The Security Hardening Guide for the MGate 5000 Series

Moxa Technical Support Team

support@moxa.com

Contents

1 Introduction 2
2 General System Information 2
2.1 Basic Information About the Device 2
2.2 Deployment of the Device 4
2.3 Security Threats and Measures 5
3 Configuration and Hardening Information 7
3.1 TCP/UDP Ports and Recommended Services 8
3.2 Serial Ports and Recommended Services 15
3.3 HTTPS and SSL Certificates 16
3.3.1 Behavior of the SSL Certificate on an MGate Device 17
3.3.2 MGate Self-signed Certificate 17
3.3.3 Importing a Third-party Trusted SSL Certificate 17
3.4 Account Management 19
3.5 Accessible IP List 23
3.6 Logging and Auditing 25
3.7 DoS Defense 28
4 Patching/Upgrades 28
4.1 Patch Management Plan 28
4.2 Firmware Upgrades 28
4.3 Firmware Integrity Verification (User Responsibility) 31
5 Testing the Security Environment 32
6 Decommissioning Suggestion 33
7 Security Information and Vulnerability Feedback 33

 Released on Sep 14, 2026

About Moxa

Moxa is a leading provider of edge connectivity, industrial computing, and network infrastructure solutions for enabling connectivity for the Industrial Internet of Things. With 35 years of industry experience, Moxa has connected more than 82 million devices worldwide and has a distribution and service network that reaches customers in more than 80 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for industrial communications infrastructures. Information about Moxa's solutions is available at www.moxa.com.

1 Introduction

This document provides guidelines on how to configure and secure the MGate 5000 Series. Consider the recommended steps in this document as best practices for security in most applications. We recommend that you thoroughly review and test the configurations before implementing them in your production system to ensure your application remains unaffected. Also, maintain the security settings regularly to ensure that the configurations meet your security requirements.

2 General System Information

2.1 Basic Information About the Device

Model	Function	Operating System	Firmware Version
MGate 5101 Series	PROFIBUS-to-Modbus TCP Gateway	Linux	v2.5
MGate 5102 Series	PROFIBUS-to-PROFINET Gateway	Linux	v2.6
MGate 5103 Series	Modbus RTU/ASCII/EtherNet/ IP-to-PROFINET Gateway	Linux	v2.5
MGate 5105 Series	Modbus RTU/ASCII/TCP-to-EtherNet/IP Gateway	Linux	v4.6
MGate 5109 Series	Modbus RTU/ASCII/TCP-to-DNP3 serial/TCP Gateway	Linux	v2.6
MGate 5111 Series	Modbus/PROFINET/EtherNet/ IP-to-PROFIBUS Gateway	Linux	v2.2
MGate 5114 Series	Modbus RTU/ASCII/TCP/ IEC101-to-IEC104 Gateway	Linux	v1.6
MGate 5118 Series	CAN-J1939-to-Modbus/ PROFINET/EtherNet/IP Gateway	Linux	v2.5
MGate 5119 Series	DNP3/IEC 101/IEC 104/Modbus-to-IEC 61850 Gateway	Linux	v1.2
MGate 5216 Series	Serial/Modbus-to-EtherCAT gateway	Linux	v1.0
MGate 5217 Series	Modbus-to-BACnet/IP gateway	Moxa Operating System	v1.2
MGate 5121 Series	CANopen/J1939-to-Modbus TCP Gateway	Linux	v2.0
MGate 5122 Series	CANopen/J1939-to-EtherNet/IP Gateway	Linux	v2.0
MGate 5123 Series	CANopen/J1939-to-PROFINET Gateway	Linux	v2.0

Model	Function	Operating System	Firmware Version
MGate 5134 Series	Modbus RTU/ASCII/TCP-to-PROFINET Gateway	Linux	v1.3
MGate 5135/5435 Series	Modbus RTU/ASCII/TCP-to-EtherNet/IP Gateway	Linux	v1.3
MGate 5242/5442 Series	Serial/Modbus-to-EtherCAT gateway	Linux	v1.0
MGate 5192 Series	IEC 61850-to-DNP3/IEC 101/ IEC 104/Modbus Gateway	Linux	v1.0

The MGate 5000 Series protocol gateways allow direct network access for industrial devices. 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 the operating system, the following open-source HTTPS libraries are included and undergo regular cybersecurity enhancement reviews.

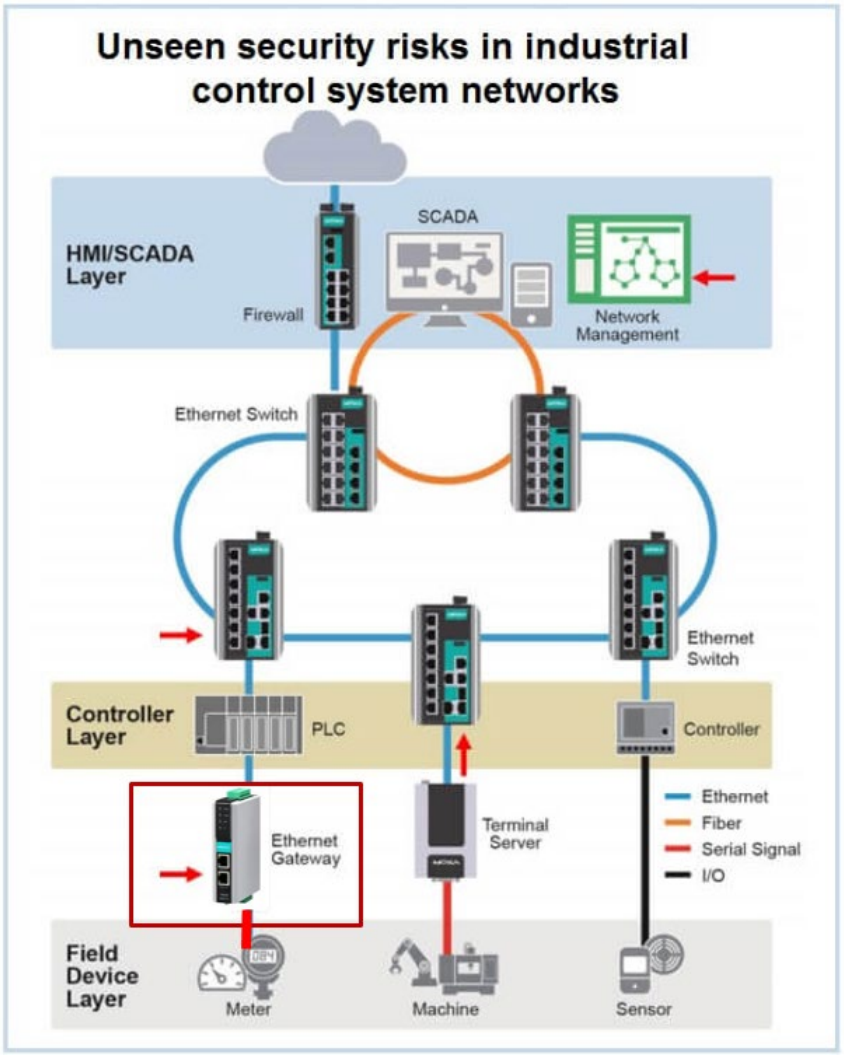
- **Linux models:**
  - For the MGate 5101/5102/5103/5105/5109/5111/5114/5118/5119 Series: openSSL v1.1.1za
  - For the MGate 5121/5122/5123/5134/5135/5435/5192 Series: openSSL v1.1.1n
  - For the MGate 5242/5442 Series: openSSL v1.1.1w
- **Moxa Operating System models:** mbed TLS v2.28.8

2.2 Deployment of the Device

Deploy the MGate 5000 Series behind a secure firewall or/and IDS/IPS network that has sufficient security features in place to ensure continuous protection from internal and external threats.

Customers who buy products from Moxa or a reseller should be aware that Moxa might have already launched a newer firmware version with enhanced security features. Check Moxa's support website for newer firmware. If so, we recommend upgrading the firmware to the newest version.

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.



2.3 Security Threats and Measures

The security threats that can harm MGate 5000 Series are:

Threat 1: Attacks over the network

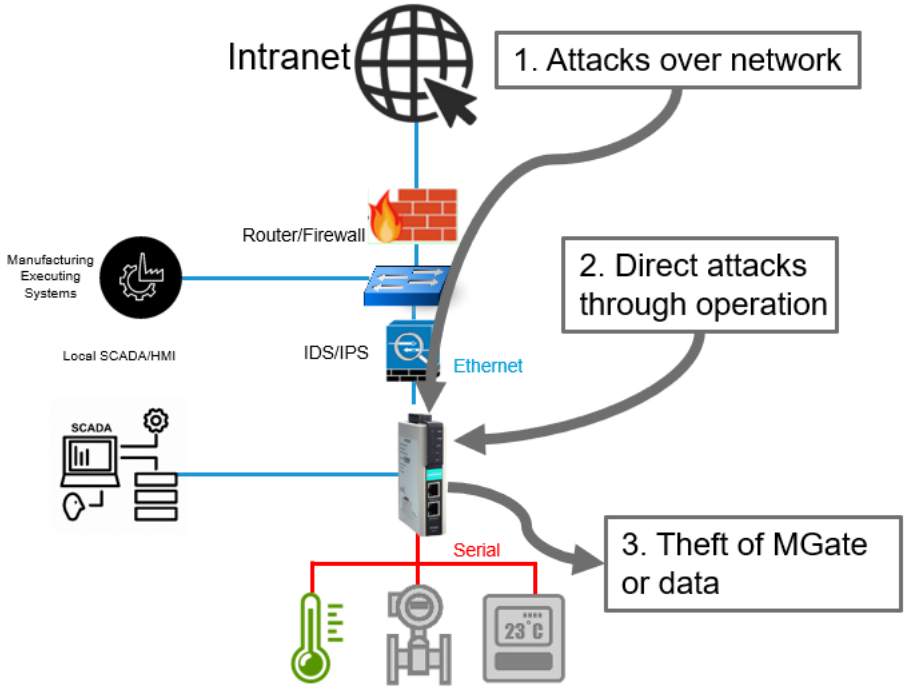
Threats from individuals with no rights to the MGate 5000 Series via networks such as intranets.

Threat 2: Direct attacks through operation

Threats where individuals with no rights to the MGate 5000 Series directly operate a device to affect the system and steal important data.

Threat 3: Theft of the MGate or data

Someone steals MGate 5000 Series devices or data and analyzes the important data.



To protect against security threats, we implemented a secure network environment and defined security measures for the MGate 5000 Series. This table shows which security measures address specific threats.

To protect the MGate and its data from theft, we advise using the MGate 5000 Series on a secure local network, as noted earlier. We recommend enabling the Accessible IP List (see chapter 3.5) and Secure Connection (see chapter 3.1) functions to restrict access and encrypt data.

Security Layer	Security Measure	Threat Mitigated/Handled				Responsibility
		Description	Threat 1	Threat 2	Threat 3	
Policy and Procedure	Establish policies and procedures to guide employees in their roles and responsibilities for the safe use of security-sensitive assets.	Vulnerabilities created because of employees' lack of security policies and awareness of procedures	Yes	Yes	Yes	Asset owner
Perimeter Security	Physical security	Physical modification, manipulation, theft, removal, or destruction of an asset	No	Yes	Yes	Asset owner
Network Security	Network firewall	Unauthorized and malicious communication from an untrusted network	Yes	No	No	Asset owner
	Network IDS/IPS/ Switch with loop protection	Network attacks from various sources, such as port scanning, DDoS, loop DoS, etc.	Yes	No	No	Asset owner
	VPN	Man-in-the-middle attacks for configuration and protocol communication	Yes	No	No	Asset owner
Device Security	Account management	Unauthorized operation of the MGate	Yes	Yes	No	Provided by the MGate
	Service management	Potential cyberattacks	Yes	No	No	
	Allowlist	Unauthorized operation of the MGate	Yes	Yes	No	
	DoS Defense*	Network attacks from various sources, such as DDoS attacks	Yes	No	No	
	Login ppolicy	Trial-and-error attack attempting to crack login credentials or unauthorized operation of the device	Yes	Yes	No	
	Certificate mnagement	Data read could be spoofed	Yes	Yes	No	
	Secure boot**	Tampering with the bootloader, OS kernel, and rootFS	Yes	Yes	No	
	Event log	Deny access, operation ofthe device	Yes	Yes	No	

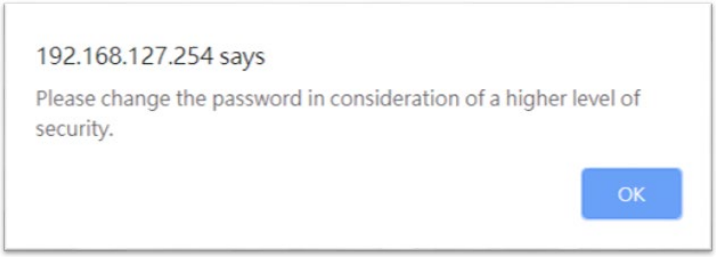
* DoS Defense features refer to Chapter 3.7 and notice that the MGate only provides basic features for defense-in-depth, not network firewall/ID/IPS devices.

** Secure boot only for MGate 5121/5122/5123/5134/5135/5435/5192.

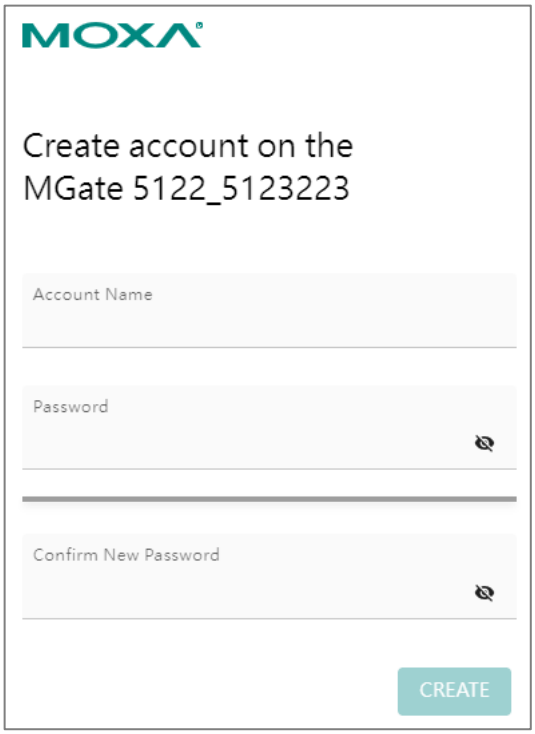
3 Configuration and Hardening Information

For security reasons, account and password protection are 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. When logging in successfully, a pop-up notification will prompt you to change your password for enhanced security.



For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, create your administration account and password when you log in the first time.



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 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
EtherCAT	Enable/ Disable	Enable	TCP	34980	34980 for EtherCAT protocol communication
DNP3	Enable/ Disable	Enable	TCP, UDP	20000	20000 for DNP3 protocol communication

Service Name	Option	Default Settings	Type	Port Number	Description
IEC-104	Enable/ Disable	Enable	TCP	2404	2404 for IEC-104 protocol communication
BACnet/IP	Enable/ Disable	Enable	UDP	47808	47808 for BACnet/IP protocol communication
IEC 61850	Enable/ Disable	Enable	TCP	102, 3782, 10043	102 for IEC 61850 protocol communication 3782 for secured IEC 61850 protocol communication 10043 for secure IEC 61850 SDK communication

The following are for the MGate 5121/5122/5123/5134/5135/5435/5192 Series:

Service Name	Option	Default Settings	Type	Port Number	Description
HTTP server	Enable/ Disable	Disable	TCP	80	Redirect to HTTPS
HTTPS server	Enable/ Disable	Enable	TCP	443	Secure web console
SDSCI	Enable/ Disable	Enable	TCP	23	For Moxa utility communication
			UDP	29168	For secure Moxa utility search function
DNS client	Enable/ Disable	Disable	UDP	53	Processing DNS and WINS (Client) data
SNMP agent	Enable/ Disable	Disable	UDP	161	SNMP handling routine
SNMP trap client	Enable/ Disable	Disable	UDP	162	Sending system/config event notifications
DHCP client	Enable/ Disable	Disable	UDP	68	DHCP client to acquire the system's IP address from the server
Syslog client	Enable/ Disable	Disable	UDP	514	Sending system logs to a remote syslog server
			TCP (TLS)	user cfg.	
Email client	Enable/ Disable	Disable	TCP	25	Sending system/config event notifications
			TLS	465	
			STAR TTLS	485	
NTP client	Enable/ Disable	Disable	UDP	123	Network Time Protocol to synchronize system time from the server
Modbus TCP server	N/A	Enable	TCP	502	502 for Modbus communication

Service Name	Option	Default Settings	Type	Port Number	Description
EtherNet/IP adapter	N/A	Enable	TCP	44818	44818 for EtherNet/IP explicit messaging
			UDP	2222	2222 for EtherNet/IP implicit messaging
PROFINET IO device	N/A	Enable	UDP	34963	34963 for PROFINET protocol communication
EtherCAT SubDevice	N/A	Enable	TCP	34980	34980 for EtherCAT protocol communication

For security reasons, 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 a 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**	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”
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
EtherCAT	**Enable**	TCP	34980	34980 for EtherCAT protocol communication

Service Name	Suggested Setting	Type	Port Number	Security Remark
DNP3	**Enable**	TCP, UDP	20000	20000 for DNP3 protocol communication
IEC-104	**Enable**	TCP	2404	2404 for IEC-104 protocol communication
BACnet/IP	**Enable**	UDP	47808	47808 for BACnet/IP protocol communication
IEC 61850	**Enable**	TCP	102, 3782, 10043	102 for IEC 61850 protocol communication 3782 for secured IEC 61850 protocol communication 10043 for secure IEC 61850 SDK communication

The following are for the MGate 5121/5122/5123/5134/5135/5435/5192 Series:

Service Name	Suggested Setting	Type	Port Number	Security Remark
HTTP server	**Disable**	TCP	80	Redirect to HTTPS
HTTPS server	**Enable**	TCP	443	Secure web console
SDSCI	**Enable**	TCP	443	For Moxa utility communication
		UDP	29168	For secure Moxa utility search function
DNS client	**Disable**	UDP	53	Processing DNS and WINS (Client) data
SNMP agent	**Disable**	UDP	161	SNMP handling routine
SNMP trap client	**Enable**	UDP	162	Sending system/config event notifications
DHCP client	**Disable**	UDP	68	DHCP client to acquire the system's IP address from the server
Syslog client	**Enable**	UDP	514	Sending system logs to a remote syslog server
		TCP (TLS)	user cfg.	
Email client	**Enable**	TCP	25	Sending system/config event notifications
		TLS	465	
		STARTTLS	485	
NTP client	**Disable**	UDP	123	Network Time Protocol to synchronize system time from a server
Modbus TCP server	**Enable**	TCP	502	502 for Modbus communication
EtherNet/IP adapter	**Enable**	TCP	44818	44818 for EtherNet/IP explicit messaging
		UDP	2222	2222 for EtherNet/IP implicit messaging

Service Name	Suggested Setting	Type	Port Number	Security Remark
PROFINET IO device	**Enable**	UDP	34963	34963 for PROFINET protocol communication
EtherCAT SubDevice	**Enable**	TCP	34980	34980 for EtherCAT protocol communication

For console services, we recommend:

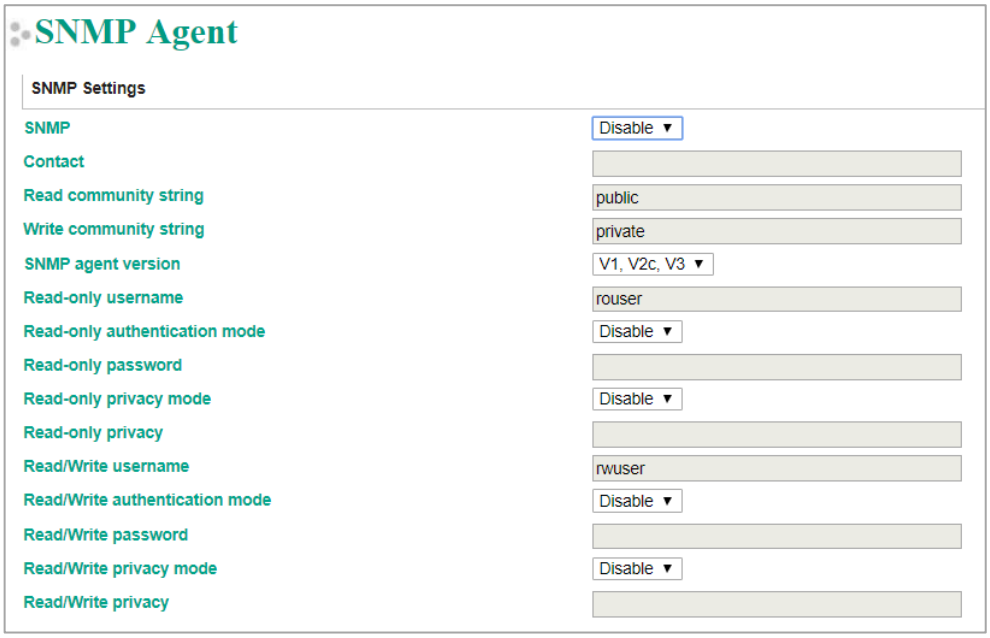
HTTP	**Disable**
HTTPS	**Enable**
Telnet	**Disable**
Moxa Command (Note: Since the search function uses the Moxa command via UDP, consider executing this action behind a firewall with a VPN.)	**Disable**

The following are for the MGate 5121/5122/5123/5134/5135/5435/5192 Series:

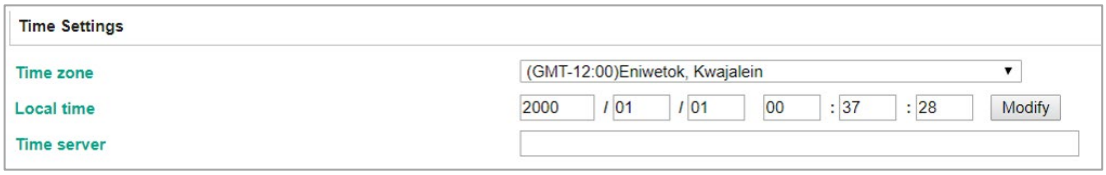
HTTP	**Disable**
HTTPS	**Enable**
SDSCI (Note: Since the search function uses SDSCI via UDP, consider executing this action behind a firewall with a VPN.)	**Enable**

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

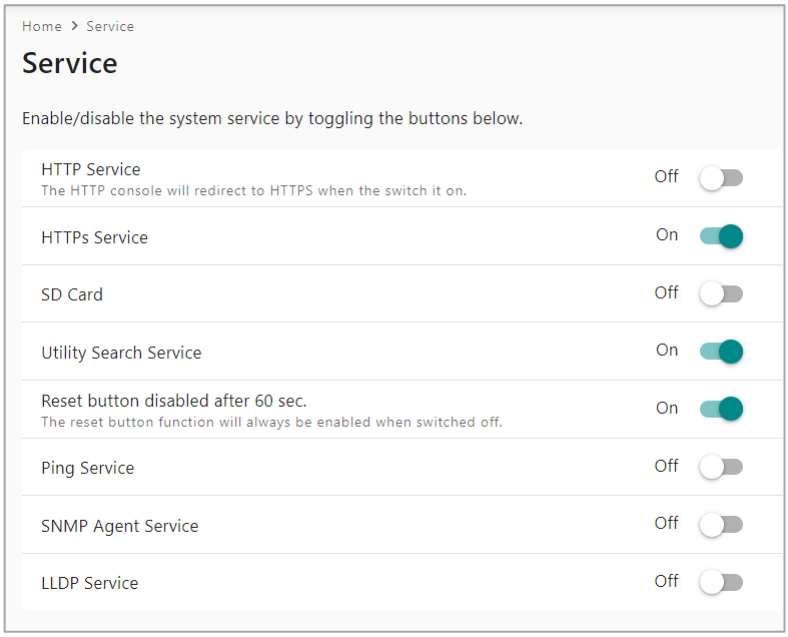
To disable the SNMP agent service, log in to the HTTP/HTTPS console and select **System Management > SNMP Agent**, then select **Disable** for SNMP.



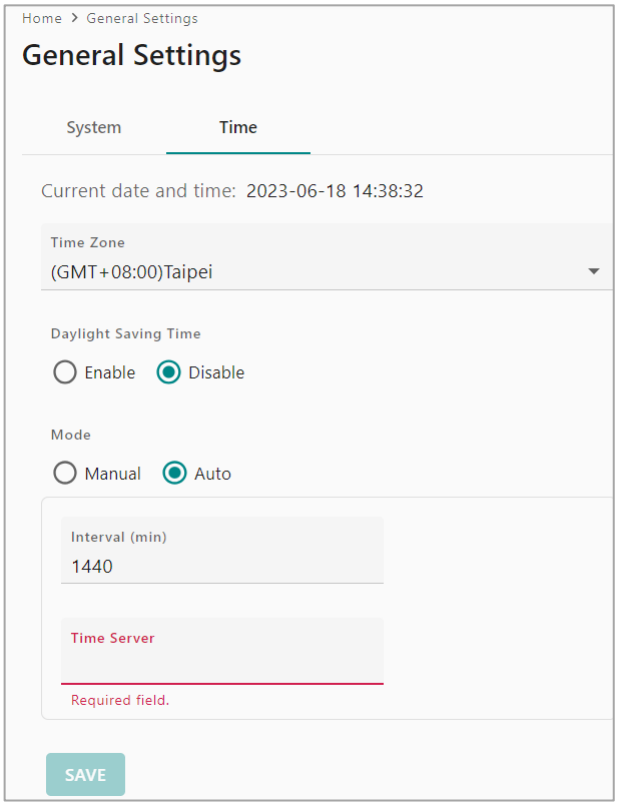
To disable the NTP service, log in to the HTTP/HTTPS console, select **Basic Settings**, and keep the **Time server** setting empty. This will disable the NTP service.



For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, to enable or disable services, log in to the HTTPS console and select **SECURITY > Service**.



To disable the NTP service, log in to the HTTPS console, select **SYSTEM SETTINGS > General Settings > Time**, and keep the Time server setting empty.



3.2 Serial Ports and Recommended Services

Refer to the table below for all serial protocols that are used to communicate between the MGate 5000 Series and other devices.

Service Name	Option	Default Settings	Type	Description
Modbus RTU/ASCII	N/A	Enable	RS-232/422/485	Modbus serial protocol
Serial proprietary	N/A	Enable	RS-232/422/485	User-configurable data frame for serial proprietary protocol
CANopen	N/A	Enable	CAN 2.0A	CANopen protocol
J1939	N/A	Enable	CAN 2.0B	J1939 protocol
CAN proprietary	N/A	Enable	CAN 2.0A/B	User-configurable data frame for CAN proprietary protocol

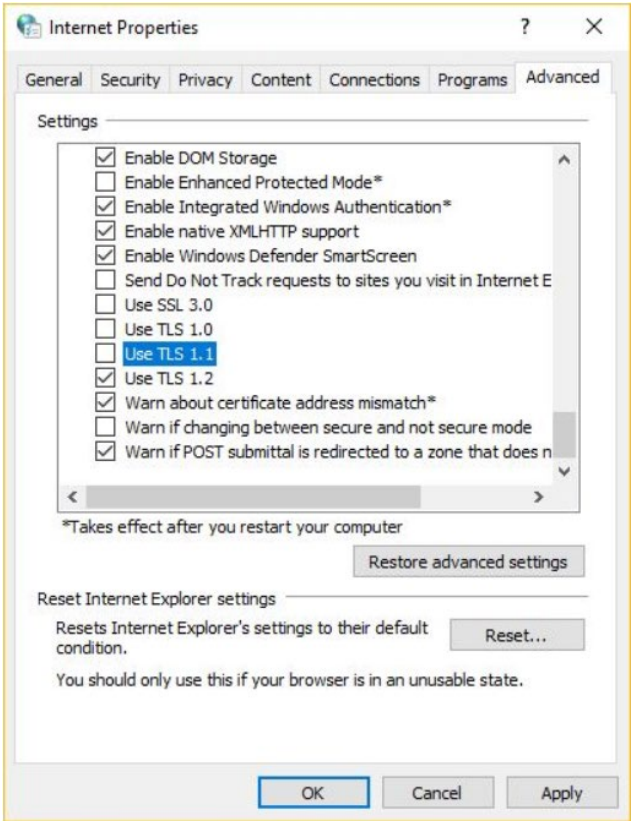
For security reasons, consider disabling unused services. The suggested serial settings in the table below depend on the different models and user preferences. Make sure serial connections and cables are under physical protection. Serial proprietary and CAN proprietary protocols are user-configurable data frames. Address user-defined data frame risks and application security requirements from a system standpoint.

Service Name	Suggested Setting	Type	Security Remark
Modbus RTU/ASCII	Enable	RS-232/422/485	Serial connections and cables are under physical protection
Serial proprietary	Enable	RS-232/422/485	Serial connections and cables are under physical protection
CANopen	Enable	CAN 2.0A	Serial connections and cables are under physical protection
J1939	Enable	CAN 2.0B	Serial connections and cables are under physical protection
CAN proprietary	Enable	CAN 2.0A/B	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 will take effect.

3.3 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 and is set to update to the newest version.



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 "MGate self-signed" certificate.

3.3.1 Behavior of the SSL Certificate on an MGate Device

MGate devices can auto-generate a self-signed SSL certificate. We recommend importing SSL certificates from a trusted third-party Certificate Authority (CA) or your organization's CA.

The length of the MGate device's self-signed private keys is 1,024 bits, which must be compatible with most applications. Some applications may need a longer key, such as 2,048 bits, requiring the import of 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.

3.3.2 MGate Self-signed Certificate

Make sure to periodically check the validity of the 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.

3.3.3 Importing a Third-party Trusted SSL Certificate

Importing a 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/)

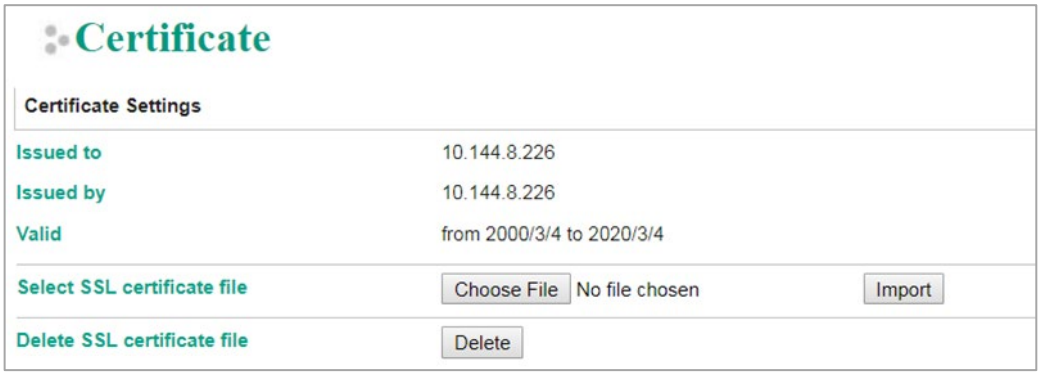
Step 2: Find a tool to issue a certificate signing request (CSR) file. Get one from a third-party CA company such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).

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.

Make sure to periodically check the validity of the certificate. If the certificate has expired, manually delete the previously imported certificate and import a new one.

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



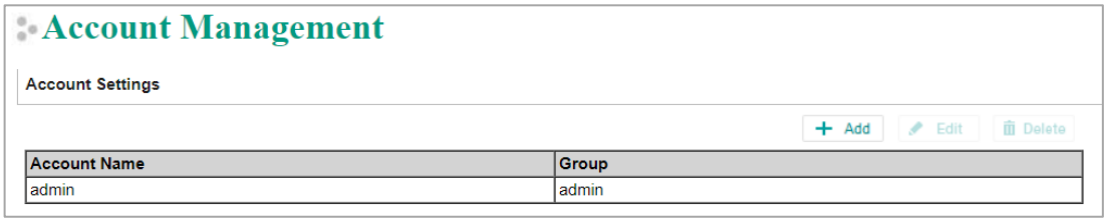
Here are some well-known third-party CA (Certificate Authority) companies for your reference (https://en.wikipedia.org/wiki/Certificate_authority):

- 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/)

3.4 Account Management

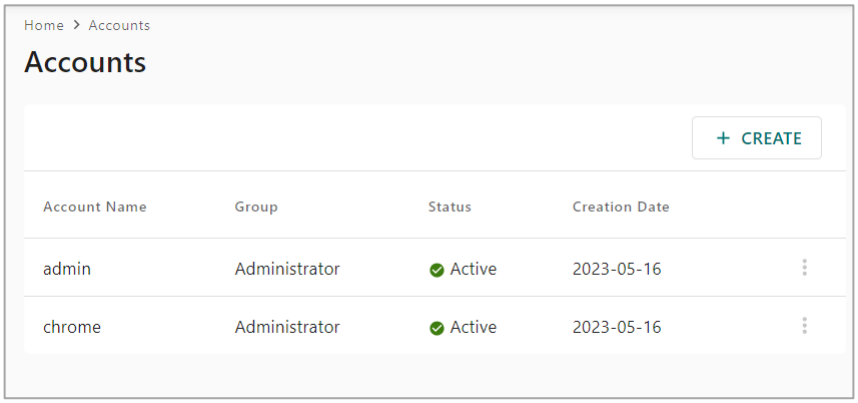
The MGate 5000 Series provides two different user levels, admin and user, with a maximum of 16 accounts. With an administrator account, you can access and change all settings through the web console. With the user account, you can only view settings.

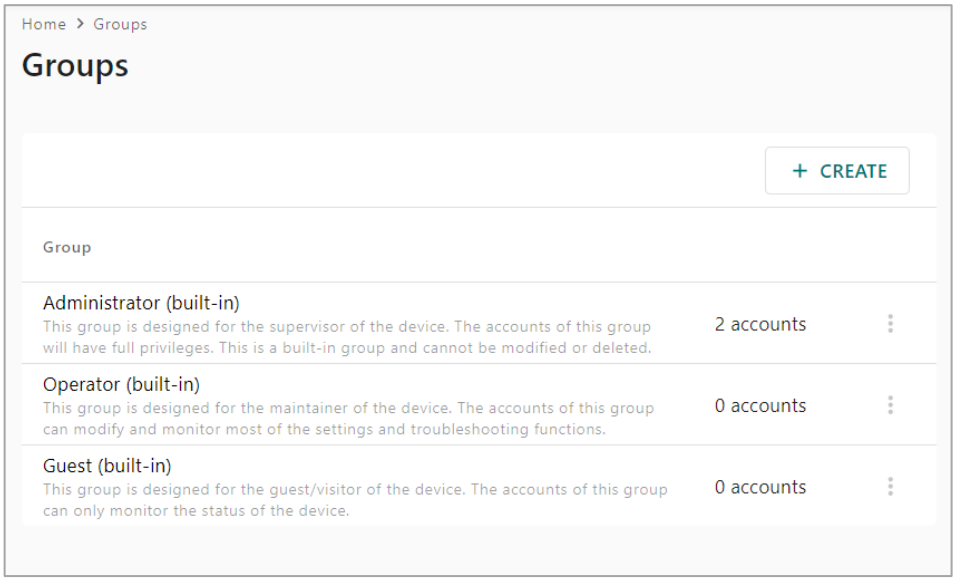
The default administrator account is **admin**, with the default password **moxa**. To manage accounts, log in to the web console and select **System Management > Misc. Settings > Account Management**. To change the password of an existing account, double-click the name of the account. Change the password on the page that opens.



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

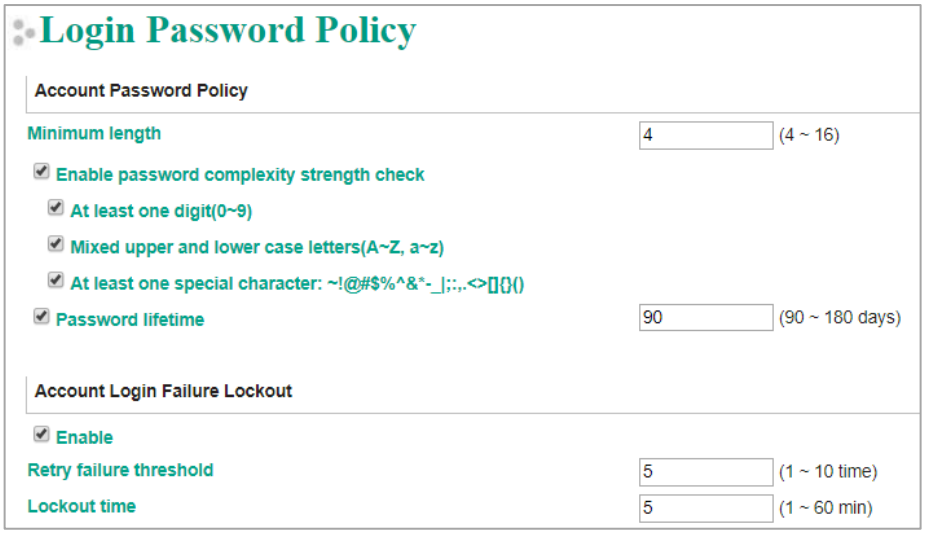
To manage accounts in the MGate 5121/5122/5123/5134/5135/5435/5192 Series, log in to the web console and select **SECURITY > Account Management > Accounts**. You can also create different security groups to fit your IT policy on the **Account Management > Groups** page.





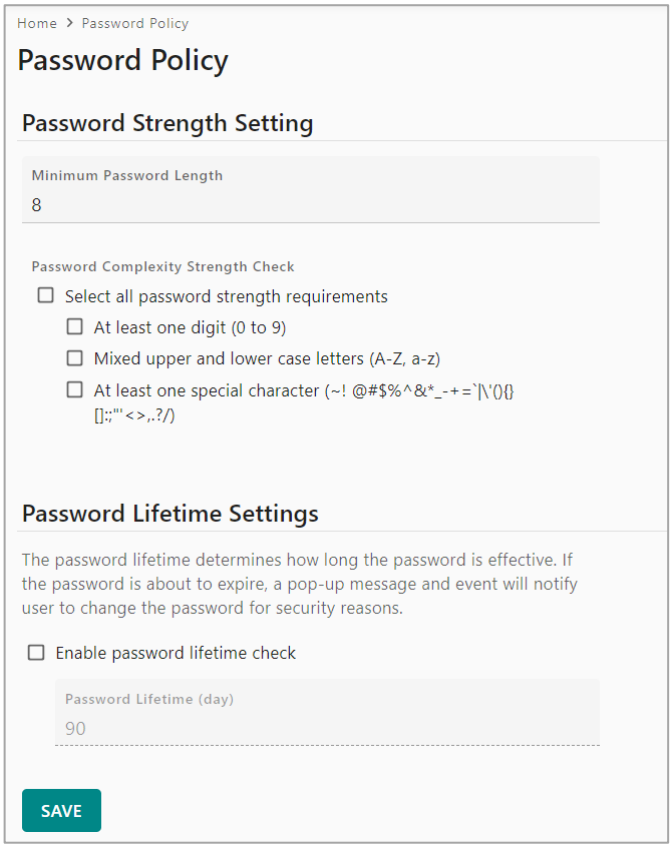
Note We suggest you manage your device with another "administrator level" account instead of using the default "admin" account, as it is commonly used by embedded systems. Once the new administrator-level account has been created, the original "admin" account must be monitored for security reasons to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

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

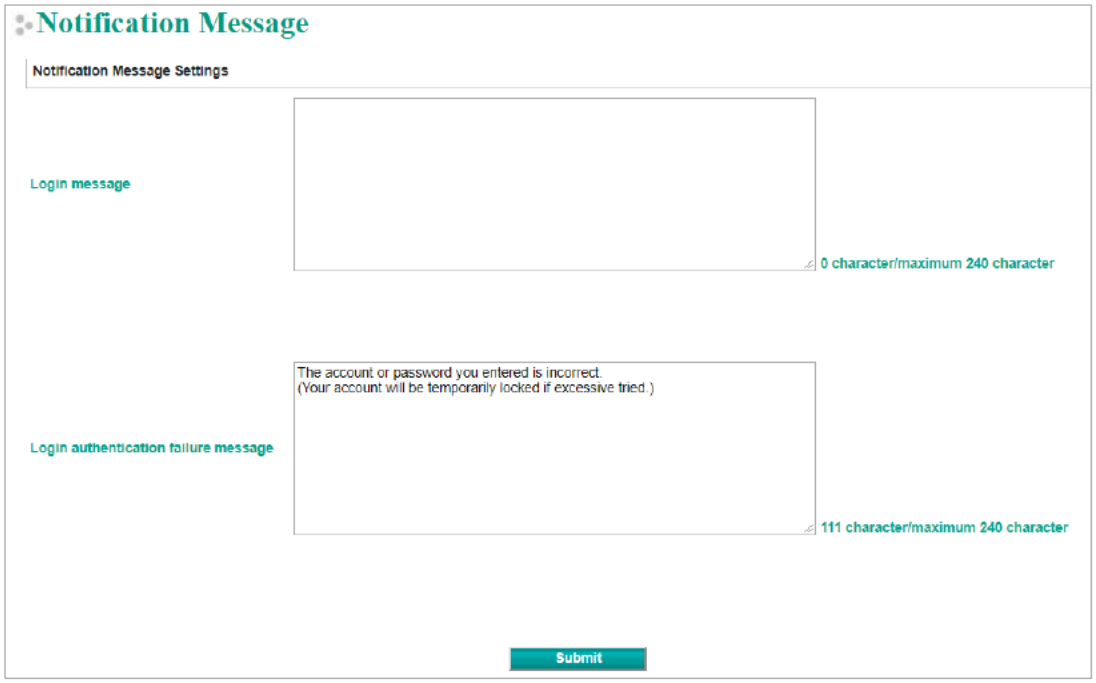


Adjust the password policy to require more complex passwords. For example, set the **Minimum length** to 16, enable all password complexity strength checks, and enable the **Password lifetime** options. Also, to avoid brute-force attacks, it's suggested that you enable the **Account login failure lockout**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

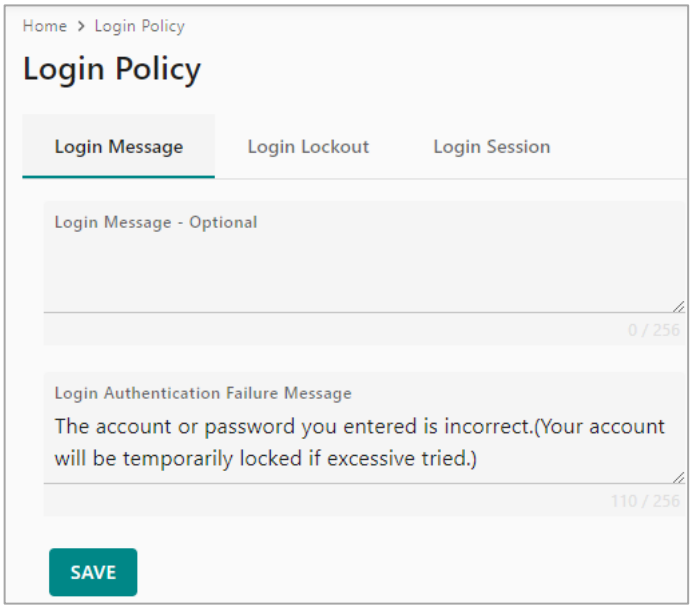
For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, select **SECURITY > Account Management > Password Policy**.



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.

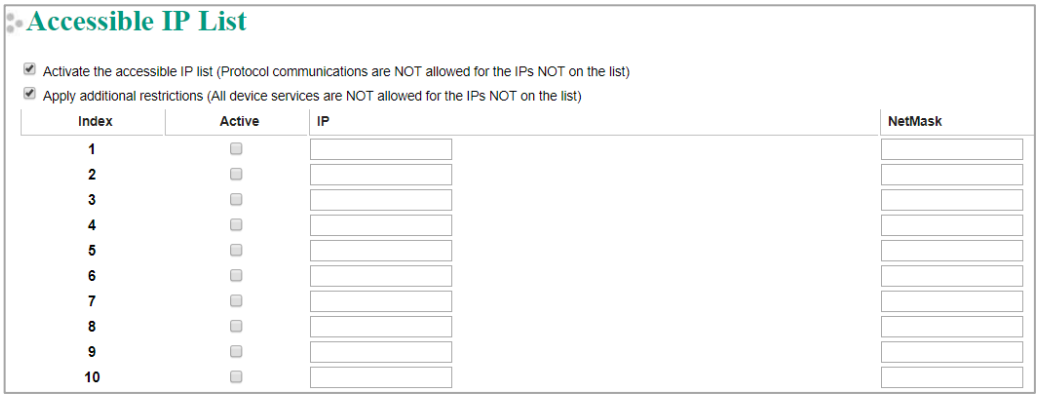


For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, select **SECURITY > Login Policy > Login Message**.



3.5 Accessible IP List

The MGate 5000 Series limits access to specific 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 5000 Series. To configure this, 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).



Activate the accessible IP list	Apply additional restrictions	IP is in the list and Active is checked	IP is not in the list OR Active is not checked
✓	–	All protocol communication and services* are allowed for the IP.	Protocol communication is not allowed, but services* are still allowed for the IP.
✓	✓	All protocol communication and services* are allowed for the IP.	All services* are not allowed for the IP.

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

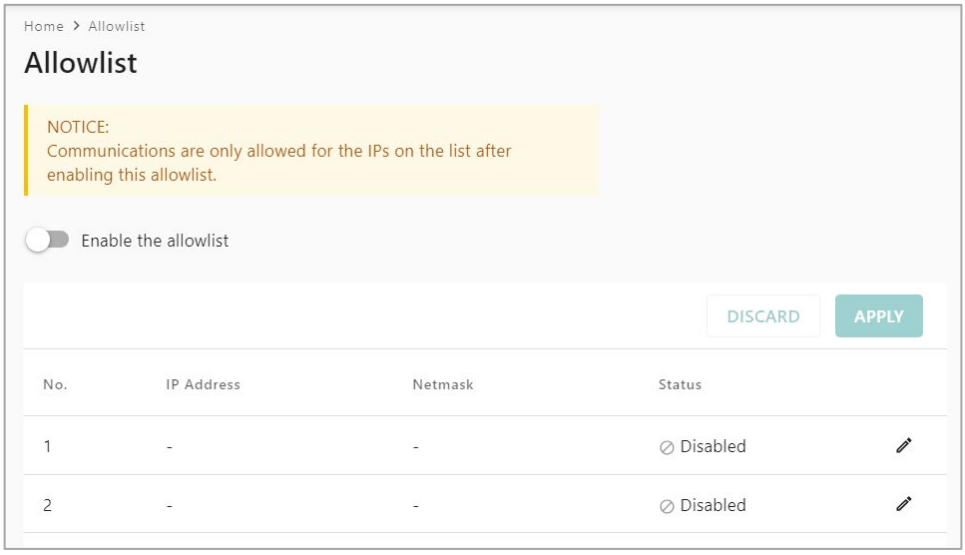
Add a specific address or range of addresses by using a combination of an IP address and a netmask:

- 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, ensure you leave unchecked the "Enable" checkbox for the accessible IP list.

The following table shows additional configuration examples.

Desired IP Range	IP Address	Netmask
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

For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, select **SECURITY > Allowlist**.



WARNING

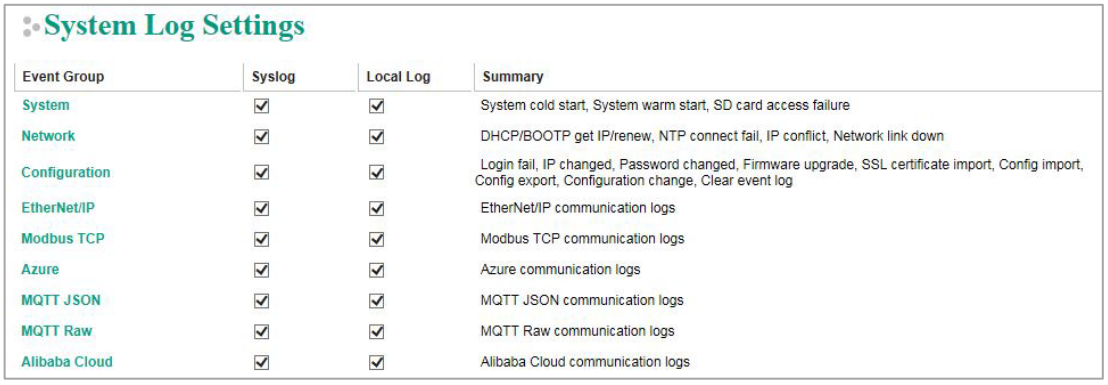
Ensure that the IP address of the PC you are using to access the web console is on the Accessible IP List. If your PC's IP address is not listed in the Accessible IP list, your PC cannot access the MGate.

3.6 Logging and Auditing

These are the events that the MGate 5000 Series will record. The SD card access failure event and protocol events vary for the different MGate 5000 models. Keep the SD card in a secure location accessible only to authorized individuals.

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 logged
Protocol	Protocol communication logs

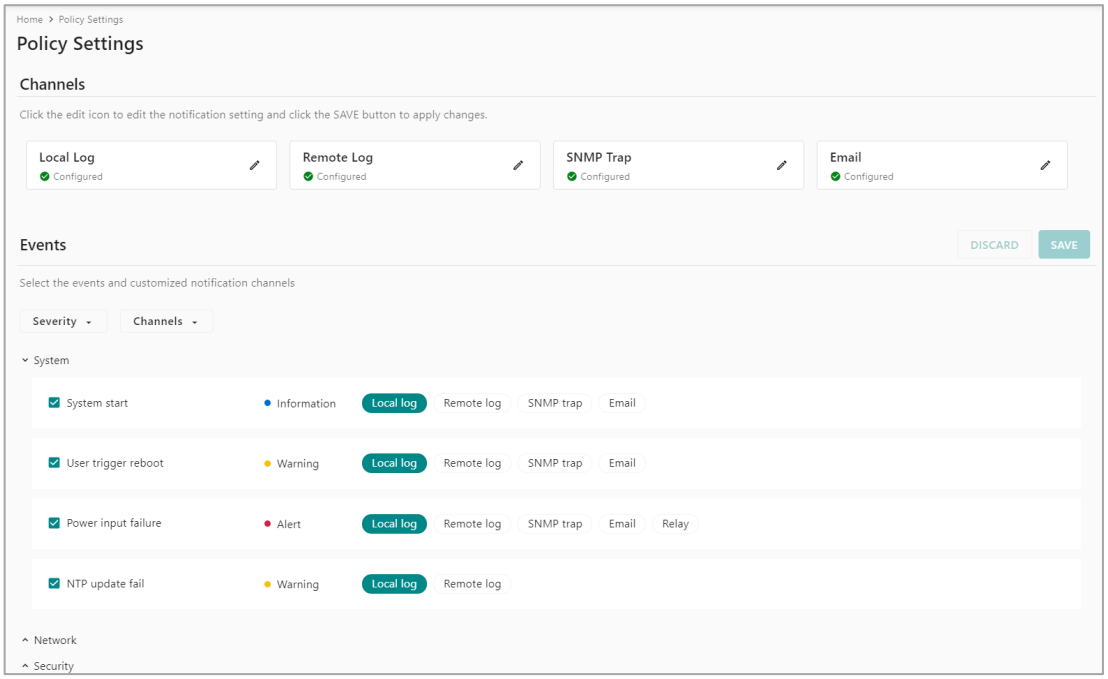
To configure this setting, log in to the HTTP/HTTPS console and select **System Management > System Log Settings**. Then, enable the **Local Log** for recording on the MGate 5000 device and/or **Syslog** for keeping records on a server. Enable system log settings to record all important system events to monitor device status and check for security issues.

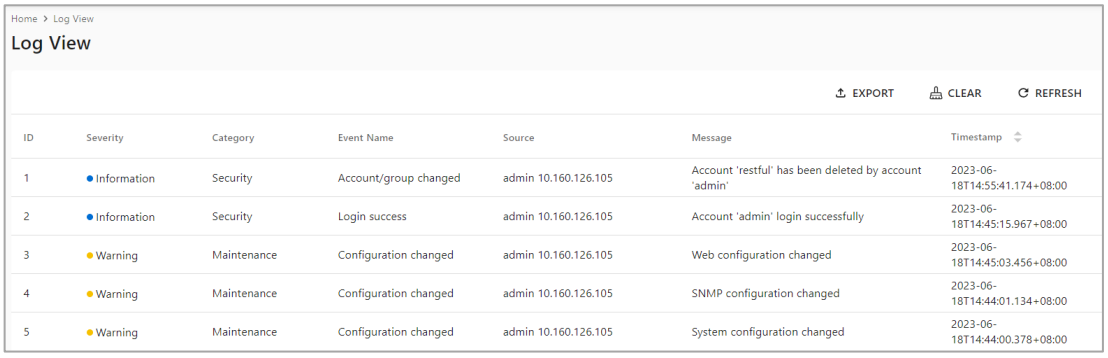


To view events in the system log, log in to the HTTP/HTTPS console and select **System Monitoring > System Log**.

For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, the events are as follows. Select **DIAGNOSTIC > Event Log > Policy Settings** and **Log View** to configure the event settings.

Event Group	Summary
System	System start, User trigger reboot, Power input failure, NTP update fail
Network	IP conflict, DHCP get IP/renew, IP changed, Ethernet link down
Security	Clear event log, Login success, Login failure, Account/group changed, Password reached lifetime, SSL certificate import, SSL certificate expired, Syslog certificate import, Syslog certificate expired
Maintenance	Firmware upgrade success, Firmware upgrade failure, Configuration import success, Configuration import failure, Configuration export, Configuration changed, Load factory default
Protocol	Protocol communication logs

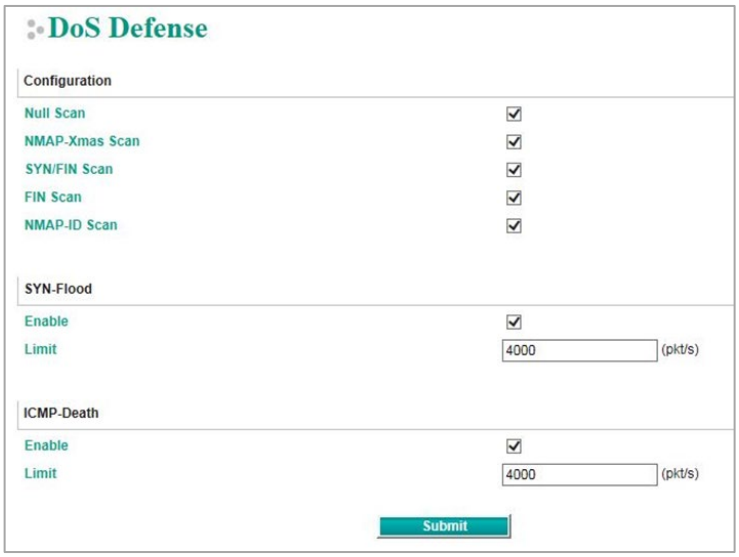




3.7 DoS Defense

Enable and configure several features to enable DoS Defense to protect against denial-of-service (DoS) attacks.

Note This function is not supported in the MGate 5217 Series.



4 Patching/Upgrades

4.1 Patch Management Plan

For patch management, Moxa releases version enhancements with thorough release notes annually.

4.2 Firmware Upgrades

The process for upgrading firmware is as follows:

1. Download the latest firmware for your MGate device from the Moxa website:
   - **MGate 5101 Series:**

     https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5101-pbm-mn-series#resources
   - **MGate 5102 Series:**

     https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/profinet-gateways/mgate-5102-pbm-pn-series#resources
   - **MGate 5103 Series:**

     https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5103-series#resources

- **MGate 5105 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5105-mb-eip-series#resources

- **MGate 5109 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5109-series#resources

- **MGate 5111 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5111-series#resources

- **MGate 5114 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5114-series#resources

- **MGate 5118 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5118-series#resources

- **MGate 5119 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5119-series#resources

- **MGate W5108/W5208 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-w5108-w5208-series#resources

- **MGate 5216 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5216-series#resources

- **MGate 5217I Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5217-series#resources

- **MGate 5121 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5121-series#resources

- **MGate 5122 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/ethernet-ip-gateways/mgate-5122-series#resources

- **MGate 5123 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/profinet-gateways/mgate-5123-series#resources

- **MGate 5134 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5134-series#resources

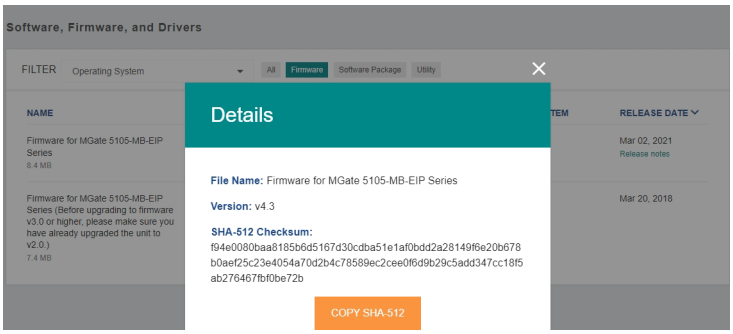
- **MGate 5135/5435 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5135-5435-series#resources

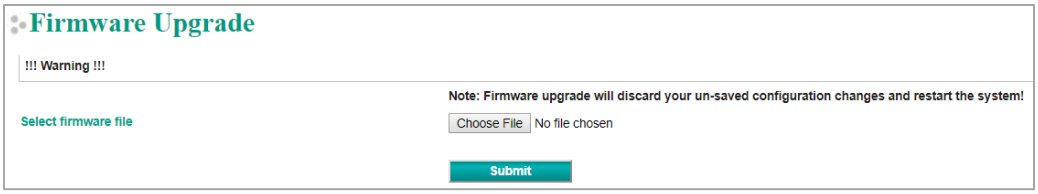
- **MGate 5192 Series:**

  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-5192-series#resources

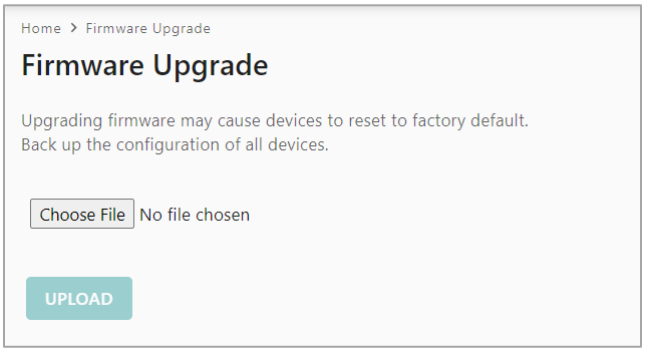
2. Moxa's website provides the SHA-512 hash value for you to double-check if the firmware is identical to the one on the website.



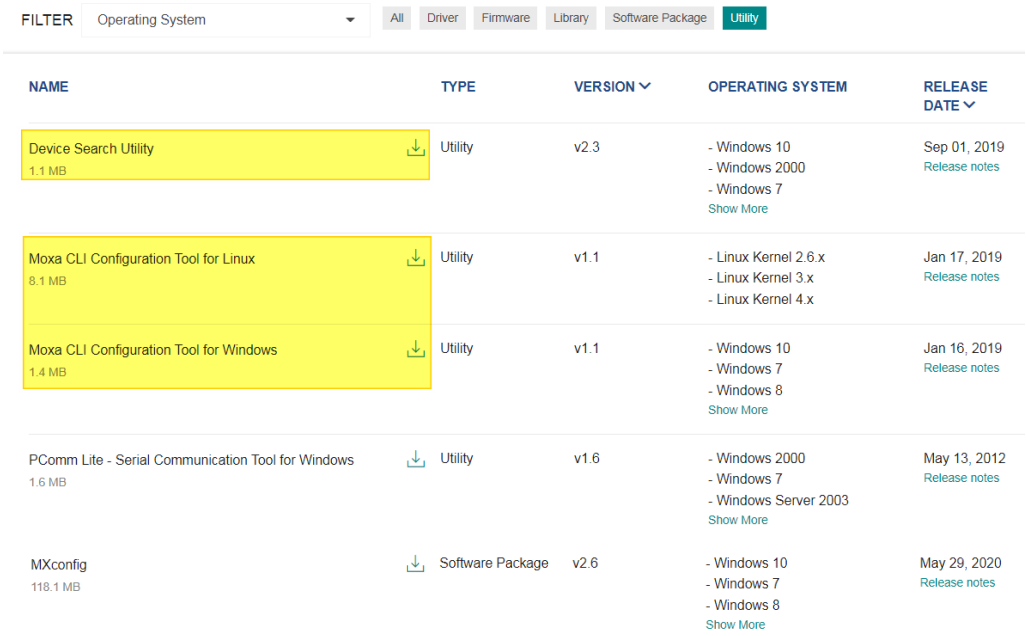
3. Log in to the HTTP/HTTPS console and select **System Management > Maintenance > Firmware Upgrade**. Click the **Choose File** button to select the proper firmware and click **Submit** to upgrade the firmware.



For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, select **MAINTENANCE > Firmware upgrade**.



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



Note For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, a firmware verification failure or hardware abnormality is indicated if the Ready LED does not turn on after powering up. Please contact Moxa Technical Support services.

4.3 Firmware Integrity Verification (User Responsibility)

The MGate does not perform cryptographic signature verification of firmware images on the device; it cannot independently determine whether a firmware file is authentic. Users are therefore responsible for validating firmware integrity before deployment:

1. Download firmware only from the official Moxa website (https://www.moxa.com) over HTTPS. Do not install firmware obtained from email, third parties, or unknown media.
2. Compute the SHA-512 hash of the downloaded file and confirm it matches the value published with the release. If the values differ, do not install the file; re-download it, and contact Moxa Technical Support if the mismatch persists.
3. Restrict who can deliver firmware to the device. Use a dedicated administrator-level account, upload only over HTTPS from a hardened workstation permitted by the Accessible IP List (see 3.5), keep the device behind a firewall on a segmented network (see 2.2), and enable Local Log/Syslog (see 3.6) so "Firmware upgraded" events can be reviewed.

Note Hash verification confirms that the file matches the one published by Moxa. It is an administrative compensating control performed by the asset owner and does not substitute for on-device signature verification.

5 Testing the Security Environment

Besides the devices that support these protective functions, network managers can follow several recommendations to protect their network and devices.

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

- Testing tools for cybersecurity environment checks are available. 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 access to the serial console, which depends on different model series, as with any physical access to the device.
- Avoid using insecure services such as SNMPv1 or v2c. We recommend disabling them completely.
- Limit the number of simultaneous web server sessions allowed. Periodically, change the passwords.
- Back up the configuration files periodically.
- Audit the devices periodically to make sure they comply with these recommendations and/or any internal security policies.
- If there is a need to return the unit to Moxa, make sure you have already backed up the current configuration before returning it.

Note DISCLAIMER: Note that the above information and 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 cyberintrusions and do not guarantee that the above information will meet your specific requirements. The above information is provided "as-is", and we make no warranties, express, implied or otherwise, regarding its accuracy, completeness, or performance.

6 Decommissioning Suggestion

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. Restart communication and check if everything works fine. If yes, decommission the old unit in the next step. If not, you may need assistance to troubleshoot the issue.
4. Keep the old unit powered on and clear all log information and reset to the default by using the hardware RESET button. Refer to the user manual for the RESET button usage.
5. After the device reboots and all user settings are reset to default, you may scrap the old MGate unit.

7 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 Product Security Incident Response Team (PSIRT) takes a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

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