Product Security User Manual

UM024004E_20241004

1. Security Guidelines

1.1. The Aim of this Manual

This manual aims to ensure the secure and proper installation, operation, maintenance, and decommissioning of the HMI and its associated software. Drawing reference from the IEC 62443-4-1 standard, it enumerates security reinforcement mechanisms relevant to configuration and project design that users might encounter while utilizing the HMI. Users are strongly encouraged to follow the procedural steps outlined in this manual to establish the highest level of security precautions prior to actual application operation. Furthermore, it is advised to sustain continuous maintenance during operation, ensuring that the application remains unaffected by negative influences until the secure decommissioning of the product.
Note: SG-X in the document represents the corresponding IEC62443-4-1 SG guidelines.

1.2. The Structure of this Manual

This manual provides an in-depth exploration of security considerations across various topics, delving into their safety aspects. These topics span different stages, from the initial configuration to software and hardware setup, and ultimately conclude with product end-of-life disposal.

- Initial Configuration: Minimizing and preventing operations during the configuration process to the greatest extent.
- Program Editing: Risks within the program editing software during programming.
- Product Operation: Managing permissions for administrators and operators during product operation.
- Remote Maintenance: Preventing unnecessary remote access through appropriate protective measures during maintenance.
- Hardware-related: External storage devices.
- Product End-of-Life: Guidelines for secure product decommissioning.

1.3. Defense in Depth

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

1.3.1. External Environment (SG-2/SG-3a)

As depicted in the illustration, the three primary lines of defense for ensuring product security within the external environment encompass plant security, followed by network security, and concluding with system integrity. Each of these areas is detailed below:

Plant Security

Ensure secure utilization of the HMI through comprehensive system checks.

- Install gated perimeters with access control in campus or factory premises.
- Implement biometric access control or locking mechanisms in laboratories or server rooms.
- Deploy alarm systems or video surveillance for enhanced monitoring.

Network Environment Security

To safeguard network communication from potential penetrations, it is important to simplify the network environment.

- Supervise the communication interface between the office and factory networks, using measures such as firewalls.
- Position network communication under routers to prevent direct access to products via public IP.
- If the products have two Ethernet ports, it is recommended to connect LAN 1 to the external network and LAN 2 to internal devices. This ensures that communication data remains segregated from external network connections.

System Integration Security

Ensure that internal protection mechanisms remain effective during system integration, including antivirus software and whitelisting.

- Maintain and update on a regular basis.
- Implement user authentication for factories or HMI operators.

1.3.2. Product Operation (SG-1/SG-3c)

The system configurations of the HMI are usually managed by personnel responsible for creating files and integrating systems. During user operation, it's crucial to prevent unauthorized modifications to parameters that could disrupt normal usage. Therefore, it's generally advisable to take the following measures:

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

1.4. General Security Maintenance (SG-3h)

This section provides guidelines and recommendations for ensuring product security. It assists users in planning and executing routine information security maintenance tasks

effectively.

- Regularly update product versions to ensure that both software and firmware are kept up-to-date. This includes applications, operating systems, and more. This practice prevents the exploitation of known vulnerabilities and introduces new security features.
- Conduct routine tests for security vulnerabilities, such as vulnerability scanning and penetration testing, to uphold product security. This approach aids in identifying and addressing potential weaknesses.
- Utilize the product's monitoring capabilities to oversee its operation, identify abnormal behavior, and track security events. Moreover, retain all records of security events for subsequent analysis and investigation.
- Deploy suitable encryption mechanisms for handling sensitive data and communications. This guarantees the confidentiality and integrity of data during transmission and storage.
- Formulate contingency plans to effectively address possible security events and execute responsive measures swiftly. Concurrently, establish a vulnerability management process to periodically assess, track, and rectify vulnerabilities.
- If this product grants access to outsourced service providers, ensure their adherence to the same security standards and regularly assess their security posture. Refer to international standards for managing outsourced suppliers (e.g. ISO 28000 / ISO 27001).

1.5. Risk Analysis and Reporting Mechanism (SG-3g)

When using the product, if any security-related risks arise, please adhere to the following process and strive to reinforce product security to meet risk management requirements.

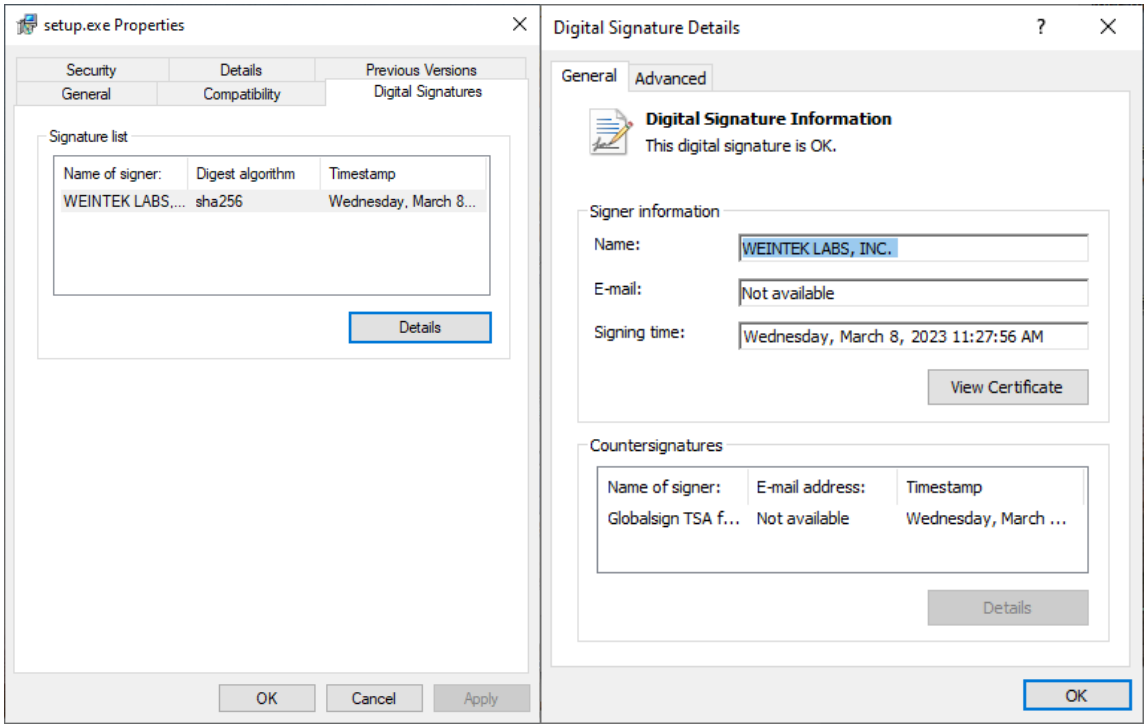
- Conduct a risk analysis.
- Refer to the product security user manual.
- Evaluate the effectiveness of risk mitigation.
- If you are unable to resolve the issue independently, please report it using the provided URL address.

2. Risks within Program Editing

2.1. Installation File Verification

2.1.1. Digital Signature

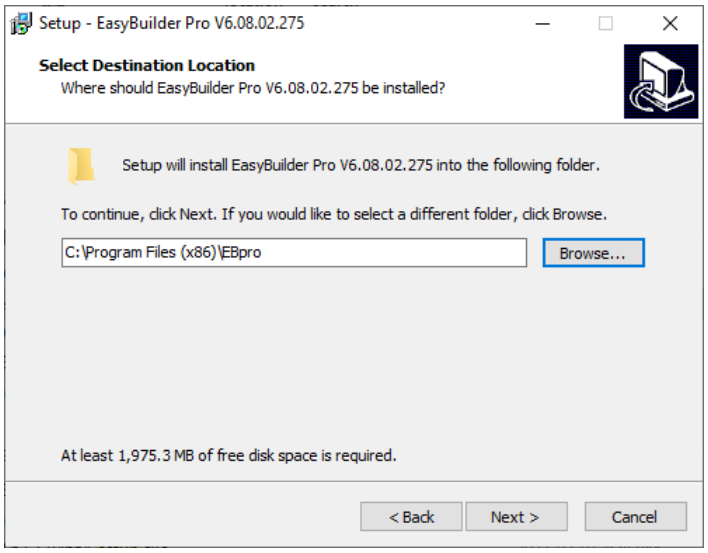
Before installing EasyBuilder Pro, please verify whether the installation file (setup.exe) has a valid digital signature and that the signature has not been tampered with. Right-click on the installation file, go to Digital Signatures tab, and click on [Details] to confirm the integrity of the digital signature.



Digital Signature

2.1.2. Installation Directory

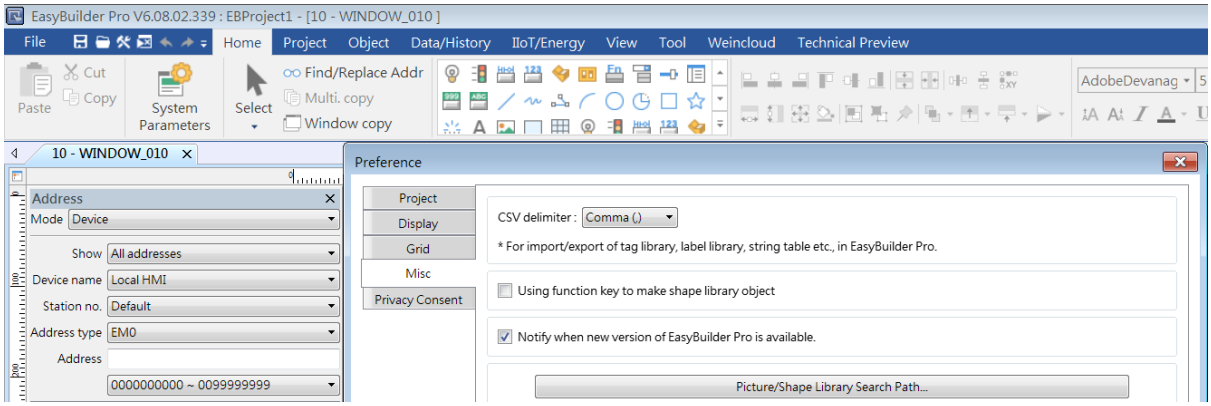
Install EasyBuilder Pro to a folder with restricted access permissions (e.g., C:\Program Files (x86)).



Installation Directory

2.1.3. Enable Automatic Updates

Enable automatic updates for EasyBuilder Pro to ensure that it promptly upgrades to new versions that address security issues. In EasyBuilder Pro, click [File] » [Preferences], open [Misc] tab, and then select [Notify when new version of EasyBuilder Pro is available] option.

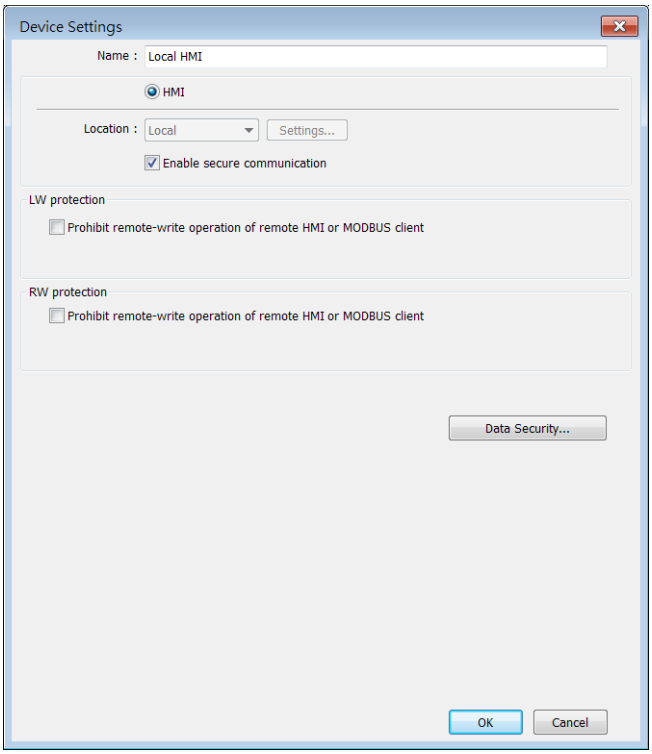


Notify when new version of EasyBuilder Pro is available

2.2. Software Security Settings (SG-3d)

2.2.1. Enable Secure Communication

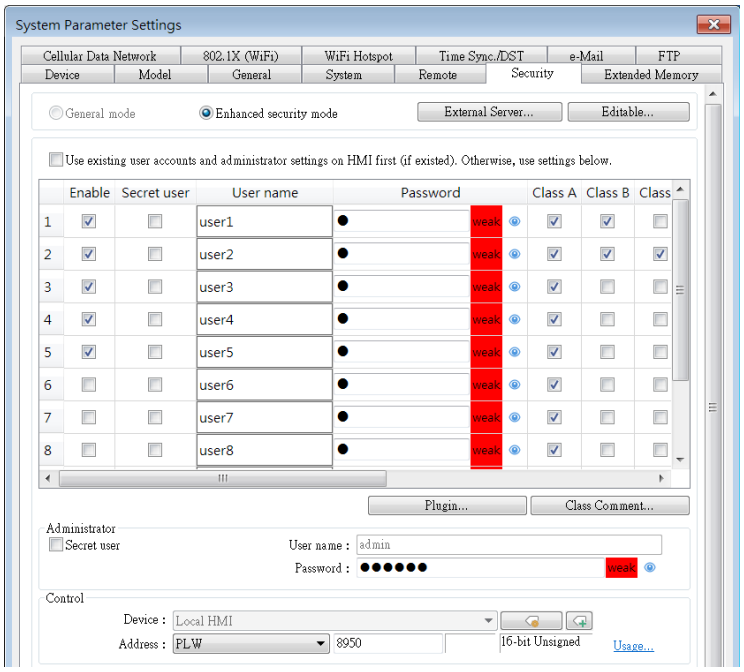
Enable secure communication to ensure that communication between the HMI and other devices is encrypted. In EasyBuilder Pro, click [Home] » [System Parameters], open [Devices] tab, select the HMI, click [Settings/Security] button, and then select [Enable secure communication] as shown below.



Enable secure communication

2.2.2. Use Enhanced Security Mode (SG-6)

Enhanced security mode is recommended for project designers to assign different privileges for different users in order to control access to objects. In EasyBuilder Pro, click [Home] » [System Parameters], open [Security] tab, and then select [Enhanced security mode], as shown below. For detailed settings, please see Chapter 10 User Password and Object Security in EasyBuilder Pro user manual.



Enhanced security mode

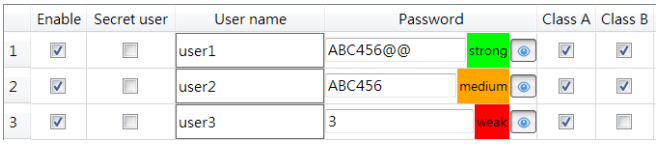
2.2.3. Use Strong User Password

Stronger passwords are less vulnerable to malicious cracking attempts. When setting up a user password, the system provides an indication of its strength through colors and labels. Password strength is determined based on four types of characters: uppercase letters, lowercase letters, numbers, and special characters. The strength is classified as follows:

Strong: Contains three or more types of the above characters and has a length greater than 8 characters. (Please refer to the guidelines below)

Medium: Contains at least two types of the above characters and has a length greater than 6 characters.

Weak: Contains only one type of the above characters or has a length of less than 6 characters.



User password strength

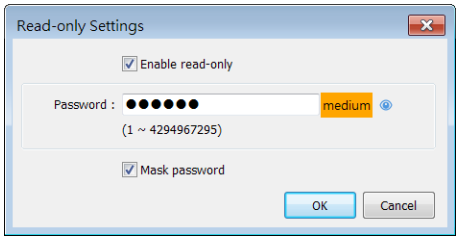
Guidelines: What constitutes a strong password?

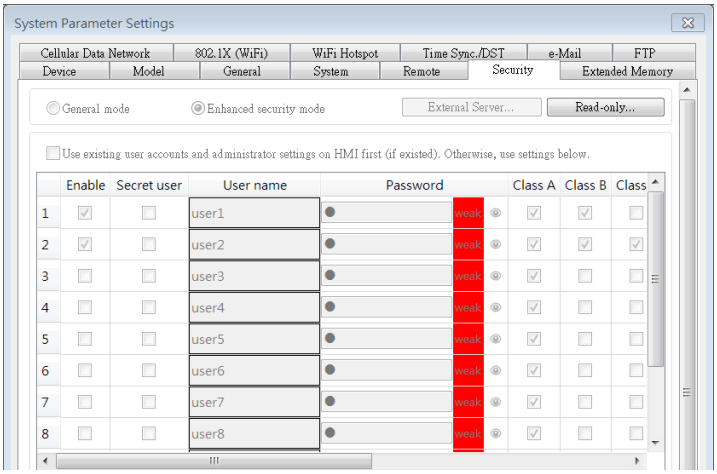
A strong password should:

- Consist of a minimum of eight characters.
- Include a combination of lowercase and uppercase letters, numbers and special characters.
- Whenever possible, not be a word listed in the dictionary (e.g., Mouse)
- Not consist of characters that are adjacent on the keyboard (e.g., 123456 or asdfg).
- Not contain repeating characters (e.g., AAAA).

2.2.4. User Password Settings Protection

Enabling the "Read-only" mode prevents unauthorized users from making security settings when obtaining the original project file from others. In Read-only mode, security settings cannot be changed, and passwords are displayed in masked form to prevent password leakage. To regain administrative privileges, the original password must be used. In the [Security] tab, select [Editable] to enter [Read-only Settings], and enable Read-only mode to protect user password information from being viewed by unauthorized individuals.

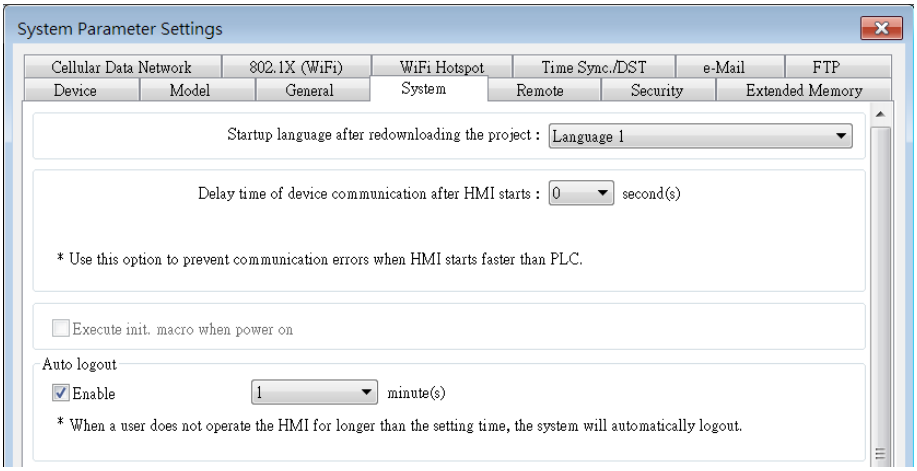




Read-only mode

2.2.5. Enable Auto. Logout

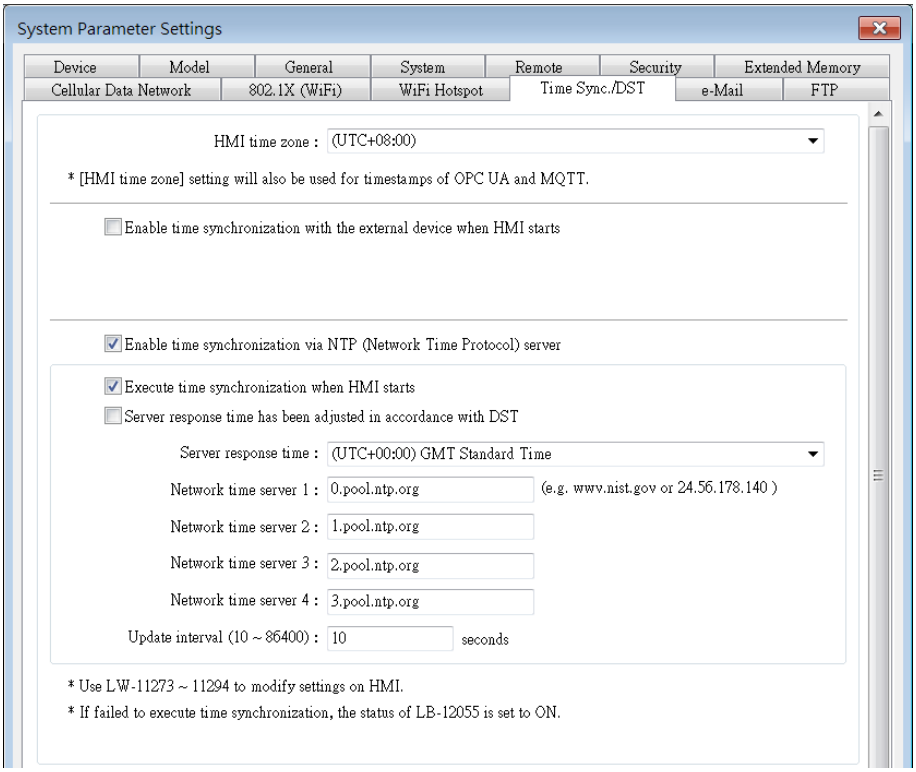
To prevent unauthorized access to previous user privileges, it is recommended to enable automatic logout for idle HMIs in EasyBuilder Pro. This feature automatically logs out the user after a period of inactivity. To enable this feature, simply go to [Home] » [System Parameters], open the [System] tab, and enable [Auto logout].



Auto logout

2.2.6. Enable Time Synchronization via NTP Server

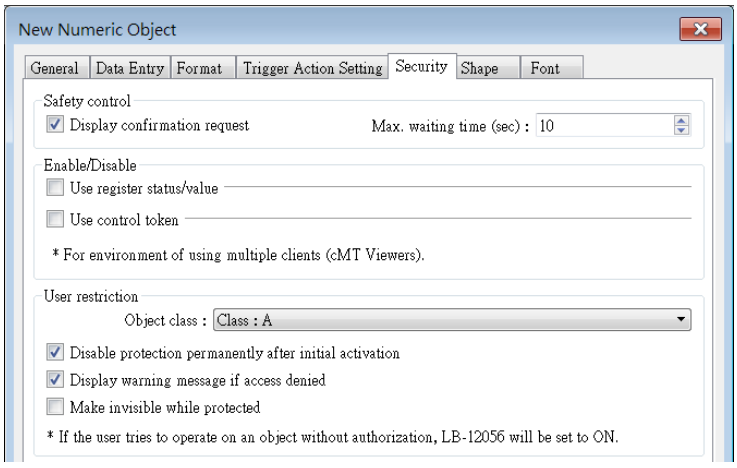
To ensure accurate timekeeping, it is recommended to regularly synchronize the time of the HMI with an NTP server. In EasyBuilder Pro, click [Home] » [System Parameters], go to the [Time Sync/DST] tab, select the [Enable time synchronization via NTP (Network Time Protocol) server] option, as shown below.



Time synchronization

2.2.7. Object Security

The basic operational element of an HMI is an object. It is recommended for users to enable security control for each operable object, which provides a confirmation function before actual command issuance. Additionally, object control can be implemented in conjunction with user password permission functionality. To enable safety control and user restriction for objects, access the object's properties and click on the [Security] tab, as shown in the example below.

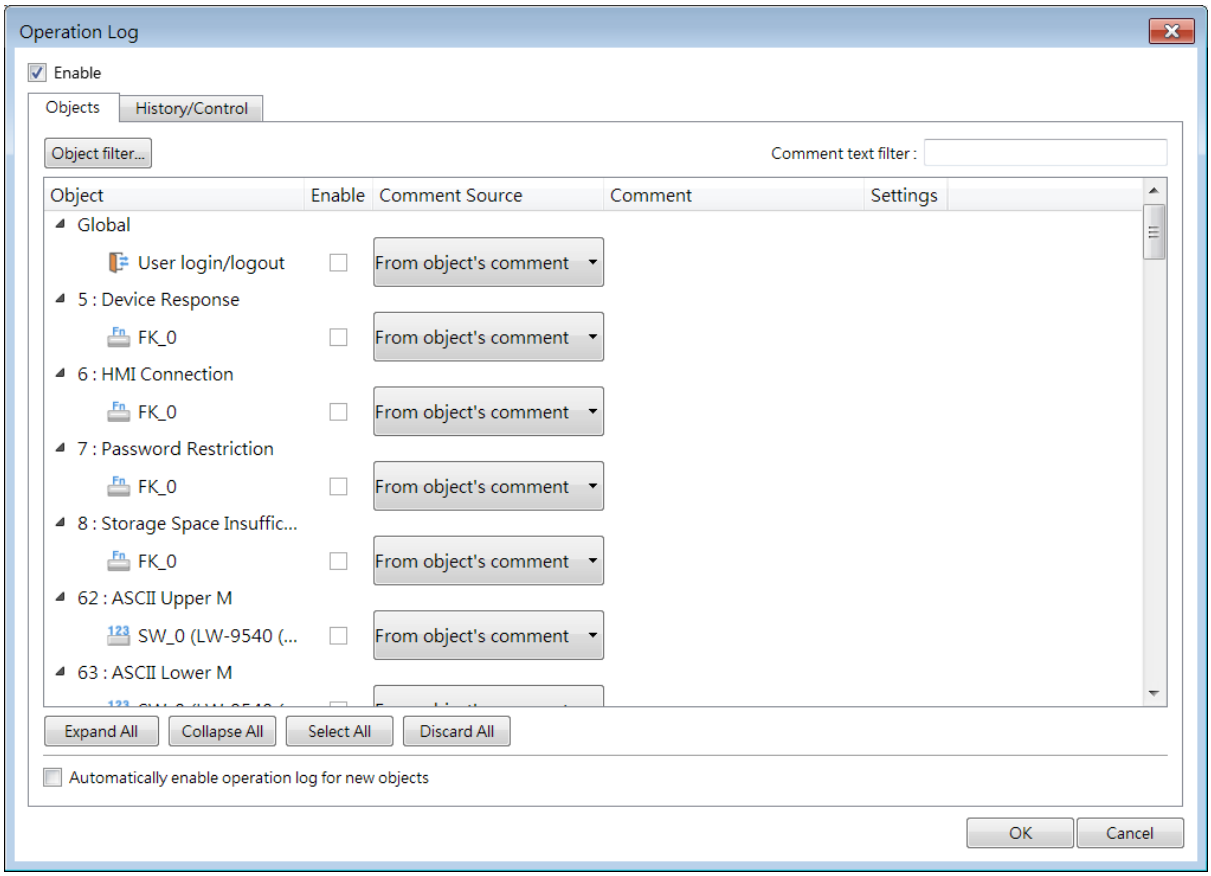


Object Security

2.2.8. Operation Log

When any operation is performed on objects, the Operation Log can record all information related to the action, including date/time, username, object class, window number, object

name, user-defined comment, action (object type), address, and changes.
Once logging is enabled, the Operation Log is stored by default in the HMI's memory in SQLite database format, and can also be backed up to external devices such as a USB drive.
To enable the Operation Log function, go to [Data/History] » [Operation Log Settings]. Select the objects for which the operation process needs to be recorded, and provide comments about the actions performed on these objects. These comments will also be recorded in the Operation Log.



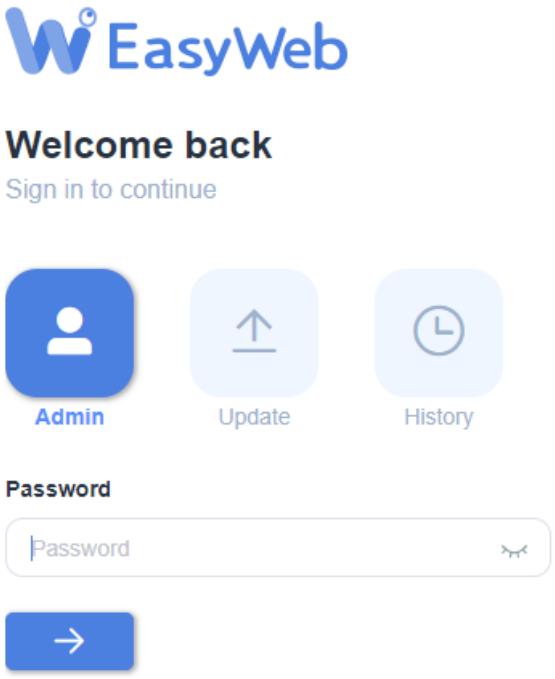
Operation Log Settings
Tip: Click on [Object Filter] to specify the objects to be viewed.

Users should be cautious with the settings on this page, as data may be lost if not configured properly. Before synchronizing data from external storage, please ensure that the maximum record count for HMI memory is not exceeded. It is also recommended to synchronize data to external devices for backup in case of insufficient space in HMI, to prevent data loss.
The Operation Log uses control addresses for command issuance or status report confirmation related to the Operation Log while HMI is running. Please use control addresses with caution to avoid accidental data deletion or disabling of the Operation Log, and report all execution results whenever possible.
An Operation Log Viewer object can be placed on the screen to view the Operation Log.

3. Risks during Product Operation (SG5)

3.1. Login Authorization

To access the web configuration page of the cMT X series HMI, open a web browser (such as Windows Edge, Chrome, or Firefox) and input the IP address of the device. If you encounter the Webview interface upon entering the IP address, input https://hmi_ip/admin to access the Easyweb 2.0 system parameter login page.
Authorization within the system is categorized into three levels: [Admin], with the highest authorization, can modify all settings; [Update] has limited settings that can be changed. For security considerations, password confirmation is required before accessing any settings. Additionally, entering the [History] section demands password authentication, allowing access to backup historical data.
It is recommended to set distinct passwords for administrators and operators to prevent operator accounts from gaining administrator privileges.



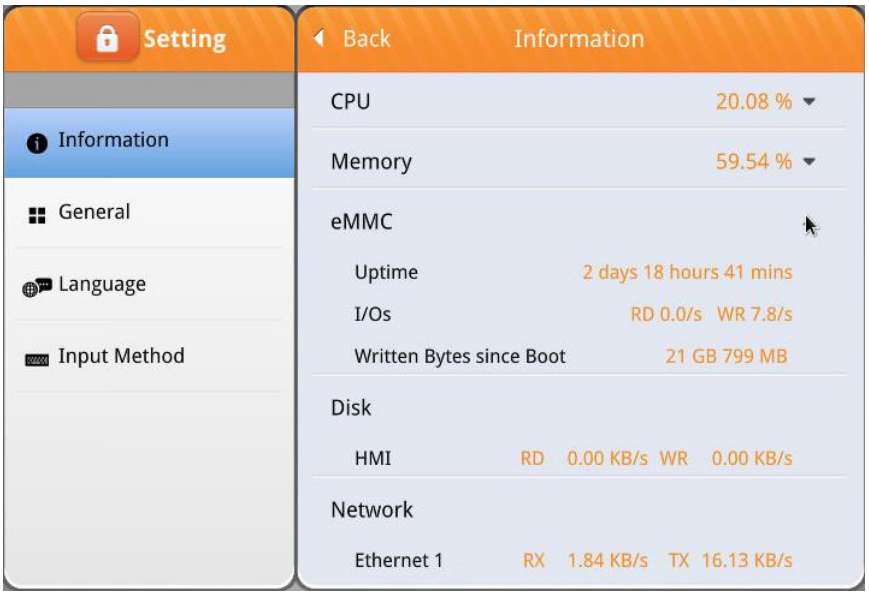
Login Authorization

3.2. History File Security

The security of history files generated by Data Sampling, Event Log, and Operation Log can be enhanced by measures explained in this section.

3.2.1. Prolong the Lifespan of Flash Memory

Due to the limited number of write cycles in the internal flash memory of the HMI, frequent or large-scale writing of historical data may shorten the lifespan of the flash memory, resulting in unreadable historical data and possible failure to start up the HMI. Therefore, it is recommended to keep the average write speed to flash memory below 1200 KB/min. (This information can be obtained in the System Setting on the HMI.)



Average write speed

Recommendations for **reducing** the write speed to the flash memory:

Data Sampling:

- If historical files are not needed and only the data generated after HMI boot-up needs to be viewed, uncheck the option to save historical data.
- Set a longer sampling time.
- Reduce the frequency of sending synchronous commends (2 or 3) to control addresses.
- If [Customized file handling] is used, reduce the frequency of file switching. If [Auto sync. periodically] is enabled, set a longer synchronization time.

Event Log:

- If historical files are not needed and only the data generated after HMI boot-up needs to be viewed, uncheck the option to save historical data.
- If it is not for alarm purposes and only specific actions need to be executed when certain conditions are met, do not check [Save to history] or use Action Trigger objects instead.
- Reduce the frequency of sending synchronous commends (2 or 3) to control addresses.
- Use Aggregate mode. (The option is “Limit write frequency to HMI flash drive”)

Operation Log:

- Reduce the frequency of sending synchronous commends to control addresses.

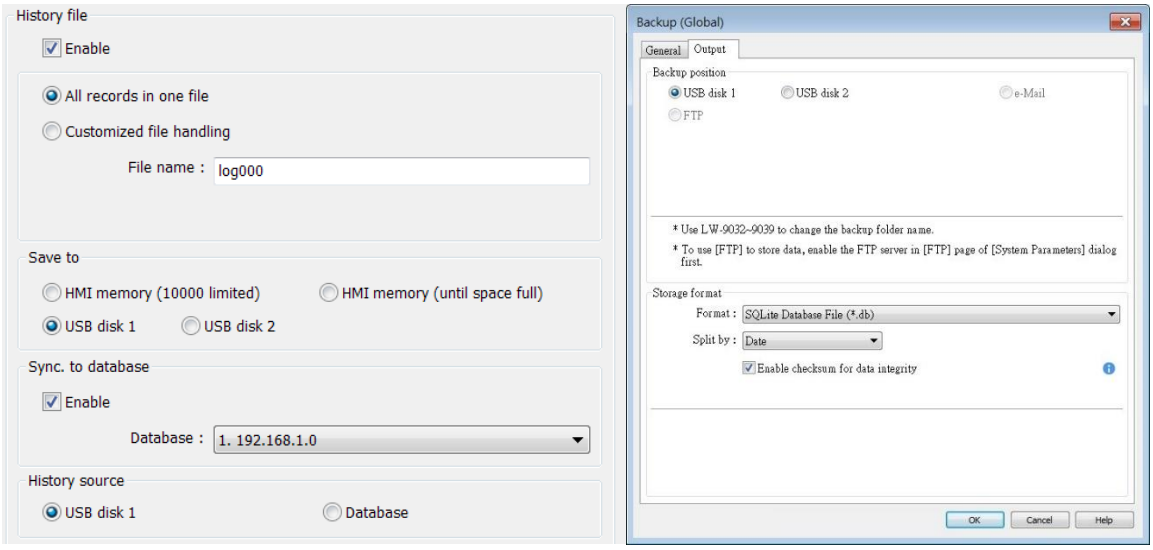
- Use Aggregate mode. (The option is “Limit write frequency to HMI flash drive”)

Note

- Before shutting down the HMI, set system register LB-9034 to ON to ensure that historical data is completely written to the flash memory.

3.2.2. Save / Backup Historical Data to an External Device

It is recommended to save or backup historical files to an external device, such as a USB drive, SD card, or synchronize to a database server, in case of insufficient space on the HMI and prevent data loss.



Save / Backup historical files to an external device, using data sampling as an example.

Recommendations for using USB drives and SD cards as external devices:

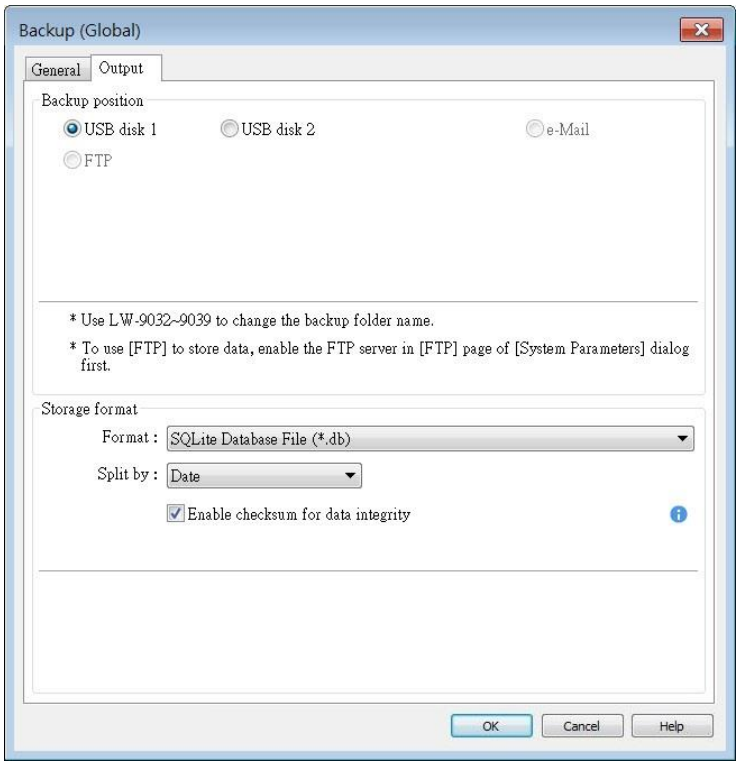
External USB drives and SD cards also have limitations on the number of write cycles, which varies depending on the type of memory. If historical data is written frequently or if historical files are to be preserved for a long time, it is recommended to use USB drives and SD cards with larger capacities (e.g. 32GB), and perform remote backups regularly (e.g. annually).

Recommendations for using a database server as an external device:

Enable RAID and perform remote backups regularly (e.g. annually).

3.2.3. Enable Checksum for Data Integrity

The EasyConverter tool provided by Weintek allows users to open SQLite files on a computer to display backup file data, and supports exporting files to Excel/CSV formats. If the backup file contains checksums, EasyConverter will verify the checksums to ensure data integrity. To enable this feature, simply check the option [Enable checksum for data integrity] when generating backup files. This feature is only supported on cMT/cMT X Series.



Checksum setting of Backup object

EasyConverter can be used to verify the integrity of backup file contents. If any file tampering is detected during the verification process, EasyConverter will send an alert.

4. Risks during Remote Maintenance

4.1. Communication Security

4.1.1. Disable Unnecessary Functions (SG-3b)

When using an HMI, it is recommended to disable unnecessary functions if they are not being used, or at least apply password protection:

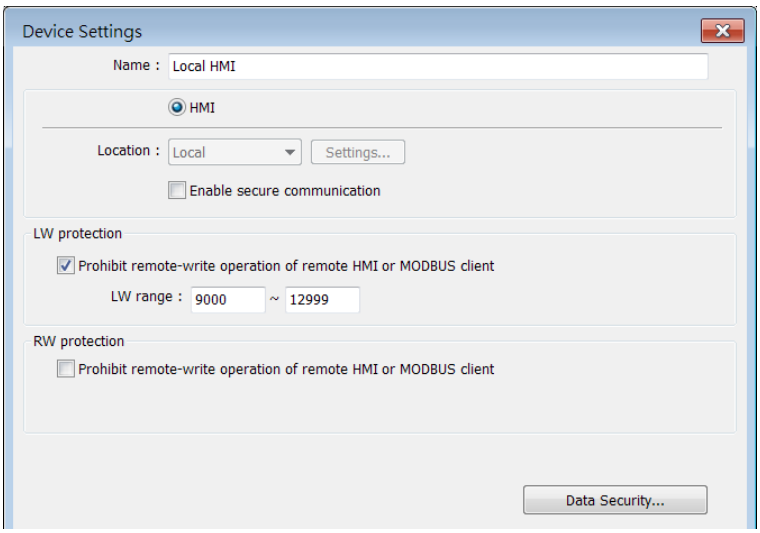
1. Remote HMI
2. PLC Control (change page)
3. Modbus Server
4. VNC Server
5. cMT Diagnoser (cMT / cMT X Series)
6. OPC UA Server (selected cMT / cMT X Series)

The list is not exhaustive.

4.1.2. Modbus Server

When a Modbus Server is used in an HMI project, navigate to the [System Parameters] » [Device] tab. From there, access [Settings/Security…] and activate [LW Protection]. This ensures that no unintended alterations occur in the system registers during communication between the HMI and the Modbus client.

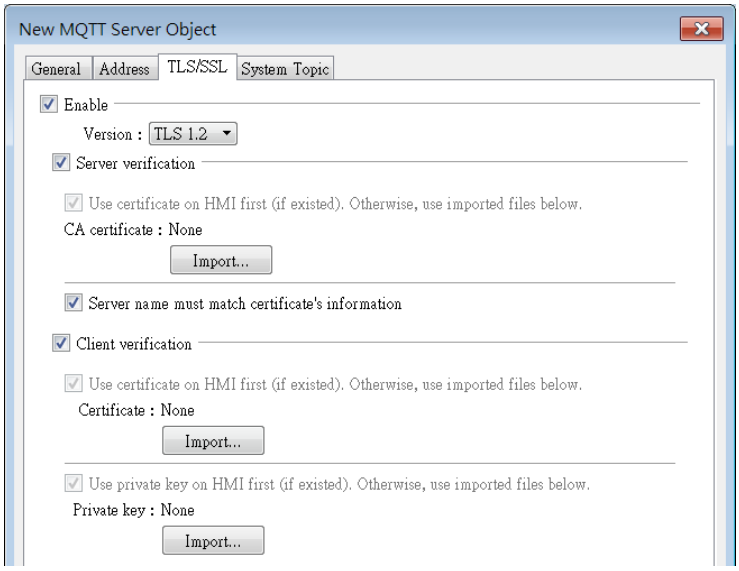
Note: To configure the protected LW range, refer to the supported range of system parameters.



LW protection

4.1.3. MQTT

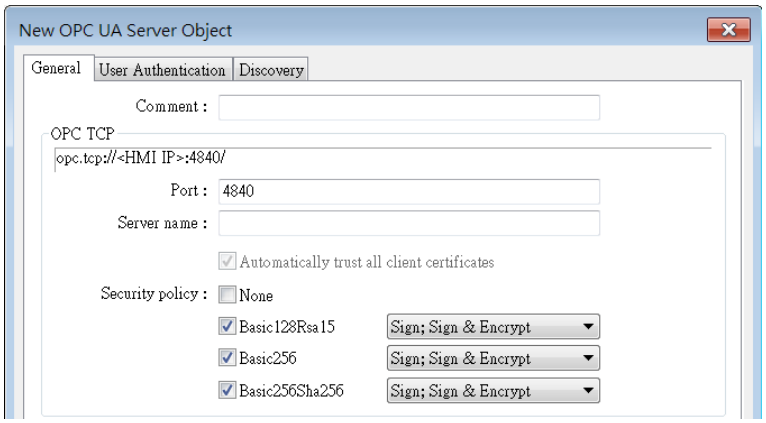
When MQTT is used in an HMI project, select TLS 1.2 encryption and import the CA certificate, client certificate, and private key. Enable encryption and verification features in the MQTT Server object settings on the [TLS/SSL] tab, as shown below.



MQTT TLS/SSL encryption

4.1.4. OPC UA Server

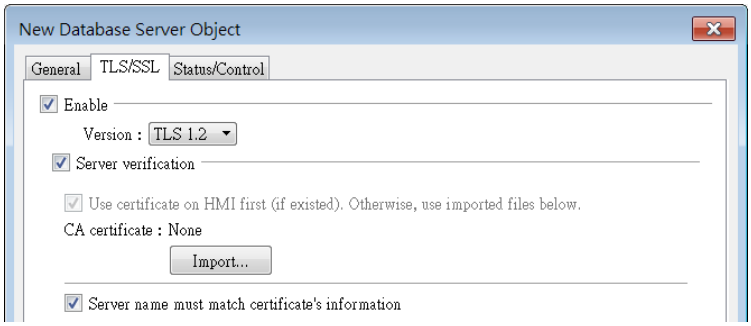
If an OPC UA server is used in an HMI project, disable the option for plain text communication and use encrypted communication instead. In the [General] tab of the OPC UA Server settings window, uncheck the [None] option for security policy to require clients to communicate with encrypted contents, as shown below.



OPC UA Server Security Policy

4.1.5. Database Server

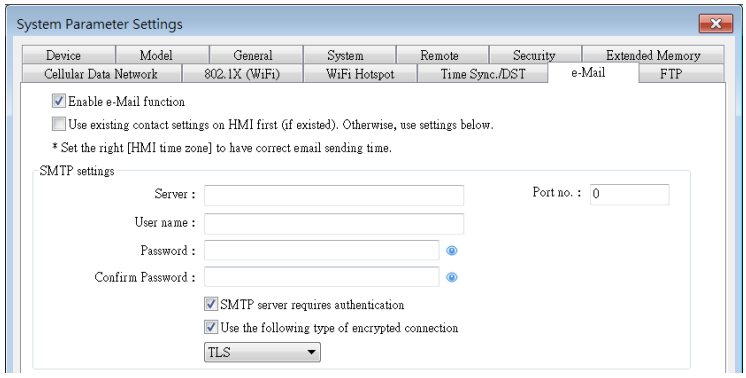
When Database Server is used in an HMI project, select TLS 1.2 encryption and import the CA certificate. Enable encryption and verification features in the Database Server object settings on the [TLS/SSL] tab, as shown below.



Database Server TLS/SSL encryption

4.1.6. e-Mail

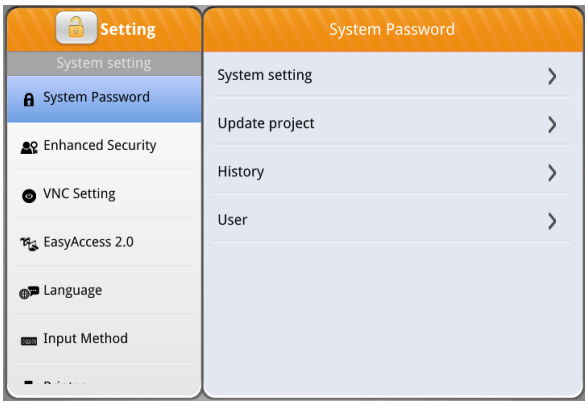
When the e-mail function is used in an HMI project, it is recommended to use an SMTP server that requires authentication and enable TLS/SSL encrypted connection type. After enabling the e-mail function in System Parameter Settings, select both [SMTP server requires authentication] and [Use the following type of encrypted connection] options as shown below.



e-Mail encryption

4.1.7. cMT Viewer Remote Monitoring

If remote monitoring is required for cMT/cMT X series HMI, users can use cMT Viewer to monitor the screens. It is recommended to set passwords for various permissions in the system settings of the HMI, and then use the corresponding passwords in cMT Viewer to log in and monitor the screens. The system password setting page is shown below.



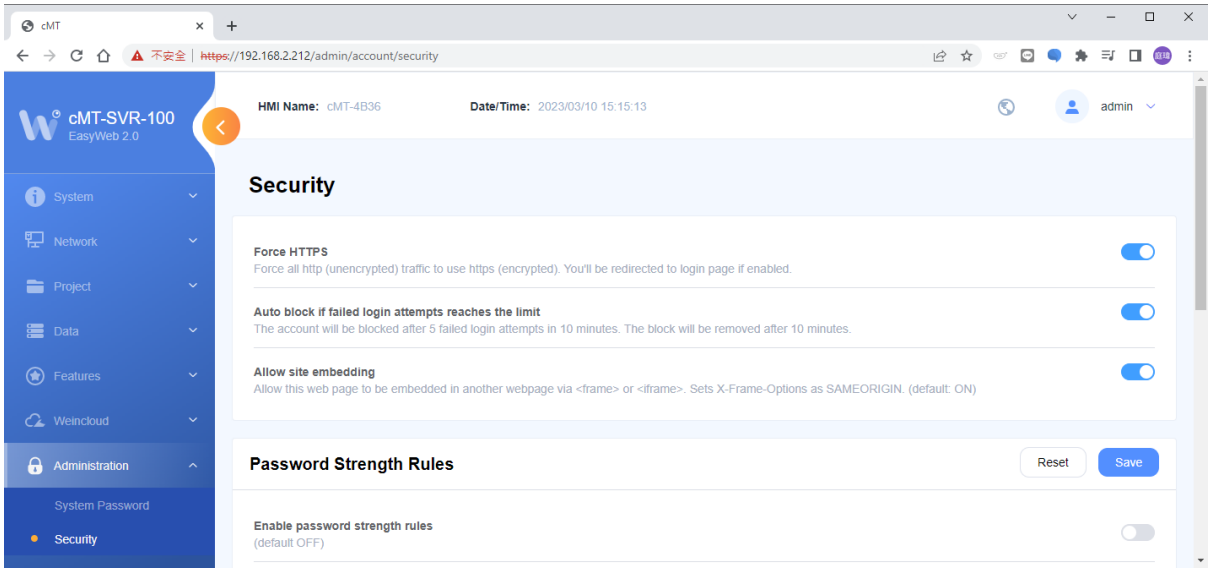
System Password

4.2. Web Page Security

When a cMT/cMT X series HMI is used, the user can access EasyWeb 2.0 page through a web browser and configure network IP settings, upload/download projects, and perform data backups. As these features involve crucial contents, it is essential to ensure the security of the web page by following the recommended settings.

4.2.1. Enable HTTPS Encryption

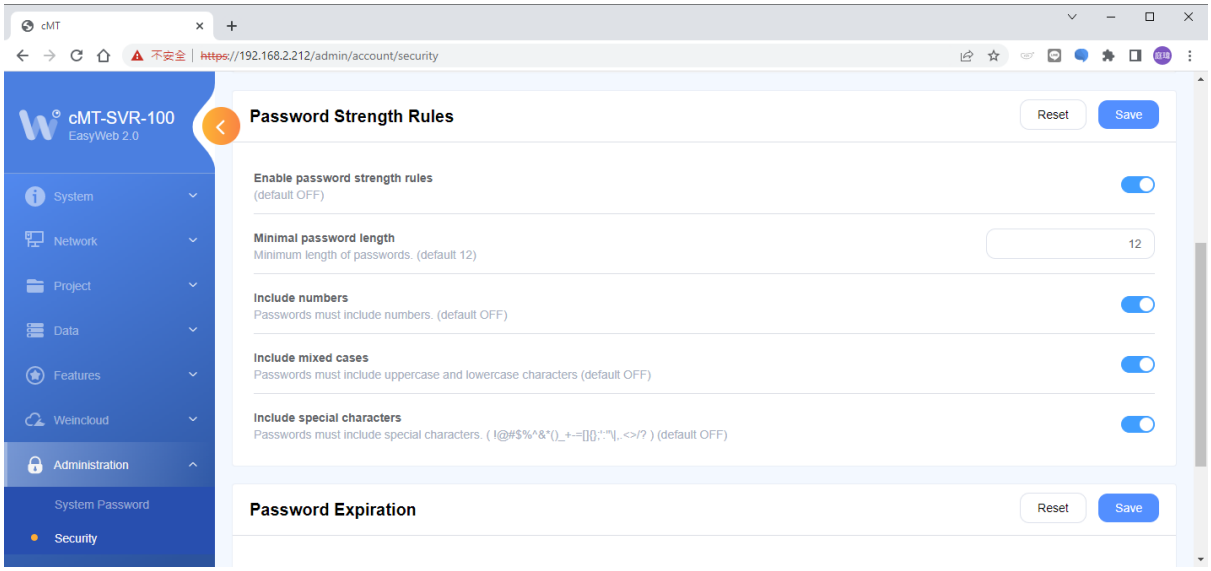
It is recommended to enable HTTPS encrypted communication. After entering EasyWeb 2.0, go to the [Administration] tab from the left-hand menu and open the [Security] page. Enable the [Force HTTPS] option, as shown below.



Force HTTPS

4.2.2. Enable Password Strength Rules

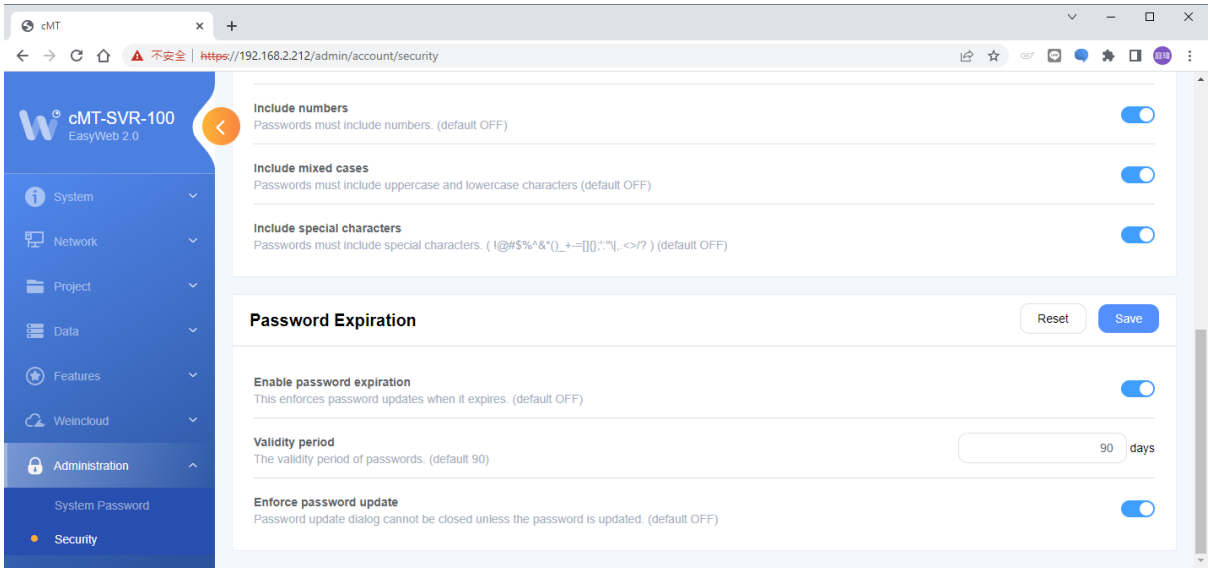
It is recommended to enable system password strength rules to enforce restrictions on password length, case, and special characters used for web page login, in order to enhance overall security. After entering EasyWeb 2.0, go to the [Administration] tab from the left-hand menu and open the [Security] page. Complete the settings within the [Password Strength Rules] section, and remember to click the [Save] button to save the settings.



Password Strength Rules

4.2.3. Enable Password Expiration

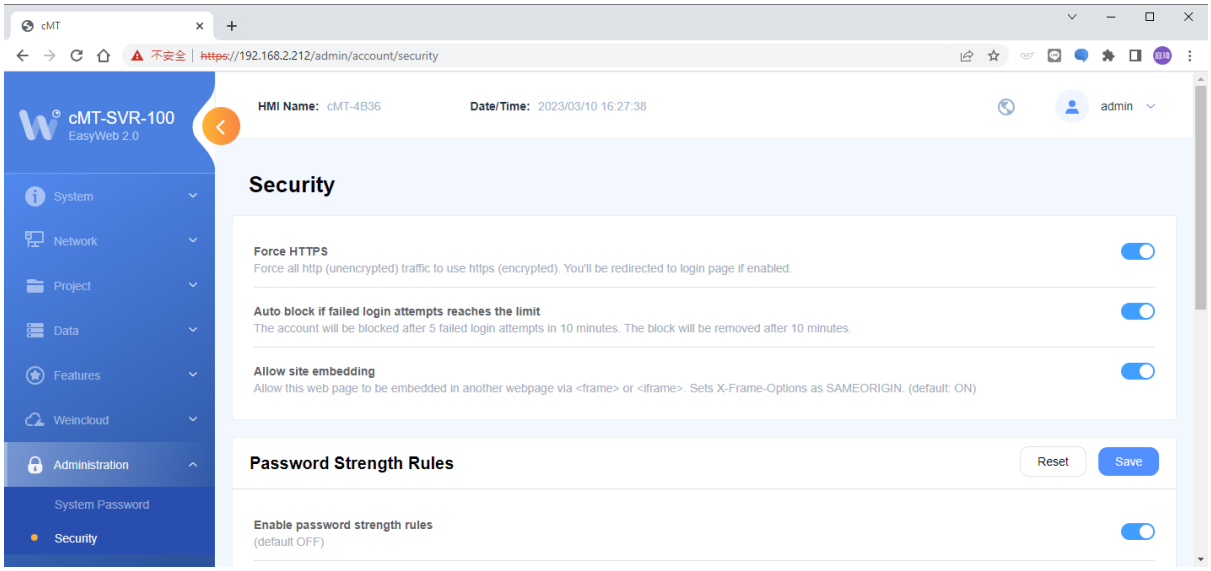
It is recommended to enable system password expiration. In the Password Expiration section, the number of days for the validity period can be set to enforce password updates after the set period has expired. After entering EasyWeb 2.0, go to the [Administration] tab from the left-hand menu and open the [Security] page. Complete the settings within the [Password Expiration] section, and remember to click the [Save] button to save the settings.



Password Expiration

4.2.4. Enable Auto Block for Failed Login Attempts

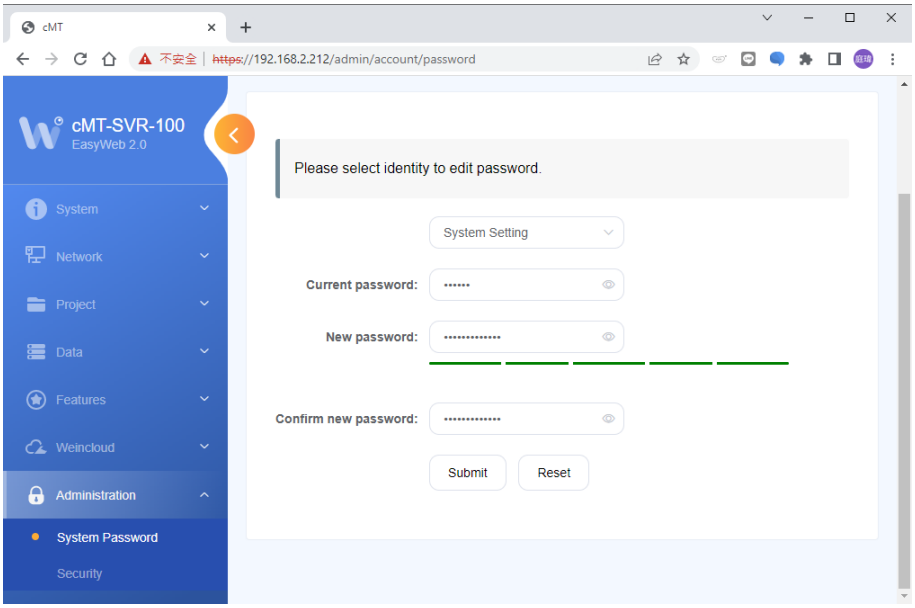
It is recommended to enable the [Auto block if failed login attempts reaches the limit] setting to automatically lock the system for 10 minutes after 5 consecutive failed login attempts with incorrect passwords. After entering EasyWeb 2.0, go to the [Administration] tab from the left-hand menu and open the [Security] page, then enable the mentioned setting as shown below.



Auto block if failed login attempts reaches the limit

4.2.5. Change System Password

After making changes to the web page settings mentioned above, please update the system password to a stronger one. After entering EasyWeb 2.0, go to the [Administration] tab from the left-hand menu and open the [System Password] page, where the system login password can be set, as shown below.



Change system password

4.3. Regular Security Maintenance Activities (SG-3f)

Engaging in regular information security maintenance activities is crucial to maintain the ongoing security of your system and data. The following practices are recommended for routine information security maintenance:

- Regular Software Updates: Ensure your operating system, applications, and related

software are consistently updated with the latest security patches. This guards against the exploitation of known vulnerabilities.

- Periodic Password Changes: It is advisable to periodically change user account passwords, requiring robust combinations of upper and lower-case letters, numbers, and special characters.
- Scheduled Data Backups: Conduct routine data backups and store them in secure locations. This precaution shields your data from potential risks like failures or malicious attacks.
- Strengthening Firewall and Intrusion Prevention Systems: Keep firewalls and intrusion prevention systems current and efficient. These tools help prevent unauthorized network traffic from infiltrating your system.
- Regular Vulnerability Scanning and Testing: Undertake consistent vulnerability scans and security testing to uncover potential security weaknesses and address them promptly.
- Periodic Review of Permissions and Access Controls: Routinely assess user permissions and access controls to ensure that only authorized users can access sensitive resources.
- Scheduled Log Monitoring: Regularly monitor system and application logs to identify potential security incidents or anomalous activities.
- Routine Security Audits: Conduct internal or external security audits at regular intervals to ensure your information security measures align with standards and best practices.

5. Product Secure Disposal Guidelines (SG-4)

This section outlines the procedures for secure product disposal to prevent information security issues (e.g. sensitive data leakage) when retiring or decommissioning an HMI product.

5.1. Recommendations for Secure Disposal

- Remove the HMI from equipment without causing physical damage.
- Completely erase programs and configuration data from the HMI by performing a reset.
- Securely delete historical files stored on both the HMI and external storage devices.
- Safely dispose of the HMI (through physical destruction) to prevent potential leakage of undeletable data stored on it.