/Disable	Enable	TCP	443	Secured web console
Telnet server	Enable/Disable	Disable	TCP	23	Telnet console
DHCP client	Enable/Disable	Disable	UDP	68	The DHCP client needs to acquire the system IP address from the server
Syslog client	Enable/Disable	Disable	UDP	514	Sending the system logs to the remote syslog server
Email client	Enable/Disable	Disable	UDP/ TCP	25	Sending system/config event notifications
SNMP trap client	Enable/Disable	Disable	UDP	162	Sending system/config event notifications
NTP client	Enable/Disable	Disable	UDP	123	Network time protocol to synchronize system time from the server
Modbus TCP client/server	Enable/Disable	Enable	TCP	502, 7502	502 for Modbus communication; 7502 for priority Modbus communication
ProCOM	Enable/Disable	Enable	TCP	950 to 953 966 to 969	Mapping additional Modbus slave role on Windows platform

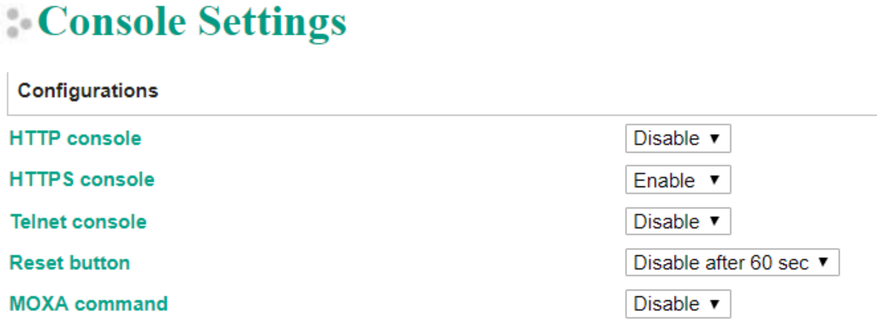
For security reasons, you should consider disabling unused services. After initial setup, use services with stronger security for data communication. Refer to the table below for the suggested settings.

Service Name	Suggested Setting	Type	Port Number	Security Remark
DSCI (Moxa Command)	**Disable**	TCP	4900	Disable this service as it is not commonly used
		UDP	4800	
DNS client	**Disable**	UDP	53	Disable this service as it is not commonly used
SNMP agent	**Disable**	UDP	161	Managing the MGate via HTTPS console will be more secure
HTTP server	**Disable**	TCP	80	Disable HTTP to prevent plain text transmission
HTTPS server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for MGate configuration
Telnet server	**Disable**	TCP	23	Disable this service as it is not commonly used
DHCP client	**Disable**	UDP	68	Assign an IP address manually for the device
Syslog client	**Enable**	UDP	514	A service for sending important system events for a diagnosis of the MGate's status
Email client	**Enable**	UDP/ TCP	25	A service for sending important system events for a diagnosis of the MGate's status
SNMP trap client	**Enable**	UDP	162	A service for sending important system events for a diagnosis of the MGate's status
NTP client	**Disable**	UDP	123	Disable this service as it is not commonly used
Modbus TCP client/server	**Enable**	TCP	502, 7502	Make sure you add your Modbus devices' IP addresses to the "Accessible IP list"
ProCOM	**Disable**	TCP	950 to 953 966 to 969	Disable ProCOM if you are not using Windows for Modbus client role

- For console services, we recommend the following:

HTTP	Disable
HTTPS	Enable
Telnet	Disable
Moxa Command	Disable

- To enable or disable these services, log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Console Settings.**

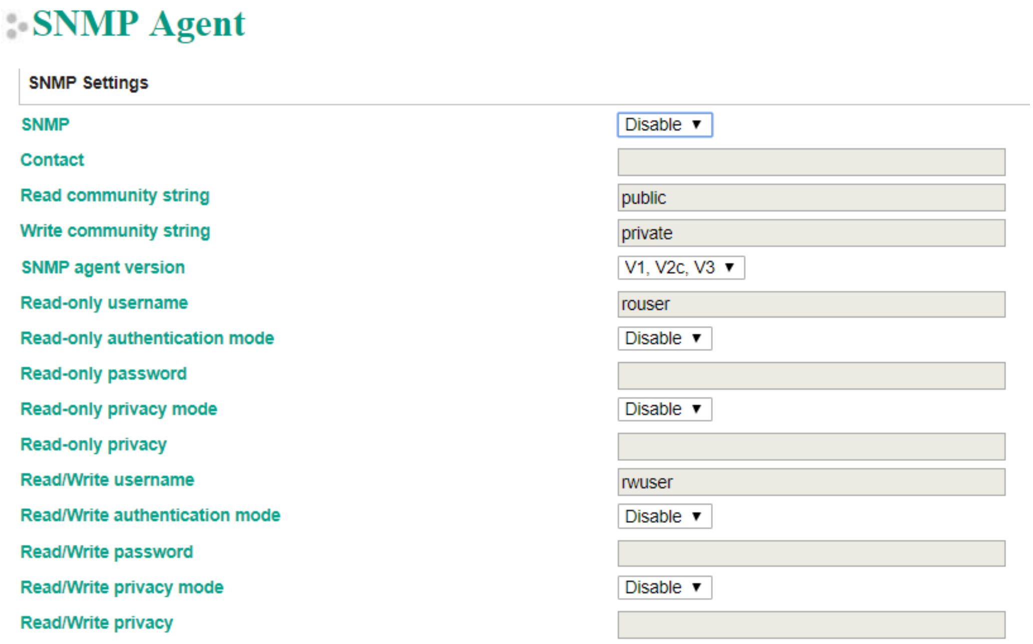


Console Settings

Configurations

HTTP console	Disable ▼
HTTPS console	Enable ▼
Telnet console	Disable ▼
Reset button	Disable after 60 sec ▼
MOXA command	Disable ▼

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

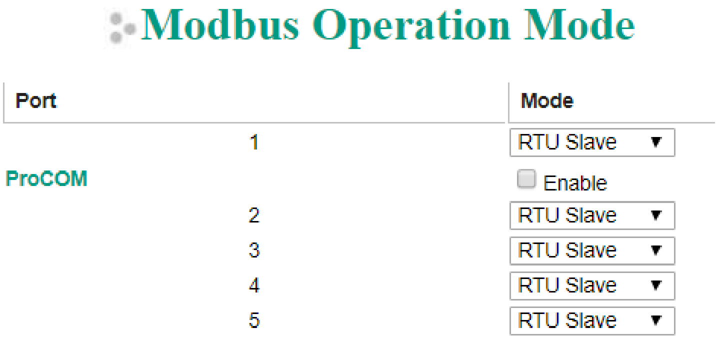


SNMP Agent

SNMP Settings

SNMP	Disable ▼
Contact	
Read community string	public
Write community string	private
SNMP agent version	V1, V2c, V3 ▼
Read-only username	rouser
Read-only authentication mode	Disable ▼
Read-only password	
Read-only privacy mode	Disable ▼
Read-only privacy	
Read/Write username	rwuser
Read/Write authentication mode	Disable ▼
Read/Write password	
Read/Write privacy mode	Disable ▼
Read/Write privacy	

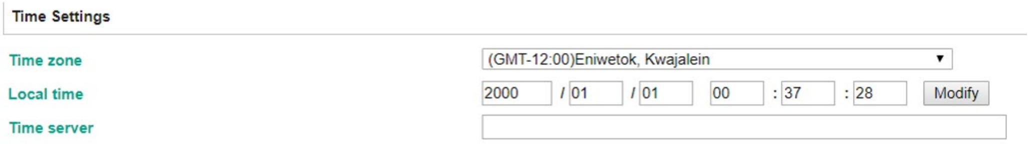
To disable the ProCOM service (only for the MGate MB3170/MB3270), log in to the HTTP/HTTPS console and select **Protocol Settings → Mode**, then uncheck Enable.



Modbus Operation Mode

Port		Mode
	1	RTU Slave ▼
ProCOM		□ Enable
	2	RTU Slave ▼
	3	RTU Slave ▼
	4	RTU Slave ▼
	5	RTU Slave ▼

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



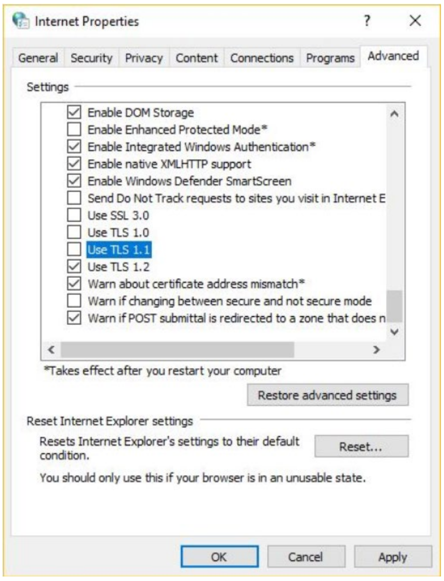
Time Settings

Time zone	(GMT-12:00)Eniwetok, Kwajalein ▼
Local time	2000 / 01 / 01 00 : 37 : 28 Modify
Time server	

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

3.2. HTTPS and SSL Certificates

HTTPS is an encrypted communication channel. As TLS v1.1 or lower has severe vulnerabilities that can easily be hacked, MGate devices use TLS v1.2 for HTTPS to ensure data transmissions are secured. Make sure your browser has TLS v1.2 enabled.


Internet Properties
? X
General Security Privacy Content Connections Programs Advanced

Settings

- ☑ Enable DOM Storage
- ☐ Enable Enhanced Protected Mode*
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable native XMLHTTP support
- ☑ Enable Windows Defender SmartScreen
- ☐ Send Do Not Track requests to sites you visit in Internet E
- ☐ Use SSL 3.0
- ☐ Use TLS 1.0
- ☐ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Warn about certificate address mismatch*
- ☐ Warn if changing between secure and not secure mode
- ☑ Warn if POST submittal is redirected to a zone that does n

*Takes effect after you restart your computer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

- In order to use the HTTPS console without a certificate warning appearing, you need to import a trusted certificate issued by a third-party certificate authority.
- Log in to the HTTP/HTTPS console and select **System Management → Certificate**. You can generate an up-to-date valid certificate by importing a third-party trusted SSL certificate or generating the "MGate self-signed" certificate.

Behavior of the SSL certificate on an MGate Device

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

MGate Self-signed Certificate

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

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

Importing a Third-party Trusted SSL Certificate

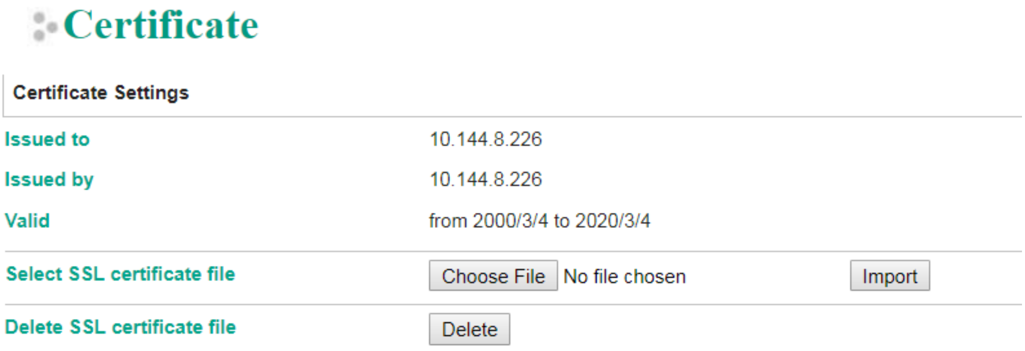
Importing the third-party trusted SSL certificate can improve security. To generate the SSL certificate through a third party, follow these steps:

- 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. You can get one from a third-party CA company such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).
- Step 3. Submit the CSR file to a public certification authority to get a signed certificate.
- Step 4. Import the certificate to the MGate device. Please note that MGate devices only accept certificates using a ".**pem**" format.

Note: The maximum supported key length for MGate devices is 2,048 bits.

Here are some well-known third-party CA (Certificate Authority) companies for your reference (https://en.wikipedia.org/wiki/Certificate_authority):

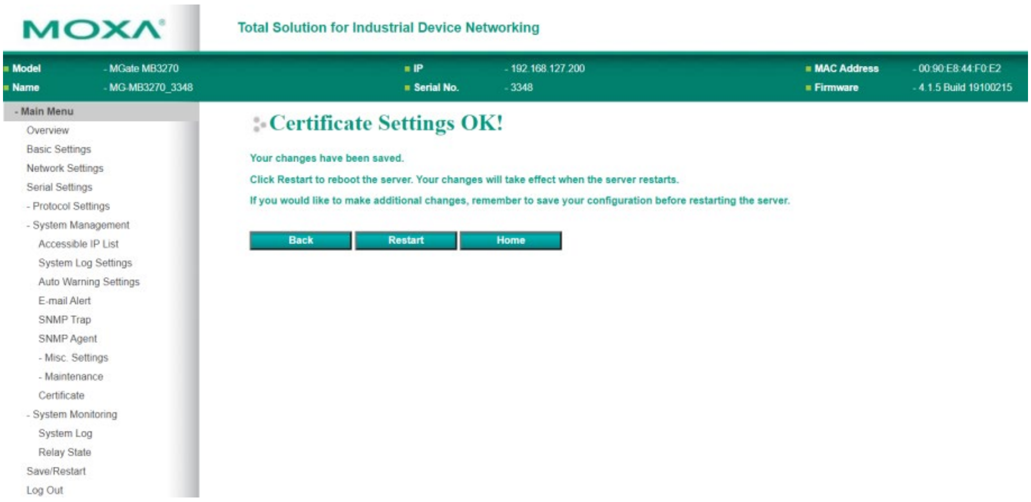
- IdenTrust (https://www.identrust.com/)
- DigiCert (https://www.digicert.com/)
- Comodo Cybersecurity (https://www.comodo.com/)
- GoDaddy (https://www.godaddy.com/)
- Verisign (https://www.verisign.com/)



Certificate

Certificate Settings

Issued to	10.144.8.226
Issued by	10.144.8.226
Valid	from 2000/3/4 to 2020/3/4
Select SSL certificate file	Choose File No file chosen Import
Delete SSL certificate file	Delete



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

Certificate Settings OK!

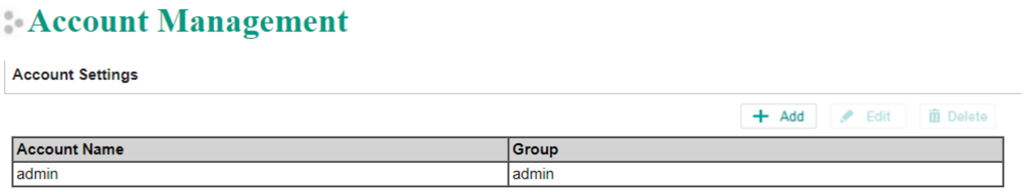
Your changes have been saved.

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

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

3.3. Account Management

- The MGate MB3170/3270/3660/3280/3480 Series provides two different user levels, admin and user, with a maximum of 16 accounts. With the admin account, you can access and modify all settings through the web console. With the user account, you can only view settings.
- The default administrator account is **admin**, with the default password **moxa**. To manage accounts, log in to the web console and select **System Management → Misc. Settings → Account Management**. To change the password of an existing account, double-click the name of the account. You can change the password on the page that opens.

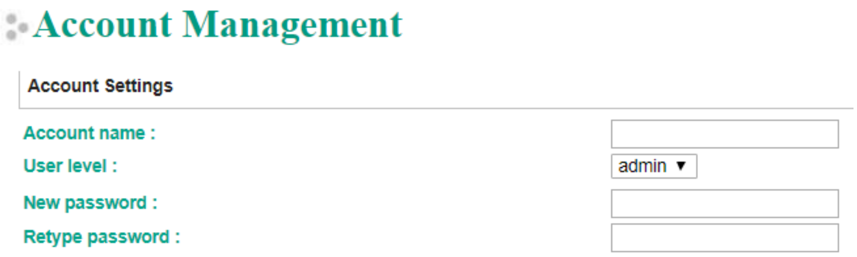


Account Management

Account Settings

Account Name	Group
admin	admin

- To add a new account, log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Account Management**. Click the **Add** button, then fill in the **Account name, User level, New password,** and **Retype password** to generate a new account.



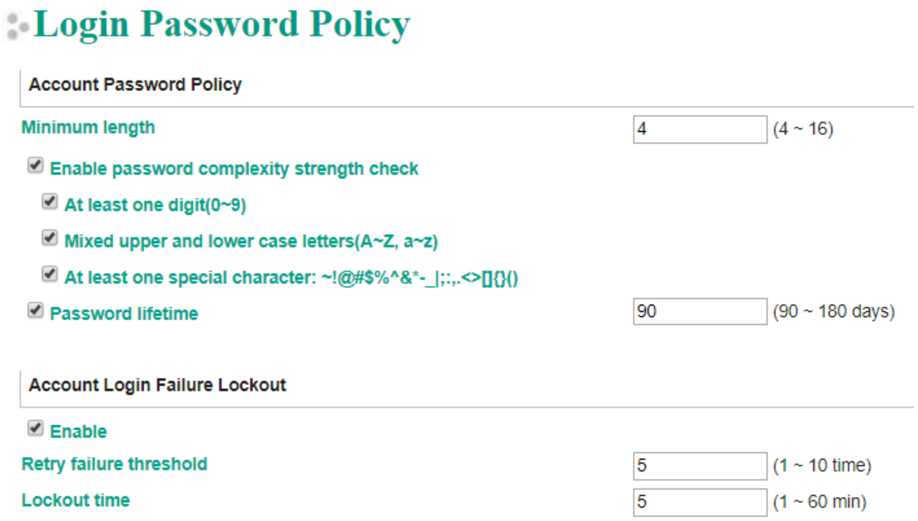
Account Management

Account Settings

Account name :	
User level :	admin ▾
New password :	
Retype password :	

Note: We suggest you manage your device with another "administrator level" account instead of using the default "admin" account, as it is commonly used by embedded systems. Once the new administrator level account has been created, it is suggested that the original "admin" account should be monitored for security reasons to prevent brute-force attacks.

- To improve security, the login password policy and account login failure lockout can be configured. To configure them, log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Login Password Policy.**



Login Password Policy

Account Password Policy

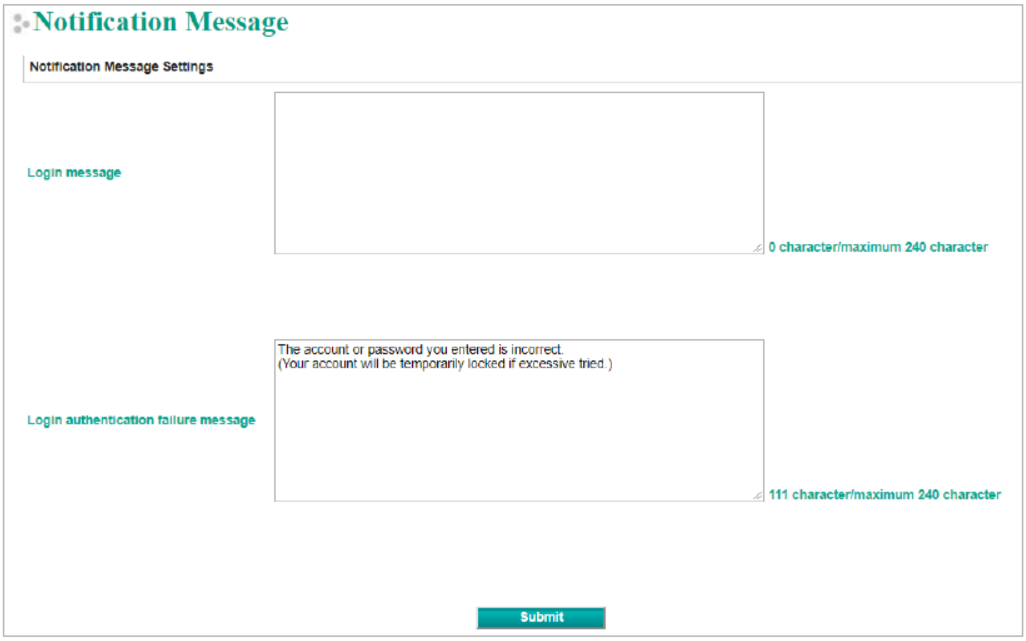
Minimum length	4	(4 ~ 16)
☑ Enable password complexity strength check		
☑ At least one digit(0~9)		
☑ Mixed upper and lower case letters(A~Z, a~z)		
☑ At least one special character: ~!@#$%^&*-_|;:,.<>[]{}()		
☑ Password lifetime	90	(90 ~ 180 days)

Account Login Failure Lockout

☑ Enable		
Retry failure threshold	5	(1 ~ 10 time)
Lockout time	5	(1 ~ 60 min)

- You should adjust the password policy to require more complex passwords. For example, set the **Minimum length** to 16, enable all password complexity strength checks, and enable the **Password lifetime** options. Also, to avoid brute-force attack, it's suggested that you enable the **Account login failure lockout** feature.

- For some system security requirements, a warning message may need to be displayed to all users attempting to log in to the device. To add a login message, log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Notification Message**, and enter a **Login Message** to use.



Notification Message

Notification Message Settings

Login message

0 character/maximum 240 character

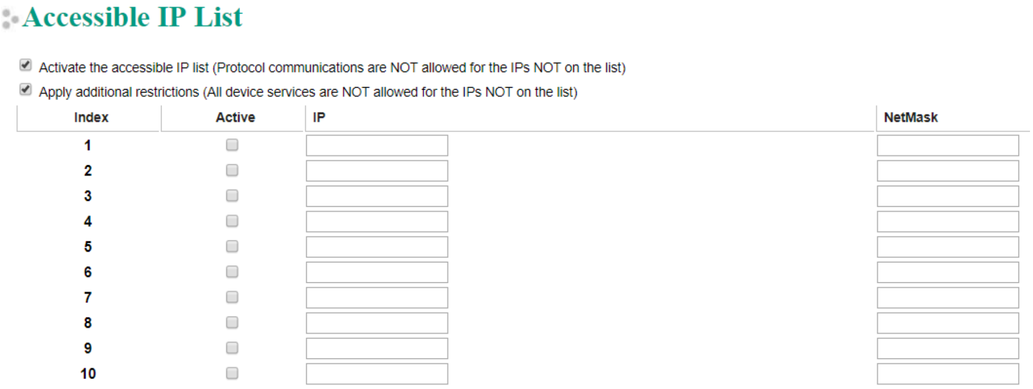
Login authentication failure message

The account or password you entered is incorrect.
(Your account will be temporarily locked if excessive tried.)

111 character/maximum 240 character

3.4. Accessible IP List

- The MGate MB3170/3270/3660/3280/3480 Series can limit access to specific remote host IP addresses to prevent unauthorized access to the gateway. If a host's IP address is in the accessible IP list, then the host will be allowed to access the MGate MB3170/3270/3660/3280/3480 Series. To configure it, log in to the HTTP/HTTPS console and select **System Management → Accessible IP List**. The different restrictions are listed in the table below (the checkbox **Apply additional restrictions** can only be activated if **Activate the accessible IP list** is activated).



Accessible IP List

☑ Activate the accessible IP list (Protocol communications are NOT allowed for the IPs NOT on the list)
☑ Apply additional restrictions (All device services are NOT allowed for the IPs NOT on the list)

Index	Active	IP	NetMask
1	□		
2	□		
3	□		
4	□		
5	□		
6	□		
7	□		
8	□		
9	□		
10	□		

Activate the accessible IP list	Apply additional restrictions	IPs on the list (Active checked)	IPs NOT on the list (Active NOT checked)
v		All protocol communication and services* are allowed.	Protocol communication is not allowed, but services* are still allowed.
v	v	All protocol communication and services* are allowed.	All services* are not allowed.

* HTTP, HTTPS, TELNET, SSL, SNMP, SMTP, DNS, NTP, DSU

- 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, then enter 255.255.255.255 for the netmask.
  - **To allow access to hosts on a specific subnet:** For both the IP address and netmask, use 0 for the last digit (e.g., "192.168.1.0" and "255.255.255.0").
  - **To allow access to all IP addresses:** Make sure that the **Enable** checkbox for the accessible IP list is not checked.

Additional configuration examples are shown in the following table:

Desired IP Range	IP Address Field	Netmask Field
Any host	Disable	Enable
192.168.1.120	192.168.1.120	255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0	255.255.255.0
192.168.1.1 to 192.168.255.254	192.168.0.0	255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0	255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128	255.255.255.128

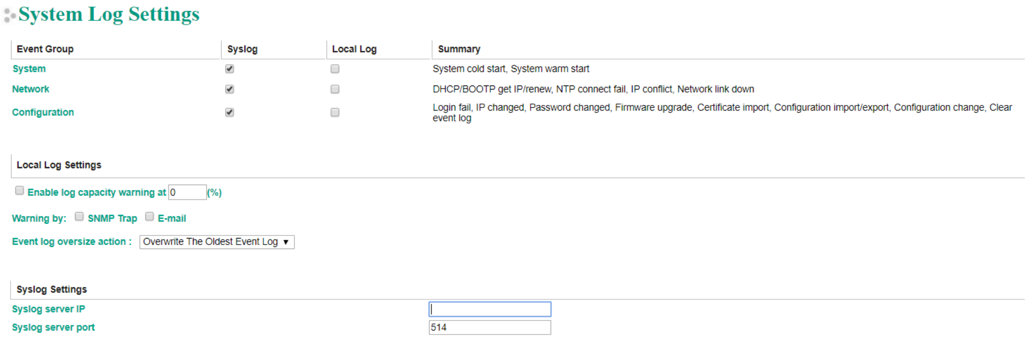
Warning Ensure that the IP address of the PC you are using to access the web console is in the Accessible IP List.

3.5. Logging and Auditing

- These are the events that will be recorded by the MGate MB3170/3270/3660/3280/3480 Series:

Event Group	Summary
System	System cold start, system warm start
Network	DHCP/BOOTP gets IP/renew, NTP connect failed, IP conflict, Network link down
Configuration	Login failed, IP changed, Password changed, Firmware upgraded, SSl Certificate imported, Configuration imported or exported, Configuration changed, Clear event logged

- To configure this setting, log in to the HTTP/HTTPS console and select **System Management → System Log Settings**. Then, enable the **Local Log** for recording on the MGate MB3170/3270/3660/3280/3480 device and/or **Syslog** for keeping records on a server. You should enable system log settings to record all important system events to monitor device status and check for security issues.



System Log Settings

Event Group	Syslog	Local Log	Summary
System	☑	□	System cold start, System warm start
Network	☑	□	DHCP/BOOTP get IP/renew, NTP connect fail, IP conflict, Network link down
Configuration	☑	□	Login fail, IP changed, Password changed, Firmware upgrade, Certificate import, Configuration import/export, Configuration change, Clear event log

Local Log Settings

□ Enable log capacity warning at 0 (%)

Warning by: □ SNMP Trap □ E-mail

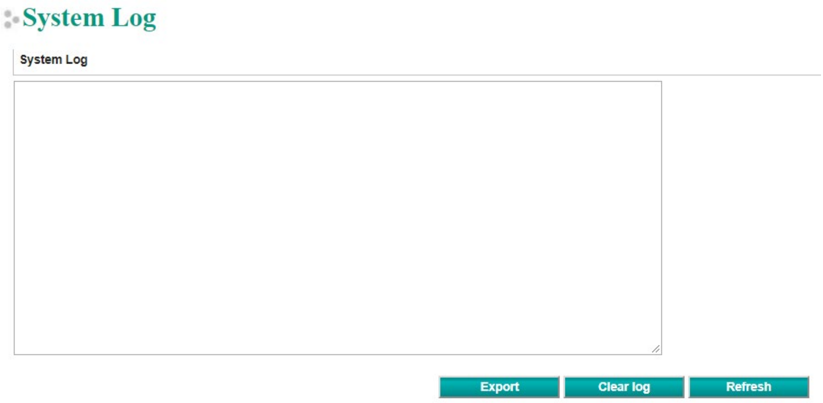
Event log oversize action : Overwrite The Oldest Event Log ▾

Syslog Settings

Syslog server IP:

Syslog server port: 514

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



4. Patching/Upgrades

4.1. Patch Management Plan

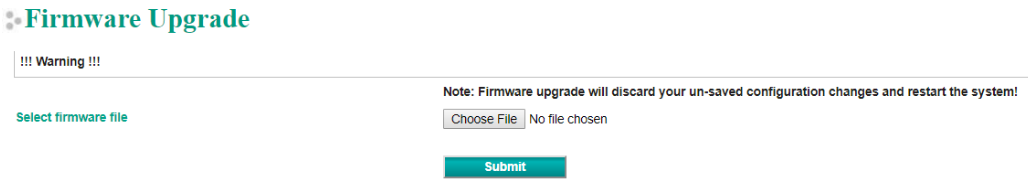
With regard to patch management, Moxa in general releases version enhancement with thorough release notes annually.

4.2. Firmware Upgrades

The process for upgrading firmware is as follows:

- Download the latest firmware for your MGate device from the Moxa website:
  - Firmware for the MGate MB3170/3270 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3170-mb3270-series#resources
  - Firmware for the MGate MB3660 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3660-series#resources
  - Firmware for the MGate MB3280/3480 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series#resources

- Log in to the HTTP/HTTPS console and select **System Management → Maintenance → Firmware Upgrade**. Click the **Choose File** button to select the proper firmware and click **Submit** to upgrade the firmware.



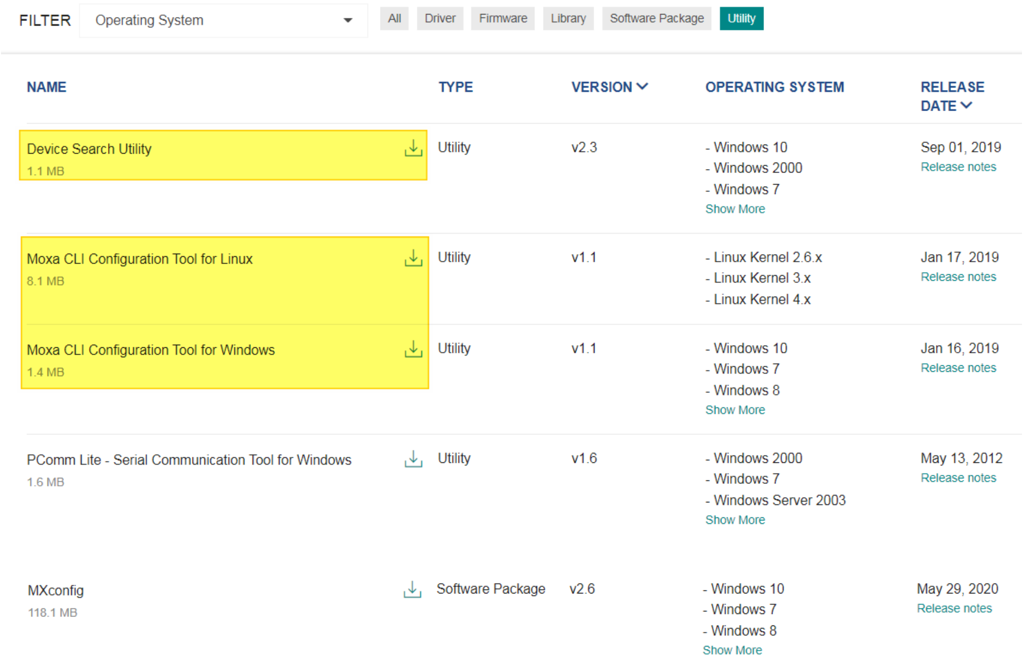
Firmware Upgrade

!!! Warning !!!

Note: Firmware upgrade will discard your un-saved configuration changes and restart the system!

Select firmware file: No file chosen

- If you want to upgrade the firmware for multiple units, download the utility Device Search Utility (DSU) or MXconfig for a GUI interface, or the Moxa CLI Configuration Tool for a CLI interface.



NAME	TYPE	VERSION	OPERATING SYSTEM	RELEASE DATE
Device Search Utility 1.1 MB	Utility	v2.3	- Windows 10 - Windows 2000 - Windows 7 Show More	Sep 01, 2019 Release notes
Moxa CLI Configuration Tool for Linux 8.1 MB	Utility	v1.1	- Linux Kernel 2.6.x - Linux Kernel 3.x - Linux Kernel 4.x	Jan 17, 2019 Release notes
Moxa CLI Configuration Tool for Windows 1.4 MB	Utility	v1.1	- Windows 10 - Windows 7 - Windows 8 Show More	Jan 16, 2019 Release notes
PComm Lite - Serial Communication Tool for Windows 1.6 MB	Utility	v1.6	- Windows 2000 - Windows 7 - Windows Server 2003 Show More	May 13, 2012 Release notes
MXconfig 118.1 MB	Software Package	v2.6	- Windows 10 - Windows 7 - Windows 8 Show More	May 29, 2020 Release notes

5. Security Information and Vulnerability Feedback

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

You can find the latest Moxa security information here: https://www.moxa.com/en/support/product-support/security-advisory