

Cybersecurity Manual

MT / cMTx

Human-Machine Interface (HMI)



Cybersecurity Manual

MT / cMTx

Document: 10014443630

Language: English

Revision: 00

Publication Date: 03/2026

The information below describes the reviews made in this manual.

Revision	Description
R00	First edition.

CONTENTS

1	INTRODUCTION	1-1
1.1	ABOUT THIS DOCUMENT	1-1
1.2	IMPORTANT NOTICE ON CYBERSECURITY AND COMMUNICATIONS	1-1
2	FUNDAMENTAL CONCEPTS OF CYBERSECURITY	2-1
2.1	OVERVIEW	2-1
2.2	FAR BEYOND IT: THE NEW FRONTIER OF CYBERSECURITY	2-1
2.3	DEFENSE IN DEPTH	2-2
2.3.1	External Environment	2-2
2.3.1.1	Plant Security	2-2
2.3.1.2	Network Environment Security	2-2
2.3.1.3	System Integration Security	2-2
2.3.2	Product Operation	2-2
2.4	GENERAL SECURITY MAINTENANCE	2-3
2.5	RISK ANALYSIS AND REPORTING MECHANISM	2-3
3	RISKS DURING PROGRAM EDITING	3-1
3.1	INSTALLATION FILE VERIFICATION	3-1
3.1.1	Digital Signature	3-1
3.1.2	Installation Directory	3-1
3.1.3	EasyBuilder Pro Version Update	3-2
3.2	SOFTWARE SECURITY SETTINGS	3-3
3.2.1	Enable Secure Communication	3-3
3.2.2	Use Enhanced Security Mode	3-3
3.2.3	Use Strong User Passwords	3-3
3.2.4	Protection of Password Settings	3-4
3.2.5	Enable Automatic Logout	3-4
3.2.6	Time Synchronization via NTP Server	3-5
3.2.7	Object Security	3-5
3.2.8	Operation Logging	3-6
4	RISKS DURING PRODUCT OPERATION	4-1
4.1	LOGIN AUTHORIZATION	4-1
4.2	LOG FILE SECURITY	4-1
4.2.1	Prolonging Flash Memory Lifespan	4-1
4.2.1.1	Recommendations to reduce write speed	4-2
4.2.2	Save or Back Up Logs to External Device	4-2
4.2.2.1	Recommendations for using USB and SD	4-3
4.2.2.2	Recommendations for using a database server	4-3
4.2.3	Enable Checksum for Data Integrity	4-3
5	RISKS DURING REMOTE MAINTENANCE	5-1
5.1	COMMUNICATION SECURITY	5-1
5.1.1	Disable Unnecessary Functions	5-1
5.1.2	Modbus Server	5-1
5.1.3	MQTT	5-2
5.1.4	OPC UA Server	5-3
5.1.5	Database Server	5-3
5.1.6	Email	5-4
5.1.7	cMT Viewer Remote Monitoring	5-4
5.2	WEB PAGE SECURITY	5-5
5.2.1	Enable HTTPS Encryption	5-5
5.2.2	Enable Password Strength Rules	5-5
5.2.3	Enable Password Expiration	5-6
5.2.4	Automatic Lockout after Login Attempts	5-6
5.2.5	Change System Password	5-6

5.3 REGULAR SECURITY MAINTENANCE ACTIVITIES 5-7

6 GUIDELINES FOR SECURE PRODUCT DISPOSAL..... 6-1

6.1 RECOMMENDATIONS FOR SAFE DISPOSAL 6-1

1 INTRODUCTION

1.1 ABOUT THIS DOCUMENT

WEG treats cybersecurity and information security with the utmost seriousness. We recognize the growing need to protect our customers and our operations in an increasingly complex environment. We operate in essential sectors where cyberattacks are not mere inconveniences, as they can impact entire communities and put lives at risk.

This reality drives us to adopt a comprehensive approach to cybersecurity, integrating the protection of our products and services with the strengthening of partnerships with other industry leaders. The development and continuous evolution of our products are guided by recommendations from internationally recognized standards, in order to meet the protection levels required by our customers and the markets in which they operate.

In this way, this manual aims to provide practical guidelines for the secure configuration, commissioning, and operation of HMIs throughout their entire lifecycle, covering everything from the initial phase to continuous operation in the field. The content has been developed with a focus on the cMTx series, considering its specific functionalities and capabilities. Even so, many of the concepts and mechanisms presented here can be applied, in whole or in part, to HMIs of the MT series.

It is important to emphasize that differences in functionalities, supported features, and capabilities may exist between the series. Therefore, it is the user's responsibility to assess the applicability of each recommendation according to the specific HMI model used and to consult the corresponding technical documentation to verify the available characteristics.

It consolidates practical guidance and mitigation measures, with an emphasis on secure HMI configuration, reducing the attack surface, hardening defense mechanisms, and managing cyber risks throughout the equipment's lifecycle, contributing to resilient operation aligned with best security practices in industrial automation systems.

**NOTE!**

The text of this manual was translated from the original portuguese version using artificial intelligence, with technical review performed by WEG.

1.2 IMPORTANT NOTICE ON CYBERSECURITY AND COMMUNICATIONS

WEG HMIs, MT and cMTx models, are capable of connecting to and exchanging information via networks and communication protocols. Although they have been designed and tested to ensure proper operation with other automation systems using the protocols mentioned in this manual, it is essential that the customer understands the responsibilities associated with information and cybersecurity when using this equipment.

Therefore, it is the customer's sole responsibility to adopt defense-in-depth strategies and implement policies and measures to ensure the security of the system as a whole, including the communications sent and received by the equipment. These measures include, but are not limited to, installing firewalls, antivirus and antimalware programs, data encryption, authentication control, and physical access control for users.

WEG and its affiliates are not responsible for damages or losses resulting from cybersecurity breaches, including, but not limited to, unauthorized access, intrusion, leakage and/or theft of data or information, denial of service, or any other form of security breach. The use of this product under conditions for which it was not specifically designed is not recommended and may result in damage to the product, the network, and the automation system.

In this regard, it is essential that the customer understands that external interventions through third-party programs, such as sniffers or programs with similar actions, have the potential to cause interruptions or restrictions in the equipment's functionality.

2 FUNDAMENTAL CONCEPTS OF CYBERSECURITY

2.1 OVERVIEW

In an increasingly digital and interconnected era, industrial infrastructures are becoming heavily dependent on integrated automation devices such as variable frequency drives, programmable logic controllers (PLCs), human-machine interfaces (HMIs), industrial gateways, etc. In this scenario, cybersecurity is no longer optional; it is an essential requirement for the safe, reliable, and continuous operation of systems.

With the constant advance of cyber threats, ever more sophisticated and targeted, traditional purely reactive security approaches have become insufficient. New attack techniques emerge daily, requiring manufacturers, integrators, and industrial operators to adopt proactive and resilient measures to protect their assets.

This growing complexity is leading governments to establish regulations that reinforce resilience, that is, the ability to recover from an attack, adapt to constantly changing threats, and improve defense mechanisms, minimizing impacts and preserving operational continuity. This involves not only implementing robust security measures, but also anticipating and responding effectively to incidents. In this context, adopting a robust cyber resilience strategy is no longer a competitive advantage; it is a critical necessity for business and for the protection of industrial and mission-critical operations.

Several jurisdictions around the world have developed regulations focused on the security of industrial systems. In the United States, the NERC-CIP set of standards establishes rigorous requirements for protecting automation systems in critical facilities. In the European Union, the recently approved Cyber Resilience Act (CRA) imposes direct obligations on manufacturers of digital products, including industrial automation equipment.

These initiatives are grounded in internationally recognized standards and frameworks such as the ISA/IEC 62443 series, the NIST framework, the ISO/IEC 27000 family, as well as specific guidelines like IEC 62351, focused on the security of automation protocols. Adopting these references helps mitigate material risks, strengthen the security of automation devices, and ensure the resilience of industrial operations in the face of complex threats, safeguarding the continuity of essential services and the integrity of the data and systems involved.

2.2 FAR BEYOND IT: THE NEW FRONTIER OF CYBERSECURITY

Traditionally, the term cybersecurity refers to the set of measures adopted to protect computer systems and networks against unauthorized access or malicious attacks. However, when applied to the context of automation and energy technologies, this concept expands significantly. In this scenario, cybersecurity encompasses practices aimed at ensuring the reliability, integrity, and availability of control and automation systems, principles widely known in the information technology (IT) realm by the acronym “CIA” (Confidentiality, Integrity, Availability).

In industrial environments, these measures are essential to prevent a range of risks, such as the leakage of sensitive information, physical damage to equipment or systems, data corruption, and operational disruptions. Such incidents can compromise not only efficiency, but also the safety of critical processes.

In IT, the priority is usually data confidentiality, followed by integrity and, lastly, availability. In Operational Technology (OT), however, this order is reversed: availability is the most important factor, followed by integrity and confidentiality, forming the acronym “AIC.” This is because, in industrial environments, keeping systems running continuously and safely is more critical than protecting information from unauthorized access.

2.3 DEFENSE IN DEPTH

The concept of defense in depth involves more than relying on a single security measure. It consists of implementing security mechanisms at multiple levels to provide robust protection. This approach significantly reduces potential risks, such as information leakage and hacker attacks, enhancing the overall security of products during installation, operation, maintenance, and disposal.

2.3.1 External Environment

The HMI must be installed and operated in industrial environments with secure network infrastructure to prevent unauthorized access. To ensure optimal performance and minimize security risks, follow the recommendations below. The external security structure consists of three main layers:

- Plant security
- Network environment security
- System integration security

2.3.1.1 Plant Security

Ensure the safe use of the HMI through comprehensive system checks.

- Install controlled perimeters with access control in industrial facilities.
- Implement biometric access control or locking systems in laboratories or server rooms.
- Use alarm or video surveillance systems.

2.3.1.2 Network Environment Security

A secure network environment is a controlled configuration in which access is limited to authorized devices, users, and services, preventing unauthorized access, data leaks, and malicious attacks. The product is designed to be used within protected internal networks. Avoid exposing it directly to public networks. If external connectivity is required, implement the following security measures, which help separate internal communication traffic from external traffic.

- Monitor communication between office and factory networks using firewalls.
- Use routers to prevent direct access via public IP.
- If the product has two Ethernet ports, connect:
 - LAN 1 to the external network
 - LAN 2 to internal devices

2.3.1.3 System Integration Security

Ensure that internal protection mechanisms remain effective during system integration.

- Keep systems regularly updated
- Use antivirus
- Implement user authentication

2.3.2 Product Operation

HMI system settings are generally managed by personnel responsible for creating files and system integration. During user operation, it is essential to prevent unauthorized changes to parameters that could disrupt normal operation. Recommended measures:

- Hide system settings
- Change default login passwords
- Use encrypted HTTPS communication on the web configuration page

The HMI includes built-in security features enabled by default, which can be configured as needed to meet installation requirements. This configuration should be performed only by qualified personnel, as incorrect changes can compromise the security of the system and the network.

2.4 GENERAL SECURITY MAINTENANCE

This section provides guidelines and recommendations to ensure product security. It helps users plan and effectively carry out routine information security maintenance tasks.

- Regularly update the product to ensure both software and firmware are always up to date. This includes applications, operating systems, and other components. This practice prevents the exploitation of known vulnerabilities and introduces new security features.
- Conduct routine security vulnerability testing, such as vulnerability scanning and penetration testing. This approach helps identify and remediate potential weaknesses.
- Use the product's monitoring capabilities to oversee its operation, identify abnormal behavior, and track security events. In addition, keep records of all security events for subsequent analysis and investigation.
- Employ appropriate encryption mechanisms for handling sensitive data and communications. This ensures the confidentiality and integrity of data during transmission and storage.
- Develop contingency plans to respond effectively to potential security events and quickly execute response measures. In parallel, establish a vulnerability management process to assess, track, and remediate vulnerabilities periodically.
- If this product grants access to third-party service providers, ensure they follow the same security standards and regularly assess their security posture. Consult international standards for third-party supplier management (for example, ISO 28000 / ISO 27001).

2.5 RISK ANALYSIS AND REPORTING MECHANISM

When using the product, if security-related risks arise, follow the procedure below:

- Conduct risk analysis.
- Consult the product safety manual.
- Evaluate the effectiveness of mitigation measures.
- If the issue cannot be resolved, contact the company's support channels.

3 RISKS DURING PROGRAM EDITING

3.1 INSTALLATION FILE VERIFICATION

3.1.1 Digital Signature

Before installing EasyBuilder Pro, check that the installation file (setup.exe) has a valid digital signature and that it has not been tampered with. Right-click the installer, open the *Digital Signatures* tab, and select *Details* to confirm the integrity of the digital signature. [Figure 3.1](#) shows the installer properties and the digital signature details.

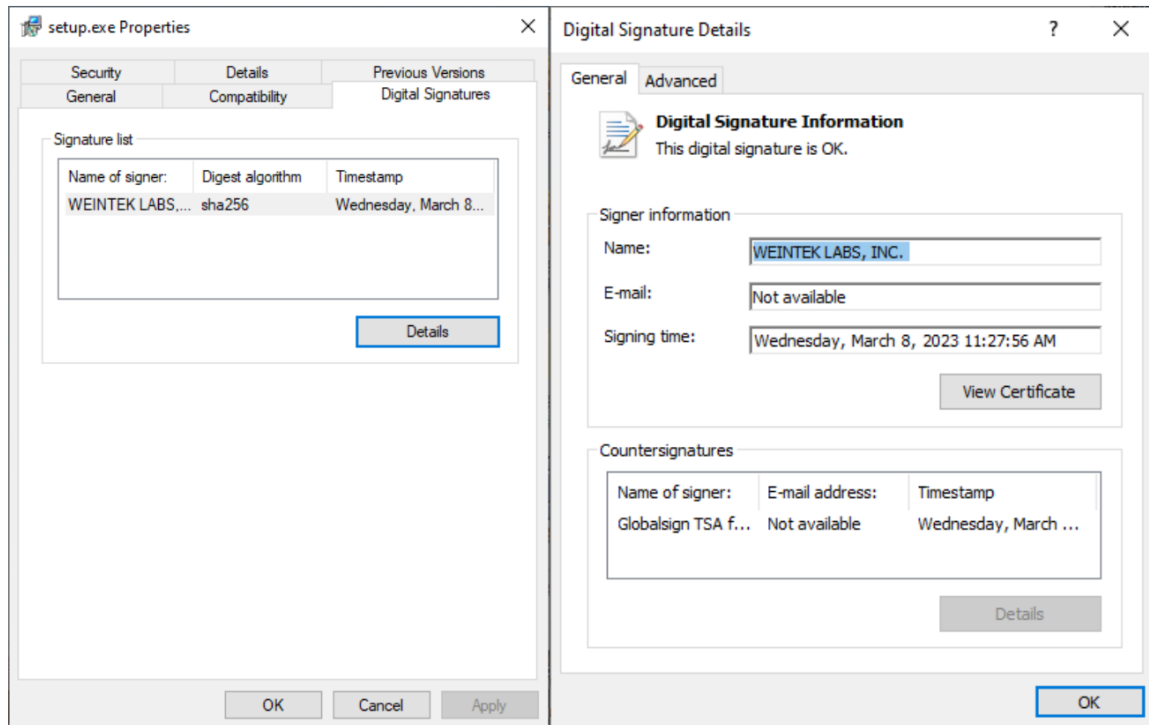


Figure 3.1: Installer digital signature.

3.1.2 Installation Directory

Install EasyBuilder Pro in a folder with restricted access permissions (for example, C:\Program Files (x86)), as shown in [Figure 3.2](#).

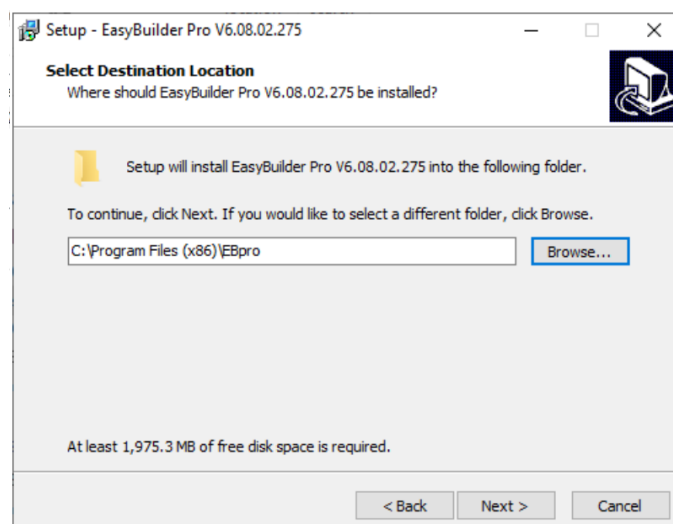


Figure 3.2: Installation directory.

3.1.3 EasyBuilder Pro Version Update

Ensure the software is updated to the latest versions that address security vulnerabilities. To check your current version and look for new updates, open EasyBuilder Pro and click *File* → *About* → *Check for updates...*, as shown in [Figure 3.3](#).

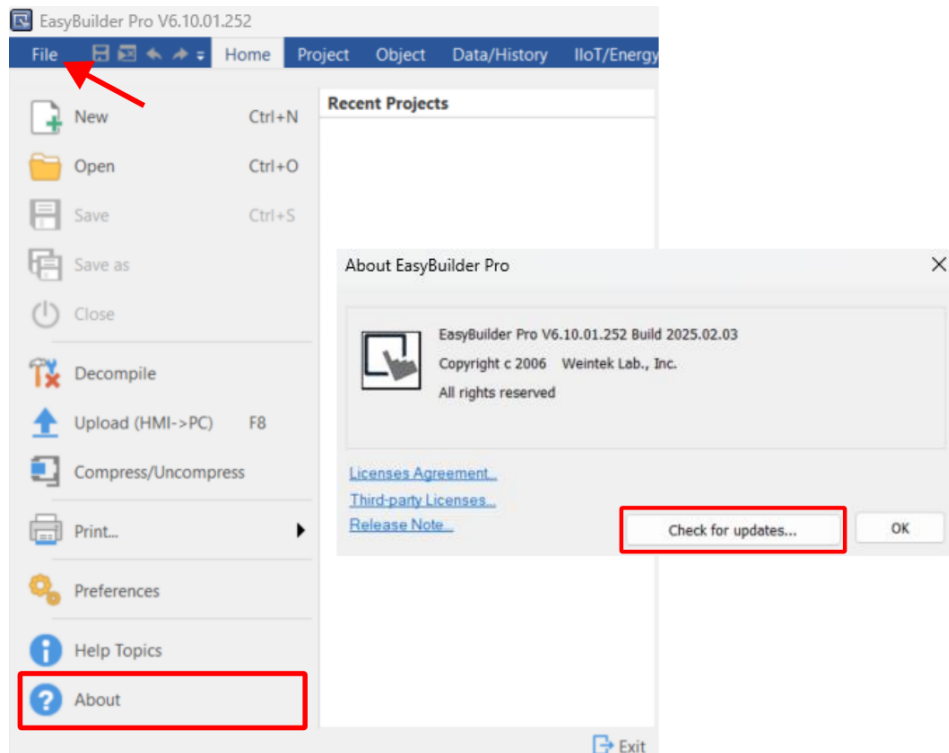


Figure 3.3: Checking the current EasyBuilder Pro version and available updates.

You can enable notifications to be automatically informed of new updates when the program starts. To do this, click *File* → *Preferences* → *Misc* and enable *Notify when new version of EasyBuilder Pro is available*, as shown in [Figure 3.4](#).

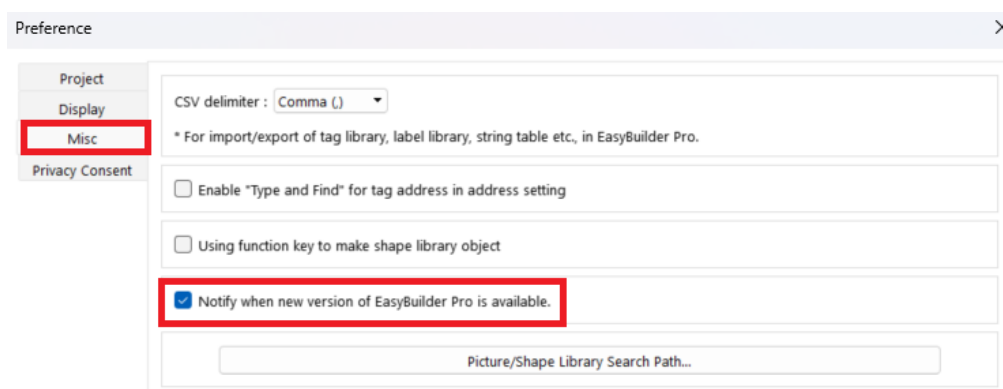


Figure 3.4: Notify when a new version of EasyBuilder Pro is available.

3.2 SOFTWARE SECURITY SETTINGS

3.2.1 Enable Secure Communication

Enable secure communication to ensure that communication between the HMI and other devices is encrypted. In an open project in EasyBuilder Pro, click *Home* → *System Parameters*, open the *Devices* tab, select the HMI, click *Settings/Security*, and enable *Enable secure communication*, as shown in [Figure 3.5](#).

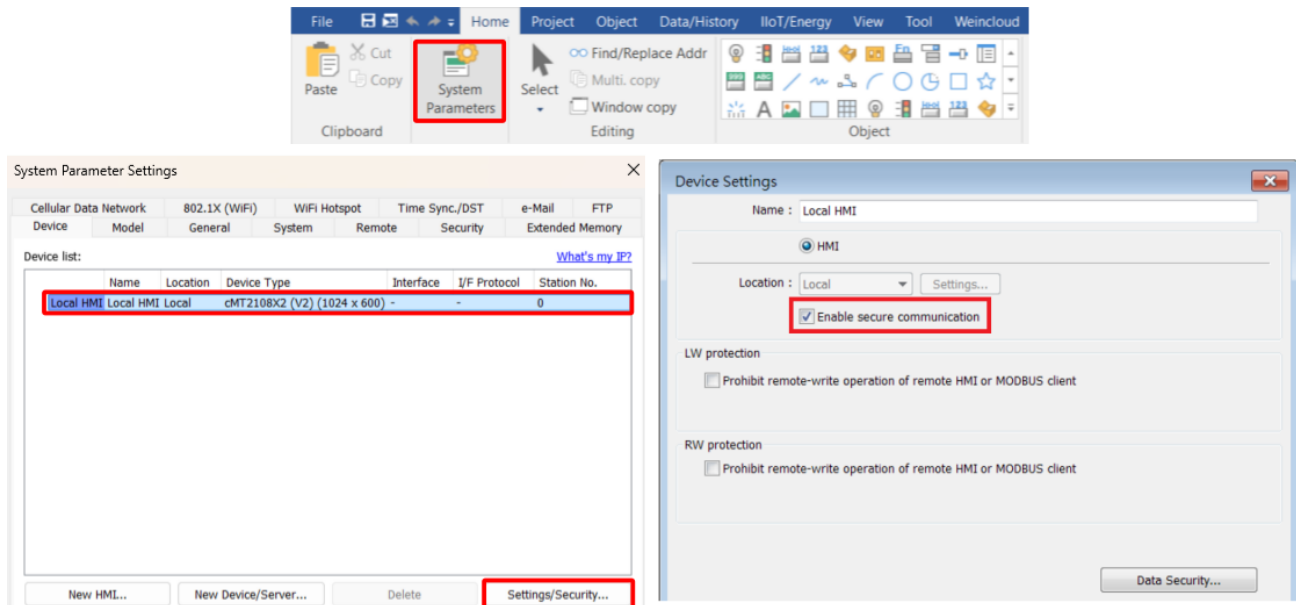


Figure 3.5: Enable secure communication.

3.2.2 Use Enhanced Security Mode

Enhanced security mode is recommended so that designers can assign different privileges to different users and control access to objects. In EasyBuilder Pro, click *Home* → *System Parameters*, open the *Security* tab, and enable *Enhanced security mode*, as demonstrated in [Figure 3.6](#). For detailed settings, refer to the chapter *User Password and Object Security* in the EasyBuilder Pro manual.

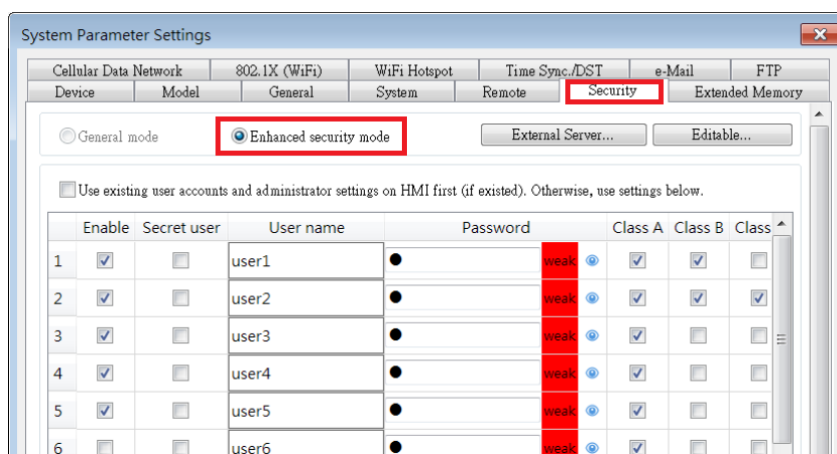


Figure 3.6: Enable enhanced security mode.

3.2.3 Use Strong User Passwords

Strong passwords are less vulnerable to cracking attempts by malicious actors. The robustness of a password is related to the number and diversity of characters used. Among the types of characters that can be employed are:

- Uppercase letters

RISKS DURING PROGRAM EDITING

- Lowercase letters
- Numbers
- Special characters

Password strength classification:

- **Strong:** three or more character types and length equal to or greater than 8 characters.
- **Medium:** at least two character types and length equal to or greater than 6 characters.
- **Weak:** only one character type or length less than 6 characters.

Figure 3.7 shows the strength classification of some example passwords.

	Enable	Secret user	User name	Password		Class A	Class B
1	☒	☐	user1	5A@C4@6B5	strong	☒	☒
2	☒	☐	user2	5AC46B	medium	☒	☒
3	☒	☐	user3	3	weak	☒	☐

Figure 3.7: Examples of password strength classification.

Guidelines for creating strong passwords:

- Use at least eight characters
- Combine uppercase letters, lowercase letters, numbers, and special characters
- Avoid dictionary words
- Avoid keyboard sequences such as 123456 or asdfg
- Avoid repeated characters such as AAAA
- Avoid alphabetical sequences such as ABCD

3.2.4 Protection of Password Settings

Enabling *Read-only* mode prevents unauthorized users from modifying security settings when obtaining the original project file. In this mode:

- Security settings cannot be changed
- Passwords are displayed in masked form
- Administrative access requires the original password

To enable it, go to the *Security* tab, click *Editable*, and configure the *Read-only Settings* options, as shown in Figure 3.8.

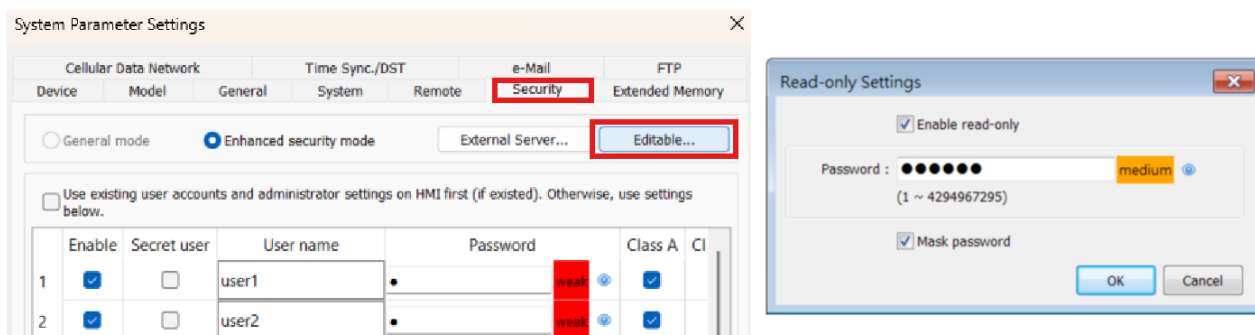


Figure 3.8: Enabling read-only mode.

3.2.5 Enable Automatic Logout

To prevent unauthorized access using open sessions, it is recommended to enable automatic logout on inactive HMIs. In EasyBuilder Pro, click *Home* → *System Parameters* → *System* and enable *Auto logout*. Figure 3.9 shows the screen to enable automatic logout.

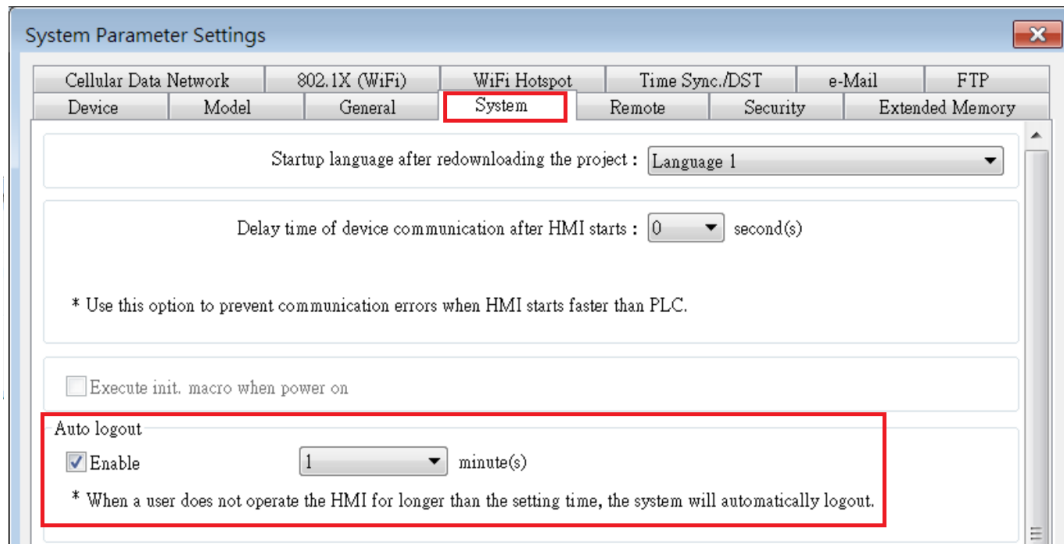


Figure 3.9: Enabling automatic logout.

3.2.6 Time Synchronization via NTP Server

To keep accurate records and logs, it is recommended to regularly synchronize the HMI clock with an NTP server. In EasyBuilder Pro, click *Home* → *System Parameters* → *Time Sync/DST* and enable *Enable time synchronization via NTP server*, as indicated in Figure 3.10.

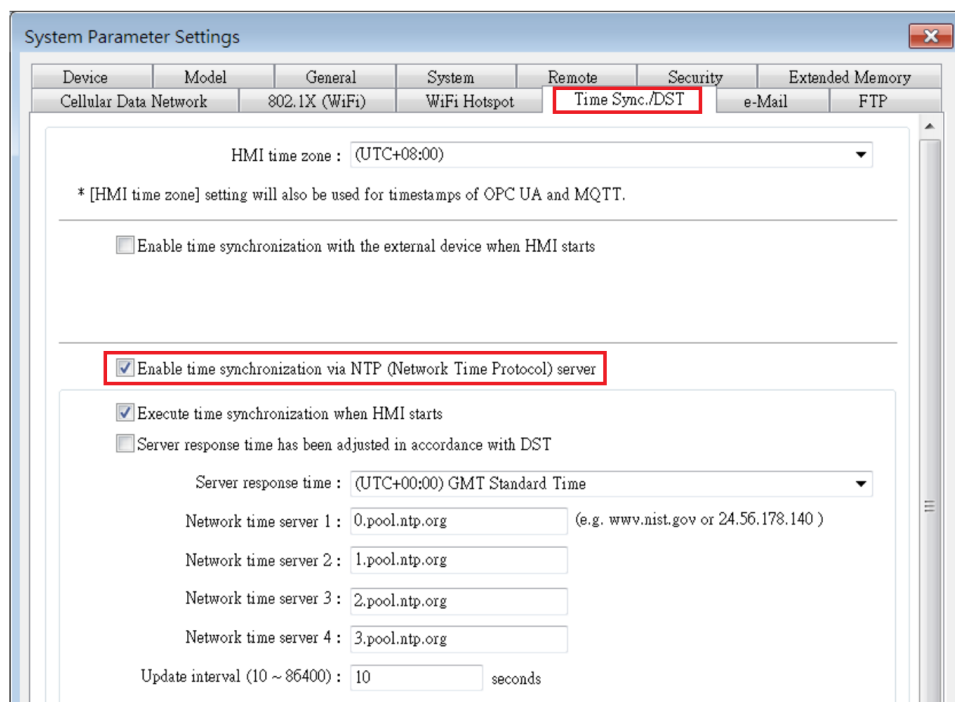


Figure 3.10: Date and time synchronization.

3.2.7 Object Security

The basic operational element of an HMI is the object. It is recommended to enable security control for each operable object, allowing for confirmation before executing commands and restriction based on user permissions. To configure it, create a new object or open the object properties by double-clicking it, then access the *Security* tab. Figure 3.11 shows the screen for configuring object security.

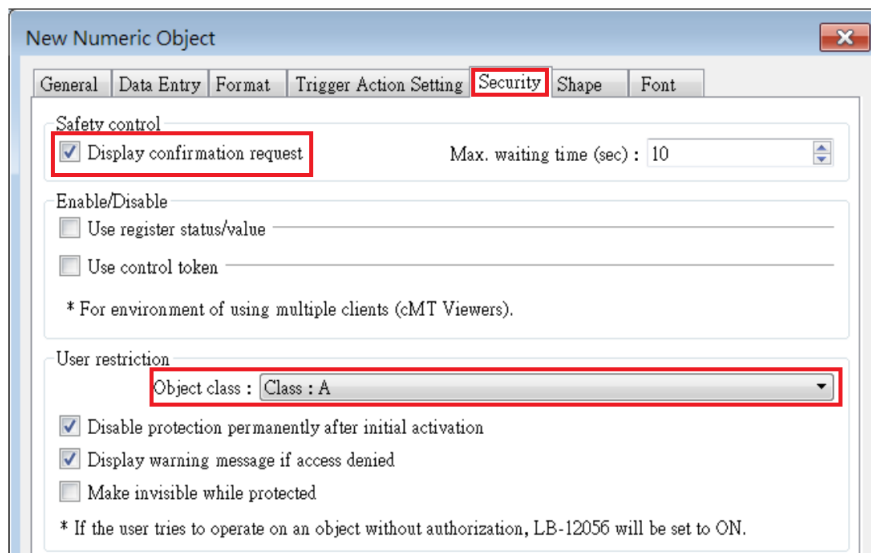


Figure 3.11: Configuring object security.

3.2.8 Operation Logging

Whenever an operation is performed on HMI objects, the *Operation Log* can record information such as:

- Date and time
- User name
- Object class
- Window number
- Object name
- User-defined comments
- Type of action performed
- Memory address
- Changes made

Logs are stored by default in the HMI memory in SQLite database format and can also be copied to external devices such as USB drives. To enable logging, go to *Data/History* → *Operation Log Settings* and configure the objects whose operations will be recorded, as shown in [Figure 3.12](#).



NOTE!

Use the *Object Filter* feature to define which objects should be displayed.



ATTENTION!

Caution is recommended when configuring this page, as incorrect settings may cause data loss. It is also advisable to synchronize logs with external devices if the HMI space is insufficient.

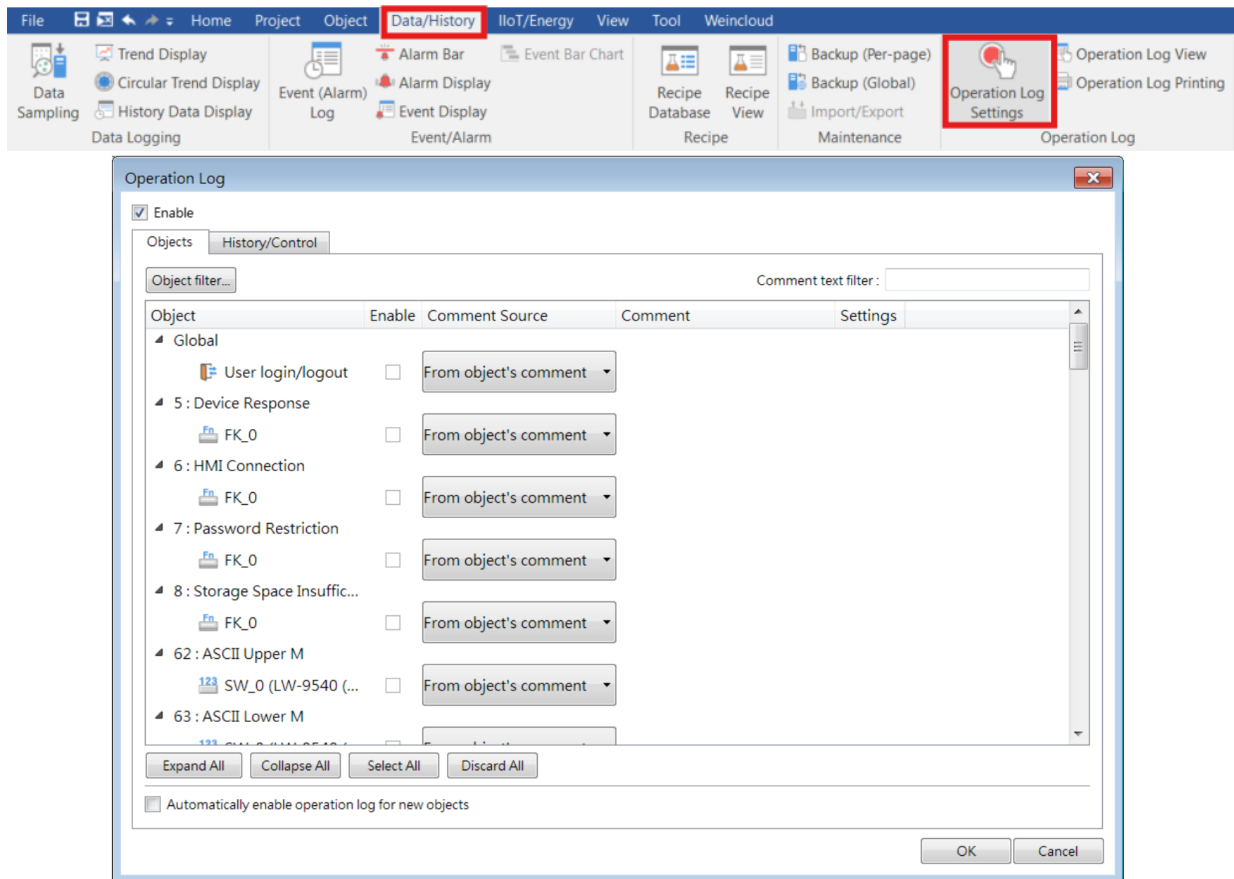


Figure 3.12: Configuring operation logs.

4 RISKS DURING PRODUCT OPERATION

4.1 LOGIN AUTHORIZATION

To access the cMTx series HMI web configuration page, open a browser (such as Edge, Chrome, or Firefox) and enter the device's IP address. If the WebView interface appears after entering the IP, use the address: https://<ihm_ip>/admin to access the EasyWeb 2.0 system parameter login page. Authorization within the system is divided into three levels:

- **Admin:** has the highest authorization level and can modify all settings.
- **Update:** has limited permissions to change settings.
- **History:** has permissions to access log data and its backup.



CYBERSECURITY NOTE!

It is recommended to set distinct passwords for administrators and operators, in order to prevent operator accounts from obtaining administrative privileges.

For security reasons, password confirmation is required before accessing the settings. In addition, access to the *History* section also requires password authentication, allowing stored logs to be viewed. [Figure 4.1](#) shows the system login page.

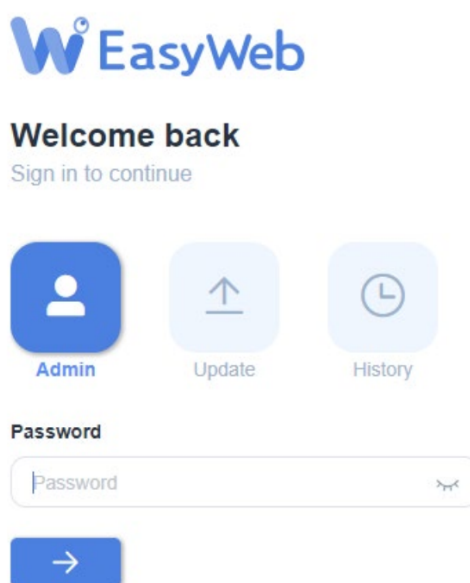


Figure 4.1: System login authorization.

4.2 LOG FILE SECURITY

The security of log files generated by *Data Sampling*, *Event Log*, and *Operation Log* can be enhanced using the measures described in the following sections.

4.2.1 Prolonging Flash Memory Lifespan

Due to the limited number of write cycles of the HMI's internal flash memory, frequent writes or large volumes of data can reduce the memory's lifespan. This can result in:

- Unreadable data
- HMI initialization failure

It is recommended to keep the average write speed to flash memory below 1200 KB/min. This information can be checked in the HMI's system settings, as indicated in [Figure 4.2](#).

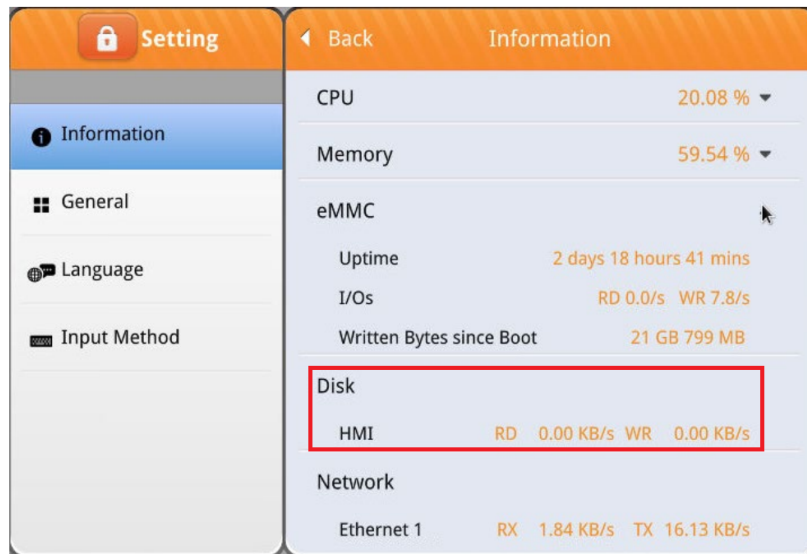


Figure 4.2: Average write speed to flash memory.

4.2.1.1 Recommendations to reduce write speed

Data Sampling

- If logs are not required, disable the option to save logs.
- Set longer sampling intervals.
- Reduce the frequency of sending synchronous commands to control addresses.
- If using customized file handling, reduce the file exchange frequency.
- If using periodic automatic synchronization, increase the synchronization interval.

Event Log

- If logs are not required, disable log storage.
- If not used for alarms, avoid enabling the *Save to history* option.
- Reduce the frequency of sending synchronous commands.
- Use the *Aggregate* mode to limit flash write frequency.

Operation Log

- Reduce the frequency of sending synchronous commands to control addresses.
- Use the *Aggregate* mode to limit write frequency.



NOTE!

Before powering off the HMI, set the system register **LB-9034** to ON to ensure that logs are completely written to flash memory.

4.2.2 Save or Back Up Logs to External Device

It is recommended to save or back up logs to external devices, such as:

- USB drives
- SD cards
- Database servers

This helps prevent data loss when the HMI's storage space is insufficient. [Figure 4.3](#) shows the available storage options for logs and the HMI's global backup.

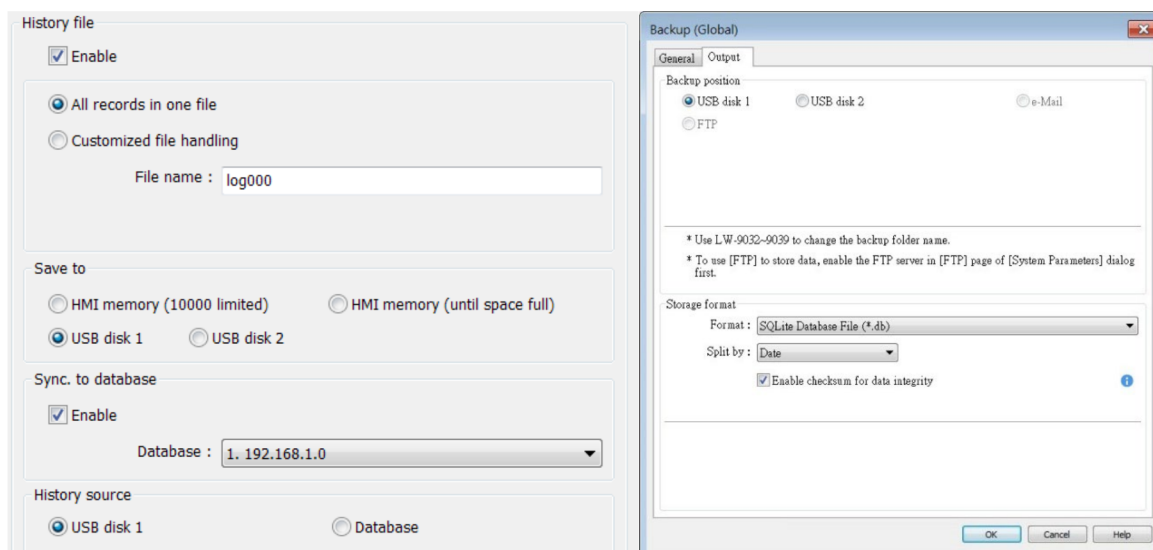


Figure 4.3: Example of log backup.

4.2.2.1 Recommendations for using USB and SD

USB devices and SD cards also have limits on write cycles.

- Use devices with larger capacity (for example, 32 GB).
- Perform periodic remote backups (for example, annually).

4.2.2.2 Recommendations for using a database server

- Enable RAID.
- Perform periodic remote backups.

4.2.3 Enable Checksum for Data Integrity

The *EasyConverter* tool allows opening SQLite files on a computer and viewing backup data, as well as exporting it to Excel or CSV formats. If the backup files contain *checksums*, EasyConverter can verify data integrity. To enable this feature, check *Enable checksum for data integrity* when generating backup files, as indicated in Figure 4.4. This feature is supported only on cMTx series.

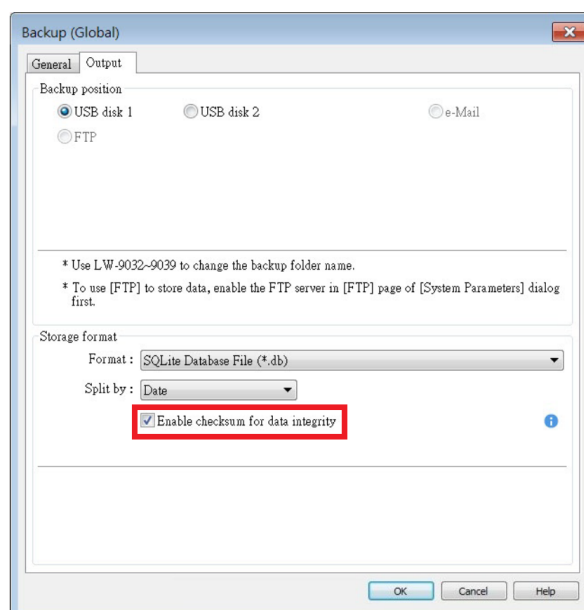


Figure 4.4: Checksum configuration for backup files.

EasyConverter can also verify the integrity of backup files. If any unauthorized modification is detected during verification, an alert will be displayed.

5 RISKS DURING REMOTE MAINTENANCE

5.1 COMMUNICATION SECURITY

5.1.1 Disable Unnecessary Functions

When using an HMI, it is recommended to disable functions that are not being used—or at least protect them with a password. Among the functions that can be disabled are:

- Remote HMI
- PLC Control (change page)
- Modbus Server
- VNC Server
- cMT Diagnoser (cMTx Series)
- OPC UA Server (on some cMTx models)

The HMI's remote access functions, VNC server and cMT Diagnoser, can be enabled and disabled in *System Parameter* → *Remote*, as shown in image [Figure 5.1](#).

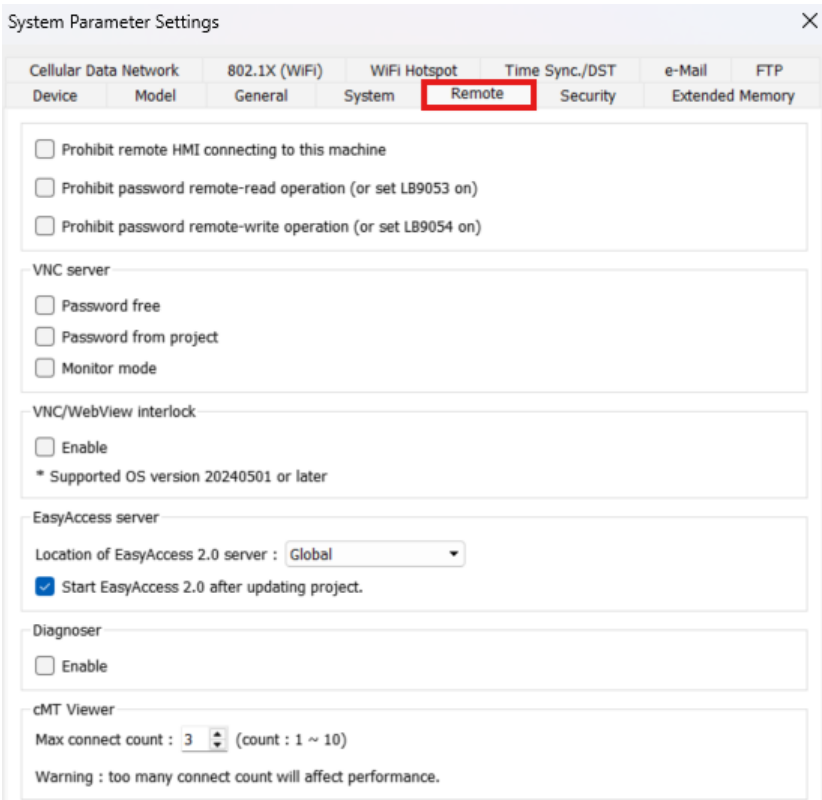


Figure 5.1: HMI remote access options.

5.1.2 Modbus Server

When a Modbus server is used in an HMI project, go to *System Parameters* → *Device* → *Settings/Security*. Enable the *LW Protection* and *RW Protection* options, as demonstrated in [Figure 5.2](#). This prevents unintentional changes to system registers during communication between the HMI and Modbus clients.



NOTE!

To configure the protected LW or RW range, refer to the range supported by the system parameters.

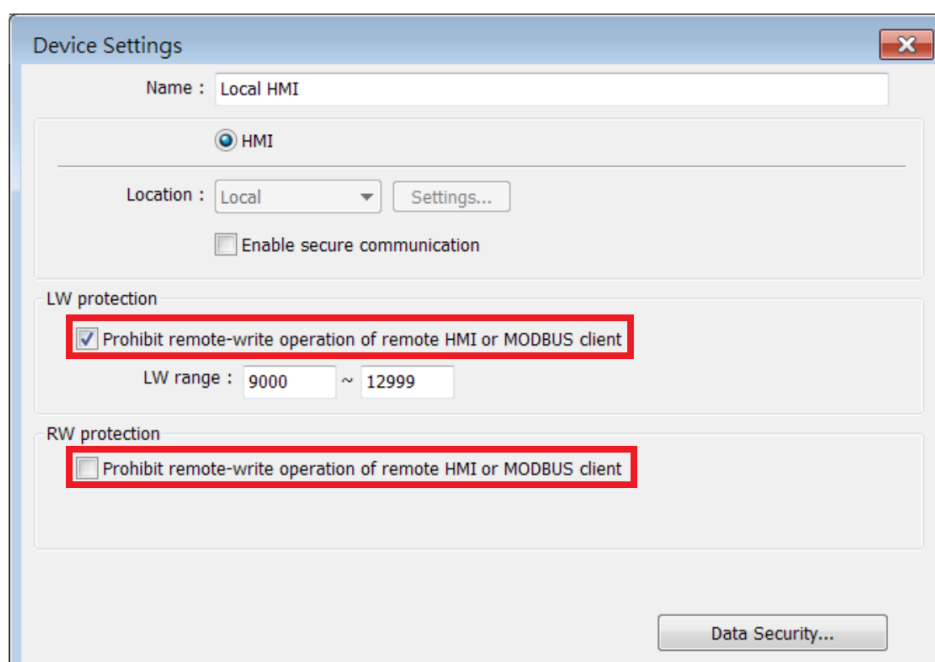


Figure 5.2: LW protection configuration for Modbus communication.

5.1.3 MQTT

When MQTT is used in an HMI project, it is recommended to use TLS 1.2 encryption. It is also necessary to import:

- Certificate Authority (CA) certificate
- Client certificate
- Private key

In the MQTT Server object settings, enable encryption and verification on the *TLS/SSL* tab, as indicated in Figure 5.3.

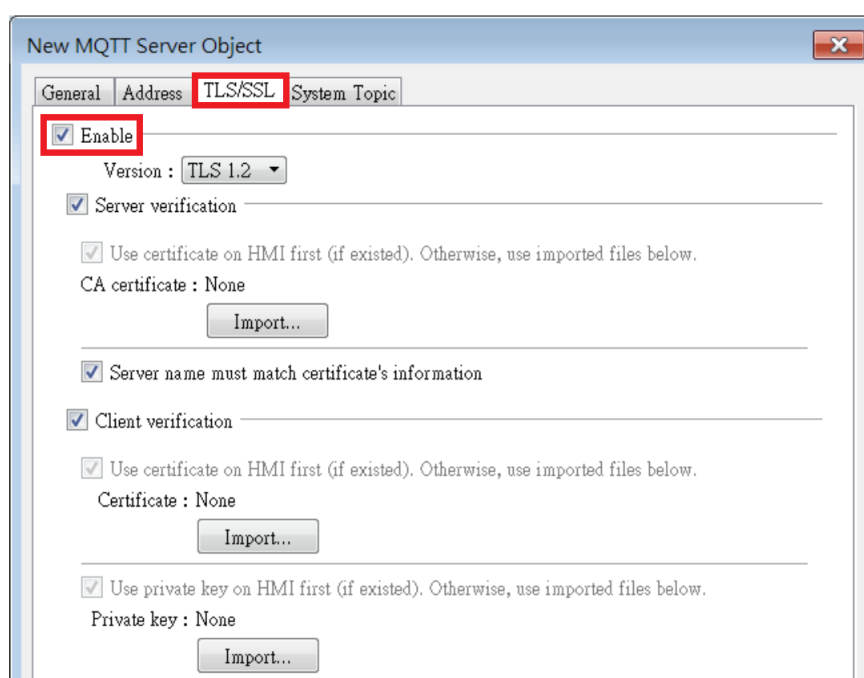


Figure 5.3: TLS/SSL encryption settings for MQTT.

5.1.4 OPC UA Server

If an OPC UA server is used in the HMI project, it is recommended to disable plaintext communication and use only encrypted communication. In the *General* tab of the OPC UA server settings, *disable* the *None* option in the security policy, as shown in [Figure 5.4](#). This ensures that clients communicate only with encrypted data.

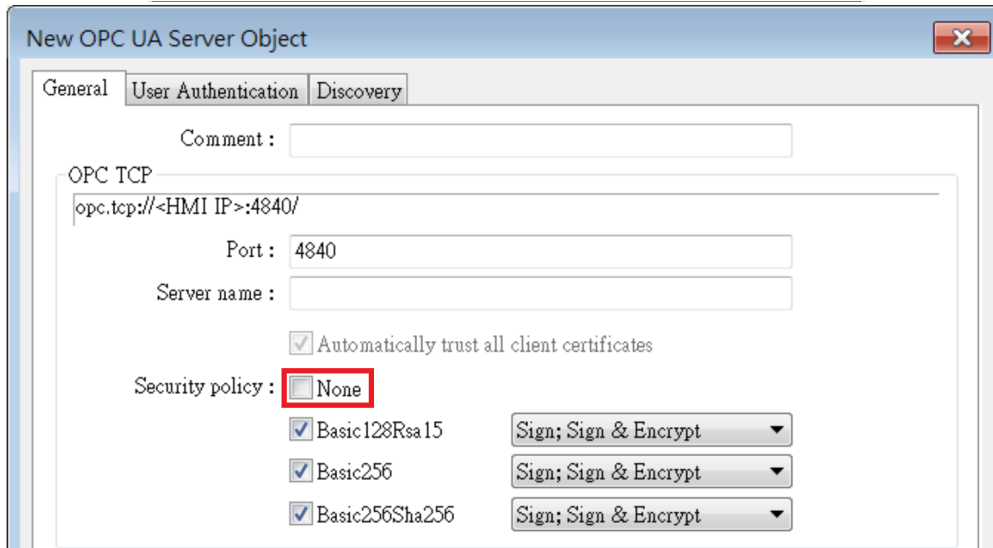


Figure 5.4: OPC UA server security policy configuration.



CYBERSECURITY NOTE!

The Basic128Rsa15 and Basic256 security policies are no longer considered secure due to the SHA-1 hash algorithm. These policies are supported for compatibility purposes only.

5.1.5 Database Server

When a database server is used in a project with an HMI, it is recommended to enable TLS 1.2 encryption. The Certificate Authority (CA) certificate should also be imported. In the Database Server object settings, enable encryption and verification on the *TLS/SSL* tab, as shown in [Figure 5.5](#).

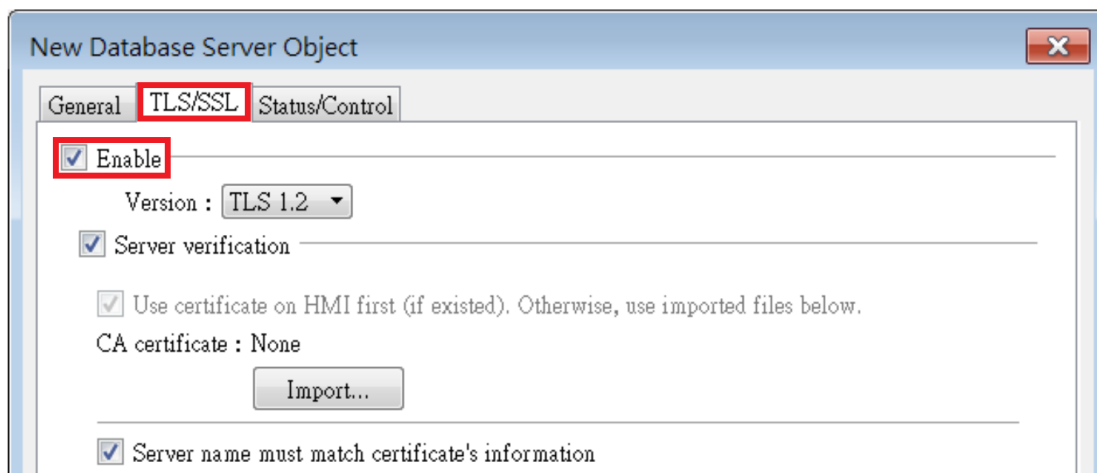


Figure 5.5: TLS/SSL encryption configuration for database server.

RISKS DURING REMOTE MAINTENANCE

5.1.6 Email

When the email sending feature is used in the HMI project, it is recommended to:

- Use an SMTP server that requires authentication
- Use a TLS/SSL encrypted connection

After enabling the email function in the system settings, check the options *SMTP server requires authentication* and *Use the following type of encrypted connection*, as in [Figure 5.6](#).

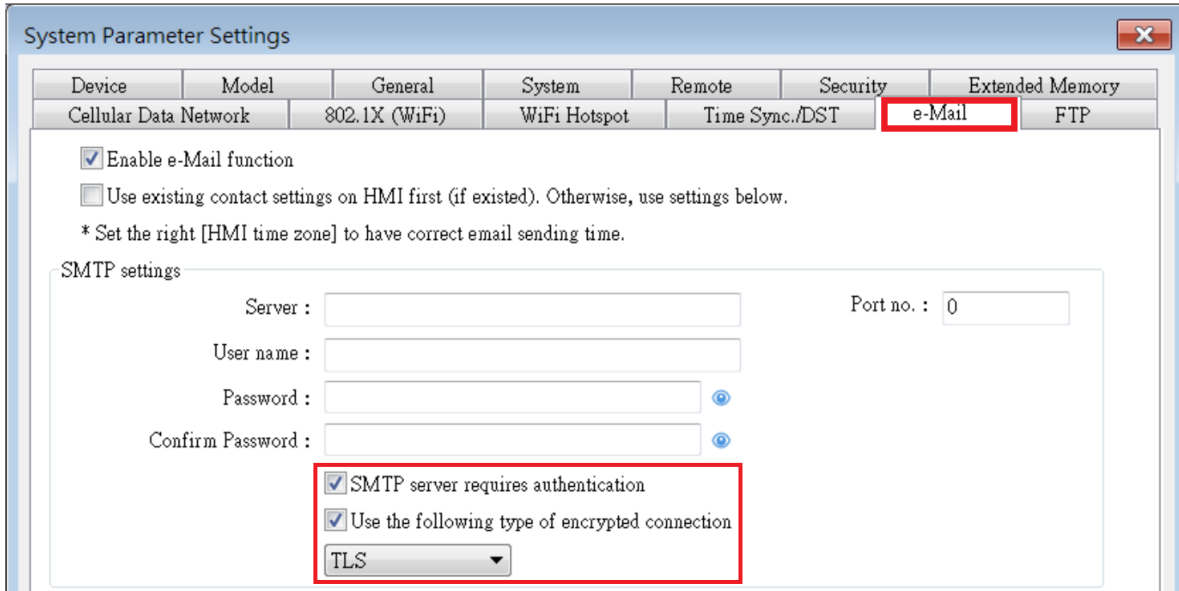


Figure 5.6: Encryption configuration for sending emails.

5.1.7 cMT Viewer Remote Monitoring

If remote monitoring of cMTx series HMIs is required, the *cMT Viewer* application can be used. It is recommended to configure passwords for different permission levels in the HMI system settings, as shown in [Figure 5.7](#). These same passwords must be used in cMT Viewer to access the screens.



Figure 5.7: System password configuration for remote access.



NOTE!

The maximum number of simultaneous HMI accesses via *cMT Viewer* can be limited in *System Parameters* → *Remote*, as shown in [Figure 5.1](#).

5.2 WEB PAGE SECURITY

When an HMI from the cMTx series is used, the user can access the EasyWeb 2.0 interface through a browser. In this interface it is possible to:

- Configure the network IP address
- Upload or download projects
- Perform data backup

Because these features involve critical operations, it is recommended to apply the following security settings.

5.2.1 Enable HTTPS Encryption

It is recommended to enable encrypted HTTPS communication. After accessing EasyWeb 2.0, open the *Administration* menu, go to the *Security* page, and enable the *Force HTTPS* option, as shown in [Figure 5.8](#).

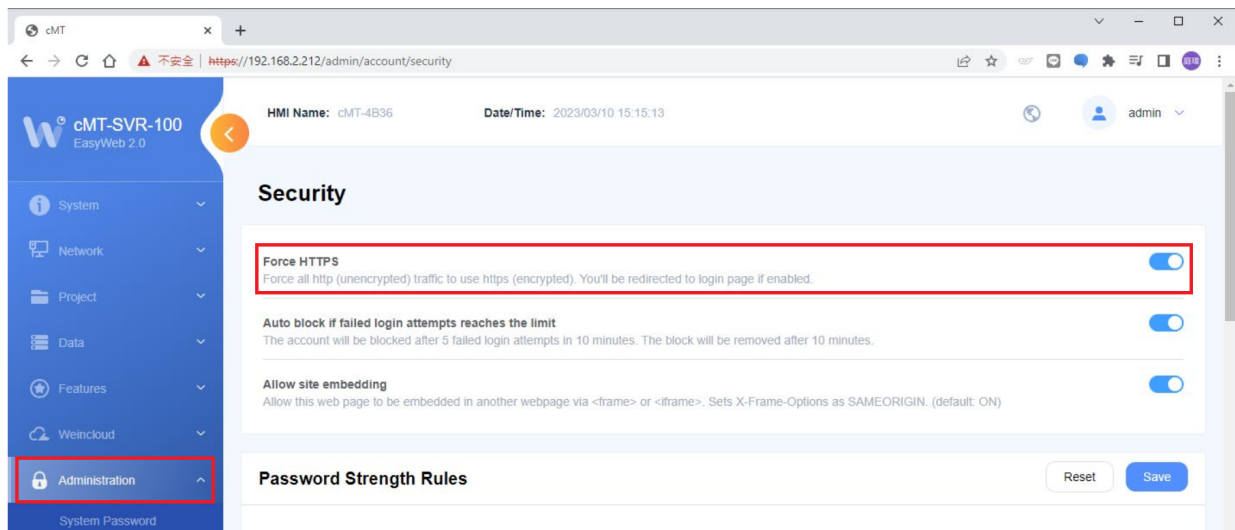


Figure 5.8: Setting to force the use of HTTPS.

5.2.2 Enable Password Strength Rules

It is recommended to enable password strength rules to enforce requirements for:

- Minimum length
- Use of uppercase and lowercase letters
- Numbers
- Special characters

In the *Password Strength Rules* section, configure the options highlighted in [Figure 5.9](#) and click *Save*.

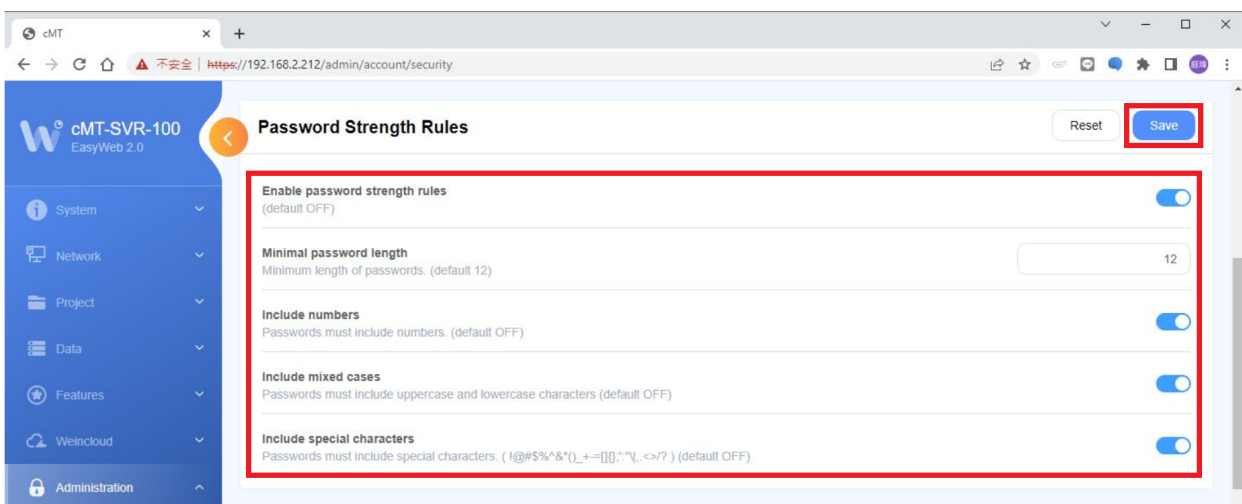


Figure 5.9: Password strength rules configuration.

RISKS DURING REMOTE MAINTENANCE

5.2.3 Enable Password Expiration

It is recommended to enable password expiration to require periodic credential updates. In the *Password Expiration* section, set the number of days for password validity, as indicated in [Figure 5.10](#), and click Save.

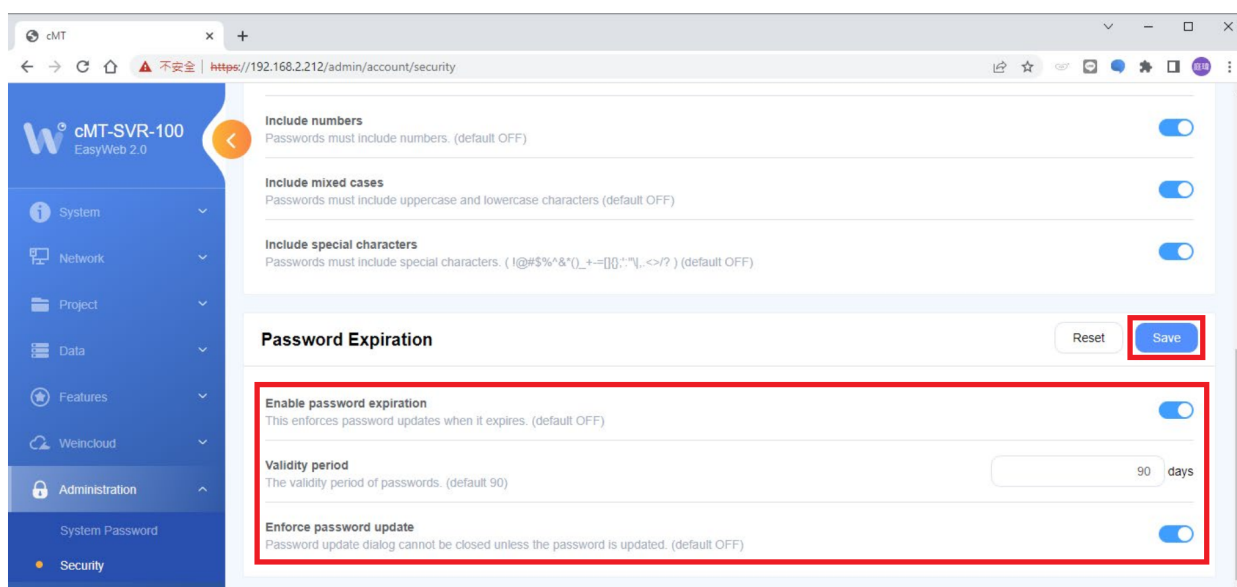


Figure 5.10: Password expiration configuration.

5.2.4 Automatic Lockout after Login Attempts

It is recommended to enable automatic lockout when multiple login attempts with the wrong password occur. When this option is enabled, the system is locked after 5 consecutive invalid login attempts, and the lockout remains active for approximately 10 minutes. The setting can be configured on the *Security* page of the *Administration* menu, as shown in [Figure 5.11](#).

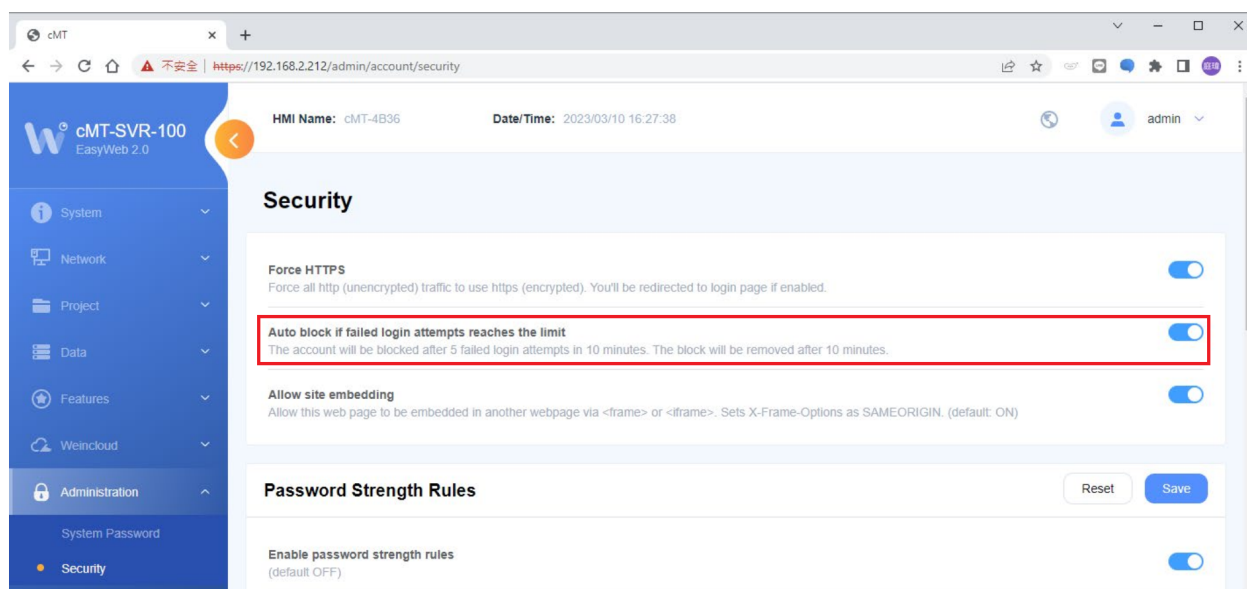


Figure 5.11: Automatic lockout configuration after failed logins.

5.2.5 Change System Password

After configuring the web interface security options, it is recommended to change the system password to a stronger one. To change it, go to *Administration*, open the *System Password* page, and set the new password, as shown in [Figure 5.12](#).

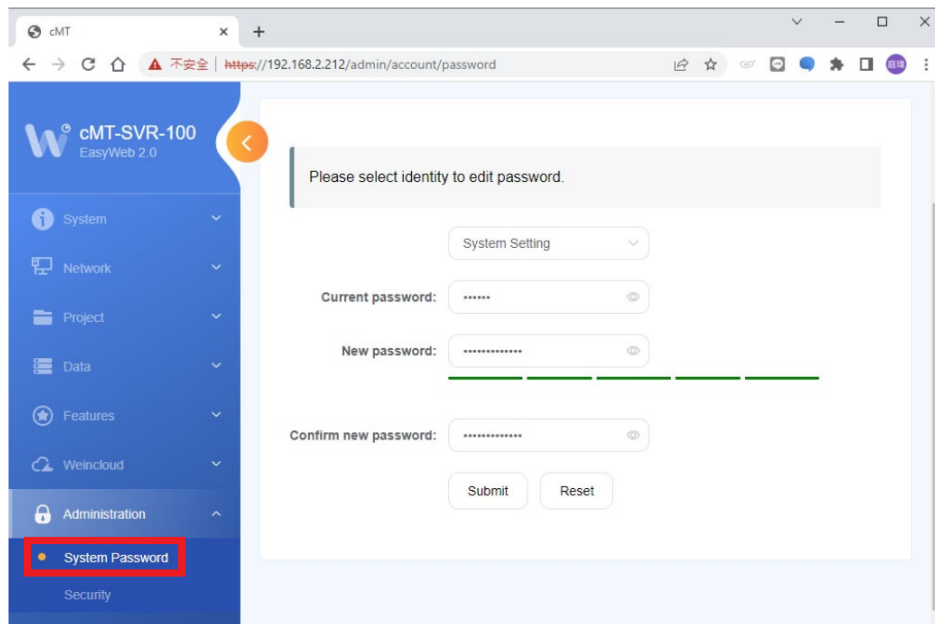


Figure 5.12: System password change configuration.

5.3 REGULAR SECURITY MAINTENANCE ACTIVITIES

Carrying out regular information security maintenance activities is essential to maintain ongoing protection of the system and data. Recommended practices include:

- Regular software updates to ensure operating systems, applications, and firmware are up to date with the latest security patches.
- Periodic password changes using robust combinations of letters, numbers, and special characters.
- Performing regular data backups and storing them in secure locations.
- Hardening firewalls and intrusion prevention systems.
- Performing periodic vulnerability scans and security tests.
- Periodically reviewing access permissions to ensure that only authorized users have access to sensitive resources.
- Regularly monitoring system and application logs to detect incidents or abnormal behavior.
- Conducting internal or external security audits to verify compliance with best practices and security standards.

6 GUIDELINES FOR SECURE PRODUCT DISPOSAL

This section describes procedures for the secure disposal of the product in order to avoid information security issues, such as leakage of sensitive data, when an HMI product is taken out of operation or decommissioned.

6.1 RECOMMENDATIONS FOR SAFE DISPOSAL

When permanently decommissioning an HMI, it is recommended to follow the practices below to ensure that information stored on the device is not exposed.

- Remove the HMI from the equipment or system without causing physical damage to the device.
- Completely erase programs and configuration data stored on the HMI by performing a system reset.
- Securely delete logs stored both on the HMI and on external storage devices.
- Perform secure physical disposal of the equipment—if necessary through physical destruction—to prevent potential leakage of data that cannot be completely removed from the device.



BRAZIL

WEG DRIVES & CONTROLS - AUTOMAÇÃO LTDA.

Av. Prefeito Waldemar Grubba, 3000

89256-900 - Jaraguá do Sul - SC

Phone: 55 (47) 3276-4000

Fax: 55 (47) 3276-4060

www.weg.net