

# **MIX60M**

## **WEB Configuration Manual**

# 【Contents】

<b>—WEB Configuration—</b> .....	<b>1</b>
Logon WEB .....	1
Premise.....	1
WEB IE Browser .....	1
<b>Main Window (Terminal Status)</b> .....	<b>2</b>
Illustration of Terminal Status.....	3
<b>User Administration</b> .....	<b>4</b>
Access Log/Query and Report .....	4
Illustration of Access Log .....	5
Auto Refresh Log.....	6
View User List .....	7
Illustration of User List .....	8
Modify User Record.....	9
Modify User List in “View User List” .....	10
Add User .....	11
Illustration of Add New User.....	12
<b>Terminal</b> .....	<b>13</b>
Terminal Status.....	13
Illustration of Terminal Status.....	14
Terminal Setup .....	15
Illustration of Terminal Configuration .....	16
Password Setup .....	18
Illustration of WEB Logon Setting/Entrance Password .....	19
System Log .....	21
Illustration of System Log.....	21
Clock Setup.....	22
Illustration of System Clock Setup .....	22
<b>Access Control</b> .....	<b>23</b>
Time Set .....	23
Illustration of Time Set .....	23
Time Zone Setup .....	24
Illustration of Time Zone List .....	24
Illustration of Time Zone Information .....	25
Group List .....	26

Illustration of Group List .....	26
Illustration of Group Information .....	27
Holiday Setup.....	28
Illustration of Holiday Setup.....	28
Door Setup .....	29
Illustration of Door Setting .....	30
Illustrations of Door Setup.....	33
Illustrations of BF-50 Card .....	35
Set WebPass .....	36
Remote Control.....	37
Illustrations of Door Status Monitoring/Security Bypass .....	38
Event Handle.....	39
Illustration of Event Handle.....	40
Multi Badge Group .....	44
Illustration of Multi Badge Group .....	44
<b>Tools.....</b>	<b>45</b>
IP Camera.....	45
Illustration of IP Camera .....	46
Backup .....	47
Illustration of Backup.....	47
Restore .....	48
Illustration of Restore.....	48
Reboot .....	48
Illustration of Reboot .....	48
Upgrade Firmware .....	49
Illustration of Upgrade Firmware .....	49
Reset.....	50
Illustration of Reset.....	50
<b>Appendix I .....</b>	<b>51</b>

Copyright @ 2009. All Rights Reserved.

Document Version: 1.2

All trademarks and trade names are the properties of their respective owners.

# — WEB Configuration —

## MX60M WEB Configuration

### ◆ Logon WEB

MX60M is with built-in HTTP server for using WEB IE Browser to connect MX60M and execute the settings of MX60M.

### ◆ Premise

Please make sure the following points before your MX60M settings:

Your PC computer may build up a physical connection with MX60M, meanwhile, both of your computer and the MX60M are within the same Network Segment.

MX60M has been installed and with power.

Should the default IP address of MX60M (192.168.0.66) has been occupied by other devices, you have to shut down all the other devices until the setting completed. Then a new IP address will be distributed to the MX60M.

### ◆ WEB IE Browser

- 1、Start the WEB IE Browser first.
- 2、Enter the <http://> and the IP address of MX60M in the address bar. For example, enter the default IP address of MX60M: <http://192.168.0.66>.


#### **Communication failure:**

When no feedback from the MX60M, please check as below:

- Is the MX60M installed properly, the local area network (LAN) connected well or the power connected fine? Try to use the “ping” command to test the communication status of MX60M IP address by the following steps:
  - Open a MS-DOS window, or a command window;
  - Input your command: ping 192.168.0.66,  
For example : C:\user\tank>ping 192.168.0.66
- If no any response, it means abnormal connection or the PC computer IP address in conflict or not match with MX60M IP address (referring to next paragraph) .
- If a PC computer with a Static IP/Fixed IP, the IP range should be defined between 192.168.0.1~ 192.168.0.65 or 192.168.0.67~192.168.0.254. So the PC computer IP may be compatible with the default IP address of MX60M, 192.168.0.66. Moreover, the Subnet Mask should be as 255.255.255.0 .
- To make sure both your PC computer and the MX60M in the same Network Segment.

## ➤ Main Window (Terminal Status)

When installation completed and well connected with MX60M, the “MAIN WINDOW” will pop up. It will show after the following connection frequently as following illustration:



**TERMINAL STATUS**

<b>Product Name :</b>	SEMAC-S2(20000)
<b>Serial No. :</b>	02f1db(153121)
<b>Firmware Version :</b>	1.50.00, Apr 18 2013(HW1.1)
<b>System Time :</b>	01/01/2000 01:04:36
<b>Terminal ID(MAC Address) :</b>	1(00:0e:e3:02:f1:db)
<b>IP Address :</b>	192.168.2.77
<b>Subnet mask :</b>	255.255.255.0
<b>Default Gateway :</b>	192.168.2.1
<b>Primary DNS :</b>	168.95.1.1
<b>Listen Port/Software IP(status) :</b>	2000/0.0.0.0(Offline)
<b>Web Management Port :</b>	80
<b>Registered User :</b>	0
<b>Available User Capacity :</b>	20000
<b>Access/System Log Count :</b>	0/20
<b>Control Mode :</b>	2 doors(1 way)(WG34)
<b>Anti-Pass-Back(Tolerance Timer) :</b>	Disabled(0)
<b>Anti-Duress :</b>	Disabled
<b>Next SEMAC(status) :</b>	0.0.0.0(Offline)

## ◆ Illustration of Terminal Status

Browse the Function Menu Bar at the left side of the Main Window by IE Browser.

► User Administration	
<b>Access Log</b>	Switch to the “Access Log” screen.
<b>Auto Refresh Log</b>	Display real time access log(s) for system
<b>View User List</b>	Switch to the “User List” screen to Modify, Delete, Deactivate and Activate the data.
<b>Add User</b>	Switch to the “User Record” screen and “Add New User”.
► Terminal	
<b>Terminal Status</b>	Switch to the “Terminal Status” screen ( Main Window)
<b>Terminal Setup</b>	Switch to the “Terminal Setup” screen.
<b>Password Setup</b>	Switch to the “WEB Logon Setting” and “Entrance Password” screen.
<b>System Log</b>	Switch to the “System Log” screen.
<b>Clock Setup</b>	Switch to the “System Clock Setup” screen.
► Access Control	
<b>Time Set</b>	Switch to the “Time Set” screen.
<b>Time Zone Setup</b>	Switch to the “Time Zone List” screen.
<b>Group List</b>	Switch to the “Group List” screen.
<b>Holiday Setup</b>	Switch to the “Holiday Setup” screen.
<b>Door Setup</b>	Switch to the “Door Setting” screen.
<b>Remote Control</b>	Switch to the “Door Status Monitoring” and “Security Bypass” screen.
<b>Event Handle</b>	Switch to the “Event Handle” screen.
<b>Multi Badge Group</b>	Switch to the “Multi Badge Group” screen.
► Tools	
<b>IP Camera</b>	Switch to the “IP Camera Configuration “screen.
<b>Backup</b>	Backup Database, User Data, User List from SEMAC system
<b>Restore</b>	Restore Database, User List from the selected backup files
<b>Reboot</b>	Switch to the “Reboot System “screen.
<b>Upgrade Firmware</b>	Switch to the “Firmware Upgrade “screen.
<b>Reset</b>	Switch to the “Reset “screen.
► Button	
<b>Refresh</b>	Refresh the WEB Status.

## ➤ User Administration

### ◆ Access Log/Query and Report

Select "Access Control" on the Main Window, you'll see the "Access Log" screen as the following picture:

#### Access Log/Query and Export

No.	User ID	User Name	Date	Time	IN/OUT	Door	Note.
1.	---	---	08/20/2013	01:51:57	---	2	(None)Closed after alert
2.	---	---	08/20/2013	01:51:57	---	1	(None)Closed after alert
3.	---	---	08/20/2013	01:51:58	---	8	(None)BF50 Online
4.	---	---	08/20/2013	01:51:58	---	4	(None)BF50 Online
5.	---	---	08/08/2013	12:53:30	---	1	(None)Emergency Close
6.	---	---	08/08/2013	12:53:22	---	1	(None)Emergency Open
7.	---	---	08/08/2013	12:53:13	---	8	(None)Forced Close
8.	---	---	08/08/2013	12:53:13	---	7	(None)Forced Close
9.	---	---	08/08/2013	12:53:13	---	6	(None)Forced Close
10.	---	---	08/08/2013	12:53:13	---	5	(None)Forced Close
11.	---	---	08/08/2013	12:53:13	---	4	(None)Forced Close
12.	---	---	08/08/2013	12:53:13	---	1	(None)Forced Close
13.	---	---	08/08/2013	12:53:02	---	3	(None)Forced Close
14.	---	---	08/08/2013	12:53:02	---	2	(None)Forced Close
15.	---	---	08/08/2013	12:42:54	---	1	(None)Enable Fire Alarm
16.	---	---	08/03/2013	01:31:47	---	8	(None)BF50 Online
17.	---	---	08/03/2013	01:31:47	---	4	(None)BF50 Online
18.	---	---	04/20/2013	07:50:07	---	8	(None)BF50 Online
19.	---	---	04/20/2013	07:50:07	---	4	(None)BF50 Online
20.	---	---	04/18/2013	21:11:02	---	8	(None)BF50 Online

Total 55 Record(s)

<< First | Prev 10 | 1 2 3 | Next 10 | End >>

#### Query and Export

Type	Selection	Start Date	End Date
<input checked="" type="radio"/> user <input type="radio"/> event	<input checked="" type="radio"/> Single <input type="radio"/> All	<input type="text" value="2013/05/20"/>	<input type="text" value="2013/05/20"/>
User ID	Card No.(DEC)		
<input type="text"/>	<input type="text"/>		
Export Type			
<input checked="" type="radio"/> Txt <input type="radio"/> Xls	<input type="button" value="Search"/>	<input type="button" value="Export"/>	

## ◆ Illustration of Access Log

▶ Access Records Illustration by Columns	
<b>No.</b>	Serial Number
<b>User ID</b>	Display the User ID for who have access the door. Clicking User ID from the access log will direct to the User Record screen for further modification.
<b>User Name</b>	A Name registered for the User to get IN/OUT. When the registered information without “Name”, this column will be blank.
<b>Date</b>	A Date allowed for the User to get IN/OUT.
<b>Time</b>	A Time allowed for the User to get IN/OUT.
<b>IN/OUT</b>	<p><b>2 Door/1 Way:</b>            IN : Open the door by sensing your Card at the “IN”Wiegand Reader installed for Door 1 or Door 2.            OUT : Open the door by pressing the push button at “OUT” location of Door 1 or Door 2.            ※ The figure in the parentheses ( ) after the “IN/OUT” record means the APB(Anti Pass Back) level.</p> <p><b>1 Door/2 Way:</b>            IN : Open the door by sensing your Card at the “IN”Wiegand Reader installed for Door 1.            OUT : Open the door by sensing your Card at the “OUT” Wiegand Reader installed for Door 1.            ※ The figure in the parentheses ( ) after the “IN/OUT” record means the APB (Anti Pass Back) level.</p> <p><b>When BF-50 connected:</b>            IN : The readers of door 3~door 8 connected with BF-50 for entering will sense the cards and open the door(s).            OUT : The readers of door 3~door 8 connected with BF-50 for exiting will sense the cards and open the door(s).</p>
<b>Door No.</b>	It stands for the Door Number controlled by MX60M.
<b>Note</b>	Show up the relative IN/OUT records automatically as Anti-Duress, Fire Alarm.....etc.
<b>the First Page</b>	Back to the 1st IN/OUT records page.
<b>the Former10 pages</b>	Forwarding 10 pages from the current IN/OUT records page.
<b>1 2 3...N page</b>	Change to any IN/OUT records page assigned.
<b>the Latter 10 pages</b>	Backwards 10 pages from the current IN/OUT records page.
<b>the Last Page</b>	Fly to the last IN/OUT records page directly.



► Query and Export	
<b>Type</b>	1、 <b>User:</b> Select user(s) for query access logs by User types and export records. 2、 <b>Event:</b> Select event(s) for query access logs by Event types and export the records.
<b>Selection</b>	1、 <b>Single:</b> Query / Export a single user's access to records or 5 records of the event within an event 2、 <b>All:</b> Can query / export all of the Access record or record of events
<b>Start/End Date</b>	Select the date by "Drop Down Menu".
<b>User ID</b>	Enter user ID to query Searchable/Export
<b>Card No</b>	Enter Card No to query Searchable/Export
<b>Event</b>	Click event Enter Event type query 5 maximum query event types.
► Button	
<b>Search</b>	Set the Search Requirement Click button to Search access records to demonstrate Requirement.
<b>Export</b>	Set the Export Requirement Click button to Export requirement TEXT or Excel file.

## ◆ Auto Refresh Log

Press Auto Refresh Log from the function menu to refresh screen:

Auto Refresh Log Tue May 21 2013 09:44:34 UTC+0800						
No.	User ID	User Name	Date	Time	IN/OUT Door	Note.

## ◆ View User List

Select 1"View User List" on the Main Window, you'll see the "User List" screen as the following picture:

**User LIST**

Search User :   By User ID  By Card No.  By User Name

No.	User ID	User Name	User Type	*Reg Type: F(Fingerprint) , P>Password) , C(Card)			Bypass Level
			Active	F	P	C	
No Registered User							

**Activate, Deactivate or Delete SELECTED Employee**

MAX60M

## ◆ Illustration of User List

▶ Search User	
<b>By “User ID”</b>	Select “User ID”and Enter your “User ID”in the textbox to search.
<b>By “Card No.”</b>	Select “Card No.”and Enter your“Card No.”in the textbox to search.
<b>By “User Name”</b>	Select “User Name.”and Enter your“User Name”in the textbox to search.
<b>Click button “GO”</b>	Start to search.
<b>Steps :</b>	
<b>1 、 Enter your “User ID”, “Card No.” or “User Name” in the “blank textbox”.</b> <b>2 、 Click button “GO” to search.</b>	
▶ User List	
<b>No.</b>	Serial Number. Tick the box before the “Serial Number” and Click the button of “Activate” , “Deactivate” or “Delete” to manage the authorization of “Activate” , “Deactivate” or “Delete” for selected users, multi-selection is allowed.
<b>User ID</b>	User’s ID. Click the “User ID” to enter the “Modify User Record” page (picture 4 ).
<b>User Type</b>	Types of the User. Whenever the “User Type” is set up in the screen of “Modify User Record”, this page will display Normal User, Super User, Visitor, Guard Touring and Defense Card according to the setup.
<b>Active</b>	Display the user’s authorization status. Green Light means the user’s authorization is Activated, otherwise it is not activated.
<b>F</b>	Not Support
<b>P</b>	When the user’s Personal Password registered, this column will be with Green Light.
<b>C</b>	When the user’s card registered, this column will be with Green Light.
<b>Bypass Level</b>	Display the user’s Time Zone level of Bypass from L1~L10.
<b>the First Page</b>	Back to the 1st page of “User List”.
<b>the Former10 pages</b>	Forwarding 10 pages from the current “User List” page.
<b>1 2 3...N page</b>	Change to any “User List” page assigned.
<b>the Latter 10 pages</b>	Backwards 10 pages from the current “User List” page.
<b>the Last Page</b>	Fly to the last “User List” page directly.
▶ Button	
<b>Activate</b>	Activate the User’s authorization.
<b>Deactivate</b>	Deactivate the User’s authorization.
<b>Delete</b>	Delete the User’s information registered.

## ◆ Modify User Record

### User RECORD

#### Modify User Record

---

User ID :  (1 ~ 20000 )

Card No. :

Name :  (Max 31 chars.)

Expire Date Check :  Disable  Enable

From  (Y)  (M)  (D)  (H)  (M)

To  (Y)  (M)  (D)  (H)  (M)

Status :  Activate  Deactivate

User Type :

Group : 1.  2.  3.  4.

Bypass TZ Level :

Personal Password :  (4 ~ 8 digits.)

Personal Confirm :

---

## ◆ Modify User List in “View User List”

► User Record	
<b>User ID</b>	Only the digit from 1~20000 is allowed, whenever over 20000 not accepted.
<b>Card No.</b>	It can be input by manual or by Card Reader.
<b>Name</b>	User's Name, max. 31 characters allowed.
<b>Expire Date Check</b>	Tick the box of “Enable” or “Disable” the user's expiry date control.
<b>Effective From ~To</b>	When “Enable” the “Expire Date Check”, you must enter the period of dates. The” Drop Down Menu” offers you the options of Year/Month/Date/Hour/Minute.
<b>Status</b>	Tick the box of “Activate” or “Deactivate” for an authorization to the user.
<b>User Type</b>	<p>Card Types of the User. The “Drop Down Menu” will list out cards for <b>Normal User, Super User, Visitor, Guard Touring, Defense Card, Manager Card-Add, Manager Card-Delete</b> as your choice. The Respective definitions are as below :</p> <p><b>Super User Card</b> : Not constrained by the limitation of APB ( Anti Pass Back).</p> <p><b>Visitor Card</b> : You may manage the visitors easily by setting the Visitor Card's Expiry Dates.</p> <p><b>Guard Touring</b> : When the Guard Touring card senses the door, only the Logs will be kept but no door-open function.</p> <p><b>Defense Card</b> : When the card sweeps the door, all the doors will activate Access Control at once. Any type of card cannot open the door until the Defense Card sweeps the door again to restore normal functions.</p> <p><b>Manager Card-Delete</b> : Assigning an user with Manager card-Delete user type for the system</p> <p><b>Manager Card-Add</b> : Assigning an user with Manager card-Add user type for the system</p>
<b>Group</b>	Each user can be assigned to 4 different groups. All of the group names existed will be automatically listed out by the “Drop Down Menu” for your choice. “Free Time Group” is a “Default Group”.
<b>Bypass TZ Level</b>	The “Bypass Time Zone Level” of each user is from L1~L10. Whenever the user's “Bypass Time Zone Level” is higher than or equal to the door's level, the door's “Bypass Time Zone”becomes invalid.
<b>Personal Password</b>	4~8 digits are required.
<b>Personal Confirm</b>	Reconfirm Personal Password.
► Button	
<b>previous</b>	Modify previous user record.
<b>save</b>	Save the modified user record.
<b>delete</b>	Delete existing user record.
<b>next</b>	Modify next user record.

## ◆ Add User

Select "Add User" on the Main Window, you'll see the User Record " screen for Add New User as the following picture:

### User RECORD

#### Add New User

---

REG :  Single  Continuous    Amount :

User ID :  (1 ~ 20000 )

Card No. :

Name :  (Max 31 chars.)

Expire Date Check :  Disable  Enable

From 2009 (Y) 09 (M) 15 (D) 13 (H) 39 (M)

To 2009 (Y) 09 (M) 15 (D) 13 (H) 39 (M)

Status :  Activate  Deactivate

User Type : Normal User

Group : 1. Free Time Group  2. Free Time Group  3. Free Time Group  4. Free Time Group

Bypass TZ Level : L1

Personal Password :  (4 ~ 8 digits.)

Personal Confirm :

---

save

## ◆ Illustration of Add New User

► User Record	
<b>REG</b>	Single: Only one user can be registered each time. Continuous: It allows you to register 1~20000 users continually. You may input required q'ty in the textbox of Amount. However, only the serial number is accepted and supported.
<b>User ID</b>	Only the digit from 1~20000 is allowed, whenever over 20000 not accepted.
<b>Card No.</b>	It can be input by manual or by Card Reader.
<b>Name</b>	User's Name, max. 31 characters allowed.
<b>Expire Date Check</b>	Tick the box of "Enable" or "Disable" the user's expiry date control.
<b>Effective From ~To</b>	When "Enable" the "Expire Date Check", you must enter the period of dates. The "Drop Down Menu" offers options of Year/Month/Date/Hour/Minute.
<b>Status</b>	Tick the box of "Activate" or "Deactivate" for an authorization to the user.
<b>User Type</b>	Card Types of the User. The "Drop Down Menu" will list out cards for <b>Normal User, Super User, Visitor, Guard Touring, Defense Card, Manager Card-Add, Manager Card-Delete</b> as your choice. The Respective definitions are as below : <b>Super User Card</b> : Not constrained by the limitation of APB (Anti Pass Back). <b>Visitor Card</b> : You may manage the visitors easily by setting the Visitor Card's Expiry Dates. <b>Guard Touring</b> : When the Guard Touring card senses the door, only the Logs will be kept but no door-open function. <b>Defense Card</b> : When the card sweeps the door, all the doors will activate Access Control at once. Any type of card cannot open the door until the Defense Card sweeps the door again to restore normal functions. <b>Manager Card-Delete</b> : Assigning an user with Manager card-Delete user type for the system <b>Manager Card-Add</b> : Assigning an user with Manager card-Add user type for the system
<b>Group</b>	Each user can be assigned to 4 different groups. All of the group names existed will be automatically listed out by the "Drop Down Menu" for your choice. "Free Time Group" is a "Default Group".
<b>Bypass TZ Level</b>	The "Bypass Time Zone Level" of each user is from L1~L10. Whenever the user's "Bypass Time Zone Level" is higher than or equal to the door's level, the door's "Bypass Time Zone" becomes invalid.
<b>Personal Password</b>	4~8 digits are required.
<b>Personal Confirm</b>	Reconfirm Personal Password.
► Button	
<b>save</b>	Save user records.

## ➤ Terminal

### ◆ Terminal Status

Select and Click "Terminal Status" on the left side of the Main Window, you'll see the "Terminal Status" screen. This screen is the Main Window for Logon. It displays the current Terminal Status and relative information of WEB setup, referring to the following picture:

## TERMINAL STATUS

<b>Product Name :</b>	SEMAC-S2(20000)
<b>Serial No. :</b>	000201(162017)
<b>Firmware Version :</b>	0.11.00,Sep 15 2009(HW1.0)
<b>System Time :</b>	09/15/2009 13:40:57
<b>Terminal ID(MAC Address) :</b>	1(00:0e:e3:00:02:01)
<b>IP Address :</b>	192.168.2.20
<b>Subnet mask :</b>	255.255.255.0
<b>Default Gateway :</b>	192.168.2.1
<b>Primary DNS :</b>	168.95.1.1
<b>Listen Port/Software IP(status) :</b>	2000/192.168.2.104(Online)
<b>Web Management Port :</b>	80
<b>Registered User :</b>	1
<b>Available User Capacity:</b>	19999
<b>Access/System Log Count :</b>	12633/73
<b>Control Mode :</b>	2 doors(1 way)(WG26)
<b>Anti-Pass-Back(Tolerance Timer) :</b>	Disabled(0)
<b>Anti-Duress :</b>	Disabled
<b>Next SEMAC(status) :</b>	0.0.0.0(Offline)



## ◆ Illustration of Terminal Status

► Terminal Status	
<b>Product Name</b>	Model Number of MX60M
<b>Serial No.</b>	Serial Number of MX60M
<b>Firmware Version</b>	Firmware and Hardware Version of MX60M
<b>System Time</b>	System Time of MX60M
<b>Terminal ID (MAC Address)</b>	Terminal ID and MAC address of MX60M
<b>IP Address</b>	IP address of SECMAC-S2
<b>Subnet mask</b>	Subnet mask of MX60M
<b>Default Gateway</b>	Default Gateway address of MX60M
<b>Primary DNS</b>	Primary DNS address of MX60M
<b>Listen Port/Software IP(status)</b>	Listen Port and Networking Software IP address ( status : Online or Offline)
<b>WEB Management Port</b>	WEB communication number of MX60M
<b>Registered User</b>	Registered user number of MX60M
<b>Available User Capacity</b>	Available Capacity of MX60M to register users; Available user number(s) to be registered = Sum (20000) – Registered user(s)
<b>Access/System Log Count</b>	The Sum from access and system logs of MX60M
<b>Control Mode</b>	1 door(2 way) or 2 doors (1 way) of MX60M
<b>Anti-Pass-Back (Tolerance Timer)</b>	Enable or Disable the MX60M APB (Anti Pass Back) function (including its Tolerance Timer).
<b>Anti-Duress</b>	Enable or Disable the MX60M function of Anti Duress.
<b>Web management Port</b>	Input HTTP port number (Default is 80)
<b>Next SEMAC(status)</b>	IP Address of Next MX60M and its networking status ( Online or Offline)
<b>Fast Reg Card mode</b>	Enable or disable Fast Registry Card Mode of the system.
► Button	
<b>Save</b>	Save terminal configuration to current system

## ◆ Terminal Setup

Select and Click "Terminal Setup" on the left side of the Main Window, you'll see the "Terminal Configuration", referring to the following picture:

**Terminal Configuration**

---

**Terminal Setting :** Terminal ID :

\*IP Address :  .  .  .

\*Subnet Mask :  .  .  .

\*Gateway :  .  .  .

\*DNS Server :  .  .  .

**Software :** \*TCP Port(Software Used) :  \*Software IP :

**Control Mode :**  2 Doors(1 way)  1 Door(2 way)

**Web Language :**  ▾

**Anti Pass Back :**  Enable  Disable

Tolerance Timer  (Minute, Maximum 65535, 0 means No Tolerance)

**Anti Duressed :**  Enable  Disable

Password  (Max 3 digits,default is 9)

**WEB Managemant Port :** Http Port:

**Next SEMAC(for APB):** IP Address :  .  .  .

**Fast Reg Card Mode :**  Enable  Disable

---

**Terminal may need to restart after configuration saved.**

M

## ◆ Illustration of Terminal Configuration

▶ Terminal Configuration	
<b>Terminal Setting</b>	For setting the Terminal ID of MX60M. Default ID=1, max. 65535, no ID duplicated.
<b>IP Address</b>	For setting the IP Address of MX60M
<b>Subnet Mask</b>	For setting the Subnet Mask of MX60M
<b>Gateway</b>	For setting the Default Gateway of MX60M
<b>DNS Server IP Address</b>	For setting the DNS Server IP Address of MX60M. Default DNS Server IP Address is <b>168.95.1.1</b> .
▶ Software	
<b>TCP Port (Software Used)</b>	For setting the TCP Port of the Software to communicate with MX60M. Default TCP Port is <b>2000</b> .
<b>Software IP</b>	For setting the Software IP to communicate with MX60M Default Software IP is 0.0.0.0.
▶ Control Mode	
<b>2 Doors (1 way)</b>	Tick this circle and the Control Mode of MX60M will be as 2 Doors (1 way) status. It may control Door 1 and Door 2 for coming in only.
<b>1 Door(2 way)</b>	Tick this circle and the Control Mode of MX60M will be as 1 Door (2 way) status. It may control both in and out for Door 1.
▶ Web Language	
<b>English</b>	When you choose the "English" language from the "Drop Down Menu", the WEB page of MX60M will be switched to "English" interface .
<b>Chs</b>	When you choose the "Chs" language from the "Drop Down Menu", the WEB page of MX60M will be switched to "Simplified Chinese" interface .
<b>Others</b>	When you choose "Others" from the "Drop Down Menu", the WEB page of MX60M will be switched to "Traditional Chinese" interface or other languages.
▶ Anti Pass Back	
<b>Enable</b>	Tick this circle to enable the "APB" (Anti Pass Pack) function.
<b>Disable</b>	Tick this circle to disable the "APB" (Anti Pass Pack) function.
<b>Tolerance Time</b>	Set up the restored time back to original setting after the "APB" triggered. The unit of time is "minute" and the max. Value is "65535". If the value is "0", then it will never be restored until you disable the "APB" by manual.
▶ Anti Duress	
<b>Enable</b>	Tick this circle to enable the "Anti Duress" function.
<b>Disable</b>	Tick this circle to disable the "Anti Duress" function.
<b>Password</b>	Set your password of "Anti Duress", default value = 9, max. 3 digits.
▶ WEB Management Port	

<b>Http Port</b>	Set your WEB port for MX60M, default value=80.
<b>► Next SEMAC( for APB)</b>	
<b>IP Address</b>	Set your IP address for Next MX60M, but only available for the structure of multi MX60M. Whenever this IP for next MX60M is set up, all the levels settings of original MX60M will be copied to next MX60M.
<b>Fast Registry Card Mode</b>	
<b>► Fast-Registry mode</b>	
<b>Active</b>	Fast-Registry mode will be active when selecting Active <b>Note: Disable Fast-Registry mode is necessary after new user card is registered</b>
<b>Inactive</b>	Select Inactive to disable Fast-Registry mode
<b>► Button</b>	
<b>Save</b>	Save the Terminal configuration settings.

## ◆ Password Setup

Select "Password Setup" on the left side of the Main Window, you'll see the "WEB Logon Setting/Entrance Password" screen, referring to the following picture:

### WEB Logon Setting

---

Administrator WEB Logon User Name :	<input type="text" value="admin"/>	(47 Char. Max)
Administrator WEB Logon Password :	<input type="password" value="•••••"/>	(35 Char. Max)
Operator WEB Logon User Name :	<input type="text" value="user"/>	(47 Char. Max)
Operator WEB Logon Password :	<input type="password" value="••••"/>	(35 Char. Max)
USER WEB Logon User Name :	<input type="text" value="user0"/>	(47 Char. Max)
USER WEB Logon Password :	<input type="password" value="•••••"/>	(35 Char. Max)

### Entrance Password

---

Administrator Password :	<input type="text"/>	(4 ~ 8 digits.)
Common Password :	<input type="text" value="1234"/>	(4 ~ 8 digits.)
Fast Reg Password :	<input type="text" value="1111"/>	(4 digits.)

MOA

## ◆ Illustration of WEB Logon Setting/Entrance Password

▶ WEB Logon Setting	
<b>Administrator WEB Logon User Name</b>	Input the required Administrator's logon user name for WEB management, max. 47 characters, default value: "admin".
<b>Administrator WEB Logon Password</b>	Input the required Administrator's logon password for WEB management, max. 35 digits, default value: "admin".
<b>Operator WEB Logon User Name</b>	Input the required Operator's logon user name for WEB management, max. 47 characters, default value: "user".
<b>Operator WEB Logon Password</b>	Input the required Operator's logon password for WEB management, max. 35 digits, default value: "user".
<b>User WEB Logon User Name</b>	Input the required User's logon user name for WEB management, max. 47 characters, default value: "user0".
<b>User WEB Logon Password</b>	Input the required User's logon user name for WEB management, max. 35 digits, default value: "user0".
The Administrator, Operator and User have their respective authorizations, referring to the following "Authorization Table".	
▶ Button	
<b>Save</b>	Save all the WEB Logon Settings.
▶ Entrance Password	
<b>Common Password</b>	Set your "Common Password" here. Meanwhile, you have to select "001 Any Time" for "Common Password Time Zone" simultaneously to support this setting (for example: Door Setup → Door Setting → Click "Door1" → Door 1 Setting → Select "Common Password Time Zone" → Select "001 Any Time" from the "Drop Down Menu"). Default value: "1234".
<b>Administrator Password</b>	Set a Administrator Password if needed to reflect to Door Time Zone.
<b>Fast Reg Password</b>	Input 4 digit numbers for the Fast Registry mode password
▶ Button	
<b>Save</b>	Save the Password setting.

Authorizations Table (“●” = Access Permission)

WEB Function	Administrator User Name: admin Password : admin	Operator User Name: user Password : user	User User Name: user0 Password : user0
Upgrade Firmware	●		
Password Setup	●		
Terminal Setup	●		
Door Setup	●		
Event Handle	●		
Reboot	●		
Clock Setup	●		
Reset	●		
Upgrade Firmware	●		
Password Setup	●		
Terminal Setup	●		
User Data	●	●	
Time Set	●	●	
Time Zone Setup	●	●	
Group List	●	●	
Holiday Setup	●	●	
Lift Setup	●	●	
Multi Badge Group	●	●	
Remote Control	●	●	
Access Log	●	●	●
View User List	●	●	●
Terminal Status	●	●	●
System Log	●	●	●
IP Camera	●	●	●

## ◆ System Log

Select "System Log" on the left side of the Main Window, you'll see the "System Log" screen as the following picture:

**System Log**

No.	Date	Time	Description
1	09/15/2009	13:46:44	Disconnected by Server
2	09/15/2009	13:43:39	PC Server Connected
3	09/15/2009	13:43:06	Connect PC Server Fail
4	09/15/2009	13:39:51	Set Date(09/09/15)Day(2)Time(13:39:52) via Software
5	09/15/2009	13:39:50	PC Server Connected
6	09/15/2009	13:30:37	Connect PC Server Fail
7	09/15/2009	13:29:51	System Warm Start
8	09/15/2009	13:29:50	System Terminal Setup from Web
9	09/15/2009	13:29:41	System Warm Start
10	09/15/2009	13:29:40	System Terminal Setup from Web
11	09/15/2009	13:16:08	Connect PC Server Fail
12	09/15/2009	13:15:27	Disconnected by Server
13	09/15/2009	13:14:01	PC Server Connected
14	09/15/2009	13:12:59	Connect PC Server Fail
15	09/15/2009	13:12:18	Disconnected by Server
16	09/15/2009	13:11:28	PC Server Connected
17	09/15/2009	13:08:52	Connect PC Server Fail
18	09/15/2009	13:08:11	Disconnected by Server
19	09/15/2009	13:07:39	PC Server Connected
20	09/15/2009	12:00:00	Connect PC Server Fail

Total 76 Record(s) << [First](#) | [Prev 10](#) | [1](#) [2](#) [3](#) [4](#) | [Next 10](#) | [End](#) >>

## ◆ Illustration of System Log

▶ System Log	
<b>No.</b>	Serial Number of the log
<b>Date</b>	Date of the log
<b>Time</b>	Time of the log
<b>Description</b>	Description of the system operation records
※ Max. logs capacity : 1536 entries, for checking by authorized person(s) only, no logs export provide.	



## ◆ Clock Setup

Select and Click "Clock Setup" on the left side of the Main Window, you'll see the "System Clock Setup" screen, referring to the following picture:

### SYSTEM CLOCK SETUP

Time Server :  Disable  Enable

*Recommend: time.windows.com or time.nist.gov*

Time Zone:

New Date :  (mm/dd/yyyy)

New Time :  (hh:mm:ss)

## ◆ Illustration of System Clock Setup

▶ Time Server	
<b>Disable</b>	Tick this circle to shut up the Time Server network connection.
<b>Enable</b>	Tick this circle to start the Time Server network connection.
<b>Time Zone</b>	The "Drop Down Menu" offers you all the Time Zones available up to your option, default time zone : (GMT)England.
<b>"Save" button</b>	Save the Time Server Settings and adjust the time.
When enable the "Time Server", please key in the IP address or <a href="http://">http://</a> of the "Time Server". Then select the required Time Zone and Save it to connect the "Time Server" for a time adjustment.	
<b>New Date</b>	The date of networked PC computer. You may adjust the date to your requirement as the format of " <b>mm/dd/yyyy</b> ".
<b>New Time</b>	The date of networked PC computer. You may adjust the time to your requirement as the format of " <b>hh:mm:ss</b> ".
<b>"Save"</b>	Save the configuration of this page and upgrade the date/time for the networked PC computer.

## ➤ Access Control

### ◆ Time Set

Select and Click “Time Set ” on the left side of the Main Window, you’ll see the “Time Set” screen, referring to the following picture:

#### Time Set

Time Set List :

000	00:00 ~ 00:00		001	00:00 ~ 23:59	
002	04:00~17:00	DELETE	003	18:00~23:00	DELETE
004	02:00~05:30	DELETE	005	15:00~19:00	DELETE
006	16:00~19:00	DELETE	007	07:00~16:00	DELETE
008	17:30~21:30	DELETE	009	03:45~09:30	DELETE
010	10:00~14:00	DELETE	011	09:00~17:00	DELETE
012	17:00~22:00	DELETE	013	00:00~13:00	DELETE
014	19:00~23:00	DELETE	015	07:30~15:00	DELETE
016	16:00~20:00	DELETE	017	12:58~19:56	DELETE
018	12:58~18:59	DELETE	019	02:00~08:00	DELETE
020	03:00~05:00	DELETE	021	07:00~13:00	DELETE

Time Set :  From  H :  M To  H :  M

### ◆ Illustration of Time Set

▶ Time Set List	
<b>Time Set List</b>	It will display all the configured time set(s). The System Default Time sets are: 00:00~00:00 and 00:00~23:59.
<b>Time Set</b>	Select your time set serial number. The “Drop Down Menu” offers you all the options for your choice, max. 255 time sets allowed. System built-in values are “000” and “001”.
<b>From ~ To</b>	Insert a time set period, for example : 8:00am to 17:00am as one period, then Time Set : <input type="text" value="002"/> From <input type="text" value="00"/> H : <input type="text" value="00"/> M To <input type="text" value="23"/> H : <input type="text" value="59"/> M <input type="button" value="SET"/> It is the same way to the others.
▶ Button	
<b>Delete</b>	Delete an existing “Time Set”.
<b>Set</b>	Add a new “Time Set”.

## ◆ Time Zone Setup

Select and Click "Time Zone Setup" on the left side of the Main Window, you'll see the "Time Zone List" screen as below:

### Time Zone List

Time Zone List :

000	Deactivate		001	Any Time	
002	<a href="#">2</a>	DELETE	003	<a href="#">3</a>	DELETE
004	<a href="#">4</a>	DELETE	005	<a href="#">5</a>	DELETE

Time Zone ID :

## ◆ Illustration of Time Zone List

▶ Time Zone List	
<b>Time Zone List</b>	Display all the Time Zone(s) existing. Click the Time Zone name(indicated as the Time Zone Name example) to enter its Time Zone Information Screen.
<b>Time Zone ID</b>	Select your Time Zone Serial Number from the "Drop Down Menu", system built-in numbers as "000" and "001", max. 120 Time Zones allowed.
<b>Time Zone Name</b>	Click the name of Time Zone ( for example : 2, as below picture) to enter the "Time Zone Information" screen for modification.
▶ Button	
<b>Delete</b>	Delete an existing Time Zone.
<b>Set</b>	Enter the Time Zone Information screen.

Here is an example of “Time Zone Information” screen to show how to set the daily door access and card punching authorized Time Set from Monday to Sunday and Holidays:

**Time Zone Information -- 002**

Day : Monday ▾

Time 1: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 2: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 3: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 4: <span>000 -- 00:00 ~ 0</span>
Time 5: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 6: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 7: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 8: <span>000 -- 00:00 ~ 0</span>
Time 9: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 10: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 11: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 12: <span>000 -- 00:00 ~ 0</span>
Time 13: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 14: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 15: <span>000 -- 00:00 ~ 00:00</span> ▾	Time 16: <span>000 -- 00:00 ~ 0</span>

Save Cancel

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Hc
Time 1:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00
Time 2:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00
Time 3:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00
Time 4:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00
Time 5:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00
Time 6:	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	000 -- 00:00 ~ 00:00	00

**◆ Illustration of Time Zone Information**

► Time Zone Information Settings	
<b>Day</b>	Select a weekday from Monday ~ Sunday or the Holiday. Select Time set from the pull down menu (Time set needs to be preset)
<b>Time 1 ~ Time16</b>	Select weekday from Monday ~Sunday and Holiday and total 16 time sets can be option. Time Set(s) needs to be preset before select the Time 1~16 for the weekday or holiday: <u>Step 1 : “Time Set” screen to “Set” some time sets</u> <u>Step 2 : “Time Zone Information” screen for more options than original 2 default time sets</u>
► Button	
<b>Save</b>	Save the“ Time Zone Information”.
<b>Cancel</b>	Cancel or Modify the “Time Zone Information”.
When the “ Time Zone Setup “ completed, please click the “Time Zone Name ”to enter its “Time Zone Information” screen and see the list with all of its time sets as picture 13.	

## ◆ Group List

Select "Group List" on the left side of the Main Window, you'll see the "Group List" screen as below:

### Group List

Group List :

000	Disallowed Group		001	Free Time Group	
002	2	DELETE	003	3	DELETE
004	4	DELETE			

Group ID : 005

## ◆ Illustration of Group List

▶ Group List	
<b>Group List</b>	Display all the Groups configured. Click the Group's name to enter its "Group Information" as below : (for example: click Group Name "4" as picture 14)
<b>Group ID</b>	Select your "Group ID" by serial number, default values : 000 、 001. The "Drop Down Menu" offers you all the serial number of Group ID as options, max. 255 groups allowed.
▶ Button	
<b>Delete</b>	Delete a Group ID.
<b>Set</b>	Enter the "Group Information" screen.

This is a screen to configure the door(s) of a Group ID, referring to the following picture:

### Group Information

<b>Allowed Door :</b>	<b>Time Zone ID :</b>
<input type="checkbox"/> 1.	000 Deactivate ▼
<input type="checkbox"/> 2.	000 Deactivate ▼
<input type="checkbox"/> 3.	000 Deactivate ▼
<input type="checkbox"/> 4.	000 Deactivate ▼
<input type="checkbox"/> 5.	000 Deactivate ▼
<input type="checkbox"/> 6.	000 Deactivate ▼
<input type="checkbox"/> 7.	000 Deactivate ▼
<input type="checkbox"/> 8.	000 Deactivate ▼

### ◆ Illustration of Group Information

▶ Allowed Door	
<b>Door 1</b>	Tick the box of Door 1, then the user(s) of this Group can access Door 1 within the “Time Zone ID”, otherwise prohibited.
<b>Door 2</b>	Tick the box of Door 2, then the user(s) of this Group can access Door 2 within the “Time Zone ID”, otherwise prohibited.
<b>Door 3</b>	Tick the box of Door 3, then the user(s) of this Group can access Door 3 within the “Time Zone ID”, otherwise prohibited.
<b>Door 4</b>	Tick the box of Door 4, then the user(s) of this Group can access Door 4 within the “Time Zone ID”, otherwise prohibited.
<b>Door 5</b>	Tick the box of Door 5, then the user(s) of this Group can access Door 5 within the “Time Zone ID”, otherwise prohibited.
<b>Door 6</b>	Tick the box of Door 6, then the user(s) of this Group can access Door 6 within the “Time Zone ID”, otherwise prohibited.
<b>Door 7</b>	Tick the box of Door 7, then the user(s) of this Group can access Door 7 within the “Time Zone ID”, otherwise prohibited.
<b>Door 8</b>	Tick the box of Door 8, then the user(s) of this Group can access Door 8 within the “Time Zone ID”, otherwise prohibited.
<b>Tim Zone ID</b>	The “Drop Down Menu” displays all the “Time Zones” configured in the “Time Zone Setup” for your choice.
▶ Button	
<b>Save</b>	Save the “Group Information”.
<b>Cancel</b>	Cancel or Modify the “Group Information”

## ◆ Holiday Setup

Select "Holiday Setup" on the left side of the Main Window, you'll see the "Holiday setup" screen as below:

### Holiday setup

---

01  Month / 01  Date

---

Holiday List :

01 / 01	<input type="button" value="DELETE"/>	01 / 02	<input type="button" value="DELETE"/>	01 / 03	<input type="button" value="DELETE"/>
---------	---------------------------------------	---------	---------------------------------------	---------	---------------------------------------

---

## ◆ Illustration of Holiday Setup

▶ Holiday Setup	
<b>Month</b>	Select a month from the "Drop Down Menu".
<b>Date</b>	Select a date from the "Drop Down Menu".
▶ Button	
<b>Set</b>	Add a new Holiday.
<b>Delete</b>	Delete a Holiday.

## ◆ Door Setup

Select and Click "Door Setup" on the Main Window, you'll see the "Door setting" screen as below:

### Door Setting

		Door 1	Door 2	Door 3	Door 4	Door 5	Door 6	Door 7	Door 8
	BF50(B)/WEBPASS(W)	X	X	X	B	X	X	X	B
L10	First Admin Card IN TZ	000	000	000	000	000	000	000	000
L9	2/3 Badge+Admin P TZ	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)
L8	2/3 Badge+Personal P TZ	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)
L7	2/3 Badge TZ	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)	000 (double)
L6	Card+Admin P TZ	000	000	000	000	000	000	000	000
L5	Admin P TZ	000	000	000	000	000	000	000	000
L4	Card+Personal P TZ	000	000	000	000	000	000	000	000
L3	P TZ	000	000	000	000	000	000	000	000
L2	Card Only TZ	000	000	000	000	000	000	000	000
L1	Card or P TZ	001	001	001	001	001	001	001	001
	Lock Release TZ	000	000	000	000	000	000	000	000
	Exit Button TZ	001	001	001	001	001	001	001	001
	APB IN/OUT	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
	Multiple Interlocking	N	N	N	N	N	N	N	N
	Remote Grant Needed	N	N	N	N	N	N	N	N
	Open Delay Time	10	10	10	10	10	10	10	10
	Door Open Delay Time	10	10	10	10	10	10	10	10
	Log Recorded/Sensor Mode	Y/None	Y/None	Y/None	Y/None	Y/None	Y/None	Y/None	Y/None



## ◆ Illustration of Door Setting

► Door Setting	
<b>BF-50</b>	Display connection status in Door 1/Door 2, and the BF-50/WEBPASS. V: The devices are connected. X: The devices are disconnected.
<b>L10 : First Admin Card IN TZ</b>	Display the First Admin Card IN Time Zone from Door 1 to Door 8.
<b>L9: 2/3 Badge +Admin P TZ</b>	Display the Multiple Badge+ Admin Password Time Zone from Door 1 to Door 8, accompanied by a Double or Triple verifications.
<b>L8: 2/3 Badge +Personal P TZ</b>	Display the Multiple Badge +Personal Password Time Zone from Door 1 to Door 8, accompanied by a Double or Triple verifications.
<b>L7: 2/3 Badge TZ</b>	Display the Multiple Badge Time Zone from Door 1 to Door 8, accompanied by a Double or Triple verifications.
<b>L6: Card + Admin P TZ</b>	Display the Card +Admin Password Time Zone from Door 1 to Door 8.
<b>L5: Admin P TZ</b>	Display the Admin Password Time Zone from Door 1 to Door 8.
<b>L4: Card + Personal TZ</b>	Display the Card +Personal Password Time Zone from Door 1 to Door 8.
<b>L3: Common P TZ</b>	Display the Common Password Time Zone from Door 1 to Door 8.
<b>L2: Card Only TZ</b>	Display the Card Only Time Zone from Door 1 to Door 8.
<b>L1: Card or Common TZ</b>	Display the Card or Common Password Time Zone from Door 1 to Door 8.
<b>Lock Release TZ</b>	Display the Lock Release Time Zone from Door 1 to Door 8.
<b>Exit Button TZ</b>	Display the Exit Button TZ from Door 1 to Door 8.
<b>APB IN/OUT</b>	Display the Anti Pass Back Level from Door 1 to Door 8, APB level : 0-255 for door IN/OUT.
<b>Dual Interlocking</b>	Display the Dual Interlocking function from Door 1 to Door 8, “Enabled” or “Disabled”.
<b>Remote Grant Needed</b>	Display the Remote Grant function from Door 1 to Door 8, “Enabled” or “Disabled”.
<b>Lock Release Time</b>	Display the Lock Release Time from Door 1 to Door 8, 1 – 65535 seconds allowed and 10 seconds = default.
<b>Open Delay Time</b>	Display the Door Open Delay Time from Door 1 to Door 8, 10 seconds = default.
<b>Log Recorded/Sensor Mode</b>	Display the Access Log to be Recorded or Ignored from Door 1 to Door 8, and the Door Sensor Mode.
<b>Door 1</b>	Click “Door 1” to enter the “ Door 1 Setting” screen.
<b>Door 2</b>	Click “Door 2” to enter the “ Door 2 Setting” screen.
<b>Door 3</b>	Click “Door 3” to enter the “ Door 3 Setting” screen.

<b>Door 4</b>	Click “Door 4” to enter the “ Door 4 Setting” screen.
<b>Door 5</b>	Click “Door 5” to enter the “ Door 5 Setting” screen.
<b>Door 6</b>	Click “Door 6” to enter the “ Door 6 Setting” screen.
<b>Door 7</b>	Click “Door 7” to enter the “ Door 7 Setting” screen.
<b>Door 8</b>	Click “Door 8” to enter the “ Door 8 Setting” screen.
<b>► Button</b>	
<b>Search BF-50</b>	Tap the button to manually search BF-50 device(s) that managed by MX60M system
<b>Save BF-50</b>	Save BF-50 current status after Update BF-50 card(s)
<b>Set BF-50 Card (List)</b>	Input 50 sets of card numbers to BF-50. When MX60M is disconnection with any of BF-50 devices, BF-50 will react for these cards which have saved to the card list and then open the door.
<b>Set WebPass (List)</b>	Input IP address information when any WebPass readers are in the connection. Port number for each WebPass is also needed to communication with MX60M.
<b>Update BF-50 Card</b>	Tap the button to update BF-50 card(s) information to all connecting BF-50 managed by BF-870W. Note: When Tapping “Update BF-50 Card” button, suggestion to wait at least two minutes for system upgrade needed.

## Door 1 Setting

First Admin Card IN Time Zone :	001 Any Time	▼			
Multiple Badge+Admin Password Time Zone :	000 Deactivate	▼	Double	▼	
Multiple Badge+Personal Password Time Zone :	000 Deactivate	▼	Double	▼	
Multiple Badge Time Zone :	000 Deactivate	▼	Double	▼	
Card+Admin Password Time Zone :	000 Deactivate	▼			
Admin Password Time Zone :	000 Deactivate	▼			
Card+Personal Password Time Zone :	000 Deactivate	▼			
Common Password Time Zone :	000 Deactivate	▼			
Card Only Time Zone :	000 Deactivate	▼			
Card or Common Password Time Zone :	001 Any Time	▼			
Lock Release Time Zone :	000 Deactivate	▼	First Card	No Need	▼
Exit Button TZ :	001 Any Time	▼			
Anti Pass Back Level :	IN :	0	OUT :	0	( 0 - 255)
Dual Interlocking:	Disabled	▼			
Remote Grant:	Disabled	▼			
Lock Release Time :	10	Sec ( 1 - 65535, 10 = default )			
Door Open Delay Time :	10	Sec default			
Access Log :	Recorded	▼			
Door Sensor Mode:	Normal Open/Close	▼			

SET

2 3 4 5 6 7 8

MOA

## ◆ Illustrations of Door Setup

▶ Door 1 Setting	
<p><b>First Admin Card IN Time Zone</b></p>	<p>Set up the time zone of First Administrator's Card to open the door as the bypass time zone of Door 1 ( default- "000 Deactivate"). When this time zone is chosen, the user can only use the card of Administrator to scan/sweep the controller first and the other users may enter Door 1. Nobody may enter without using this First Admin Card to scan the controller of Door 1 in advance.</p> <p>※ Should the user's bypass time zone level is L10, he/she may access by scanning the card and enter the Door 1 directly; however when the bypass time zone setup of Door 1 is " Lock Release Time Zone ", the user may access directly without any limitation.</p>
<p><b>Multiple Badge +Admin Password Time Zone</b></p>	<p>Set up the Multiple Badge + Administrator Password time zone as the bypass time zone of Door 1 ( default- "000 Deactivate"). Before setting this time zone, you must choose the function of " Multi Badge Group "to come to the "Multi Badge Group " screen and give the user ID in this time zone, max. 3 user IDs allowed; the user needs both 2 or 3 user ID cards and the Administrator's password to enter the Door 1 successfully. No any order limitation for scanning the cards first or enter the password first. You may scan the cards first then enter the password, or in reverse order.</p> <p>※ Should the user's bypass time zone level is L9~L10, he/she may access by scanning the card and enter the Door 1 directly; however when the bypass time zone setup of Door 1 is " Lock Release Time Zone ", the user may access directly without any limitation.</p>
<p><b>Multiple Badge +Personal Password Time Zone</b></p>	<p>Set up the Multiple Badge + Personal Password time zone as the bypass time zone of Door 1 ( default-000 Deactivate"). Before setting this time zone, you must choose the function of "Multi Badge Group"to come to the "Multi Badge Group" screen and give the user ID in this time zone, max. 3 user IDs allowed; the user needs both 2 or 3 user ID cards and the Personal password to enter the Door 1 successfully. No any order limitation for scanning the cards first or enter the password first. You may scan the cards first then enter the password, or in reverse order. However, the order of personal passwords will make differences. For example, there are two cards + passwords belonged to A and B. Should A card be scanned first, A has to enter his/her password first. Password B is not allowed to be entered before Password A.</p> <p>※ Should the user's bypass time zone level is L8~L10, he/she may access by scanning the card and enter the Door 1 directly; however when the bypass time zone setup of Door 1 is " Lock Release Time Zone ", the user may access directly without any limitation.</p>

<p><b>Multiple Badge Time Zone</b></p>	<p>Set up the Multiple Badge time zone as the bypass time zone of Door 1 ( default-“ 000 Deactivate“). Before setting this time zone, you must choose the function of “Multi Badge Group”to come to the “Multi Badge Group” screen and give the user ID in this time zone, max. 3 user IDs allowed; the user needs both 2 or 3 user ID cards to enter the Door 1 successfully. No any order limitation for scanning the cards          ※ Should the user’s bypass time zone level is L7~L10, he/she may access by scanning the card and enter the Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>
<p><b>Card +Admin Password Time Zone</b></p>	<p>Set up the Card + Admin Password time zone as the bypass time zone of Door 1 (default-“ 000 Deactivate“). The user has to scan the card and enter the Admin Password to access Door 1. No any order limitation for scanning the cards first or enter the password first.          ※ Should the user’s bypass time zone level is L6~L10, he/she may access by scanning the card and enter the Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>
<p><b>Admin Password Time Zone</b></p>	<p>Set up the Admin Password time zone as the bypass time zone of Door 1 (default-“000 Deactivate“). The user has to enter the Admin Password to access Door 1.          ※ Should the user’s bypass time zone level is L5~L10, he/she may access by scanning the card and enter Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>
<p><b>Card +Personal Password Time Zone</b></p>	<p>Set up the Card+ Personal Password time zone as the bypass time zone of Door 1 ( default-“ 000 Deactivate“). The user has to scan the card and enter the Personal Password to access Door 1. No any order limitation for scanning the cards first or enter the password first.          ※ Should the user’s bypass time zone level is L4~L10, he/she may access by scanning the card and enter Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>
<p><b>Common Password Time Zone</b></p>	<p>Set up the Common Password time zone as the bypass time zone of Door 1 (default-“000 Deactivate“). The user has to enter the Common Password to access Door 1.          ※ Should the user’s bypass time zone level is L3~L10, he/she may access by scanning the card and enter Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>
<p><b>Card Only Time Zone</b></p>	<p>Set up the Card Only time zone as the bypass time zone of Door 1 ( default –“ 000 Deactivate“). The user has to scan the card to access Door 1.          ※ Should the user’s bypass time zone level is L2~L10, he/she may access by scanning the card and enter Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.</p>

<b>Card or Common Password Time Zone</b>	Set up the Card or Common Password time zone as the bypass time zone of Door 1 ( default as “ 001 Any Time“). The user has to scan the card or enter the Common Password to access Door 1. ※ Should the user’s bypass time zone level is L1~L10, he/she may access by scanning the card and enter Door 1 directly; however when the bypass time zone setup of Door 1 is“ Lock Release Time Zone “, the user may access directly without any limitation.
<b>Lock Release Time Zone</b>	Set up the Lock Release time zone as the bypass time zone of Door 1 (default-“000 Deactivate“). The user needs no any verification to access Door 1; however, if the “First Card” setup is “Needed”, the use has to scan a “First Card” in advance to activate the “Lock Release Time Zone” function.
<b>Exit Button TZ</b>	Set up the Exit Button time zone as the bypass time zone of Door 1, supporting “OUT ”for Door 1 only (default as “ 001 Any Time“).
<b>Anti Pass Back Level</b>	Set up the Anti Pass Back Level of “IN” and “OUT” for Door 1, level 0~255.
<b>Dual Interlocking</b>	Disable or Enable the “Dual Interlocking” function. Upon this function enabled, the user enters Door 1 and cannot enter the other door until Door 1 close.
<b>Remote Grant</b>	Disable or Enable the “Remote Grant” access control function. Upon this function enabled, the Software will take a remote control over the door’s open or close.
<b>Lock Release Time</b>	Set up the “Lock Release Time”, default as 10 seconds.
<b>Door Open Delay Time</b>	Set up “Door Open Delay Time” , default as 10 seconds.
<b>Access Log / Sensor Mode</b>	Set up “Ignored” or “Recorded” the Access Log (default as “Recorded”) / Set up the Mode of Sensor, options for “Normal Open/Close” or “Circuit Short/Open” (default as “Normal Open/Close”). Should it is “Circuit Short/Open ” selected, the Door 1 Setting will display “Circuit Short” when the door is in short circuit or broken.

Remarks: Same setting ways for Door 2~Door 8, and so on.

<b>► WebPass Setting</b>	
<b>WebPass 1~8</b>	Enter the linked WebPass IP address and Port number in the blank column.
<b>► Button</b>	
<b>Set</b>	Save all the configurations.
<b>Cancel</b>	Quit from this window.

## ◆ Illustrations of BF-50 Card

<b>► BF-50 Setting</b>	
<b>NO</b>	Total 50 card numbers can be set to the BF-50
<b>Card No</b>	Enter card number for BF-50
<b>► Button</b>	
<b>Set</b>	Save all card numbers only

※ Press “Upgrade to BF-50” button to update the card numbers we Set to BF-50.

## ◆ Set WebPass

Set up IP address and Port number for all the connected WebPass readers at the same domain for communicating with MX60M. Tap the SET button to save the configuration.

### WEBPASS Setting

	IP	PORT
WEBPASS 1 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 2 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 3 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 4 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 5 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 6 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 7 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>
WEBPASS 8 :	<input type="text" value="0.0.0.0"/>	<input type="text" value="2000"/>

MX60

## ◆ Remote Control

Select and Click "Remote Control" on the left side of the Main Window, you'll see the "Door Status Monitoring /Security Bypass" screen as below:

### Door Status Monitoring

No Response 
  close 
  open 
  Circuit short,Circuit open,Intrude,Open too long

	Door 1	Door 2	Door 3	Door 4	Door 5	Door 6	Door 7	Door 8
Door State	<input checked="" type="radio"/>	<input checked="" type="radio"/>	X	X	X	X	X	X
BF50 Status	X	X	X	X	X	X	X	X
Fire Alarm Detection	on		Defense State		off			

### Security Bypass

	Door 1	Door 2	Door 3	Door 4	Door 5	Door 6	Door 7	Door 8
State	Normal	Normal	Normal	Normal	Normal	Normal	Normal	Normal

Door 1 
  Door 2 
  Door 3 
  Door 4 
  Door 5 
  Door 6 
  Door 7 
  Door 8

MW



## ◆ Illustrations of Door Status Monitoring/Security Bypass

► Door Status Monitoring	
<b>Door Status</b>	Display the most updated status from Door 1 to Door 8. No light Displayed means no response; Green light means door closed; Yellow light means door opened; Red light means abnormal status ( for example, short circuit, intruded, door opened overtime, and so on. )
<b>WebPass/BF50 status</b>	Displaying WebPass/BF-50 status. X indicating no equipped with WebPass and BF50 devices
<b>Fire Alarm Detection</b>	Display whether the “Fire Alarm Detection” function enabled or not.
► Security Bypass	
<b>State</b>	Display the “Security Bypass State” from Door 1 to Door 8, Pulse Open/Normal/Force Open/Force Close.
<b>Door 1</b>	Tick the box of Door 1 to monitor the Security Bypass of Door 1.
<b>Door 2</b>	Tick the box of Door 2 to monitor the Security Bypass of Door 2.
<b>Door 3</b>	Tick the box of Door 3 to monitor the Security Bypass of Door 3.
<b>Door 4</b>	Tick the box of Door 4 to monitor the Security Bypass of Door 4.
<b>Door 5</b>	Tick the box of Door 5 to monitor the Security Bypass of Door 5.
<b>Door 6</b>	Tick the box of Door 6 to monitor the Security Bypass of Door 6.
<b>Door 7</b>	Tick the box of Door 7 to monitor the Security Bypass of Door 7.
<b>Door 8</b>	Tick the box of Door 8 to monitor the Security Bypass of Door 8.
<b>Select All</b>	Click this button and tick all the boxes from Door 1 to Door 8.
<b>Cancel All</b>	Click this button and cancel all the ticks of the boxes before Door 1 ~ Door 8.
<b>Pulse Open Door</b>	Click this button to open the door(s) remotely for all the door(s) ticked. This function works when the Security Bypass state is normal.
<b>Force Close</b>	Click this button to make a force close on the door(s) remotely for all the door(s) ticked. Hence the state(s) of all the door(s) ticked will display “Force Close “. Even the RFID card scanned through the door(s), you may not access the door(s).
<b>Back to Normal</b>	Click this button to remotely restore all the door(s) ticked back to normal Security Bypass status.
<b>Force Open</b>	Click this button to make a force open on the door(s) remotely for all the door(s) ticked. Hence the state(s) of all the door(s) ticked will display “Force Open “ and the door(s) will stay at “Lock Release ” status.
<b>Emergency Open All Door</b>	Click this button to make a force open on all the door(s) remotely and the door(s) will stay at “Lock Release” status.
<b>Emergency Close All Door</b>	Click this button to make a force close on all the door(s) remotely and the door(s) cannot be accessed normally.
<b>Fire Alarm Detection ON</b>	Click this button to activate the “Fire Alarm Detection” function and the door(s) state will display “on”.
<b>Fire Alarm Detection OFF</b>	Click this button to deactivate the “Fire Alarm Detection” function and the door(s) state will display “off”.
<b>Alarm OFF</b>	Click this button to deactivate all the Alarms already triggered.

## ◆ Event Handle

Select "Event Handle" on the left side of the Main Window, you'll see the "Event Handle" screen as below:

### Event Handle

Event Type				
Unregistered User ▾	Latched Time : (sec,Max 65535 : 0 means unlimited)	Level :	Alarm :	IP Camera :
	0	0 ▾	Enable ▾	Disable ▾
Alarm :	5 ▾			
E-mail Alerts				
Location :				
	(max59)			
SMTP Mail Server :				
	(max47)			
Mail from :				
	(max47)			
SMTP Server Requires Authentication :	No ▾	username :		
			(max45)	
		password :		
			(max29)	
Mail To :				
	(max47)			
Mail Cc :				
	(max47)			
Set				

Event	Latched Time	Level	Alarm	IP Camera
Unregistered User	0	0	●	●
Deactivated User	0	0	●	●
Not Allowed Door	0	0	●	●
Multi-Badge Violation	0	0	●	●
Time Zone Violation	0	0	●	●
Expired User	0	0	●	●
Anti Pass Back Violation	0	0	●	●
Door open too long	0	0	●	●
Backup Power Used	0	0	●	●
Tamper Switch Breakdown	0	0	●	●
BF50 connection down	0	0	●	●
Door Intruded	0	4	●	●
Duress Alarm On	0	4	●	●
Fire Alarm On	0	5	●	●

## ◆ Illustration of Event Handle

▶ Event Type	
<b>Unregistered User</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the user unregistered, one unregistered record will be shown on the “ Access Log ”screen (referring to the sample as below); if the event level equal to or higher than the “Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0, referring to the below picture</p>
<b>Deactivated User</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the user deactivated, one “Deactivated” message will be recorded and shown on the “Access Log”screen (referring to the example as below); if the event level equal to or higher than the “Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “E-mail Alerts”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<b>Not Allowed Door</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the user’s “Group” setting different from the Door Settings, one “DISALLOWED DOOR” message will be recorded and shown on the “ Access Log ”screen; if the event level equal to or higher than the “Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out. (referring to below examples of user’s Group setting and Door setting) ( steps : Access Log→ Click the User ID→ Enter the “User RECORD” screen to modify the configuration of “Group”)</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<b>Multi-Badge Violation</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the “Multi-Badge “ verification failed, one “(1)DOUBLE REJ” message will be recorded and shown on the “ Access Log” screen (referring to the example as below); if the event level equal to or higher than the” Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>

<p><b>Time Zone Violation</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the user’s “Group” setting different from the Door Settings, one “(1)Open Time Error ”message will be recorded and shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<p><b>Expired User</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the user’s “Expiry Date” overdue, one “(1)EXPIRED ”message will be recorded and shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<p><b>Anti Pass Back Violation</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the doors with “Anti Pass Back Level ”configuration, one “(1)ANTI_PB REJ ”message will be recorded and shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p> <p>※ Only 1 Door (2 way ) is supported with this function.</p>
<p><b>Door open too long</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the door closes over the time set after the user card being scanned, one “(O)Open too long ”message will be recorded and shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>

<p><b>Backup Power Used</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the backup battery is applied, one “Battery Power On ”message will be shown on the Access Log ”screen; if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<p><b>Tamper Switch Breakdown</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the device is opened forcibly, one “CASE OPENED” message will be shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p>
<p><b>BF-50 connection down</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the BF-50 is disconnected, one “BF-50 OFFLINE ”message will be shown on the Access Log ”screen; if the event level equal to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</p> <p>※ SEMAC-S1 is not supported by this function.</p>
<p><b>Door Intruded</b></p>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the door is accessed forcibly and abnormally, one “(O) DOOR INTRUDED ” message will be shown on the Access Log ”screen (referring to the example as below); if the event level equal to or higher than the “ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 4.</p>

<b>Duress Alarm On</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and the “Duress Alarm ”of a door is triggered by the user ( note : you have to key in the “Anti Duress Password” and press “ENT ”before scanning the user card), one “ANTI DURESS” message will be shown on the Access Log ”screen; if the event level equal to or higher than the “ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 4.</p>
<b>Fire Alarm On</b>	<p>1、It will be listed in the “Drop Down Menu”. When it’s selected and if the “Fire Alarm ”is triggered, one “FIRE ALARM” message will be recorded and shown on the Access Log ”screen; if the event level equal to or higher than the “ Alarm Trigger Level”, the Relay will be triggered and the E-mail will alert when “ E-mail Alerts ”is configured and one alert e-mail will be sent out.</p> <p>2、When the “Latched Time : 0”, the alert can only be lifted/stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 5.</p>
<b>Latched Time</b>	The “Latched Time” can be set up to 65535 seconds. When the “Latched Time : 0”, it means the latched status will never be restored until the alert be lifted/stopped by manually clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function.
<b>Level</b>	Set the “Event Type Level”. When the Event Level higher than or equal to the “Alarm Trigger Level”, the Alarm Relay will be triggered; otherwise the Alarm Relay will not be triggered.
<b>Alarm</b>	Enable or disable alarm for the selected Event type(s)
<b>Alarm (Trigger Level)</b>	Set the “Alarm Trigger Level”. When the Event Level higher than or equal to the “Alarm Trigger Level”, the Alarm Relay will be triggered; otherwise the Alarm Relay will not be triggered.
<b>IP Camera</b>	Display if IP Camera will take shot for the event(s)
<b>► E-mail Alerts</b>	
<b>Location</b>	Enter the equipment name for alarming. 59 characters description is allowed
<b>SMTP Mail Server</b>	Enter the Mail Server address of sending Alarm E-mail. 47 characters server address is allowed. 47 characters allowed
<b>Mail from</b>	Input sender’s email address.47 characters allowed
<b>Mail To</b>	Input receiver’s email address. 47 characters allowed
<b>Mail Cc</b>	Input c.c receiver email address. 47 characters allowed
<b>“Set”( button )</b>	Save the configured information.

## ◆ Multi Badge Group

Select and Click "Multi Badge Group" on the left side of the Main Window, you'll see the "Multi Badge Group" screen as below:

### Multi Badge Group

Multi Badge Group	User ID 1	User ID 2	User ID 3
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>
6.	<input type="text"/>	<input type="text"/>	<input type="text"/>
7.	<input type="text"/>	<input type="text"/>	<input type="text"/>
8.	<input type="text"/>	<input type="text"/>	<input type="text"/>
9.	<input type="text"/>	<input type="text"/>	<input type="text"/>
10.	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="set"/>			

## ◆ Illustration of Multi Badge Group

► Multi Badge Group	
<b>Multi Badge Group</b>	Max. 10 Groups to be set. , each group with 2~3 registered users can be set
<b>User ID 1</b>	Enter the User ID 1 for Multi Badge Group.
<b>User ID 2</b>	Enter the User ID 2 for Multi Badge Group.
<b>User ID 3</b>	Enter the User ID 3 for Multi Badge Group.
<b>Set ( button)</b>	Save all the configurations.

## ➤ Tools

### ◆ IP Camera

Select "IP Camera" on the left side of the Main Window, you'll see the "IP Camera" screen as the following example:

IP Camera(IP) :	PORT	TYPE	門 1	門 2
1. 192.168.3.10	80	VIVOTEK IP7133/7330	----	----
2. 192.168.3.10	80	VIVOTEK IP7133/7330	✖	✖
3. 192.168.3.10	80	VIVOTEK IP7133/7330		
4. 192.168.3.10	80	VIVOTEK IP7133/7330		
5. 192.168.3.10	80	VIVOTEK IP7133/7330		
6. 192.168.3.10	80	VIVOTEK IP7133/7330		
7. 192.168.3.10	80	VIVOTEK IP7133/7330		
8. 192.168.3.10	80	VIVOTEK IP7133/7330		

門 3	門 4	門 5
----	----	----
✖	✖	✖

門 6	門 7	門 8
----	----	----
✖	✖	✖



## ◆ Illustration of IP Camera

▶ IP Camera	
<b>IP Camera 1</b>	Enter the IP address of IP Camera 1 to be lined.
<b>IP Camera 2</b>	Enter the IP address of IP Camera 2 to be lined.
<b>IP Camera 3</b>	Enter the IP address of IP Camera 3 to be lined.
<b>IP Camera 4</b>	Enter the IP address of IP Camera 4 to be lined.
<b>IP Camera 5</b>	Enter the IP address of IP Camera 5 to be lined.
<b>IP Camera 6</b>	Enter the IP address of IP Camera 6 to be lined.
<b>IP Camera 7</b>	Enter the IP address of IP Camera 7 to be lined.
<b>IP Camera 8</b>	Enter the IP address of IP Camera 8 to be lined.
<b>Door 1</b>	Display the captured and the most updated picture of Door 1.
<b>Door 2</b>	Display the captured and the most updated picture of Door 2.
<b>Door 3</b>	Display the captured and the most updated picture of Door 3.
<b>Door 4</b>	Display the captured and the most updated picture of Door 4.
<b>Door 5</b>	Display the captured and the most updated picture of Door 5.
<b>Door 6</b>	Display the captured and the most updated picture of Door 6.
<b>Door 7</b>	Display the captured and the most updated picture of Door 7.
<b>Door 8</b>	Display the captured and the most updated picture of Door 8.
<b>Set ( button)</b>	Save all the configurations.
<b>Refresh ( button)</b>	Refresh the WEB page of IP Camera.

## ◆ Backup

Select "Backup" from the menu to enter to Backup system screen:

### Backup

---

**Tips :**

**This command will export the User Registry data for backup purpose.**

Database(database.cfg)  User Data(userdata.cfg)  User List(userlist.txt)

BACKUP

## ◆ Illustration of Backup

► Backup	
<b>Database (database.cfg)</b>	Backup Project for : Terminal Setup, Password Setup, Time Set, Time Zone Setup Group List, Holiday Setup, Door Setup.
<b>User List (userlist.txt)</b>	Backup Project for : User ID, Card No, Name, User Type, Group.

## ◆ Restore

Select "Restore" from the menu to enter Restore/Import configuration screen as below:

### RESTORE / IMPORT

Select a File to Restore / Import :

Database(database.cfg/userdata.cfg)  User List(userlist.txt)

(It may takes few minutes to restore the database.)

## ◆ Illustration of Restore

► Restore	
<b>Database (database.cfg)</b>	Restore Project for : Terminal Setup, Password Setup, Time Set, Time Zone Setup Group List, Holiday Setup, Dorr Setup.
<b>User List (userlist.txt)</b>	Restore Project for : User ID, Card No, Name, User Type, Group.

## ◆ Reboot

Select "Reboot" on the left side of the Main Window, you'll see the "Reboot System" screen as below:

### Reboot System

## ◆ Illustration of Reboot

► Button	
<b>Reboot</b>	Reboot the MX60M, similar to warm boot a computer.

## ◆ Upgrade Firmware

Select "Upgrade FIRMWARE" on the left side of the Main Window, you'll see the "FIRMWARE UPGRADE" screen as below:

### FIRMWAWE UPGRADE

Warning: Upgrade must NOT be interrupted

Please select a file to upgrade :

瀏覽...

UPGRADE



## ◆ Illustration of Upgrade Firmware

### ► Steps

Press button "Browse" to search your firmware to be upgraded.

Press button "Upgrade" to execute the firmware upgrade action.

### ► Note

Please upgrade the "System Code" first then upgrade "WEB code".

## ◆ Reset

Select "Reset" on the left side of the Main Window, you'll see the "Reset" screen as below:

### Reset

User Data
  Access Logs
  Group
  Time Zone
  Time Set
  Holiday
  System Logs

Reset System to Factory Default -

## ◆ Illustration of Reset

▶ Data Reset	
<b>User Data</b>	Tick the box before "User Data" and Click "Delete" button to delete all the User Data.
<b>Access Log</b>	Tick the box before "Access Log" and Click "Delete" button to delete all the Access Logs.
<b>System Logs</b>	Tick the box before "System Logs" and Click "Delete" button to delete all the System Logs.
<b>Group</b>	Tick the box before "Group" and Click "Delete" button to delete all the Groups.
<b>Time Zone</b>	Tick the box before "Time Zone" and Click "Delete" button to delete all the Time Zone configurations.
<b>Time Set</b>	Tick the box before "Time Set" and Click "Delete" button to delete all the Time Set configurations.
<b>Holiday</b>	Tick the box before "Holiday" and Click "Delete" button to delete all the Holiday configurations.
▶ Button	
<b>Select All</b>	Tick the box before above item.
<b>Delete</b>	Delete above item(s) selected.
Steps:	
1、Tick the item above to be deleted.	
2、Click button "Delete".	
▶ Reset System to Factory Default	
<b>Factory Default</b>	Execute this command to restore the system back to the factory default.

## ➤ Appendix I

Event name	Event status	How to revive
Door open delay	Door open time over the default time (with door sensor)	Close the door
Door closed	Door closed after “Door open delay” event triggered.	N/A
Pulse Open	Pulse open door from remote site	Tap “Back to Normal” button to turn to normal
Pulse Close	Pulse close door from remote site	Tap “Back to Normal” button to turn to normal
Back to Normal	Door status back to normal	N/A
Identification failure	User identification failed	Check access method for user is to conform to door’s policy
Unregistry	Card is not registered	Register the card
Inactive	User authority and data invalid	Active user’s authorization
APB violation	APB policy violated when APB function is activated	Check APB level
Not Allowed	User Group is not allowed to access a certain door	Check setting of user Group
Door intruded	Door intruded illegally	Check door sensor functionality
Tamper switch breakdown	Tamper switch is being triggered	Check tamper switch on the terminal status
Push Button	Open door by push button	N/A
Normal Close	Door closed after door opened	N/A

Anti-Duress	Anti-Duress event triggered. (User requires to input Anti-duress password then scan card)	N/A
Fire Alarm	Fire alarm triggered	Check fire alarm signal is being triggered. Release the fire alarm signal.

MAX60M