FDA 21 CFR Part 11 Compliance

UM019002E_20240319

INTRODUCTION 3

FDA 21 CFR PART 11 COMPLIANCE 4

GUIDELINES 10

Enhanced Security Mode 10

Object Security Class 10

User Information Setup 11

User Login/Logout Operation 12

Run-time change 14

Protection of security settings 14

Event log with Status Code 15

Miscellaneous 17

Security of Macro and Objects 17

Operation Log 18

Configuration 18

Backup File Integrity 19

Electronic Signature 19

Security and Operation Log 19

Handwritten Signature 21

Data Sampling and Event Log 22

Record Retention 22

Historical File 22

Backup File Integrity 23

Database Server 23

General Data Integrity 24

System Development and Management 25

System Registers 26

Configuring Initial State..... 27

PRACTICE 29

REFERENCES..... 29

Introduction

HMI and computer controlled systems are becoming indispensable for today's manufacturing systems, so are the electronic records they generate. However, electronic records being more susceptible to tampering, rules need to be in place to preserve their integrity.

FDA 21 CFR Part 11, by Food and Drug Administration (FDA) of the US government, defines the criteria under which electronic records and electronic signatures can be treated with same degree of validity as paper-based records. Since the scope of FDA's regulatory authority is very broad, Part 11 has an impact on all computer systems in life science industry.

This guide is aimed at helping users understand how to comply with FDA 21 CFR Part 11 when using Weintek HMI. In this document, Part 11 codes are reviewed article by article, in the context of HMI, followed by discussion of related features and configuration options that will help meet the requirements. If using the system with Weintek HMI in regulated environment, users are requested to create and administer their systems according to the guidelines in this document.

Users are advised, though, that the requirements for FDA 21 CFR Part 11 apply to the entire project, not just the HMI alone. HMI functions can facilitate compliance regarding electronic data generated by the HMI, but implementing only what is described in this document does not guarantee compliance with FDA 21 CFR Part 11 for the entire setup. Thorough audit of the entire system must be carried out by professionals in the field. Nonetheless, if any electronic data generated on HMI are used, the procedures in this document should be followed.

FDA 21 CFR Part 11 Compliance

This chapter is a review of the FDA 21 CFR Part 11 with the remarks on compliance with respect to HMI.

Subpart B—Electronic Records

Sec. 11.10 Controls for closed systems	Applied?	Remarks
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:		
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	N/A	System validation should be done by users as the criteria vary from case to case.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Yes	Records are stored in proprietary binary or sqlite database format, and may be converted to human readable form using tools provided.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	Redundant functions are available.
(d) Limiting system access to authorized individuals.	Yes	Enhanced Security Mode allows user access control on the HMI.
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required	Yes	All on screen operations, along with their details, can be recorded in the Operation Logs, which may be inspected on HMI or by database tool. Its file records may be secured by checksum.

	for the subject electronic records and shall be available for agency review and copying.		
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	Operation logic and sequencing of steps are integral to HMI's project design, using combination of window design, logic control, enhanced security mode, and macro commands.
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Yes	Appropriate project design with Enhance Security Mode can ensure system is accessed by authorized personnel only. Additional security policies should be in place to implement access control to the HMI.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Yes	Enhanced Security Mode allows authentication of user which can validate the source of data input associated with the user. Additionally, logics can be incorporated in project designs to further examine data source validity.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	N/A	Users are to ensure that persons who use the system possess appropriate qualifications.
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	N/A	Users are required to establish binding policies and implement its adherence with respect to electronic signatures.
(k)	Use of appropriate controls over systems documentation including:		
	(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Yes	Latest user manuals of Weintek HMI are available on Weintek's official website. Users are responsible for documentation specific to their system.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	N/A	Users are responsible for documentation related to modifications of their system.

Sec. 11.30 Controls for open systems	Applied?	Remarks
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in §11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	N/A	For open systems, users must establish and adhere to additional codes that govern data safety and integrity. It should be noted that various remote access solutions exist and they should be also taken into consideration.

Sec. 11.50 Signature manifestations	Applied?	Remarks
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	Yes	Electronic record signing can be designed with Operation Log, and Enhanced Security Mode
(1) The printed name of the signer;		
(2) The date and time when the signature was executed; and		
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.		
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	Yes	Electronic record signing can be designed with Operation Log, and Enhanced Security Mode

Sec. 11.70 Signature/record linking	Applied?	Remarks
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Yes	Can be achieved by linking Security authentication with the signing procedure. Data recorded in the operation log database should be protected from alteration.

Subpart C—Electronic Signatures

Sec. 11.100 General requirements	Applied?	Remarks
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	N/A	Users must ensure that existing security options are not modified.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	N/A	The organization users belong to should perform identity verification before sanctioning. Only after confirmation of identity should the individual be given his/her login credentials.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	N/A	Users should report their intention to relevant authority for such usage of the electronic signature.
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	N/A	Users should submit the certification to relevant authority.
(2) Persons using electronic signatures shall, upon agency request, provide additional	N/A	Users should provide material to relevant authority upon request.

certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.		

Sec. 11.200 Electronic signature components and controls	Applied?	Remarks
(a) Electronic signatures that are not based upon biometrics shall:		
(1) Employ at least two distinct identification components such as an identification code and password.	Yes	Enhanced Security Mode requires a user ID and password for user identification.
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	Yes	Username and password are both required for any log in attempt. Projects can be designed to enforce this. Alternative sign-in method(by index) is available that allows password only access.
(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Yes	Username and password are both required for any signings log in attempt.
(2) Be used only by their genuine owners; and	N/A	The user is responsible for this requirement.
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	N/A	System administrator should establish relevant protocols to address this situation.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	N/A	If using biometric-based mechanism such as fingerprint for login, users should be responsible for any security measure relating to

		its use.

Sec. 11.300 Controls for identification	Applied?	Remarks
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:		
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	YES	Enhance Security Mode configuration will detect and does not allow duplicated ID/Password.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Yes	Account expiration is provided for temporary account by default. Other password measures can be handled with user-defined actions.
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	N/A	The user should establish and implement loss management procedures.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	Yes	Failed log-in attempts can be logged as events, which can be configured to send notification via various means.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	N/A	The user should periodically conduct tests to ensure the functionality and integrity of the devices.

Guidelines

This section describes the relevant features of Enhanced Security Mode, Operation Log, Data Sampling, Event Log, as well as general project design techniques and system management principles for compliance with FDA 21 CFR Part 11 using Weintek HMI.

Enhanced Security Mode

Enhanced Security Mode allows user authentication for the purpose of managing user access to HMI control.

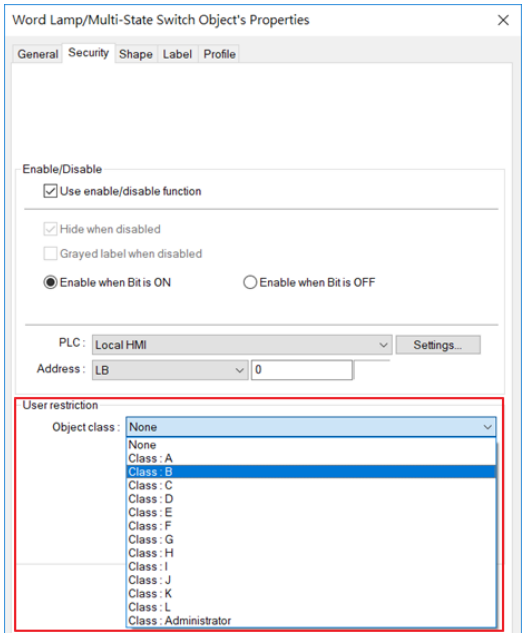
Setup and principles:

- Applicable objects can be assigned a security class.
- Each user is assigned security classes for which access is granted.

As a result, Enhanced Security Mode can provide access control down to individual object level, adding great flexibility to project design. (Sec 11.10)

Object Security Class

The security class of each object may be configured in their respective property window, under the [Security] tab, in [User restriction]. An object may be set to belong to only one security class. Available classes are A, B, C….to L, and an Administrator class.



Object class settings

User Information Setup

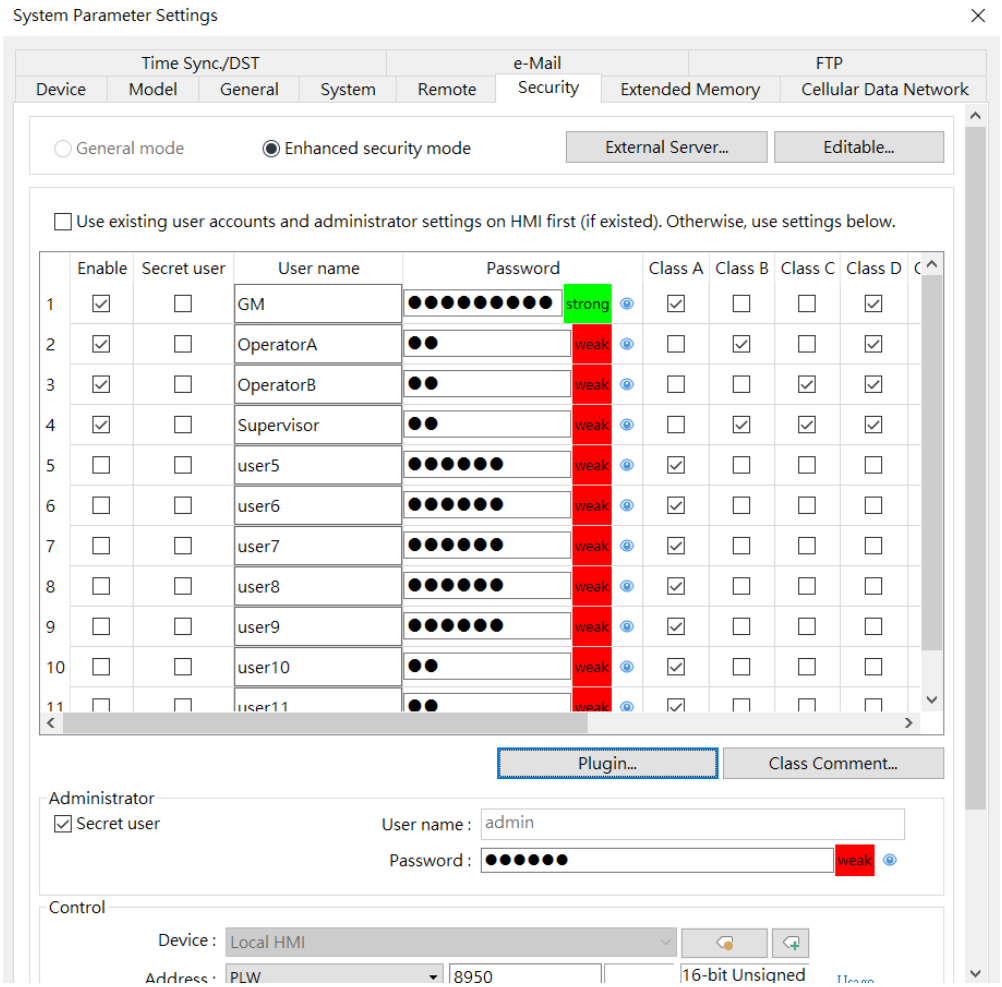
Under the [Security] tab in [System Parameter Settings] is the main configuration page for security feature. Use only Enhance security mode instead of General mode, as General mode lacks many key features for complying with 21 CFR Part 11.

In this page, the user account information, including account availability, secrecy, user name, password, and accessible classes may be customized. ***In this configuration page, username uniqueness is checked (Sec 11.300), and password complexity is evaluated.***

For cMT/cMT X Series, in the interest of centralized user account management, authentication can also take place on an external server which can be another HMI or an Active Directory via LDAP. When utilizing this, user account authority is obtained from the external server, so authority settings on the external servers should correctly reflect the authority levels appropriate for each user. Additionally, there are fingerprint and smart card login that can be used to complement username/password authentication.

Administrator account which has access to all security classes is always enabled. Therefore, its password should be changed from the default for security purpose. In addition, make it a secret user so that it does not appear in any option list.

Control addresses play an important role in operation of security feature, and in this page, starting address of the control address may be configured as well.



Enhanced Security Configuration in [System Parameter Settings]

User Login/Logout Operation

All operations at runtime, including login, logout and account management, involve the use of the control addresses, which are user-assigned LW word registers. The following table lists the control address functions starting with LW-n, where n is the starting address designated in EasyBuilder Pro.

Address	Length	Actual LW For n=8950	Tag Name	Description
LW-n	1	8950	Command	Commands to be executed: Login, Logout, Add/Setting/Delete Accounts, etc.
LW-n + 1	1	8951	Command Execution Result	Displays the result of executing commands.

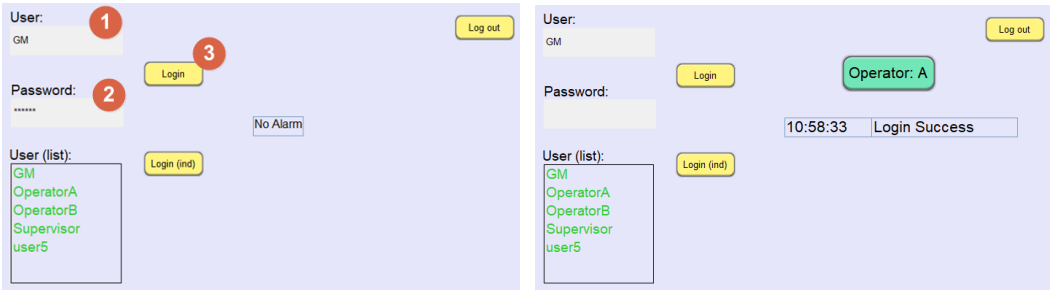
LW-n + 2	1	8952	User index	The index of accounts (used with Option List Object).
LW-n + 3	1	8953	User Privilege	Binary value. Level A = bit0, Level B = bit1, …
LW-n + 4	8	8954~8961	User name	Account name (Case-sensitive; letters and numbers only).
LW-n + 12	8	8962~8969	Password	Account password (Case-sensitive; letters, number special characters only).

Example 1: Logging in

To log in, first input the user name and password to their respective [User name] and [Password] registers, and then issue the login command at the [command] register.

Steps	Action (LW-n=8950)
1. Enter the user name in [User name].	Enter the user name to registers starting at LW-8954
2. Enter the password in [Password].	Enter the password to registers starting at LW-8962
3. Issue login command, by setting the [Command] to 1.	Write the value 1 to LW-8950

The system will verify user and password from the registers. Once verified, the user is now logged in and the objects for which the user has access to will be available.



Before Login vs. Logged-in as the user

Example 2: Logging out

1. To logout, simply issue the logout command, by setting the [Command] to 3.

Username and password combination is required for login. (Sec 11.200) Alternatively, it is

possible to list all available users within a dropdown list in the login by index mode, and login with password only. It is suggested that ***login by index mechanism be used only for "subsequent secondary authentication within a single session" as set forth in Sec 11.200***.

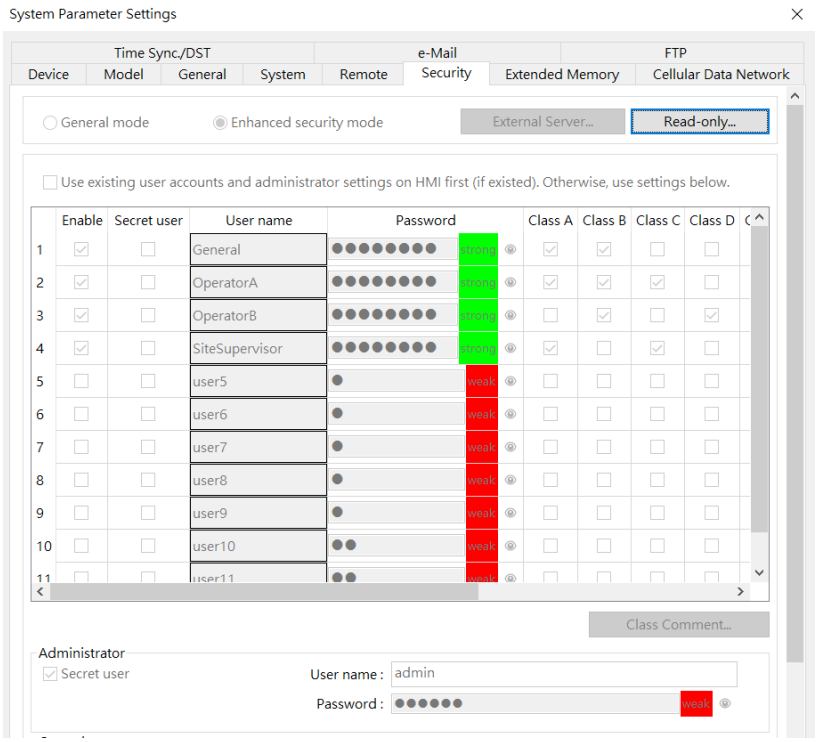
The control addresses and all of their functions are documented in detail in Chapter 10 of the EasyBuilder Pro user manual.

Run-time change

While user accounts, their passwords and authorizations can be configured in EBPro during design phase of the project, it is also possible to perform account management on HMI during runtime. Runtime operations include: change password, add/modify temporary account, add/modify expiring account, add/delete fingerprint/smart card associated with an account, and modify account rights…etc. ***Users may use, for example, expiring accounts to periodically recall and renew accounts to address the account aging issue.(Sec 11.300)*** Runtime user account administration is achieved by configuring the control address in combination with suitable control objects. Refer to Chapter 10 of the EasyBuilder Pro user manual for full detail.

Protection of security settings

Enabling "Read only" mode prevents unauthorized access to the security feature, even if others are in possession of the original project file. When in "Read Only" mode, security settings cannot be modified, and passwords are marked with asterisks (*) to prevent inadvertent disclosure. The originally-set password will be required to regain access.

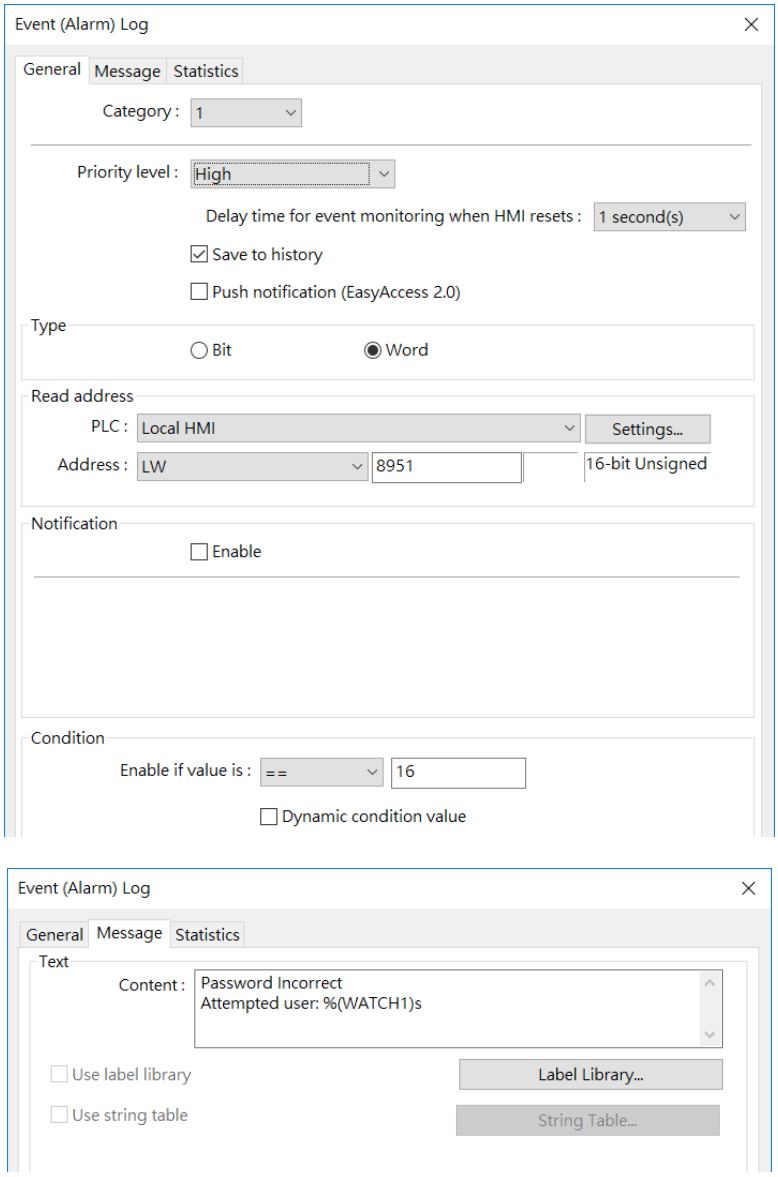


Read-only mode

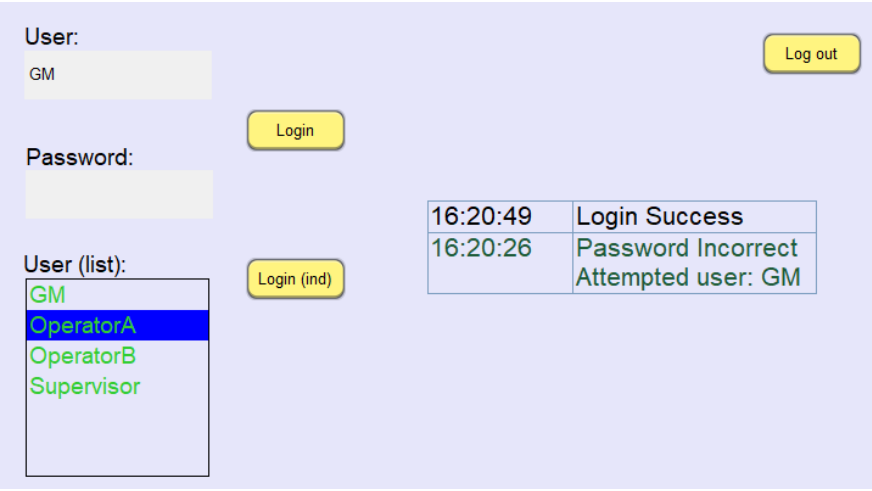
Event log with Status Code

The control address Command execution result (LW-n+1) is the status code that indicates execution result of any user account operation. The status code, in combination with event log reporting, can be used to confirm log-in or report abnormal log-in operations. ***Should there be abnormal log-in operation detected, one can then respond to the situation accordingly. (Sec 11.300)***

To realize such a setting, the user can add a new event in Event (Alarm) Log, and then designating the [Read address] to LW-n + 1, the [command execution result]. For the alarm text, the [Content] text box under the [Message] tab is where users can write the messages to be displayed in Event Display Object to show command execution result in meaningful text.



Event setting logging the command execution result



Event Log showing login result

Miscellaneous

Flush the data in username and password registers periodically, or upon each login, so as to prevent use by another person. Likewise, use Auto logout (enabled in System Parameter Settings) to prevent unauthorized access in case the previous user forgets to log out.

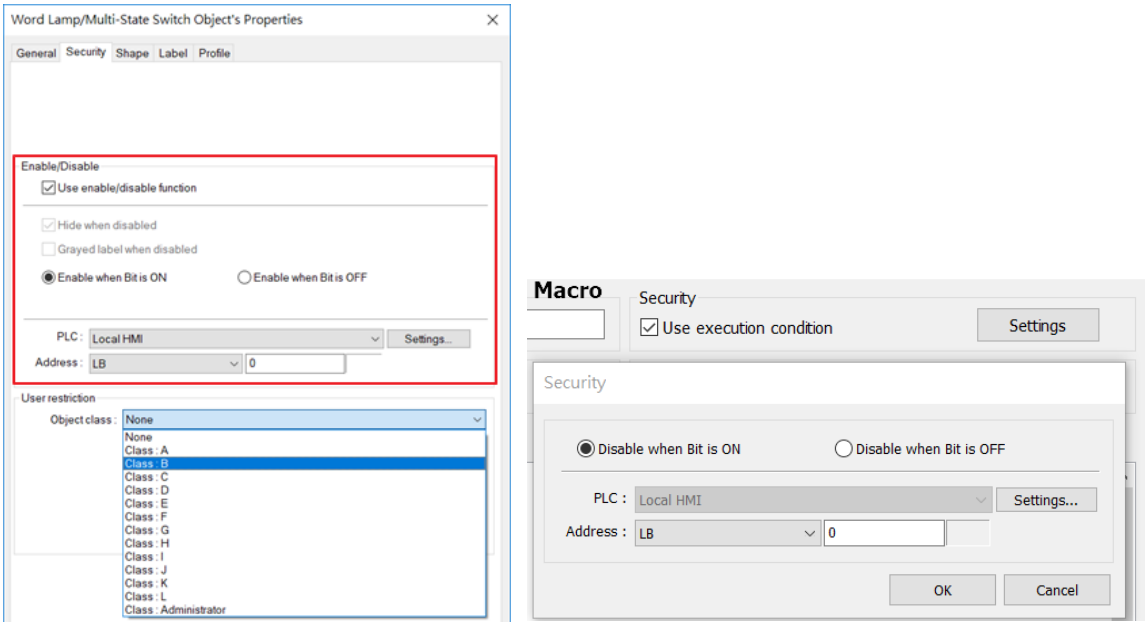
Using Weintek HMI security features will facilitate compliance to FDA 21 CFR Part 11, but will not be sufficient for all the requirements, the user must establish proper Standard Operating Procedures and strictly enforce the established guidelines.

Example guidelines include but are not limited to the followings…

- Authorized account holders must only use their own user accounts to log in to the system.
- Safeguarding of the login credentials is the user's responsibility. Any sharing of login credentials, including but not limited to username/password and smart cards, should be strictly prohibited.
- Password Complexity must be strong, including at least a number and a special character, and using common phrases as a password or part of a password is discouraged.

Security of Macro and Objects

Beside object security ***class*** setting, objects or macro has individual security setting, allowing them to be enabled/disabled by a bit register. When secured, the object will be disabled and disappear; for macro, it will not run even if trigger conditions has been met.



Security setting of an object and macro

Operation Log

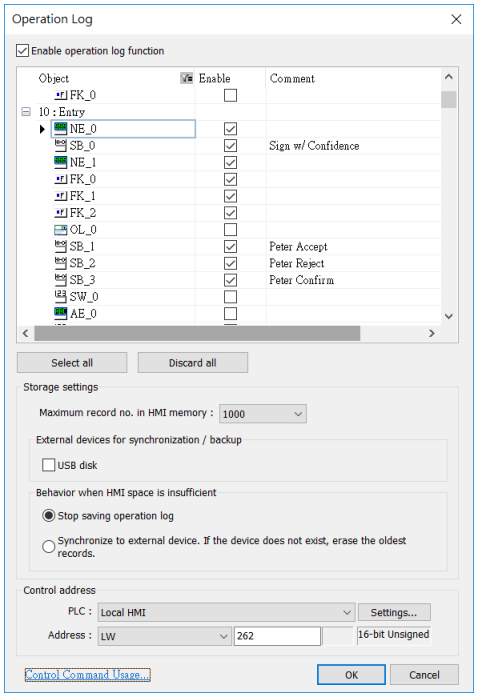
Operation log function records all information related to an action that have been taken for objects in question. Information recorded may include: Date/Time, Username, Class, Window, Object Name, Comment (user-defined), Action (object type), Address, and Information (what was changed). Operation log, if configured properly, may be used to satisfy the requirement for audit trail and electronic signature. (Sec 11.10)

Once recorded, operation log is stored in sqlite database format and by default stored on HMI memory. It may be backed up to a plugged-in external device, such as a USB drive. As an option, the backup copy can be set to include checksum to ensure its integrity.

EasyConverter tool provided by Weintek can be used to open the sqlite file on PC. It can display operation log content and support file export in PDF or excel/CSV format; and where possible, choose to export to PDF. In addition, for a backup file with checksum, EasyConverter can perform integrity check by verifying its checksum.

Configuration

Enable operation log function in [Objects] » [Operation Log] » [Operation Log Settings]. Select all objects for which actions should be recorded, and write comments describing their actions. These comments will also be recorded in the operation log.



Operation log setting

Tips: click on the filter funnel logo to specify what objects to view

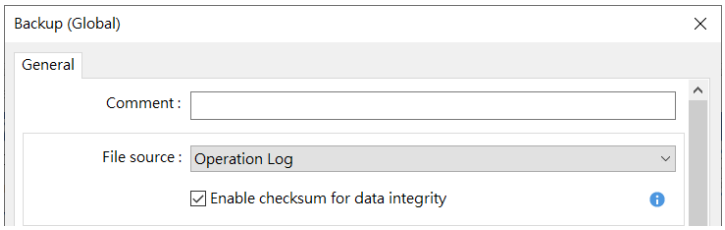
Users must be mindful of the settings here, as data may be lost if not properly configured. Make sure that Maximum record no. in HMI memory is not reached before data has been synchronized to an external device. Sync also to the USB disk simultaneously as a redundant measure, in which case, should HMI space become insufficient, all data are synchronized to the external device to avoid data loss.

Just like security function, operation log function also uses control address for runtime command and status report, which should be treated with care as well. Avoid possibility of clearing records or disabling operation log function, and notify all results if possible.

An operation log view object may be placed on screen to view its content.

Backup File Integrity

To ensure data integrity, one can include checksum in the operation log backup file. Simply check the option [Enable checksum for data integrity] for the backup instance that requires checksum. Note this is only for cMT/cMT X Series.



Backup checksum setting

Given an operation log backup file, use EasyConverter to examine the integrity of its content. The EasyConverter gives an alert when it encounters a file that might have been tampered with.

Electronic Signature

This section gives some examples of electronic signature generation. (Sec 11.10, Sec 11.50)

Security and Operation Log

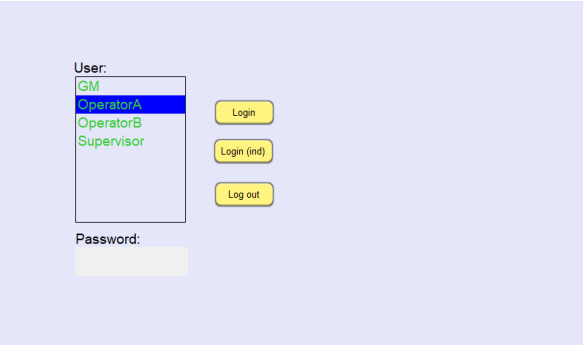
By combining security and operation log, it is possible to record user actions that is equivalent to the effect of electronic signature.

Example:

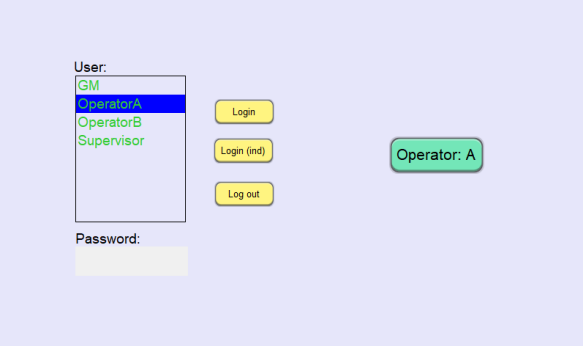
First, design a login page (Window 15), where there is a change-window function key button that changes base window to 16 but is visible only upon appropriate login action. Therefore, it can be assumed that any operation in page 16 is done by the logged-in, authorized user. Then, configure page 16 with action buttons which correspond to signature actions and record these objects' actions in the operation log. When an action button is triggered, its trigger time, operator, action descriptions will all be recorded in the operation log. Assuming that all requirements of data integrity have been met, the information contained in the operation log can be considered as valid digital signatures.

Illustrative view:

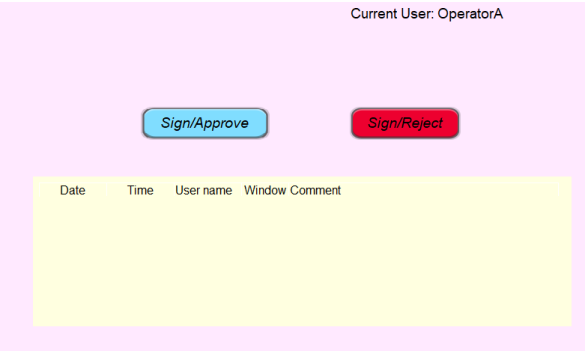
1. On page 15, log in with the username/password.



2. Once logged in, the function key for window change appears.



3. Two signature buttons are available to press. Each represents different action, and once a button is pressed, the other will be gone (by object security).

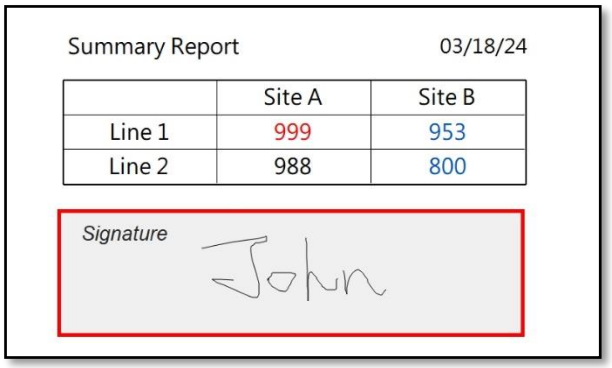


4. Having pressed one of the buttons, the action is recorded in the operation log database.

Handwritten Signature

JS Object provides a way to custom-build screen features that are otherwise not available with built-in elements. With JS Object, it is possible to create a digital drawing pad that allows users to sign their names as they would on paper.

Example:
Place the report contents and a JS Object signature field on the same page, and capture the screenshot after someone signs. The saved screenshot may be treated as a signed report with an electronic signature.



Signature field
(JS Object canvas implementation)

Note: JS object is supported on cMT X models only. Example projects containing a JS Object signature field can be provided upon request.

Examples in this section are some practical ways to generate electronic signature, but they are certainly not all. Applying similar concepts with other design elements such as macro, pop up window…etc, it is possible to generate electronic signature with same effects but distinctive operational experience.

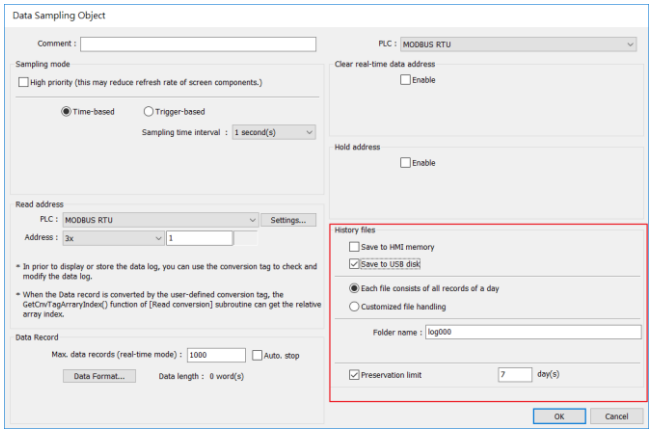
Data Sampling and Event Log

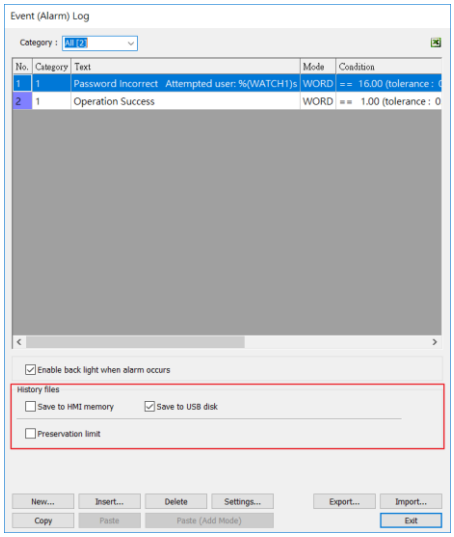
Record Retention

Data Sampling and Event (Alarm) Log generate electronic records and save data as dtl, evt, or .db files. Similar to the case of operation log, users must be mindful of their settings, as data may be lost if not properly configured.

Enable history file saving to HMI memory or an external device (USB disk/SD card) to ensure that data is retained when HMI is powered off. In the case where large quantity of data and/or high-frequency data logging is expected, saving to an external device is preferred. Note that there is an option that allows FTP client to access data on USB/SD card; the option should be turned off to avoid mishandling of data.

Preservation limit should be set no shorter than the record retention period set forth by the regulation. (Sec 11.10) Also, back up periodically, either to the USB disk or to the backup server. If backed up to an external server, procedures for proper handling of such data should be followed.



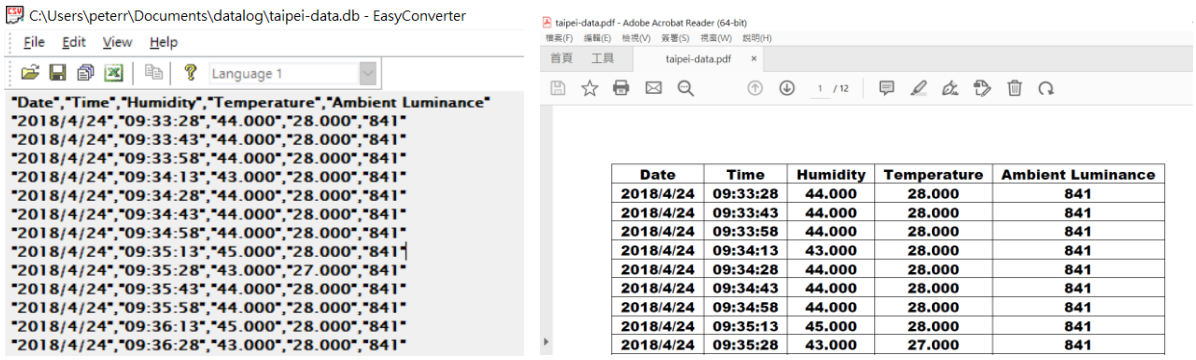


Enable saving to history file

Historical File

The binary and proprietary nature of the dtl and evt files implies that the data files are not easily read and falsified. (Sec 11.10)

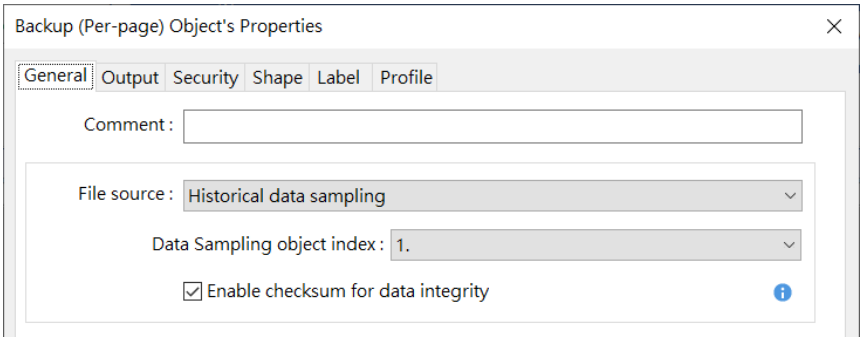
To read data from dtl,evt, or db format files, use the PC-based EasyConverter tool provided by Weintek. Only use the tool packaged in the official release by Weintek. EasyConverter will display record data and output files in PDF or excel/CSV format. The user should then handle such data in accordance with all data handling protocols. Where possible, output to PDF over other formats.



Using EasyConverter to read a db file and save as PDF

Backup File Integrity

To ensure data integrity, one can include checksum in the data sampling and event log backup file. Simply check the option [Enable checksum for data integrity] for the backup instance that requires checksum. Note this is only for cMT/cMT X Series.



Backup checksum setting

Given a data sampling or event log backup file, use EasyConverter to examine the integrity of its content. The EasyConverter gives an alert when it encounters a file that might have been tampered with.

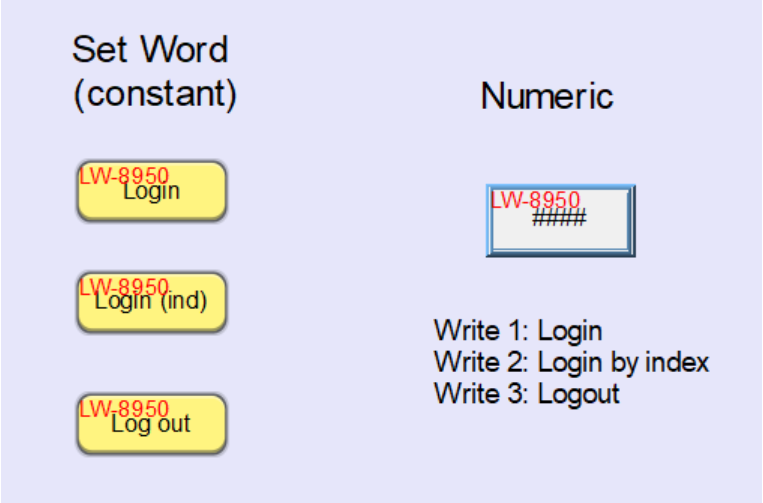
Database Server

For cMT/cMT X series models, data sampling, event log, and operation log may be synchronized to an external MySQL or MS SQL database. Moreover, cMT/cMT X series feature direct database server access by SQL queries. While care must still be taken, given a secure and protected target database server, database server shall serve as a valid alternative to file-based data storage on HMI.

General Data Integrity

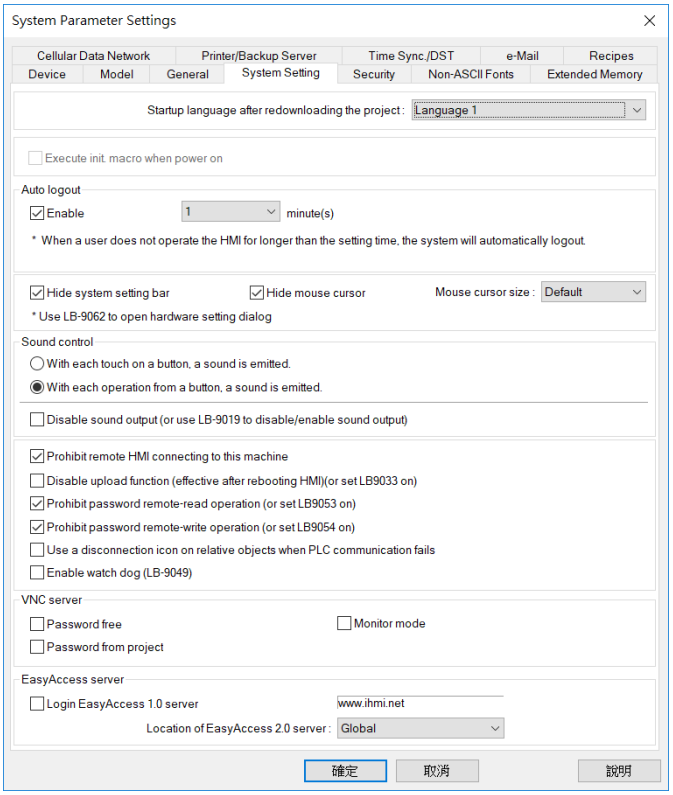
To preserve data integrity, restrict access to system registers and function control addresses of which unintended modification might result in undesirable outcomes. (Sec 11.70) These include, but are not limited to, system registers that effect any historic file change on HMI, control address of enhanced security mode, and control addresses of operation log, data sampling, and event log. What this implies is that the project should not have objects that can possibly be made to access those registers freely. In addition, as it's often overlooked, access from external source needs to be restricted and closely monitored.

Locally, use security and objects that have predictable behavior, instead of ones that allow free adjustment. For instance, use a "Set Word" object writing a constant instead of a numeric object. Also, review the background objects that may affect a wide range of registers, such as macro or Data Transfer and avoid the use of index register without setting its boundary.



Using Set Word vs. Numeric

In terms of access from external source, if any of the control addresses is LW, disable remote HMI access to the HMI (in System Parameter Settings, or with system registers). Also, MODBUS server should not be used. Since MODBUS server registers are mapped directly to LW/LB/RW, any write command to the MODBUS server will affect those registers. In the case where the control address is a PLC address, all access policies to the PLC address must be examined.



Settings that prohibit remote connection to HMI

System Development and Management

1. Design the project so that upon reboot, the entry page will require users to log in before granting any further access. Logging out after a certain period of inactivity if screensaver is used, it should return to the log in page. (Sec 11.10)

2. HMI program can be designed freely, with security feature to enforce operation sequencing to permit sequencing of steps and events, as appropriate. (Sec 11.10)

3. It is important that only authorized and qualified persons should be given access to the system. Anyone who has access to the system should have been properly trained to operate the system. Picture View or PDF readers may be useful in displaying important instructions for the operator.

4. The following features should either not be activated, be deactivated or guarded with password:
   a、 Remote HMI
   b、 PLC control (Page change)

c、 Modbus server
d、 VNC server
e、 cMT Diagnoser (cMT/cMT X Series)
f、 OPC UA server (selected cMT/cMT X Series)
The list should not be deemed exhaustive.

5. Passwords for the followings should be changed from the default password to prevent unauthorized, unwanted access to the system:

   a、 HMI Password (Download, Upload, and Reset data)
   b、 CXOB password (for compilation/decompilation)
   c、 VNC Server (or enable view only mode)
   d、 FTP (upload history password)
   e、 System setting, Update project, History, and User Passwords (cMT/ cMT X Series)
   f、 Web server (cMT/cMT X Series), WebView (cMT X series)
   The list should not be deemed exhaustive.

6. Password-protect the EasyBuilder Pro project.
7. In addition to visual check on site, be aware of the PLC communication parameters at all time to ensure HMI is accessing the intended machine. At runtime, system registers are helpful for viewing the parameters. (Sec 11.10) Alternatively, assign alarm conditions on the parameters to detect any change.

8. Hide the system setting tool bar to avoid unauthorized changes to system settings such as system time, HMI passwords, and other key operations.

9. Do not allow writing to local system time to ensure the correctness of data timestamp. If internet access is available, using a trusted NTP server is one way to ensure the accuracy of timestamp.

10. Latest user manual of Weintek HMI is always available on Weintek's website, www.weintek.com (Sec 11.10)

System Registers

The following table lists the system registers that are relevant. Note this is not an exhaustive list and that the compliance requirements vary by application.

Address	Description
LB-9020	show (set ON)/ hide (set OFF) system setting bar
LW-9081	screen saver time (unit : minute)
LB-9025	delete the earliest data sampling file on HMI memory (set ON)
LB-9026	delete all data sampling files on HMI memory (set ON)
LB-9034	save event/data sampling to HMI, USB disk, SD card (set ON)
LB-11949	delete the earliest data sampling file on SD card (set ON)
LB-11950	delete all data sampling files on SD card (set ON)
LB-11951	refresh data sampling information on SD card (set ON)
LB-11952	delete the earliest data sampling file on USB disk (set ON)
LB-11953	delete all data sampling files on USB disk (set ON)
LB-9022	delete the earliest event log file on HMI memory (set ON)
LB-9023	delete all event log files on HMI memory (set ON)
LB-11940	delete the earliest event log file on SD card (set ON)
LB-11941	delete all event log files on SD card (set ON)
LB-11942	refresh event log information on SD card (set ON)
LB-11943	delete the earliest event log file on USB disk (set ON)
LB-11944	delete all event log files on USB disk (set ON)
LW-9200~LW9260	Address index 0~31
LB-9044	disable remote control (when ON)
LB-9053	prohibit password remote-read operation (when ON)
LB-9054	prohibit password remote-write operation (when ON)
LB-9197	support monitor function only for remote HMIs (when ON)
LB-9198	disable local HMI to trigger a MACRO (when ON)
LB-9199	disable remote HMI to trigger a MACRO (when ON)
LB-12088	enable VNC monitor mode (when ON)
LB-12092	enable VNC (set ON), disable VNC (set OFF)
LB-12361	status of operation log function (OFF : disabled, ON : enabled)

Configuring Initial State

Many of the conditions discussed above require that register values be set when HMI starts. There are a number of ways to do that.

With objects

1. Take a “Set Bit” object and set its action to “Set ON when window opens” or “Set OFF when window opens,” whichever applies.

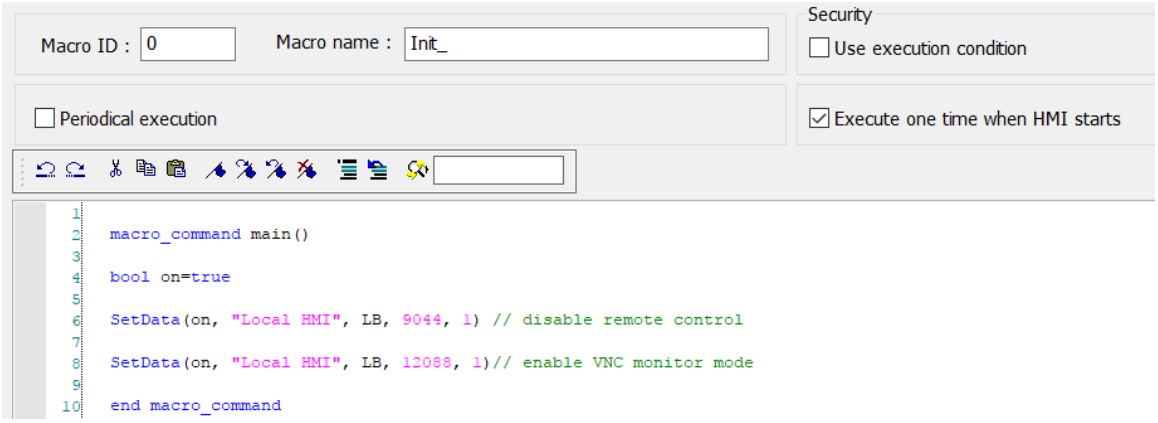
For word registers, use a “Set Word” object and set its action to “Set when window opens” and enter appropriate constant value.”

2. Place the objects in the startup window as specified in the system parameter settings, or in the common window (window no.4)

With macro

1. Write a macro that sets the register values.
2. Enable the option “Execute one time when HMI starts”
3. Alternatively, in System Parameter Settings, under System Setting tab, check the option “Execute init. Macro when power on” and use the macro in the previous step.

The following figure shows sample code for disabling remote control and enabling VNC monitor mode at HMI startup.



Sample Macro Code

Practice

Many of the rules specified in FDA 21 CFR Part 1 can be satisfied by proper configuration and operation of Weintek HMI described in this document. For other requirements not applicable on an HMI, users should establish procedures and follow them strictly in order to meet the regulations.

References

Code of Federal Regulations, Title 21. Electronic Records; Electronic Signatures. (2016)