# 10.User Password and Object Security

This chapter discusses the protection for operations provided by setting up user passwords and security classes.

10.1.	Overview	10-2
10.2.	User Password and Operable Object Classes	10-2
10.3.	Enhanced Security Mode and Control Address	10-6
10.4.	Enhanced Security Mode Usage	10-10
10.5.	Object Security Settings	10-25
10.6.	Example of Object Security Settings	10-30
10.7.	Protecting Password Settings from Unauthorized Editing	10-33
10.8.	Bulk Changing of Security Settings of Multiple Objects	10-34



#### 10.1. Overview

This chapter discusses the protection for operations provided by setting up user passwords and security classes. Authentication modes are:

- General Mode
- Enhanced Security Mode

In addition, cMT / cMT X series allows the use of LDAP protocols for user authentication.

To set up the protection system, please:

- 1. Set user password and operable classes.
- 2. Set object class for objects.

An object belongs only to one security class. Setting the object class to "None" means any user can operate this object.

#### 10.2. User Password and Operable Object Classes

The security parameters can be found in [System Parameter Settings] » [Security].

#### 10.2.1. General Mode

Up to 12 sets of user and password are available. A password should be one non-negative integer. There are six security classes: A to F.

Once the password is entered, the objects that the user can operate are classified. As shown below, "User 1" can only operate objects with class A or class C.

### Note

General Mode is not used for cMT / cMT X Series.

ellula	r Data Net	work 802.1X	(Wi-Fi) P:	rinter/Backup Serve	r Time Sync.	/DST e-Mai	il Recipe I	Databa
Devi	ice	Model	General	System	Remote	Security	Extended Me	mory
۲	General m	ode	hanced s	ecurity mode	L	DAP	Editable	
Selec	t operable:	classes for each	user					
Pass	word rang Enable	e : 0 ~ 4294967: Password	295 Class	A Class B	Class C	Class D	Class E	
Pass No.	word rang Enable	e : 0 ~ 4294967: Password 111111	295 Class	A Class B	Class C	Class D	Class E	-
Pass No. 1 2	word rang Enable	e : 0 ~ 4294967 Password 111111 222222	295 Class	A Class B	Class C	Class D	Class E	-
Pass No. 1 2 3	word rang Enable	Password 111111 222222 333333	Class	A Class B	Class C	Class D	Class E	A
Pass No. 1 2 3 4	word rang Enable V V	Password 111111 222222 333333 0	295 Class [ [	A Class B	Class C	Class D	Class E	•
Pass No. 1 2 3 4 5	word rang	e : 0 ~ 4294967 Password 111111 222222 333333 0 0	Class [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [	A Class B	Class C	Class D	Class E	E
Pass No. 1 2 3 4 5 6	word rang	e : 0 ~ 4294967 Password 111111 222222 333333 0 0 0 0	Class [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [	A Class B	Class C	Class D	Class E	
Pass No. 1 2 3 4 5 6 7	word rang	e : 0 ~ 4294967 Password 111111 222222 333333 0 0 0 0 0 0	Class [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [ [	A Class B V V V V V V V V V V V V V V V	Class C	Class D	Class E	





Click the icon to download the demo project. Please confirm your internet connection before downloading the demo project.

#### 10.2.2. Enhanced Security Mode

Up to 11 users can be set here. In addition, [Administrator] setting is provided. Administrator has all privileges and can operate all object classes. A username can contain Chinese characters, letters, and numbers, and a password can only contain letters and numbers. Each user can have up to 12 operable classes: A to L. (Up to 127 users can be set in Administrator Tools. Please see "10.4 Enhanced Security Mode Usage" for more details.)

Enhanced Security Mode provides a [Control address] for users to manage the accounts directly on HMI. Please see "10.3 Enhanced Security Mode and Control Address" for more details. Alternatively, use USB Security Key to log in automatically. Insert the USB disk in which the key is saved to log in. Please see "10.4.3 Login / Logout Automatically with USB Security Key" for more details. Login can also be achieved using fingerprint or RFID. Upon successful fingerprint recognition or RFID card scanning, the linked account will be automatically logged in, see "10.4.7 Login / Logout with Plugins" for more details.

Dev	Cellular rice	Data Network Model	General	Time Syn Sys	c./DST tem	Remote	e-Mai	il Secu:	ity	FT. Extende	P d Mem	or
C	)General n	10de	Enhanced s	ecurity mode	13	Ex	ternal Se	erver		Edital	ole	
	]Use existi	ng user account	s and administra	tor settings o	n HMI fir	st (if existed).	Otherwi	ise, u	se settings i	below.		
	Enable	Secret user	User n	ame		Password	ł ł		Class A	Class B	Class	
1	1		user1		•••		weak	۲		<b>V</b>		
2	1		user2			••	weak	۲			1	
3			user3		•		weak	۲				
4			user4		•		weak	۲				
5			user5		•		weak	۲			E	
6			user6		•		weak	۲				L
7			user7		••		weak	۲				
8			user8		••		weak	0				
•			III						10 - D		Þ	ĺ
						Plugin			Cla	iss Comme	ent	
Ad	ministratoi Secret use	r r		User nam	e: admir							
				Passwor	d: •••	••••				weal	•	
Co	ntrol	D						_		-		
		Address : PL	oal HMI N	•	8950		<b></b>	16-b:	t Unsigned	≝ ∐∞	00	
										0.00	<u>A0111</u>	
Exec	cute auto.ic Enable	ogin/logout whe	n insert an USB	key into Hiv.		Ĩ	Setti	ngs	. ]	0		
CM.	TP file pas	sword				3 						
	Check p	assword when o	pen CMTP file				Sett	ings.				



# Note

- In Enhanced Security Mode on a cMT / cMT X model, the Control Address can only be assigned to a word register of Local HMI. Please note that security features will work only on HMI when the control address is LW. Remote login on cMT Viewer will not be possible.
- EasyAccess 2.0's HMI Viewer on a eMT/iE/XE/mTV model doesn't support Enhance Security Mode, please use VNC Viewer instead.
- Usernames that contain Chinese characters cannot be changed by using EasyWeb or HMI system settings; they can only be edited in EasyBuilder Pro.

Click the icon to download the demo project. Please confirm your internet connection before downloading the demo project.

#### 10.2.3. LDAP Mode

LDAP (Lightweight Directory Access Protocol) enables applications to access Directory server providing database-like data structure, and here, the primary use of LDAP is to enable centralized user account management. When using LDAP mode, user account management is up to the Directory server, with HMI validating user login via the LDAP protocol. To have LDAP set up on HMI, users only need to provide necessary information about the directory server and set the operable classes for each group, without the need for managing username/password for each user.



ŀΡ										
Enable										
General Error										
Host	: 19	2.	168	-	1.	100		Use doma	in name	
Port	: 389	×								
Base DN	: DC=tes	t,DC=org	1							
Users base DN	: CN=us	ers,DC=te	st,DC=or	9						
Groups base DN	: CN=bu	iltin,DC=1	test,DC=o	rg						
Directory type										
* LDAP is only su	ipported c	on Active	Directory							
Group Name	Class A	Class B	Class C	Class D	Class E	Class F	Class G	Class H	Class I	C
1 Engineer	~	~	~							
2 Management	~	~	~	~	<b>v</b>	~	<b>v</b>	~	$\checkmark$	
3 Sales	~									
III     New     Delete Import from Server										
New										

#### 10.2.4. Remote HMI Mode

In this mode, user accounts can be managed on a remote HMI, instead of the local HMI. The accounts on a remote HMI can be used to log in the local HMI; therefore, managing the accounts on the local HMI is not necessary.



None       LDAP       Remote HMI         General       Remote HMI IP: 192 . 168 . 2 . 158         Result address       Device : cocal HMI         Device : cocal HMI       Image: Cocal HMI         Address : PLW       Image: Cocal HMI         Address : PLW       Image: Cocal HMI         Result address PLW-0       If -bit Unsigned         Result address : PLW       Image: Cocal HMI         Address : PLW       Image: Cocal HMI         Address : PLW       Image: Cocal HMI         Result address PLW-0       If -bit Unsigned         I: Succeeds       State Cocal HMI connot exists         I: Password error       Image: Cocal HMI connot be connected         ID24: Remote HMI cannot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot be connected       Image: Cocal HMI connot be connected         Image: Cocal HMI connot HMI conno	External server		<b>X</b>
General         Remote HMI IP:       192       . 168       . 2       . 158         Pevice :       Local HMI       Image: Color of the color o	None	C LDAP	Remote HMI
Remote HMI IP:       192       168       2       158         Result address       Device :       Local HMI       Image: Color of the	General		
Result address Device : Local HMI Address : PLW  0 I6-bit Unsigned Result address PLW-0 1: Succeeds 3: Account not exists 16: Password error 1024: Remote HMII cannot be connected	Remo	te HMI IP: 192 . 168 . 2 .	158
Device : Local HMI Address : PLW • 0 Is-bit Unsigned Result address PLW-0 1: Succeeds 3: Account not exists 16: Password error 1024: Remote HMI cannot be connected VIII Cannot be connected	-Result addr	ess	
Address:       PLW       0       16-bit Unsigned         Result address PLW-0       1       Succeeds       1         1:       Succeeds       1       1         2:       Account not exists       1       1         1024:       Remote HIMI cannot be connected       1       1	Device	Local HMI	- <u>·</u>
Result address PLW-0         1: Succeeds         8: Account not exists         16: Password error         1024: Remote HIMI cannot be connected	Address	: PLW 👻 0	16-bit Unsigned
1: Succeeds         3: Account not exists         16: Password error         1024: Remote HMI cannot be connected	Result ac	ddress PLW-0	
8: Account not exists 16: Password error 1024: Remote HMI cannot be connected	1: 5	Succeeds	
16 : Password error 1024 : Remote HMI cannot be connected	8: A	Account not exists	
0K Cancel	16: F	assword error	
OK Cancel	1024 : F	Remote HMI cannot be connected	
OK Cancel			
OK Cancel	L		
			OK Cancel

#### **10.3.** Enhanced Security Mode and Control Address

The control address is used for login and account management, with 20 consecutive addresses designated for parameter settings. When employing a cMT/cMT X Series model, LW and PLW registers are available for selection. LW refers to local addresses on the HMI itself, while PLW refers to addresses on the client side, such as cMT-iV5, cMT-iV6, iOS, and Android devices. As each cMT/cMT X series can connect to multiple client devices, the system registers for login and account management operate independently on each client device.

To log in using the control address, select either [user name] or [user index]. Ensure to set [user name] and [password] in advance under [System Parameter Settings] » [Security] » [Enhanced security mode].

#### **10.3.1.** Control Address Settings

When control address is set to LW/PLW-n, where n is an arbitrary number, the following addresses will be designated:

Address	Tag Name	Description
LW/PLW-n (1 word)	command	Commands to be executed: Login, Logout,



		Add/Setting/Delete Accounts, etc.
LW/PLW-n + 1 (1 word)	command execution result	Displays the result of command execution.
LW/PLW-n + 2 (1 word)	user index	The index of accounts (used with Option List Object).
LW/PLW-n + 3 (1 word)	user privilege	Binary value. Level A = bit0, Level B = bit1,
LW/PLW-n + 4 (8 words)	user name	Account name (Case-sensitive and only allows Chinese characters, letters and numbers).
LW/PLW-n + 12 (8 words)	password	Account password (Case-sensitive and only allows letters, numbers, or special characters).

After setting the [Control address], the relevant addresses can be found in [Address Tag Library] » [User-defined tags].For example, setting [Control address] to LW/PLW-0: (UAC stands

for User Account Control)

LW/PLW-0  $\rightarrow$  [UAC command]

LW/PLW-1  $\rightarrow$  [UAC command execution result]

LW/PLW-2  $\rightarrow$  [UAC user index]

LW/PLW-3  $\rightarrow$  [UAC user privilege]

LW/PLW-4 ~ LW/PLW-11  $\rightarrow$  [UAC user name]

LW/PLW-12 ~ LW/PLW-20  $\rightarrow$  [UAC password]

# Note

- In Enhanced Security Mode on a cMT / cMT X model, the Control Address can only be assigned to a word register of Local HMI. Please note that security features will work only on HMI when the control address is LW. Remote login on cMT Viewer will not be possible.
- EasyAccess 2.0's HMI Viewer on a eMT/iE/XE/mTV model doesn't support Enhance Security Mode, please use VNC Viewer instead.

#### 10.3.2. Commands

Setting different values in LW-n [command] enables different commands:

Set Value	Command	Corresponding Address
1	Log in by user name	Set [user name] and [password] first. After entering the user name and password, the system will check if they are valid in [System Parameter Settings] » [Security] » [Enhanced security mode].
2	Log in by user index	Set [user index] and [password] first. Please refer to 10.4.4 Enhanced Security Mode with Option List Object.



3	Log out	
4	Change the password of current logged-in user	Set [user name] and [password] first. Please fill in the original password in [user name] and new password in [password].
5	Add an account	Set [user name], [password] and [user privilege] first.
6	Add a temporary account (minutes)	Set [user name], [password], [user privilege], and [user index] first. [user index] is for specifying a time period (in minutes), within this period the account is valid. If 0 is specified, this account stays valid until the HMI is powered off.
7	Delete an existing account by user name	Set [user name] first.
8	Delete an existing account by user index	Set [user index] first.
9	Setting the privilege of an existing account by user name	Set [user name] and [user privilege] first.
10	Setting the privilege of an existing account by user index	Set [user index] and [user privilege] first.
11	Setting the password of an existing account by user name	Set [user name] and [password] first.
12	Setting the password of an existing account by user index	Set [user index] and [password] first.
13	Read the privilege of an existing account by user name	Set [user name] first. If the command succeeds, [user privilege] can be displayed.
14	Read the privilege of an existing account by user index	Set [user index] first. If the command succeeds, [user privilege] can be displayed.
15	Add a temporary account (days)	Set [user name], [password], [user privilege], and [user index] first. [user index] is for specifying a time period (number of days), within this period the account is valid. If 0 is specified, this account stays valid until the HMI is powered off.
16	Add an expiring account (minutes)	Set [user name], [password], [user privilege], and [user index] first. [user index] is for specifying a time period (in minutes), within this period the account is valid. 0 is an invalid value for this setting.
17	Add an expiring	Set [user name], [password], [user

	account (days)	privilege], and [user index] first. [user index] is for specifying a time period (number of days), within this period the account is valid. 0 is an invalid value for this setting.
18	Remaining minutes for user name	Set [user name] first. If succeeded, the remaining time (in minutes) will be displayed in [user index].
19	Remaining minutes for user index	Set [user index] first. If succeeded, the remaining time (in minutes) will be displayed in [user index].
20	Remaining days for user name	Set [user name] first. If succeeded, the remaining time (number of days) will be displayed in [user index].
21	Remaining days for user index	Set [user index] first. If succeeded, the remaining time (number of days) will be displayed in [user index].

### Note

- Add a temporary account / expiring account: The difference between temporary accounts and expiring accounts is that temporary accounts are not stored in the system and will be invalid after HMI is turned off. Both temporary accounts and expiring accounts will be automatically deleted when they are expired.
- Delete the existing account: The currently logged in account cannot be deleted.
- Offline/Online Simulation: Simulate using the account settings in the program. Any modifications of the account during simulation will not be reserved for next simulation.
- admin: Default administrator account, cannot be deleted, has all privileges and cannot be changed.
- System Register PLW-10754: Displays current user name. (Only available for cMT / cMT X Series)
- The [user privilege] address does not display the privileges assigned to current user account, please use system register LW-9222 to display the privileges.
- LDAP mode does not support login with [user index].
- Click the icon to watch the demonstration film. Please confirm your internet connection before playing the film.

#### 10.3.3. Command Execution Results

After the command is executed, the system will store the result code to control address LW-n + 1. The listed result codes below are shown in hexadecimal format.

<b>Result Codes</b>	Command execution result
(0x001)	Succeeds



(0x002)	Invalid command
(0x004)	Account exists (when adding a new account)
(0x008)	Account not exists
(0x010)	Password error
(0x020)	Deny command
(0x040)	Invalid name
(0x080)	Invalid password character exists
(0x100)	Invalid import data
(0x200)	Out of validity range (when log in by USB Security Key).
	The [Effective Time] can be set in Administrator Tools.



Users can add a new event in Event (Alarm) Log, and designate the [Read address] to LW-n
 + 1 [command execution result]. Open [Message] tab » [Text] » [Content] and specify the message to be displayed in Event Display Object for showing command execution result.

#### 10.4. Enhanced Security Mode Usage

#### **10.4.1.** Importing User Accounts

The user accounts can be set using other tools we provide, apart from the settings in [System Parameter Settings] » [Security] tab. Administrator Tools can also be used to set user accounts. Administrator Tools can be found in the installation directory. After the program starts, select the [User Accounts] check box. Up to 127 accounts can be added.



🔄 Adn	ninistra	ator Tool	s								<b>_</b> ×
	Save	C	ontents of the USE	3 data							
•		V U:	er Accounts								
	USB Security Key										
	e-Mail SMTP Server Settings										
	e-Mail Contacts										
User	r Accou	int Settings	s								
	No.	Secret	User name	Password	Class A	Class B	Class C	Class D	Class E	Class F	Clas
	1		001001	001001							
	2		002002	002002	<b>V</b>		<b>V</b>				
	3		003003	003003	<b>V</b>						
	4		004004	004004	<b>V</b>		<b>V</b>				
•	5		005005	005005	<b>V</b>			<b>V</b>			
	6		006006	006006	<b>V</b>						
<				111							4
		Add		Remove			Impo	ort		Export	
Fff	ective 1	Time									
_											
	Restr	ict the usin	ng terms						_	_	
		2017/	十月 /25 17:27	▼	十月 /25 17:	27 💌 🛋			Save to f	older	-
Help	o Topic	<u>s</u>									

For more information, see "36 Administrator Tools".

The added accounts can be stored in USB disk or SD card and imported in HMI by a Function Key Object. To do so, create a Function Key Object, and select [Import user accounts].



New Fund	ction Key Object						
General	General Security Shape Label						
	Comment :						
	C Activate after button is released						
	×						
	Function mode						
	Import user accounts						
	○ Use [USB Security Key] to Login						
-AS	Data position						
	◯ SD card						
	Account import mode						
	Overwrite   Append						
T	Delete file after importing user accounts						
	OK Cancel						
( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( )	import user data/Use [USB Security Key]						

When finished, insert the external device to HMI, and press Function Key to import accounts. If [Overwrite] is selected, the existing accounts will be overwritten with new accounts and automatically log out after importing. If select [Delete file after importing user accounts] check box, the system will delete the account data saved in the external device after importing. If the [Effective Time] in Administrator Tools is specified, the importing can only be done in the time limit specified. The imported accounts will not be deleted by system when the effective time ends.

#### 10.4.2. Login with USB Security Key

Instead of entering user name and password to login, a key can be used to do so. In EasyBuilder Pro installation directory, launch Administrator Tools, select [USB Security Key] check box. The account information uses the predefined data in [System Parameter Settings] » [Security].



	Contents of the USB data		
	User Accounts		
× 💎	USB Security Key		
	e-Mail SMTP Server Settings		
	e-Mail Contacts		
B Security Ke	ey		
	User name :	admin	
	Password :	•••••	
	Confirm	[ annual	
	comm:	•••••	
fective Time			
fective Time			
fective Time	ne using terms		

# Note

Please note that the user accounts used for USB Security Key must already exist in HMI.

For more information, see "36 Administrator Tools".

USB Security Key can be stored in USB disk or SD card, and create a Function Key to log in by USB Security Key as shown below:



New Fun	Vew Function Key Object						
General	General Security Shape Label						
	Comment :						
	Activate after button is released						
	×						
	Function mode						
	Security key] to Login						
-AS	Data position						
	SD card     O USB disk						
	-						
	F						
H							
	Import user data/Use [USB Security Key]						

When finished, insert the external device to HMI, and press Function Key to log in using USB Security Key. If the [Effective Time] in Administrator Tools is specified, the login can only be done in the time limit specified. The system will log out automatically when the key expires.

#### 10.4.3. Login / Logout Automatically with USB Security Key

As shown below, in [System Parameter Settings] » [Security], select [Enable] check box for [Execute auto. login/logout when insert an USB key into HMI].

📝 Enable			
Status address —			
PLC :	Local HMI		Settings
Address :	LW 🗣 10	00	16-bit Unsigned

This function allows automatic login / logout using an USB security key. Insert the USB disk in which the key is saved to HMI to log in, and remove the USB disk to log out. The login / logout status will be written into a designated address, the result codes of login / logout:

0x00: No Action

0x01: Login Succeeds

0x04: Login Fails

**0x08: Login Succeeds** 

**0x10: Logout Fails** 

For more information about USB Security Key, see "36 Administrator Tools".





# Note

- When Auto Login / Logout is enabled, log in by [Function Key] object is not possible, but it is still possible to log in / out with a designated control address.
- This function does not support On-line / Off-line simulation.
- Only the USB Security Key saved in USB disk is valid.

Click the icon to download the demo project that explains how to use USB Security Key to log in / out. Please confirm your internet connection before downloading the demo project.

#### 10.4.4. Enhanced Security Mode with Option List Object

Enhanced Security Mode uses Control Address LW-n + 2 as account index. With Option List Object, account names and privileges can be displayed. Users can select whether or not to display the account privileges and secret users in Option List. Secret users are set to be hidden in [System Parameter Settings] » [Security] » [Enhanced Security Mode]; their account names will be hidden in Option List if [Secret user] check box is not selected. If the control address is set to LW-0, the monitor address for index of Option List is designated to LW-2.

New Option List Object
Option list Mapping Security Shape Label
Comment :
Mode : Drop-down List - Background :
Selection :
Direction : Down
Source of item data : User account 🗸
Display
Ascending Descending Privilege Secret user
Monitor address
PLC : Local HMI
Address : LW - 2 16-bit Unsigned

#### 10.4.5. LDAP Mode

LDAP (Lightweight Directory Access Protocol) enables applications to access Directory server providing database-like data structure, and here, the primary use of LDAP is to enable centralized user account management. When using LDAP mode, user account management is up to the Directory server, with HMI validating user login via the LDAP protocol. To have LDAP



set up on HMI, users only need to provide necessary information about the directory server and set the operable classes for each group, without the need for managing username/password for each user.



The control addresses used by LDAP Mode are the same as the control addresses used by Enhanced Security Mode. Please see chapter 10.3 in this user manual for more information on the control address. Please note that obtaining LDAP user name using Option List object is not possible; therefore, [Log in by user index] is not supported.

### Note

A user may be a member of multiple groups; in this case, the user has permission to operate all classes assigned for all the groups the user is in. As shown in the following figure, if a user is a member of both Engineer and Sales groups, the user can operate classes A~F.



The credentials in the list in Enhanced Security Mode can also be managed and validated in LDAP mode. Please note that when a username exists in the lists of both modes, the system will only validate user using Enhanced Security Mode. As shown in the following figure, in the case where username Angela exists in the user list in both LDAP server and Enhanced Security Mode, the HMI will validate user under Enhanced Security Mode.

LD	Enhanced Security Mode					
Name	Туре	No.	Enable	Secret user	User name	Password
🔍 Angela	User	1	1		Angela	1
Rella	llser	2	1		Gina	2
Cindu	User	3	1		Helen	3
Cindy	User					
💍 Dora	User					
👗 Elly	User					
📥 Fanny	User					





- LDAP Mode does not support login with [user index].
- LDAP is only supported on Active Directory.
- HMI cannot change user's password; therefore, when adding a new user in LDAP server, please do not select [User must change password next logon].

New Object - User X						
Create in:org/employee						
Password:						
Confirm password:						
User must change password at next logon						
User cannot change password						
Password never expires						
Account is disabled						
< Back Next > Cance	1					

#### 10.4.5.1. General Tab

Set LDAP server and operable classes for each group.



Host:       192       168       1       100       Use domain name         Port:       389       * Default port of LDAP is 389         Base DN:       DC=test,DC=org         Users base DN:       CN=users,DC=test,DC=org         Groups base DN:       CN=bulltin,DC=test,DC=org         Directory type										
•	* LDAP is only su Group Name	Class A	on Active Class B	Directory Class C	Class D	Class E	Class F	Class G	Class H	Class I
1	Engineer	$\checkmark$	~							
2	Management	$\checkmark$	~	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	~	
3	Sales	$\checkmark$								
< III  New Delete Import from Server										

Setting	Description
Host	Set the IP address of the host or use domain name.
Port	By default the port number is:
	LDAP: 389
	LDAPS: 636
Base DN	LDAP server's domain name (DN).
User base DN	Organizational units (OU) that hold users.
Group base DN	Organizational units (OU) that hold groups.
New	Add a new group.
Delete	Delete a group.
Import from	Log in LDAP server using user credentials to import all
Server	allowable groups.
Group Name	Select the operable classes for each group. The group
and Class	name can be 64 words in maximum, case-sensitive, and
	allows letters / numbers / symbols / Unicode.



#### 10.4.5.2. TLS/SSL Tab

Enable settings in this tab for LDAPS (LDAP over SSL) connection with the AD server.

🗸 Enable						
General	TLS/SSL	Error				
🔽 Enable	-	16				
🔽 Se	ver ver <mark>i</mark> ficat	ion ———				
Us	e certificate	on HMI first (i	f existed). Other	wise, use impoi	rted files below.	
CAC	ertificate : N	lone	Import			
						 7

Setting	Description
Enable	Enable TLS/SSL security for secured LDAP
	communication.
Server	When establishing connection, the HMI will verify
verification	whether the certificate supplied by the server matches
	the one stored on HMI.
Use certificate	Lise surrent certificate on HMI or import a new
on HMI (if	costificate
existed)	

#### 10.4.5.3. Error Tab

When LDAP server cannot be connected, an error code shows in the designated address.



LDAP (Lightweight Directory Access Protocol)	
Ceneral SSL Error	
- Error address	
Device : Local HMI	]
Address : PLW v 0 16-bit Unsigned	Ē
Error : PLW-0	
(0: none, 1 or more : error)	

Setting	Descrip	tion	
Error address	The result of login is output to this address.		
	Value	Description	
	0	No error	
	1	1 Error on LDAP server or no password is	
		entered.	
	2	Unknown error	
	257 Remote LDAP server cannot be connected.		
	258	Wrong username or password.	
	259	Verification failed	
	512	Unknown TLS	
	513	Domain name does not match CN.	



#### 10.4.5.4. LDAP Settings (Import from Server)

Get group information from LDAP server.

Fetch all groups	
Group Name	
1 🔽 Engineer	
2 📝 Management	
3 🔽 Sales	

Setting	Description			
Username	Log in LDAP Server using us	Log in LDAP Server using username.		
Password	Log in LDAP Server using pa	Log in LDAP Server using password.		
Fetch all	Fetch all groups of the DN i	Fetch all groups of the DN in LDAP server.		
groups	Error Message	Description		
	Can't contact LDAP server	LDAP server cannot be		
		connected.		
	Invalid Credentials	Invalid Credentials Wrong username or		
		password used for login		
		LDAP server.		
	Unknown	Error on LDAP server or no		
		password is entered.		

# Note

The maximum number of groups allowable in LDAP mode is 128 groups. When importing from LDAP server, the system will check the number of groups in LDAP server first, exceeding 128 groups will result in unsuccessful import.



Importing duplicate group name will not clear the operable classes of that group.

#### 10.4.6. Remote HMI Mode

In this mode, user accounts can be managed on a remote HMI, instead of the local HMI. The accounts on a remote HMI can be used to log in the local HMI; therefore, managing the accounts on the local HMI is not necessary.

External server		×				
None	LDAP	Remote HMI				
General						
Remote	HMIIP: 192 . 168 . 2 . 158	3				
Result addre	/5					
Device : Address :		16-bit Unsigned				
Result add	iress PLW-0					
8: Ad	8: Account not exists					
16: Pa 1024: Re	ssword error mote HMI cannot be connected					
		OK Cancel				
Setting	Description					
Remote HMI IP	The IP address of the	remote HMI that holds the				
	accounts					
cesuit address	when an error occurs	while trying to authentical				
	account or connect to	the remote HMI, the				
	corresponding error c	ode will be output to the				
	designated result add	ress.				

# Note

The accounts can be authenticated via both local and remote HMI. When the same account exists on both local and remote HMI, the authentication is done via the local HMI, instead of the remote HMI. As shown below, user Angela will be authenticated via local



HMI.

			Accounts on Remote HMI			Accounts on Local HMI			
le Secret user	User name	Password			Enable	Secret user	User name	Password	
	Angela	111	weak	(e)	<b>V</b>		Angela	1 weak	
	Bella	222	weak	<u>()</u> 2	<b>V</b>		Amy	2 weak	
	Gigi	333	weak	۵ 3	<b>V</b>		Allen	3 weak	
		Angela Bella Gigi	Angela 111 Bella 222 Gigi 333	Angela     111     weak       Bella     222     weak       Gigi     333     weak	Angela     111     weak     0       Bella     222     weak     0       Gigi     333     weak     0	Angela     111     weak     2     2       Bella     222     weak     3     2	Angela     111     veak     2     2     1       Bella     222     veak     3     2     1	Image: Sector data of the sector d	



#### 10.4.7. Login / Logout with Plugins

After enabling the plugin, users have the option to log in either through a fingerprint recognition device for accounts linked to fingerprints or via a USB scanner for accounts linked to RFID cards or barcodes.

Plugin	Plugin
Fingerprint       USBScanner         Image: Stable of Control       Image: Stable auto login ()         Control       Device : Local HMI         Device :       Local HMI         Address :       PLW         If 6-bit Unsigned	Fingerprint:       USBScanner         Image: Control       Image: Control         Device :       Local HMI         Address :       PLW         Image: Control       Image: Control
OK Cancel	Settings VID 16C0 PID 27DB • Scan USB Devices OK Cancel

When configuring the USB scanner, to prevent interference from other USB devices during login, it's necessary to first set the VID and PID of the USB scanner. After clicking [Scan USB Devices], the system will prompt a message "Please insert your USB Device". Once the USB scanner is inserted into the PC, the system will obtain a unique VID and PID for the USB scanner. Click [Save], and the system will automatically incorporate this VID and PID into the settings.

[Enable auto login]: Select the [Enable auto login] option to keep the fingerprint/USB scanner



10-23

in a state where it is always ready for login, without the need to activate the scanner through a command. To revert to the default state where the scanner is activated via command, use command 7 (Pause auto login) or command 8 (Resume auto login) to pause/resume the auto login status.

#### **Control Address Settings**

When control address is set to PLW-n, where n is an arbitrary number, the following addresses will be designated:

Address	Tag Name	Description
PLW-n (1 word)	Command	Commands to be executed: Login, Add Fingerprint / RFID Card, Remove Fingerprint / RFID Card, etc.
PLW-n + 1 (1 word)	Result	Displays the result of command execution.
PLW-n + 2 (1 word)	Status	The initialization status of the plugin server.
PLW-n + 3 (1word)	Error	The error code from the device server.

#### Commands

Setting different values in PLW-n [command] enables different commands:

Set Value	Command	Corresponding Address
1	Log in by fingerprint / RFID / barcode	
2	Add fingerprint / RFID / barcode by user name	Set [user name] first.
3	Add fingerprint / RFID / barcode by user index	Set [user index] first. Please refer to 10.4.4 Enhanced Security Mode with Option List Object.
4	Remove fingerprint / RFID / barcode by user name	Set [user name] first.
5	Remove fingerprint / RFID / barcode by user index	Set [user index] first.
6	Remove all fingerprints / RFID / barcodes	
7	Pause auto login	
8	Resume auto login	



#### **Command Execution Results**

After the command is executed, the system will store the result code at control address PLW-n + 1.

Result Codes	Command execution result
0	Succeeds
1	Unknown error
6	Canceled
101	Account not linked
115	Authentication failed
Others	System error

#### **Error Codes**

When the plugin server initializes, the system will store the result code at control address PLWn + 3.

Error Codes	Command execution result
0	Initialization succeeds
1	Unknown error
2 or more	System error

#### **10.5.** Object Security Settings

Settings in the Security tab allow users to configure conditions so that the object is operable when the condition is met. The sound emitted when operating the object can be selected. cMT, cMT X Series eMT, iE, XE, mTV Series



#### User Password and Object Security

General Security Shane Font	Ground Security Chara Label
General Socurity Chape Font Safety control Mn. press time Display confirmation request Enable/Display confirmation request Enable/Display confirmation request Enable/Display confirmation request Enable/Display confirmation request Device : Local HMI  ddfres : L6 • 0 Enable if bit is : N • Use control token • 0 Enable if it is : N • Use control token • 1: Control Token - Local Only • Token Library Enable if token is : Acquired • Action : Do nothing when disabled User restriction Object class : Class : A • • Display protection permanently after initial activation Display manifer access denied Make invinible while protected Feedback Sound	General Security Shape Label Safety control Min. press time Display confirmation request Enable/Disable User restriction Object class : Class : A  General Security after initial activation Display warning message if access denied Make invisible while protected Feedback Sound
OK Cancel Help	OK Cancel Help

#### 10.5.1. Security Tab

Setting	Description			
Min. press	Press and hold the object for longer than the [Min. press			
time (sec)	time] set here to activate the object.			
Display	After pressing the object, a dialog appears for operation			
confirmation	confirmation. If the response to this dialog comes later			
request	than the set [Max. waiting time (sec)], this dialog			
	disappears automatically and the operation will be			
	canceled.			
	Please confirm the operation OK Cancel			

#### **10.5.2.** Enable/Disable

When [Use register status/value] or [Use control token] is selected, whether the object is operable is determined by the status of the designated address or acquisition the control token, respectively. As shown in the following figure, only when LB-0 is in OFF state and "2: Control Token" is acquired will this object be operable.



Enable/Disable           Issable           Issable
Mode : Bit
Device : Local HMI   Address : LB   0
Enable if bit is : ON
Control token : 1: Control Token - Local Only 🔻 Token Library
Enable if token is : Acquired
Action : Do nothing when disabled Do nothing when disabled User restriction Hilde when disabled Grayed label when disabled Object crass : proper

The following table describes the action this object will take when it's token is not acquired.

Setting	Description
Do nothing	When the control token is not acquired, the object is still
when disabled	displayed.
Hide when	When the control token is not acquired, the object is
disabled	hidden.
Grayed label	When the control token is not acquired, the label of the
when disabled	object turns gray.
	toggle

#### 10.5.2.1. Use Register Status/Value

When selected, the status of the designated bit/word address determines whether the object is operable.

Mode	Description
Bit	The object is operable when the designated bit is in
	On/Off state.
Word	When [Use Register Status/Value] and [Word] are both
	selected, the status of a designated word address
	determines whether the object is operable.
	Enable if value is: >, <, ==, <>, >=,<=
	When the value in the word address reaches the
	condition specified here, the object is operable.
	<b>Tolerance:</b> This setting is available for <> and ==.
	<>: The object will be operable when:
	value in address > [value in address + tolerance]
	or
	value in address < [value in address - tolerance]
	==: The object will be operable when:
	value in address is between [value in address + tolerance]



	and [value in address - tolerance] (including value in address $\pm$ tolerance)			
	For example: Enable/Disable Vode : Word Device : Local HMI Address : WW • 0 16-bit Unsigned Enable if value is : • 10 Tolerance : 1 When the value in the designated word address is			
	between 9~11, the object is operable.			
Condition	When [Use Register Status/Value] and [Condition object]			
object	are both selected, whether the object is operable is			
	determined by the On/Off state output by the specified			
	Condition object.			

### Note

 Word objects supported on cMT/cMT X Series include: Set Word, Numeric, ASCII, Combo Button.

Word objects supported on iE/XE/eMT/mTV Series include: Set Word, Numeric.

#### 10.5.2.2. Control Token



One cMT / cMT X HMI can be simultaneously controlled by multiple cMT Viewer clients. To ensure system safety by preventing an object to be controlled by multiple clients simultaneously, a control token can be set. Only one cMT Viewer client can acquire the control token at a time, and only the cMT Viewer client that acquires control token can operate the object. The rest of the clients can acquire the token one by one when the token is not occupied.

The applicable objects include: Combo Button, Numeric, ASCII, Direct Window, and Indirect



Californ	Desertation				
Setting	Description				
Control Token	Select a control token for the object.				
Token Library	Add/delete control token.				
	For more information, please see "Chapter 34 Control				
	Token" in this user manual.				
Enable if Token is	When [acquired] is selected, only the device that				
	obtains the control token can operate the object.				
	When [unacquired] is selected, only the devices that				
	do not obtain the control token can operate the				
	object.				

#### 10.5.3. User Restriction

Set the security class of the object to be operated by an authorized user.

User restriction	
Object class :	Class : A 🗸 🗸
📃 Disable protec	tion permanently after initial activation
📃 Display warni	ng message if access denied
🔲 Make invisible	e while protected

Setting	Description
<b>Object class</b>	"None" means any user can operate this object. Only
	account "admin" can operate "Administrator" object
	class.
Disable	Once the permitted class of the user matches that of the
protection	object, the system will stop checking the security class
permanently	permanently, that means, any user can operate this
after initial	object freely after it is unlocked.
activation	
Display	When an unauthorized user attempts to operate the
warning	object, a warning dialog (Window no. 7) appears. The
message if	content of the message in the dialog can be modified.
access denied	
Make invisible	When the user's privilege does not match the object
while	class, the object will be hidden.
protected	





#### **10.6.** Example of Object Security Settings

The following shows an example of setting object security class:

 Create a project, go to [System Parameter Settings] » [Security] » [General] to enable 3 users:

User 1 = Operable class: A

User 2 = Operable class: A, B

User 3 = Operable class: A, B, C

2. Design Window no. 10 as shown:



Create two [Numeric Input] objects:

[LW-9219] User no. (1~12), Length = 1word

[LW-9220] For entering user password. Length = 2 words

Create a [Numeric Display] object:

[LW-9222] Displays the operable object class of current user. (16-bit Binary)

Create a [Set Bit] object

[LB-9050] logout

Create three [Set Bit] objects:

Each set to different classes but all select [Made invisible while protected].

**3.** After setting, please save and compile the project and execute off-line simulation. The below shows how it works when simulating.



User name : 1
Password : 0 LW9220
hit 15 hit 0
Current status : 00000000000000000000000000000000000
Logout LB9050



User name : 3 LW9219 Password : 333 LW9220 bit 15 bit Current status : 00000000000000 LW9222 Logout LB9050 Before entering the password, it displays "000000000000000, which means that the user operable object class is "None". [Class A Button] ~ [Class C Button] objects are classified from "A" to "C" and selected [Made invisible while protected]; therefore they are hidden at this moment.

Enter User 1 password "111". Since User 1 is only allowed to operate class A objects, [Class A Button] object appears for operating. [LW-9222] bit 0 turns to "1" means that user can operate class A objects.

Enter User 3 password "333". Since User 3 is allowed to operate class A, B, C objects, [LW-9222] bit 0 ~ bit 2 turns to "1", means that user can operate class A ~ C objects.

Click [Logout] button to log out, the system will return to the initial state, and current user can only operate class "None" objects.



# Note

- Password input: If the password is incorrect, [LB-9060] will be ON; if the password is correct, [LB-9060] will be OFF. All user passwords (User 1 to User 12) can be obtained from system registers [LW-9500] ~ [LW-9522], 24 words in total.
- Changing password directly on HMI: When [LB-9061] is set ON, the system will read data in [LW-9500] ~ [LW-9522] to update user password. The new password will be used in future operations. Please note that the user operable object classes will not be changed due to the change of password.



#### **10.7.** Protecting Password Settings from Unauthorized Editing

Before sending the project to others who may edit the project afterwards, it is recommended to click [Editable] button in Security settings tab to open read-only mode. This mode can protect password settings from unauthorized editing.

Cellular Data Network Pri		nter/Backup Server	Time Sync./DST		e-Ma	il	Recipes		
Device	Model	General	System Setting	Security	Non-ASC	II Fonts	Extended Memory		
🔘 General mode		mode	Enhanced security mode		Г	Editable			
Select op	erable class e existing u	es for each user ser accounts on 1	HMI first (if existed).	Otherwise, us	e settings bela	ow.			
No.	Enable	Secret user	User name	Password		Class A	Class I	B 🔺	
▶ 1	V	<b></b>	user1	1		V	8		
2	V	(m)	user2	2		1	1	/ E	
3			user3	3		1	E		
4	(m)	(C)	user4	4		V	E	-	
5		<b></b>	user5	5		V	E		
6		(m)	user6	6		1	17	T	
Class Admini Sec Control	sC strator ret use laddre: PLC Lddress : I	Password :	111111 Mask password + 8950	(1 ~ 429496	07295) DK	Cancel		-	
En 📝	able		Setting	s					
Execute : En Status a	auto.login/l able ddress PLC : [] Address : []	ogout when inse .ocal HMI .W	rt en USB key into H	MI	▼ Se 16-bit	ttings Unsigned			

When [Enable read-only] is selected, a password will be required for changing security settings in the project.

When [Mask password] is selected, passwords will be masked by asterisks (\*).



The protected projects cannot be decrypted since they are encrypted by users, therefore, please remember your password.



Selecting multiple objects in a group and then selecting [Security settings] in the right-click menu can open an Objects' Security Properties window that allows users to change the security settings of all the selected objects at a time.

Safety control			1
👿 Display confirmation request		Max. waiting time (sec) : 10	
Enable/Disable			
👿 Use registe:	r status/value		-
It Bit		💿 Word	
Device :	Local HMI	✓ Settings	-
Address :	LB	• 0	
* For environn	nent of using multiple clien	ts (cMT Viewers). Action : Do nothing when disabled	-
-User restriction	l Clam : A		_
Object class : [			_
Object class : ( Disable pr Display w Make inv: * If the user tri	rotection permanently after aming message if access de isible while protected es to operate on an object w	initial activation nied vithout authorization, LB-12056 will be set to Ol	¥.
Object class : ( Disable pr Display w Make inv: * If the user tri Sound	rotection permanently after aming message if access de isible while protected es to operate on an object w	initial activation nied vithout authorization, LB-12056 will be set to Ol	¥.
Object class : ( Disable pu Display w Make inv: * If the user tri Sound Fable	rotection permanently after aming message if access de isible while protected es to operate on an object w Sound LibraryBeep	initial activation nied vithout authorization, LB-12056 will be set to Ol	¥.
Object class : [ Disable pn Display w Make inv: * If the user tri Sound Enable	rotection permanently after aming message if access de isible while protected es to operate on an object w Sound Library Beep Play	initial activation nied vithout authorization, LB-12056 will be set to Ol	N.

# Note

When the selected objects have different security settings pages, Objects' Security Properties will automatically adjust and show the settings that users are allowed to change. The rest of the settings will be hidden or greyed out. The following is a window that shows when selecting a Bit Lamp and a Numeric object.



e	
security	
Enable/Disable —	
Vse register st	atus/value
O Bit	Word
Device : L	ocal HMI
Address : L	B VO
Enable if bit is :	ON -
	Action : Hide when disabled
User restriction —	
Object class : Cla	ass : A
Make invisib	le while protected
	a

