The Security Hardening Guide for the MGate 5000 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
Fax: +886-2-8919-1231

1. Introduction

We at Moxa understand completely why more and more of our customers are concerned about the security of their network systems. Naturally, these concerns also extend to indivual devices. Moxa is committed to cybersecurity and endeavors to make our products as secure as possible. In support of our customers to meet certain security guidelines and frameworks, this document intends to provide guidelines on how to configure and secure the installation of Moxa's devices.

We want to reiterate that the recommended steps for securing a Moxa device, discussed in this document, are guidelines as applications vary from one Moxa customer to another. Furthermore, these recommendations are best practices for most applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict or affecting your application, it's highly recommended to review and test the configuration thoroughly before implementing it in your production system.

2. General System InformationBasic Information About the Device

Model	Function	Operating System	Firmware Version
MGate 5101 Series	PROFIBUS-to-Modbus TCP Gateway	Linux	Version v2.2
MGate 5102 Series	PROFIBUS-to-PROFINET Gateway	Linux	Version v2.3
MGate 5103 Series	Modbus RTU/ASCII/EtherNet/IP-to-PROFINET Gateway	Linux	Version v2.2
MGate 5105 Series	Modbus RTU/ASCII/TCP-to-EtherNet/IP Gateway	Linux	Version v4.3
MGate 5109 Series	Modbus RTU/ASCII/TCP-to-DNP3 serial/TCP Gateway	Linux	Version v2.3
MGate 5111 Series	Modbus/PROFINET/EtherNet/IP-to-PROFIBUS Gateway	Linux	Version v1.3
MGate 5114 Series	Modbus RTU/ASCII/TCP/IEC101-to-IEC104 Gateway	Linux	Version v1.3
MGate 5118 Series	CAN-J1939-to-Modbus/PROFINET/EtherNet/IP Gateway	Linux	Version v2.2
MGate W5108/W5208 Series	IEEE 802.11 a/b/g/n wireless Modbus/DNP3 Gateway	Linux	Version v2.4

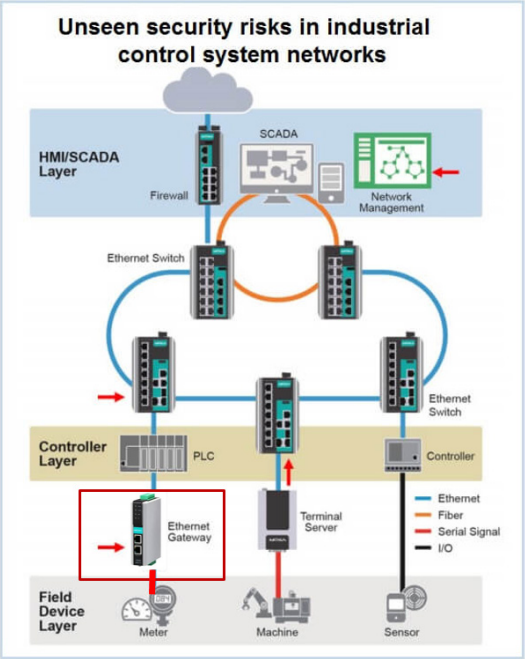
The MGate 5000 Series is a protocol gateway specifically designed to allow industrial devices to be directly accessed from a network. Thus, legacy fieldbus devices can be transformed into different protocols, which can be monitored and controlled from any network location or even the Internet.

To harden the security of this proprietary operating system, the open source HTTPS library, openSSL v1.1.1b, is also included and periodically reviewed for cybersecurity enhancement.

2.2. Deployment of the Device

It is suggested to deploy the MGate 5000 Series behind a security firewall network that has sufficient security features in place and ensures that networks are safe from internal and external threats.

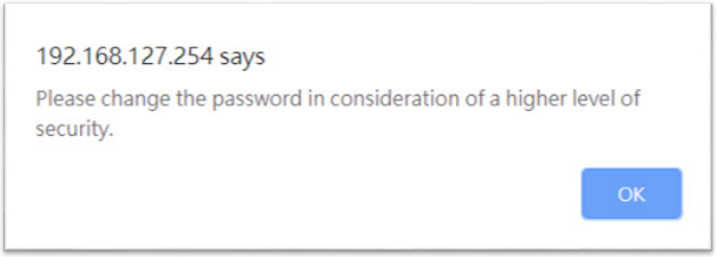
Make sure that the physical protection of the MGate devices and/or the system fulfill the requirements of basic risk management. Depending on the environment and the threat situation, the form of protection can vary significantly.



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. A screenshot of the GUI for the web console is shown below.



3.1. TCP/UDP Port Status

Please refer to the table below for all the ports, protocols, and services that are used to communicate between the MGate 5000 Series and other devices.

Service Name	Option	Default Settings	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	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
EtherNet/IP	Enable/Disable	Enable	TCP, UDP	2222, 44818	2222 for EtherNet/IP implicit messaging 44818 for EtherNet/IP explicit messaging
PROFINET	Enable/Disable	Enable	UDP	34963	34963 for PROFINET protocol communication
DNP3	Enable/Disable	Enable	TCP, UDP	20000	20000 for DNP3 protocol communication
IEC-104	Enable/Disable	Enable	TCP	2404	2404 for IEC-104 protocol communication

For security reasons, you can consider disabling unused services and using a higher security level of services for data communication. Please refer to the table below for the suggested settings.

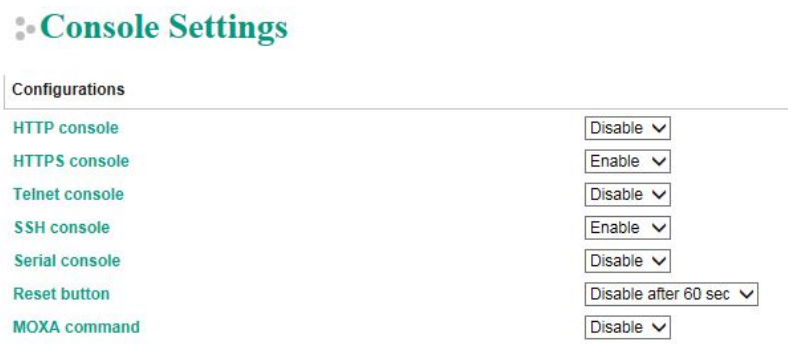
Service Name	**Suggested Settings**	**Type**	**Port Number**	**Security Remark**
DSCI (Moxa Command)	**Disable**	TCP	4900	Disable service that is not commonly used
		UDP	4800	
DNS client	**Disable**	UDP	53	Disable service that is not commonly used
SNMP agent	**Disable**	UDP	161	Suggest to manage the MGate via HTTPS console
HTTP server	**Disable**	TCP	80	Disable service for HTTP from plain text transmission
HTTPS server	**Enable**	TCP	443	Encrypted data channel with trusted certificate for the MGate configuration
Telnet server	**Disable**	TCP	23	Disable service that is not commonly used

DHCP client	**Disable**	UDP	68	Suggested to assign a system IP in static manner
Syslog client	**Enable**	UDP	514	The MGate in the syslog client role sends important system for a diagnosis of the MGate's status
Email client	**Enable**	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 service that is not commonly used
Modbus TCP client/server	**Enable**	TCP	502, 7502	Suggested to add communicating Modbus devices' IP address to the "Accessible IP list".
EtherNet/IP	**Enable**	TCP, UDP	2222, 44818	2222 for EtherNet/IP implicit messaging; 44818 for EtherNet/IP explicit messaging
PROFINET	**Enable**	UDP	34963	34963 for PROFINET protocol communication
DNP3	**Enable**	TCP, UDP	20000	20000 for DNP3 protocol communication
IEC-104	**Enable**	TCP	2404	2404 for IEC-104 protocol communication

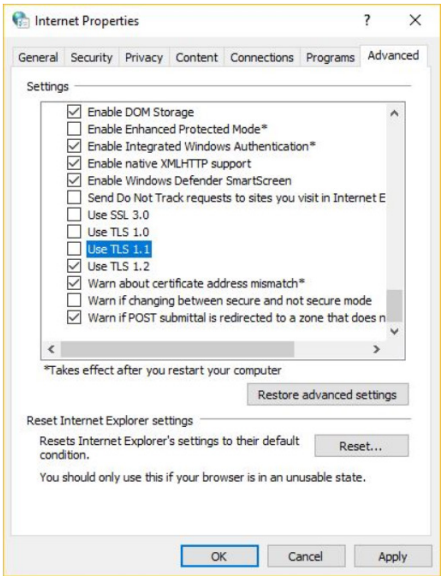
- For the console services

HTTP	Disable
HTTPS	Enable
Telnet	Disable
Moxa Command	Disable

Log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Console Settings**. Then, you can select to enable or disable services as suggested. A screenshot of the GUI for the web console is shown below.



HTTPS is an encrypted communication channel. The encryption algorithm, which is lower than TLS v1.1, has severe vulnerabilities that can easily be hacked. Therefore, the design of the MGate is TLS v1.2 or above. So, please make sure to check TLS v1.2 in your browser.



In order to use HTTPS console without a certificate warning shown by web browsers, you need to import the trusted certificate issued by a third-party certificate authority. The web browsers would validate the certificate in the HTTPS connection initialization stage and determine if the certificate from the MGate 5000 Series server could be considered as trustworthy or not.

Log in to the HTTP/HTTPS console and select **System Management → Certificate**. Users can regenerate the up-to-date valid certificate through importing third-party trusted SSL certificate or regenerating the "MGate self-signed" certificate.

Behavior of the SSL certificate on the MGate device

The MGate Series devices generate the SSL self-signed private keys automatically. Since the certificate is automatically generated, making it convenient for the device user, it shows some security loopholes.

- The MGate 5000 Series auto-generates a self-signed SSL certificate. It is recommended to use SSL certificates that are either certified by a trusted third-party Certificate Authority (CA) or by an organization's CA. You may import the certificate to MGate 5000 devices when you have received them.
- The length of the MGate device's self-signed private keys is 1,024 bits. It should be feasible to most of the applications; some applications prefer a longer key, such as 2,048 bits, which is considered to import the third-party authorized certificate. Please note that the longer the key of certificate is that you implement, the longer time it takes to browse the web console due to the encryption or decryption of the communicated data.

For the MGate self-signed certificate:

When we encounter the valid date of the certificate expired, we can regenerate the "MGate self-signed" certificate with the following steps.

- Step1. Users should **Delete** the SSL certificate file originated from the MGate device.
- Step2. Then, **Enable** the NTP server by setting up the time zone and local time.
- Step3. After restarting the device, the "MGate self-signed" certificate will be regenerated with the updated valid time.

For importing a third-party trusted SSL certificate:

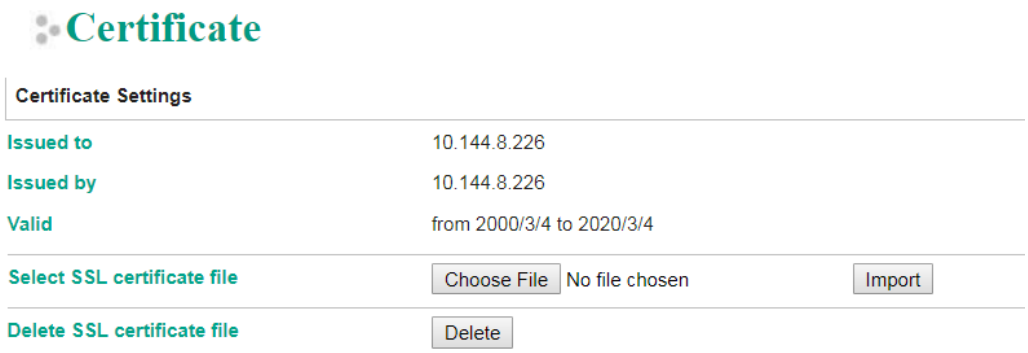
By importing the third-party trusted SSL certificate, the security level can be enhanced. A screenshot of the GUI for the web console is shown below. To generate the SSL certificate through the third party, follow these steps:

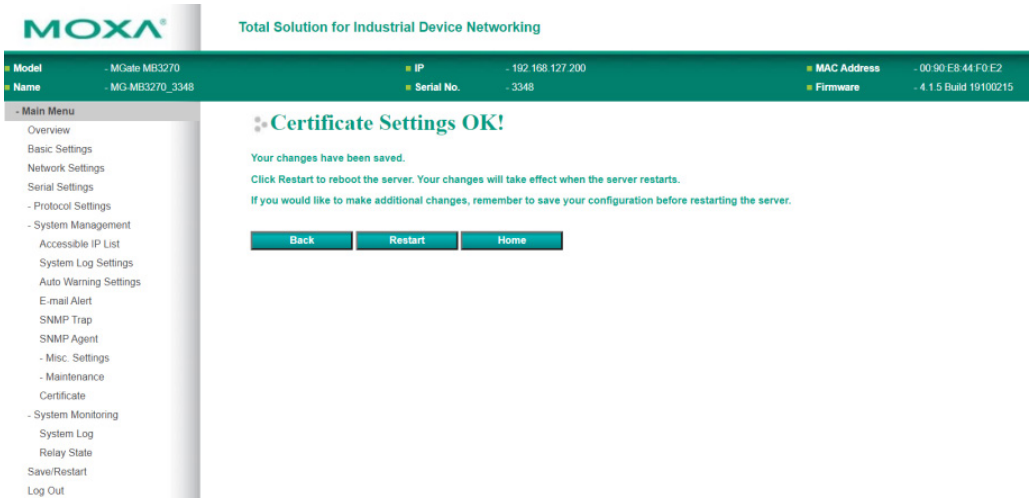
- Step1. Create a certification authority (Root CA), such as Microsoft AD Certificate Service (https://mizitechinfo.wordpress.com/2014/07/19/step-by-step-installing-certificate-authority-on-windows-server-2012-r2/)
- Step 2. Find a tool to issue a "Certificate Signing Requests" file, where you can find it from the third-party CA companies, such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).
- Step3. Submit it to a public certification authority for signing the certificate.
- Step4. Import the certificate to the MGate Series. Please note that the MGate Series only accepts "xxxx.**pem**" format.

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

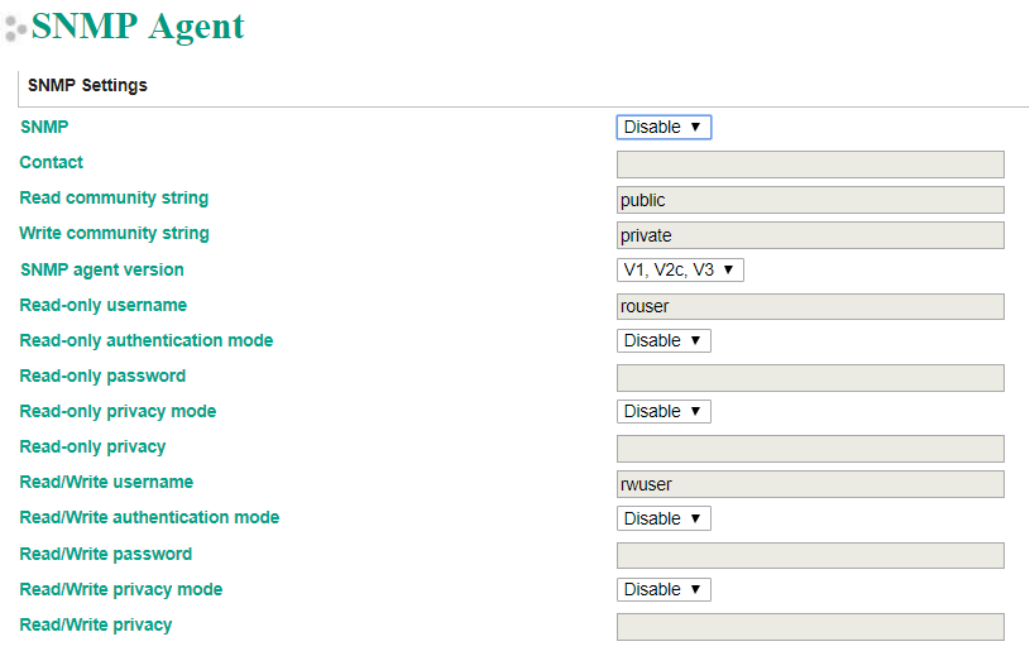
Some well-known third-party CA (Certificate Authority) companies are listed below for your reference (https://en.wikipedia.org/wiki/Certificate_authority):

- 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/)





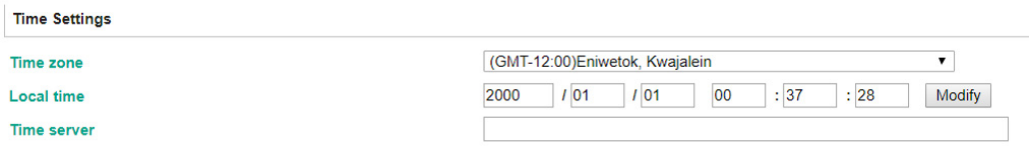
- For the SNMP agent service, log in to the HTTP/HTTPS console and select **System Management → SNMP Agent**. Then, select **Disable** for the SNMP agent service. A screenshot of the GUI for the web console is shown below.



- For the NTP service.

NTP	Disable

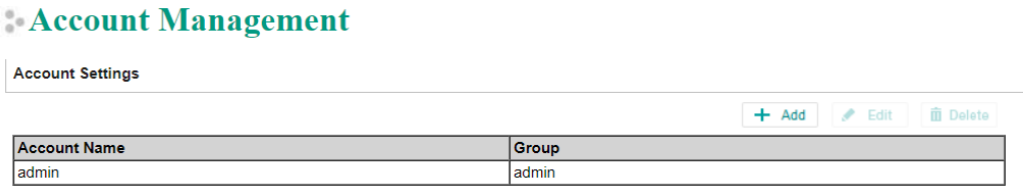
While entering the HTTP/HTTPS console, select **Basic Settings** and keep the **Time server** setting empty (which is meant to disable NTP service). A screenshot of the GUI for the web console is shown below.



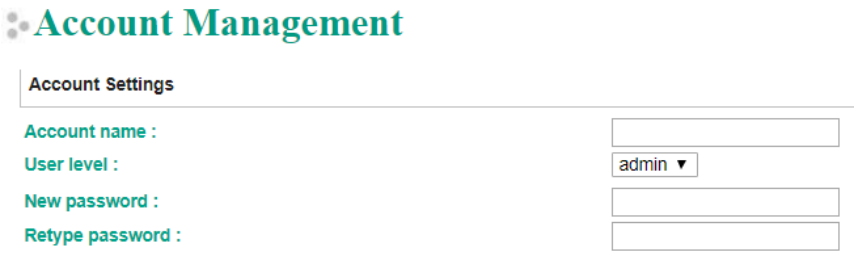
Note: For every instruction above, click the **Submit** button in order to save all the settings you have done. Then restart the MGate 5000 Series to make the new settings effective.

3.2. Account Management

- The MGate 5000 Series provides two different user levels: admin and user with a maximum of 16 accounts. The admin account accesses and modifies all the settings through the web console. The user account only views the settings and cannot change anything.
- By default, the administration account, admin, is generated with the password **moxa**. To execute the account management, please log in to the web console, select **System Management → Misc. Settings → Account Management**. In order to change the password of the existing account, please double-click the assigned account. You will then enter the webpage to change the password (at least 4 characters by default). A screenshot of the GUI for the web console is shown below.



- To add a new account, please log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Account Management**. By clicking the **Add** button, the account settings interface will be shown for configuration. Fill in the **Account name, User level, New password,** and **Retype password** to generate a new account. A screenshot of the GUI for the web console is shown below.

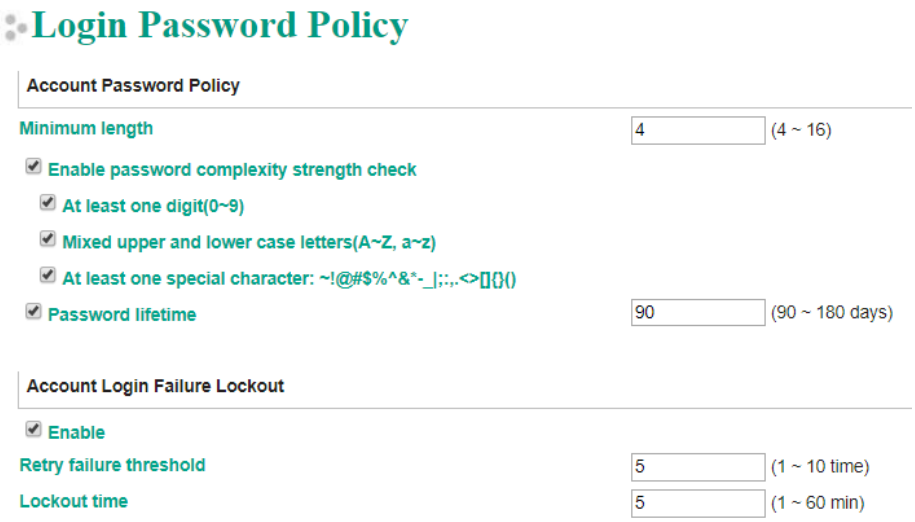


Note: It is suggested to manage MGate 5000 Series in another "administration level" account instead of using the default "admin" account, as it is commonly used by embedded systems. Once the new administration level account has been created, it is suggested that the original "admin" account should be monitored for security reasons to avoid a brute-force attack.

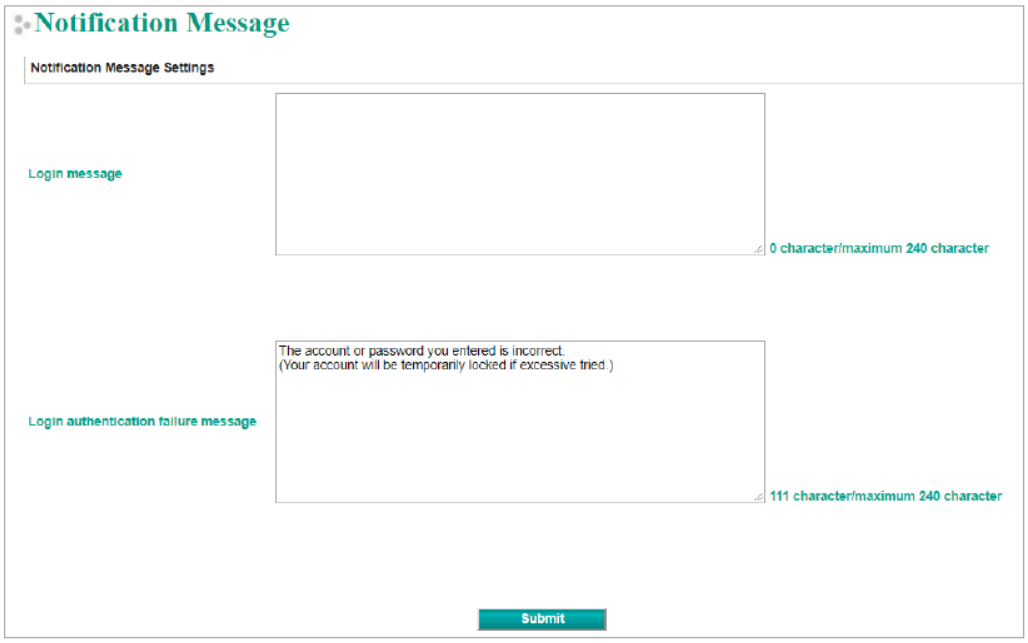
Considering security levels, the login password policy and failure lockout can be configured. To configure it, please log in to the HTTP/HTTPS console and select **System Management → Misc. Settings → Login Password Policy**. Not only can the **Account Password Policy** be configured, but the **Account Login Failure Lockout** can be further enabled to increase the security level of the account management.

It is suggested to set the password policy at a higher complexity. For example, set the **Minimum length** to 16; enable all password complexity strength checks; and enable the **Password lifetime** checking mechanism. Also, to avoid a brute-force attack, it's suggested that you enable the **Account login failure lockout** feature.

A screenshot of the GUI for the web console is shown below.

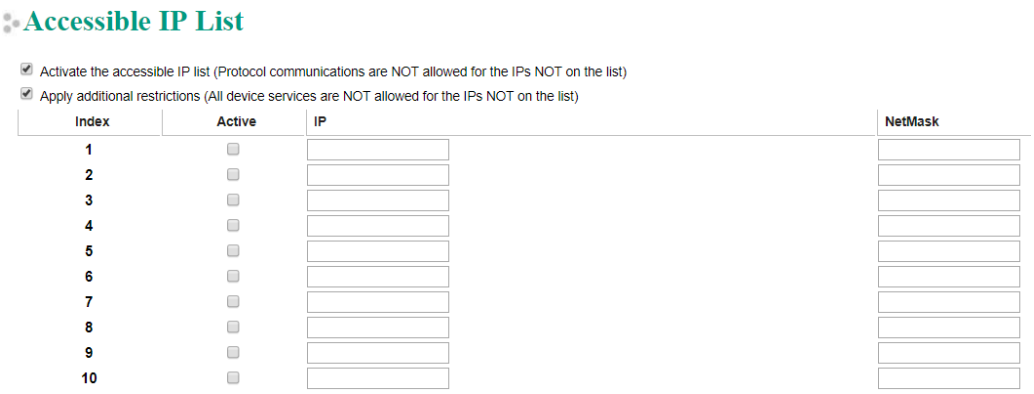


- For some system security requirements, it is needed to display an approved warning banner to all users attempting to access the device. In addition to the warning banner, please log in to the HTTP/HTTPS console, and select **System Management → Misc. Settings → Notification Message**. You can type in the warning message in the **Login Message** at all access points.



3.3. Accessible IP List

- The MGate 5000 Series has a feature that can add or block remote host IP addresses to prevent unauthorized access to the gateway. So if a host's IP address is in the accessible IP table, then the host will be allowed to access the MGate 5000 Series. To configure it, please 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). A screenshot of the GUI for the web console is shown below.



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.

* Indicate 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; 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 **Enable** 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

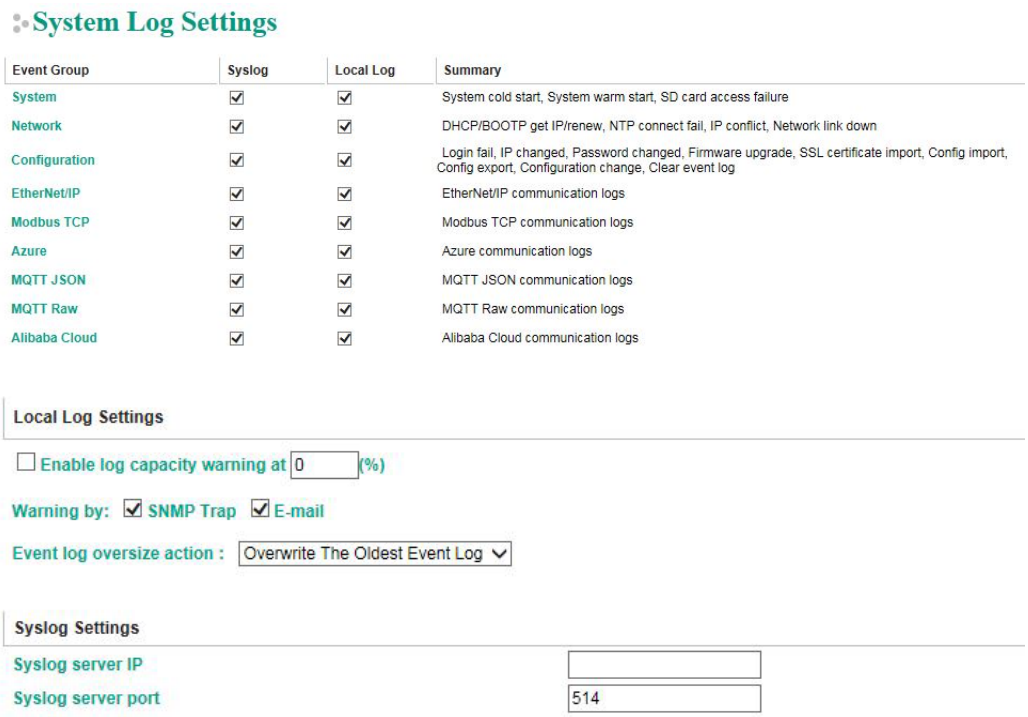
Warning Ensure the communication peer is listed in the Accessible IP List for entering the web console.

3.4. Logging and Auditing

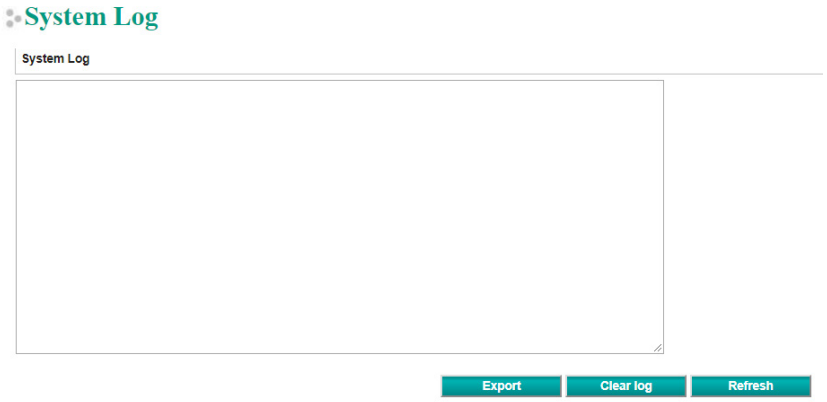
- Please refer to the table below for all the events that will be recorded by the MGate 5000 Series. The SD card access failure event and protocols event vary in the different MGate 5000 models.

Event Group	Summary
System	System cold start, system warm start, SD card access failure
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/exported, Configuration changed, Clear event log
Protocol	Protocols communication logs

- 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 5000 device and/or **Syslog** for keeping records of the network on a server. It is suggested to enable system log settings to record all important system events to monitor any security issue with the device status.



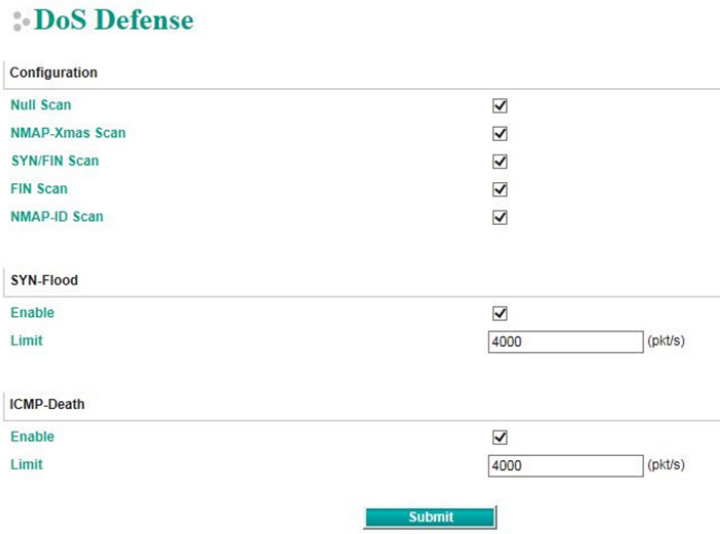
- To review above events, log in to the HTTP/HTTPS console and select **System Monitoring → System Log**. A screenshot of the GUI for the web console is shown below.



3.5. DoS Defense

Users can select from several options to enable DoS Defense in order to fend off cybersecurity attacks. A denial-of-service (DoS) attack is an attempt to make a machine or a network resource unavailable.

Users can select from the following options to counter DoS attacks:



4. Patching/Upgrades

4.1. Patch Management Plan

With regard to patch management, Moxa in general releases version enhancement with thorough release notes annually. If any security vulnerability issue is identified, Moxa will release a beta fix within 30 days.

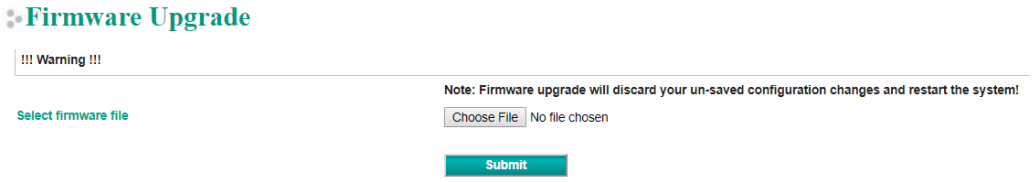
4.2. Firmware Upgrades

The process of firmware and/or software upgrade is instructed as below.

- We will release the latest firmware and software along with its released notes on our official website. The links below are listed for specified items of the MGate 5000 Series.
  - Firmware for the MGate 5101 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5101-pbm-mn-series#resources
  - Firmware for the MGate 5102 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/profinet-gateways/mgate-5102-pbm-pn-series
  - Firmware for the MGate 5103 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5103-series#resources
  - Firmware for the MGate 5105 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5105-mb-eip-series#resources
  - Firmware for the MGate 5109 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5109-series#resources
  - Firmware for the MGate 5111 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5111-series#resources
  - Firmware for the MGate 5114 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5114-series#resources

- Firmware for the MGate 5118 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5118-series#resources
- Firmware for the MGate W5108/W5208 Series: https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-w5108-w5208-series#resources

- If a user wants to upgrade the firmware of the MGate 5000 Series, then please download the firmware from website first. Log in to 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.



- If a user wants to upgrade the firmware for multiple units, then please download the utility Device Search Utility (DSU) or MXconfig for a GUI interface, or the Moxa CLI Configuration Tool for a CLI interface to do mass deployment.

FILTER Operating System All Driver Firmware Library Software Package Utility

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 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 below linkage:

https://www.moxa.com/en/support/product-support/security-advisory