The Security Hardening Guide for the MGate 5000 Series

Moxa Technical Support Team

support@moxa.com

Contents

Released on Dec 26, 2024

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 highly 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	v2.2
MGate 5102 Series	PROFIBUS-to-PROFINET Gateway	Linux	v2.3
MGate 5103 Series	Modbus RTU/ASCII/EtherNet/IP-to-PROFINET Gateway	Linux	v2.2
MGate 5105 Series	Modbus RTU/ASCII/TCP-to-EtherNet/IP Gateway	Linux	v4.3
MGate 5109 Series	Modbus RTU/ASCII/TCP-to-DNP3 serial/TCP Gateway	Linux	v2.3
MGate 5111 Series	Modbus/PROFINET/EtherNet/IP-to-PROFIBUS Gateway	Linux	v1.3
MGate 5114 Series	Modbus RTU/ASCII/TCP/IEC101-to-IEC104 Gateway	Linux	v1.3
MGate 5118 Series	CAN-J1939-to-Modbus/PROFINET/EtherNet/IP Gateway	Linux	v2.2
MGate 5119 Series	DNP3/IEC 101/IEC 104/Modbus-to-IEC 61850 Gateway	Linux	v1.1
MGate W5108/W5208 Series	IEEE 802.11 a/b/g/n wireless Modbus/DNP3 Gateway	Linux	v2.4
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

Model	Function	Operating System	Firmware Version
MGate 5123 Series	CANopen/J1939-to-PROFINET Gateway	Linux	v2.0
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 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:** openSSL v1.1.1b

  For the MGate 5121/5122/5123/5134/5135/5435/5192 Series:

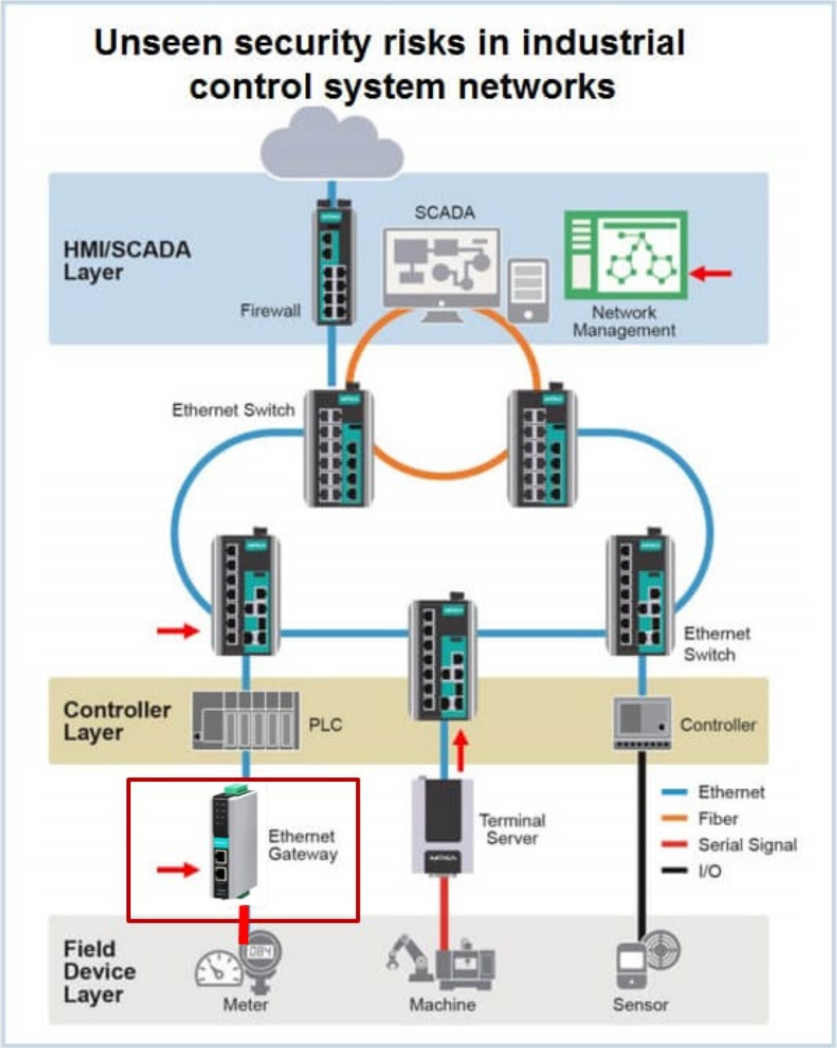
  Linux models: openSSL v1.1.1s
- **Moxa Operating System models:** mbed TLS v2.7.5

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.

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

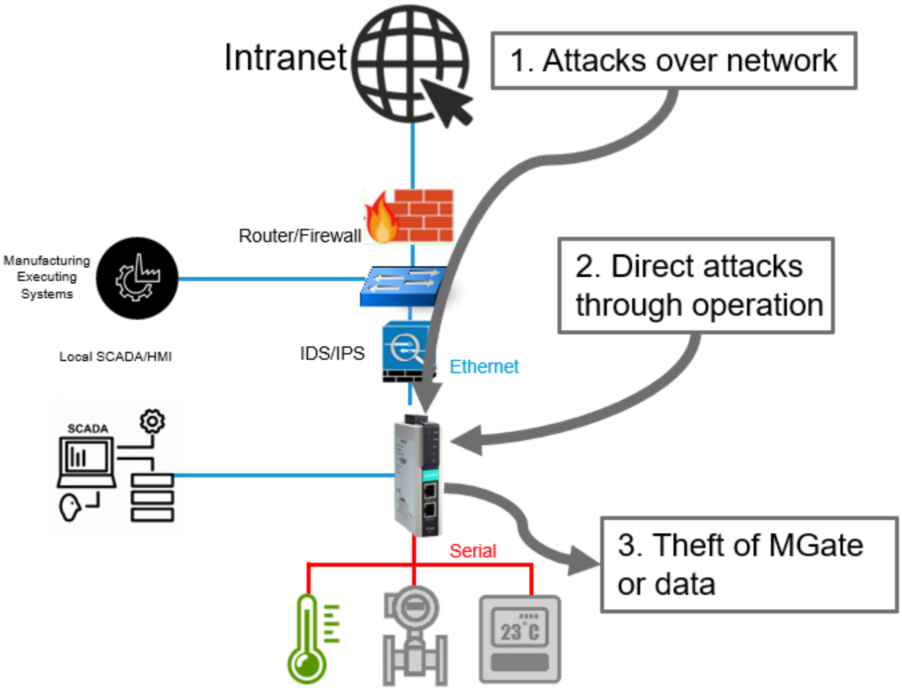
Threats from individuals with no rights to the MGate 5000 Series via networks such as intranets.

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.


Intranet
1. Attacks over network
Router/Firewall
Manufacturing Executing Systems
2. Direct attacks through operation
Local SCADA/HMI
IDS/IPS
Ethernet
SCADA
Serial
3. Theft of MGate or data
23°C

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 on their role and responsibilities for 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 asset	No	Yes	Yes	Asset owner
Network Security	Network firewall	Unauthorized and malicious communications from untrusted network	Yes	No	No	Asset owner
	Network IDS/IPS	Network attacks from various sources, such as port scanning, DDOS, 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 attack	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 of bootloader, OS kernel, and rootFS	Yes	Yes	No	
	Event log	Deny access, operation ofthe device	Yes	Yes	No	

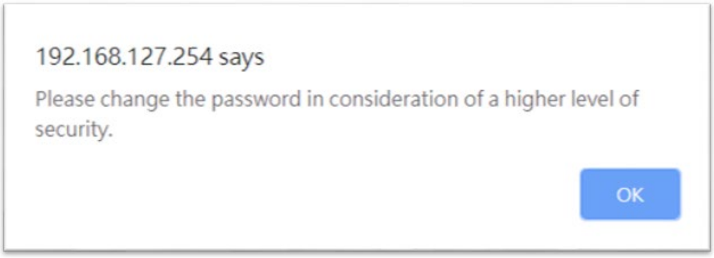
* DoS Defense features refer to Chapter 3.7 and notice that the MGate only provides basic features for defense-in-depth, not the network firewall/ID/IPS devices.

** 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.

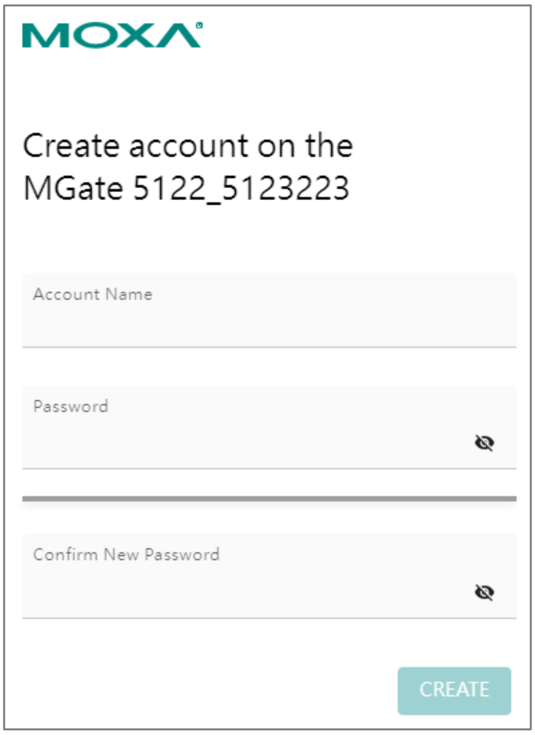
The default account and password are **admin** and **moxa** (both in lowercase letters), respectively. After successful login, a pop-up notification will prompt you to change your password for enhanced security.



192.168.127.254 says

Please change the password in consideration of a higher level of 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
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

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 notification
DHCP client	Enable/ Disable	Disable	UDP	68	DHCP client to acquire system IP address from server
Syslog client	Enable/ Disable	Disable	UDP	514	Sending system logs to remote syslog server
			TCP (TLS)	user cfg.	
Email client	Enable/ Disable	Disable	TCP	25	Sending system/config event notifications
			TLS	465	
			STARTTLS	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
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

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
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

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 notification
DHCP client	**Disable**	UDP	68	DHCP client to acquire system IP address from server
Syslog client	**Enable**	UDP	514	Sending system logs to remote syslog server
		TCP (TLS)	user cfg.	
Email client	**Enable**	TCP	25	Sending system/config event notification
		TLS	465	
		STARTTLS	485	
NTP client	**Disable**	UDP	123	Network time protocol to synchronize system time from 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
PROFINET IO device	**Enable**	UDP	34963	34963 for PROFINET protocol communication

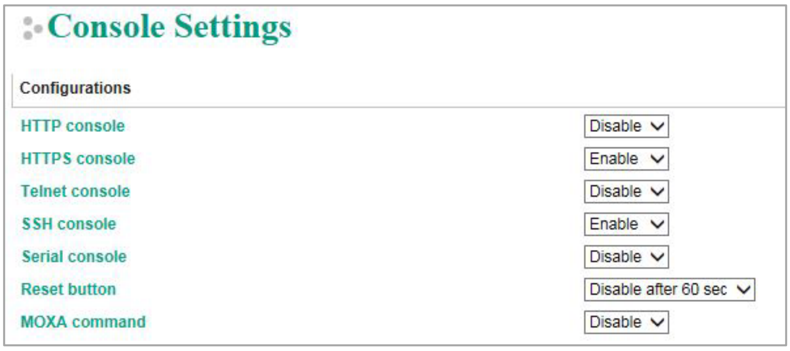
For console services, we recommend:

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**.

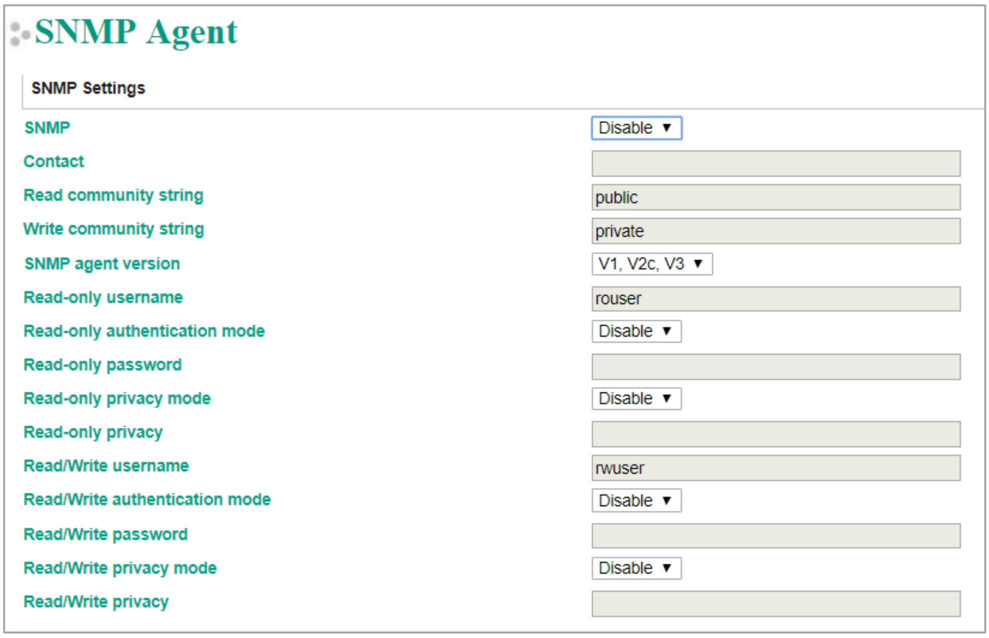


Console Settings

Configurations

HTTP console	Disable
HTTPS console	Enable
Telnet console	Disable
SSH console	Enable
Serial 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.

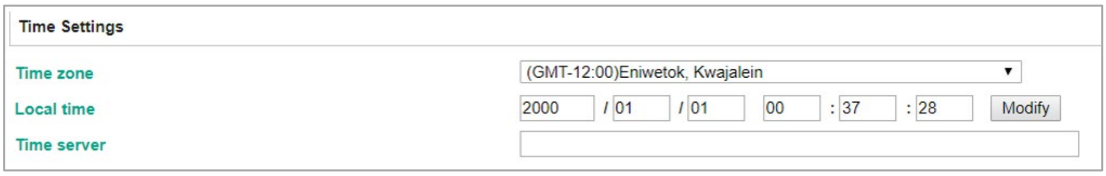


SNMP Agent

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	

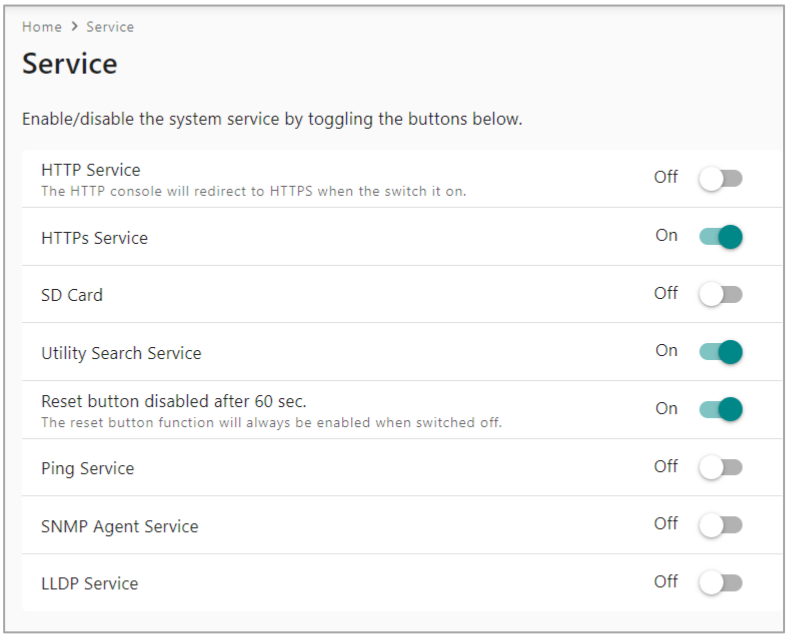
To disable the NTP service, log in to the HTTP/HTTPS console, select **Basic Settings**, and keep the **Time server** setting empty. This will disable the NTP service.



Time Settings

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

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**.

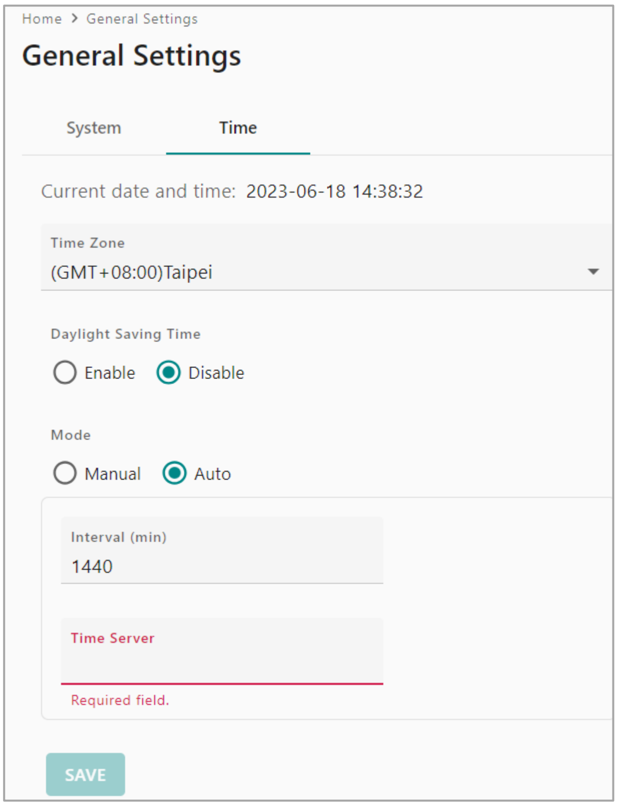


Service

Enable/disable the system service by toggling the buttons below.

HTTP Service The HTTP console will redirect to HTTPS when the switch it on.	Off
HTTPs Service	On
SD Card	Off
Utility Search Service	On
Reset button disabled after 60 sec. The reset button function will always be enabled when switched off.	On
Ping Service	Off
SNMP Agent Service	Off
LLDP Service	Off

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



Current date and time: 2023-06-18 14:38:32

Time Zone: (GMT+08:00)Taipei

Daylight Saving Time: ○ Enable ● Disable

Mode: ○ Manual ● Auto

Interval (min): 1440

Time Server:

Required field.

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

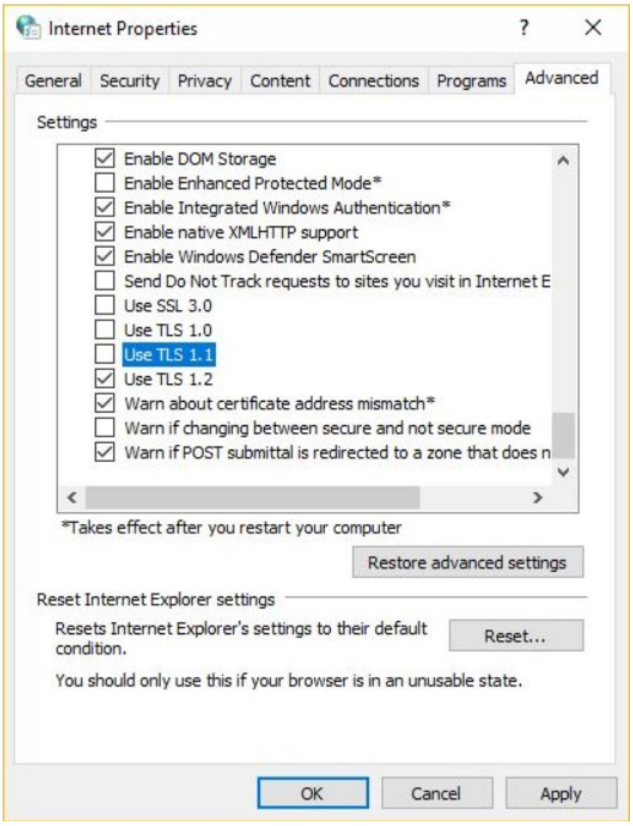
For security reasons, consider disabling unused services. The suggested serial settings in the table below depend on the different model and user preferences. Make sure serial connections and cables are under physical protection. Serial proprietary or CAN proprietary protocol are user-configurable data 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.



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.

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, which require importing a third-party certificate. Note that longer keys will mean browsing the web console will be slower because of the increased complexity of encrypting and decrypting communicated data.

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 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/)

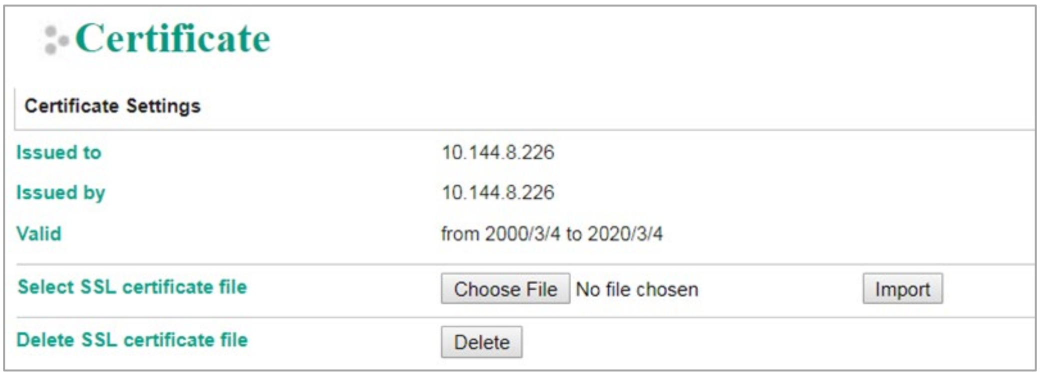
Step 2: Find a tool to issue a certificate signing request (CSR) file. Get one from a third-party CA company such as DigiCert (https://www.digicert.com/easy-csr/openssl.htm).

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.

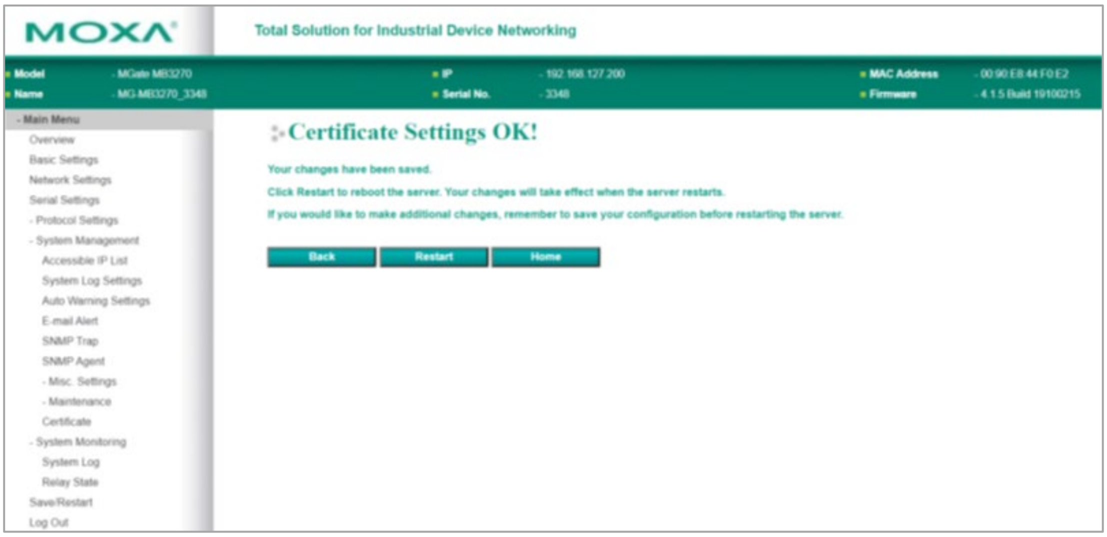
Note The maximum supported key length for MGate devices is 2,048 bits.



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.

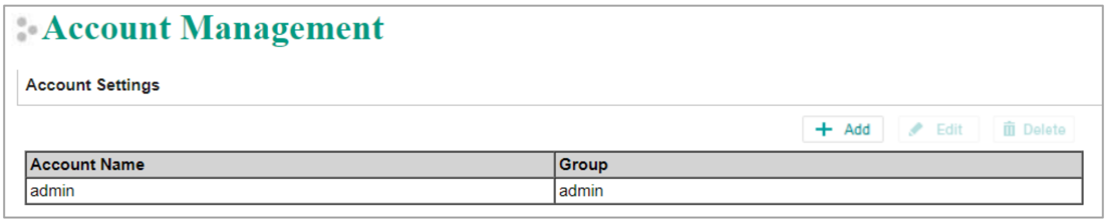
Here are some well-known third-party CA (Certificate Authority) companies for your reference (https://en.wikipedia.org/wiki/Certificate_authority):

- 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

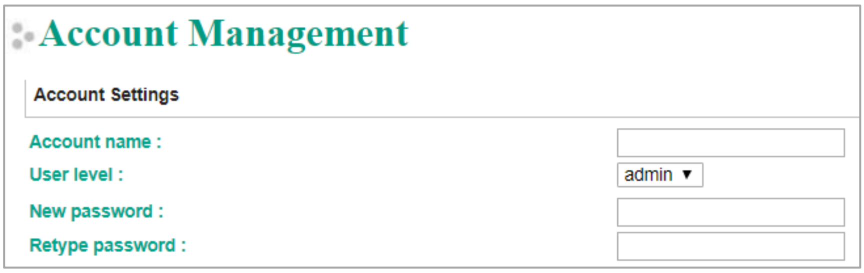
The MGate 5000 Series provides two different user levels, admin and user, with a maximum of 16 accounts. With an administrator account, you can access and change all settings through the web console. With the user account, you can only view settings.

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.



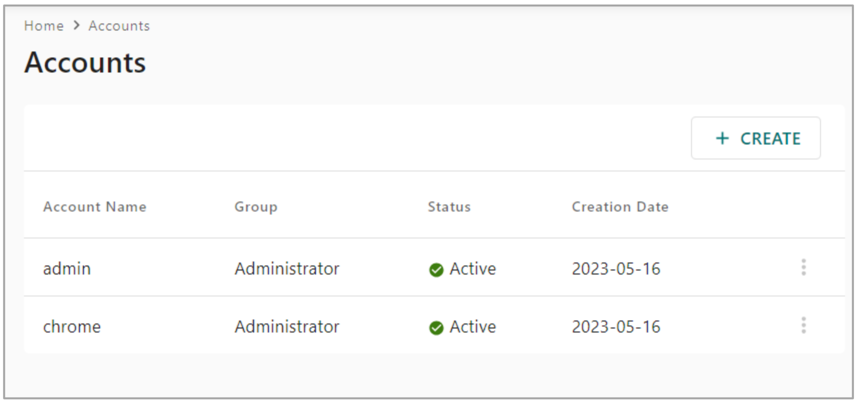
Account Name	Group
admin	admin

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.

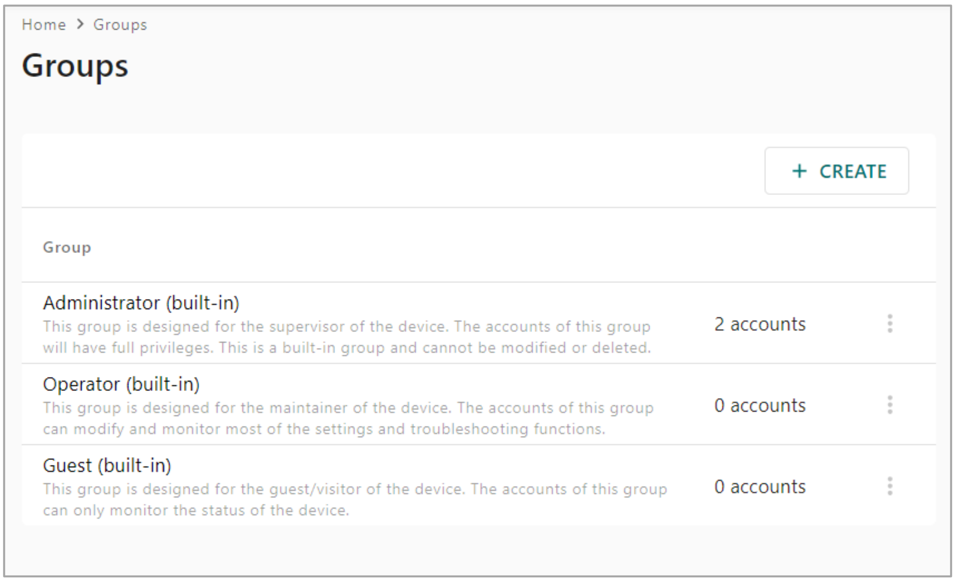


Account name :	
User level :	admin ▼
New password :	
Retype password :	

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 in the **Account Management > Groups** page.



Account Name	Group	Status	Creation Date
admin	Administrator	✓ Active	2023-05-16
chrome	Administrator	✓ Active	2023-05-16



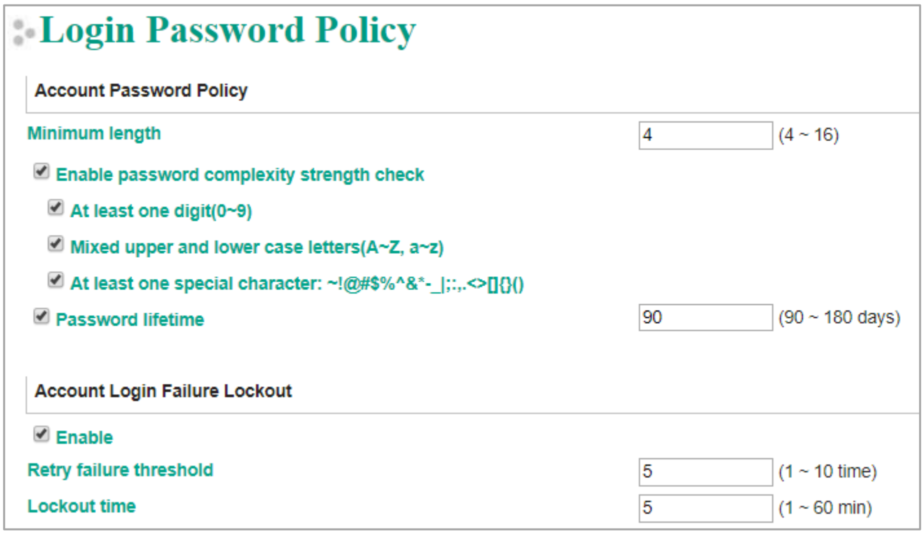
Home > Groups

Groups

Group		
Administrator (built-in) This group is designed for the supervisor of the device. The accounts of this group will have full privileges. This is a built-in group and cannot be modified or deleted.	2 accounts	⋮
Operator (built-in) This group is designed for the maintainer of the device. The accounts of this group can modify and monitor most of the settings and troubleshooting functions.	0 accounts	⋮
Guest (built-in) This group is designed for the guest/visitor of the device. The accounts of this group can only monitor the status of the device.	0 accounts	⋮

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**.



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

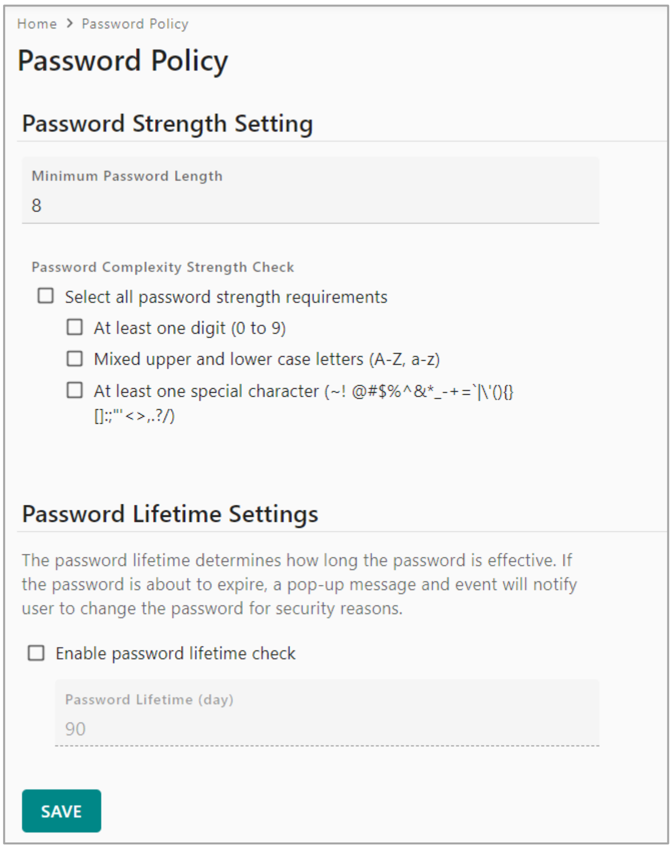
☑ Enable

Retry failure threshold 5 (1 ~ 10 time)

Lockout time 5 (1 ~ 60 min)

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



Home > Password Policy

Password Policy

Password Strength Setting

Minimum Password Length: 8

Password Complexity Strength Check

- □ Select all password strength requirements
  - □ At least one digit (0 to 9)
  - □ Mixed upper and lower case letters (A-Z, a-z)
  - □ At least one special character (~! @#$%^&*_-+=`|\'(){}[]:;"'<>,.?/)

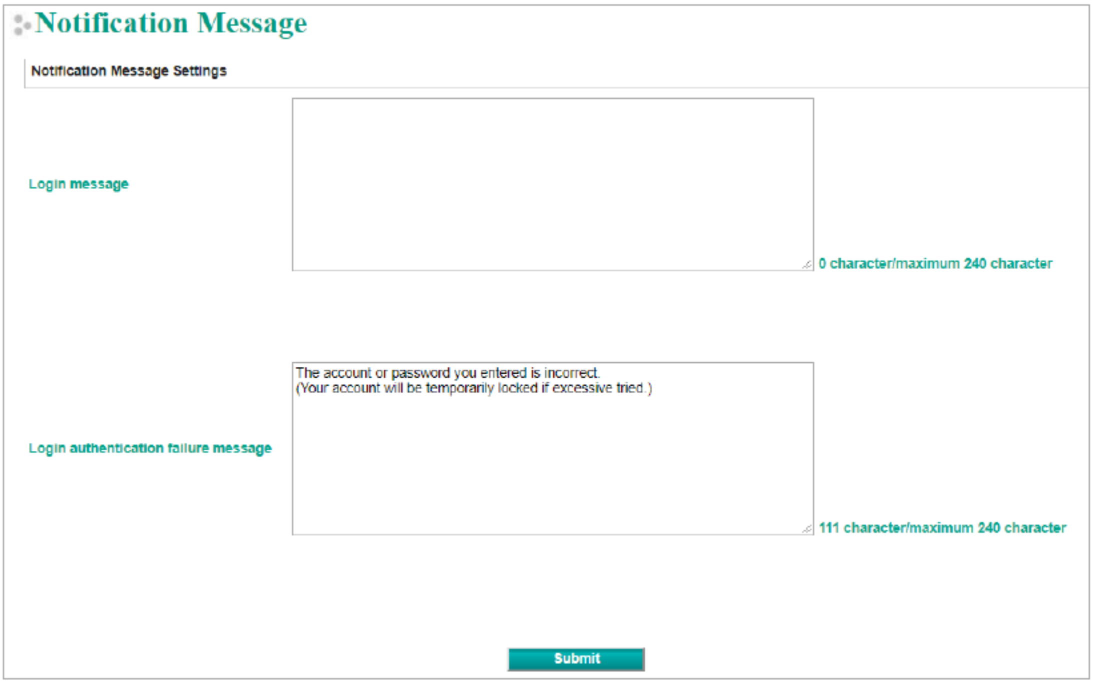
Password Lifetime Settings

The password lifetime determines how long the password is effective. If the password is about to expire, a pop-up message and event will notify user to change the password for security reasons.

□ Enable password lifetime check

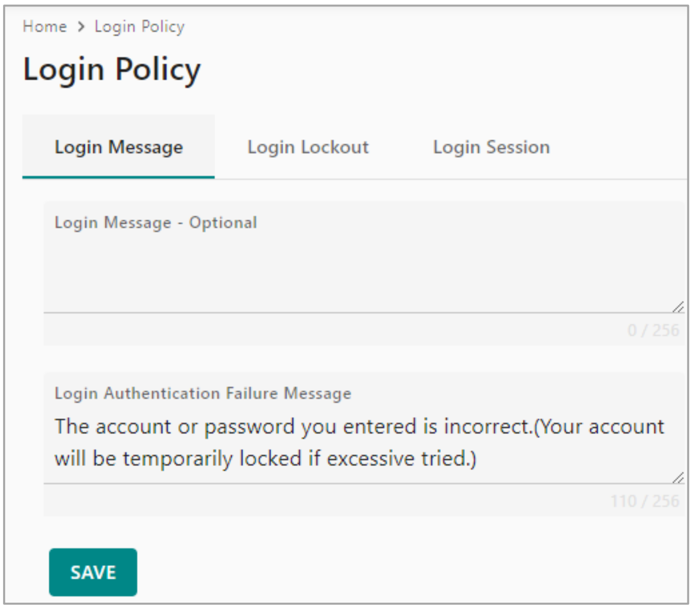
Password Lifetime (day): 90

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
111 character/maximum 240 character
Submit

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

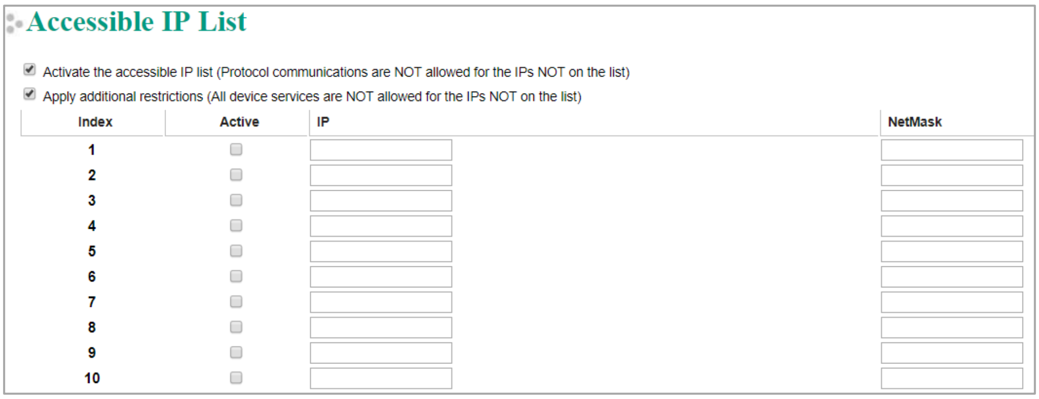
For the MGate 5121/5122/5123/5134/5135/5435/5192 Series, select **SECURITY > Login Policy > Login Message**.



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

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).



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	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

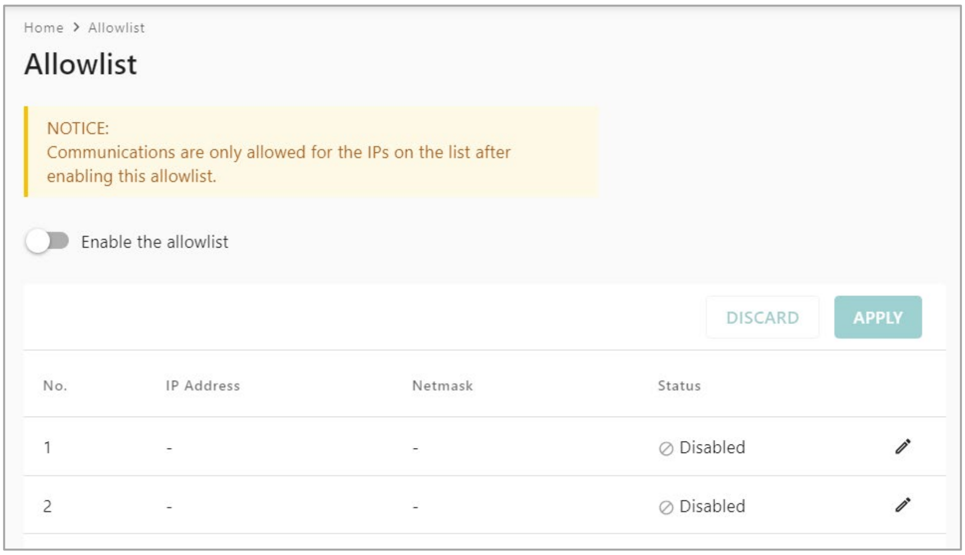
Add a specific address or range of addresses by using a combination of an IP address and a netmask:

- 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**.



Home > Allowlist

Allowlist

NOTICE:
Communications are only allowed for the IPs on the list after enabling this allowlist.

○ Enable the allowlist

No.	IP Address	Netmask	Status
1	-	-	⊘ Disabled
2	-	-	⊘ Disabled

WARNING

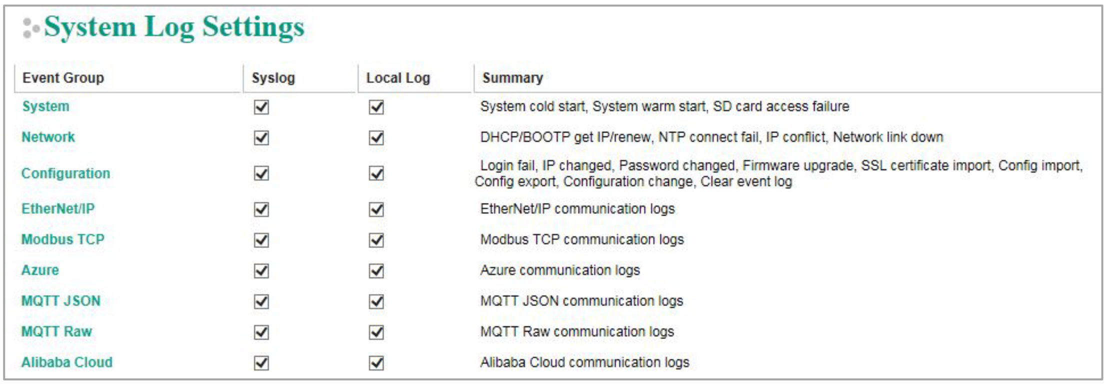
Ensure that the IP address of the PC you are using to access the web console is on the Accessible IP List. If your PC's IP address is not listed in the Accessible IP list, your PC cannot access the MGate.

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.

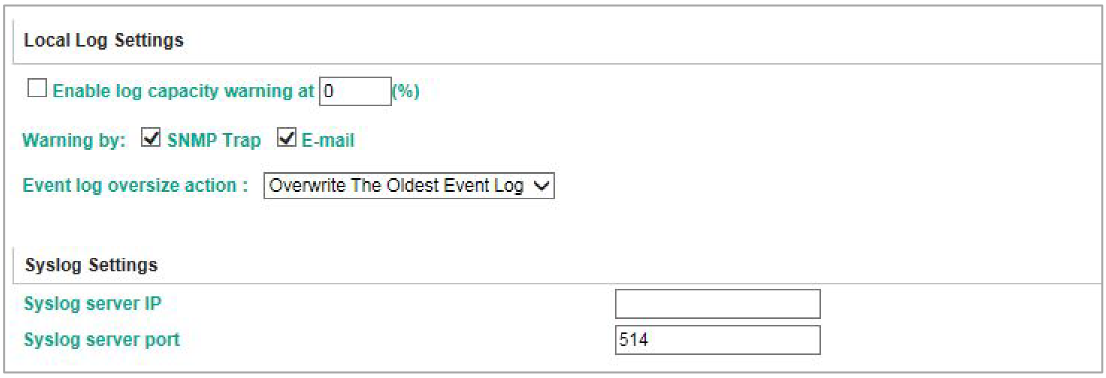
Event Group	Summary
System	System cold start, system warm start, SD card access failure
Network	DHCP/BOOTP gets IP/renew, NTP connect failed, IP conflict, Network link down
Configuration	Login failed, IP changed, Password changed, Firmware upgraded, SSL Certificate imported, Configuration imported/exported, 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.



System Log Settings

Event Group	Syslog	Local Log	Summary
System	☑	☑	System cold start, System warm start, SD card access failure
Network	☑	☑	DHCP/BOOTP get IP/renew, NTP connect fail, IP conflict, Network link down
Configuration	☑	☑	Login fail, IP changed, Password changed, Firmware upgrade, SSL certificate import, Config import, Config export, Configuration change, Clear event log
EtherNet/IP	☑	☑	EtherNet/IP communication logs
Modbus TCP	☑	☑	Modbus TCP communication logs
Azure	☑	☑	Azure communication logs
MQTT JSON	☑	☑	MQTT JSON communication logs
MQTT Raw	☑	☑	MQTT Raw communication logs
Alibaba Cloud	☑	☑	Alibaba Cloud communication logs



Local Log Settings

☐ Enable log capacity warning at 0 (%)

Warning by: ☑ SNMP Trap ☑ E-mail

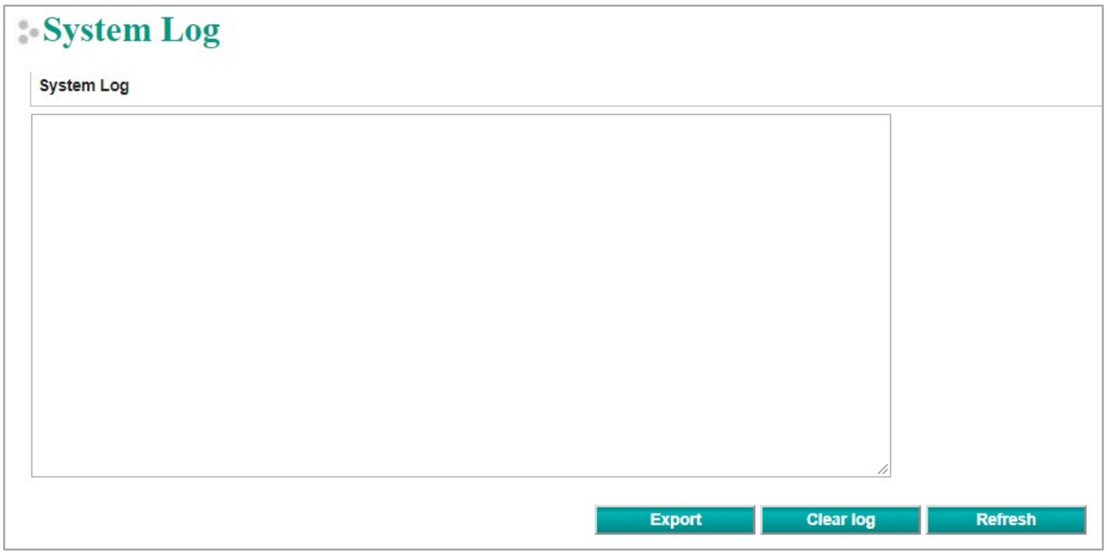
Event log oversize action : Overwrite The Oldest Event Log

Syslog Settings

Syslog server IP

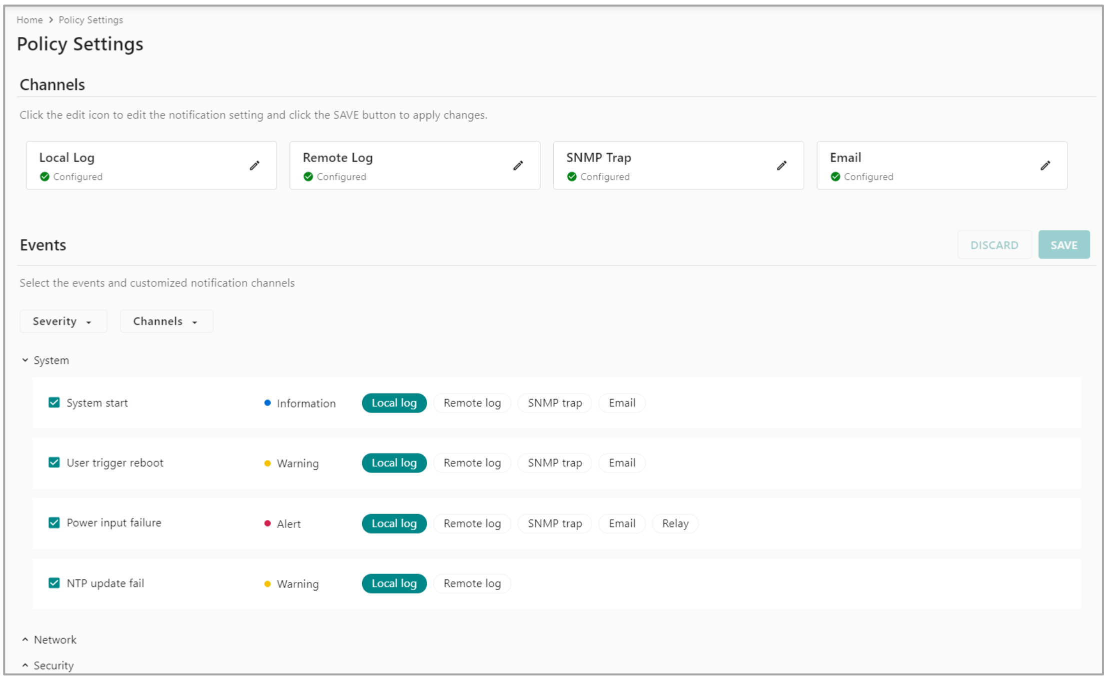
Syslog server port 514

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



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



Home > Policy Settings

Policy Settings

Channels

Click the edit icon to edit the notification setting and click the SAVE button to apply changes.

- Local Log – ✓ Configured
- Remote Log – ✓ Configured
- SNMP Trap – ✓ Configured
- Email – ✓ Configured

Events

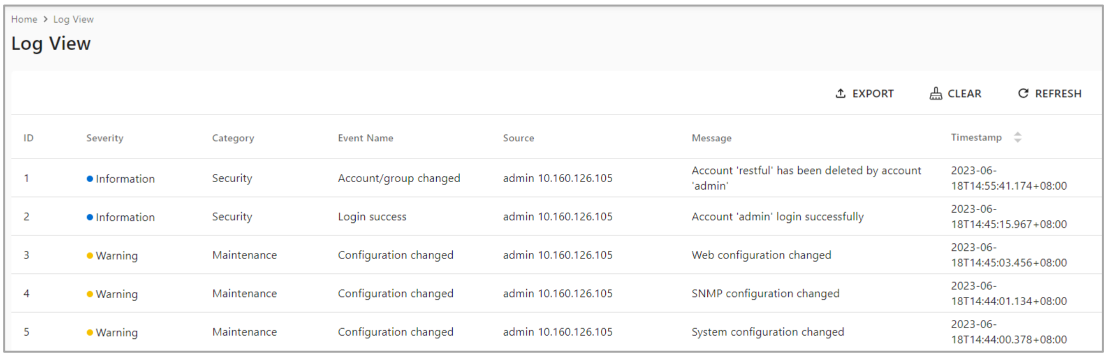
Select the events and customized notification channels

System

☑ System start	● Information	[✓ Local log] Remote log SNMP trap Email
☑ User trigger reboot	● Warning	[✓ Local log] Remote log SNMP trap Email
☑ Power input failure	● Alert	[✓ Local log] Remote log SNMP trap Email Relay
☑ NTP update fail	● Warning	[✓ Local log] Remote log

Network

Security



Home > Log View

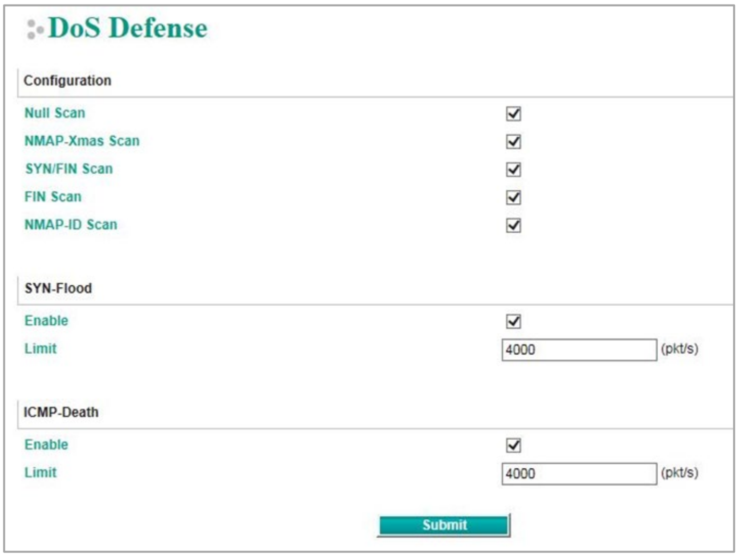
Log View

ID	Severity	Category	Event Name	Source	Message	Timestamp
1	● Information	Security	Account/group changed	admin 10.160.126.105	Account 'restful' has been deleted by account 'admin'	2023-06-18T14:55:41.174+08:00
2	● Information	Security	Login success	admin 10.160.126.105	Account 'admin' login successfully	2023-06-18T14:45:15.967+08:00
3	● Warning	Maintenance	Configuration changed	admin 10.160.126.105	Web configuration changed	2023-06-18T14:45:03.456+08:00
4	● Warning	Maintenance	Configuration changed	admin 10.160.126.105	SNMP configuration changed	2023-06-18T14:44:01.134+08:00
5	● Warning	Maintenance	Configuration changed	admin 10.160.126.105	System configuration changed	2023-06-18T14:44:00.378+08:00

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.



DoS Defense

Configuration

Null Scan	☑
NMAP-Xmas Scan	☑
SYN/FIN Scan	☑
FIN Scan	☑
NMAP-ID Scan	☑

SYN-Flood

Enable	☑
Limit	4000 (pkt/s)

ICMP-Death

Enable	☑
Limit	4000 (pkt/s)

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
   - **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:**

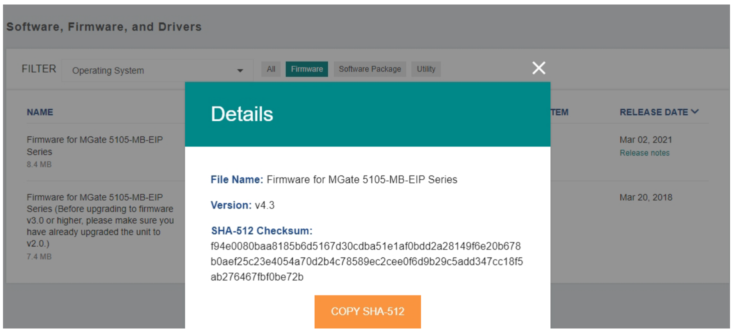
  https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/profinet-gateways/mgate-5123-series#resources

- **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.



Software, Firmware, and Drivers

Firmware for MGate 5105-MB-EIP Series 8.4 MB — Mar 02, 2021 Release notes

Firmware for MGate 5105-MB-EIP Series (Before upgrading to firmware v3.0 or higher, please make sure you have already upgraded the unit to v2.0.) 7.4 MB — Mar 20, 2018

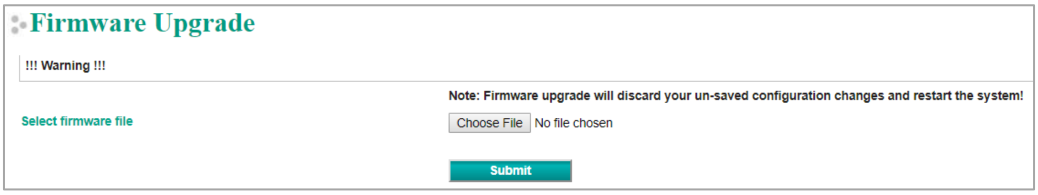
Details

File Name: Firmware for MGate 5105-MB-EIP Series

Version: v4.3

SHA-512 Checksum:
f94e0080baa8185b6d5167d30cdba51e1af0bdd2a28149f6e20b678
b0aef25c23e4054a70d2b4c78589ec2cee0f6d9b29c5add347cc18f5
ab276467fbf0be72b

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.



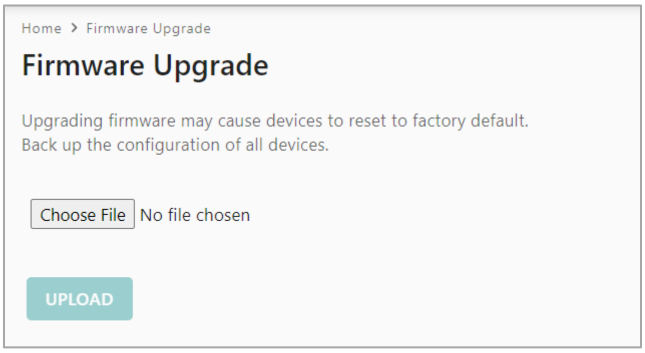
Firmware Upgrade

!!! Warning !!!

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

Select firmware file

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

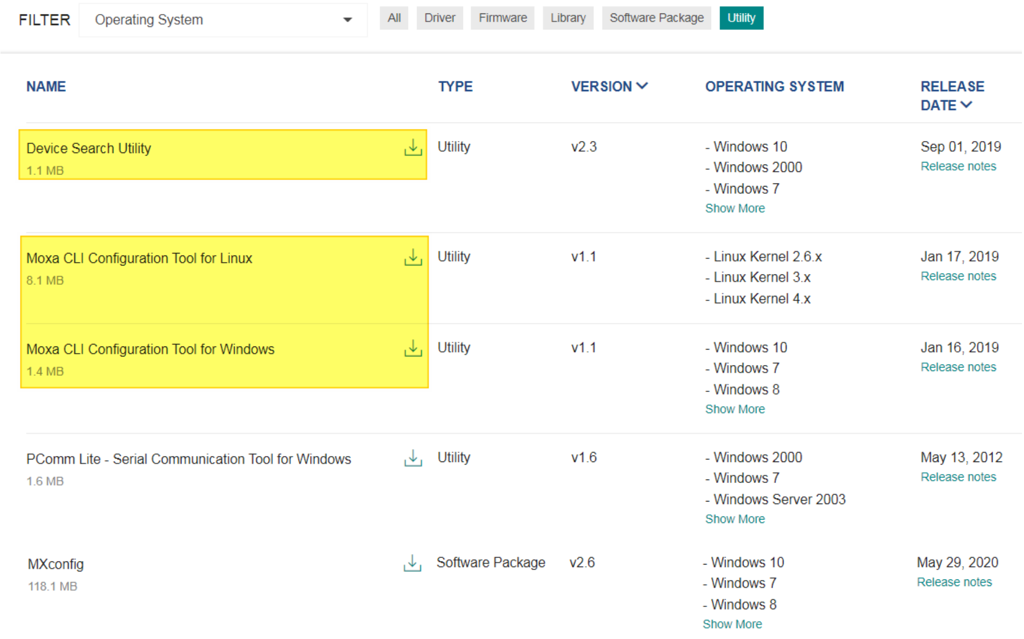


Home > Firmware Upgrade

Firmware Upgrade

Upgrading firmware may cause devices to reset to factory default.
Back up the configuration of all devices.

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.



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

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.

5 Testing the Security Environment

Besides these 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 the 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 no, 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 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