

# **MX60**

# **Web User Manual**

For 1.00.00: Jul-18th-2012 (HW1.0)

MX60 Series Web Ver 1.0

Build Date Jul-17th-2012

# 【Contents】

<b>—WEB Configuration—</b> .....	1
WEB Logon .....	1
Preparation .....	1
How to search MX60 .....	1
How to log on to MX60 web browser.....	5
<b>TERMINAL STATUS</b> .....	7
Illustration of Terminal Status : .....	8
<b>USER ADMINISTRATION</b> .....	9
Access Log.....	9
Illustration of Access Log : .....	10
Auto Refresh Log.....	11
Illustration of Auto Refresh Log : .....	11
View User List .....	12
Illustration of User List : .....	13
Modify User Record.....	14
Illustration of Modify User Record in User Record : .....	15
Add User .....	16
Illustration of Add New User : .....	17
<b>TERMINAL</b> .....	18
Terminal Status.....	18
Illustration of TERMINAL Status : .....	19
Terminal Setup .....	20
Illustration of Terminal Configuration : .....	21
Password Setup .....	23
Illustration of WEB Logon Setting/ Entrance Password : .....	24
System Log .....	26
Illustration of System Log : .....	26
Clock Setup.....	27
Illustration of System Clock Setup : .....	27
<b>ACCESS CONTROL</b> .....	28
Time Set .....	28
Illustration of Time Set : .....	28
Time Zone Setup .....	29
Illustration of Time Zone List : .....	29

Illustration of Time Zone Information : .....	31
Group List .....	32
Illustration of Group List : .....	32
Illustration of Group Information : .....	33
Holiday Setup.....	34
Illustration of Holiday Setup : .....	34
Door Setup .....	35
Illustration of Door Setting : .....	36
Set up BF-50 with card list .....	38
Illustrations of BF-50 Card : .....	38
Remote Control.....	39
Illustrations of Door Status Monitoring/Security Bypass : .....	40
Event Handle.....	41
Illustration of Event Handle : .....	43
<b>TOOLS</b> .....	47
IP Camera.....	47
Illustration IP Camera : .....	47
BACKUP .....	48
Illustration of Backup : .....	48
RESTORE.....	49
Illustration Restore : .....	49
Reboot.....	50
Illustration of Reboot : .....	50
Upgrade Firmware .....	51
Illustration of Upgrade Firmware : .....	51
Reset.....	52
Illustration of Reset : .....	52
Appendix.....	Appendix 1

Copyright @ 2011. All Rights Reserved.

Document Version: 1.0 《2011-05-24》

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

# — WEB Configuration —

## WEB Logon

MX60 contains a HTTP server, thus MX60 can link and connect through Web Browser, and then conduct setting.

## Preparation

Before conducting MX60 setting, please assure the following:

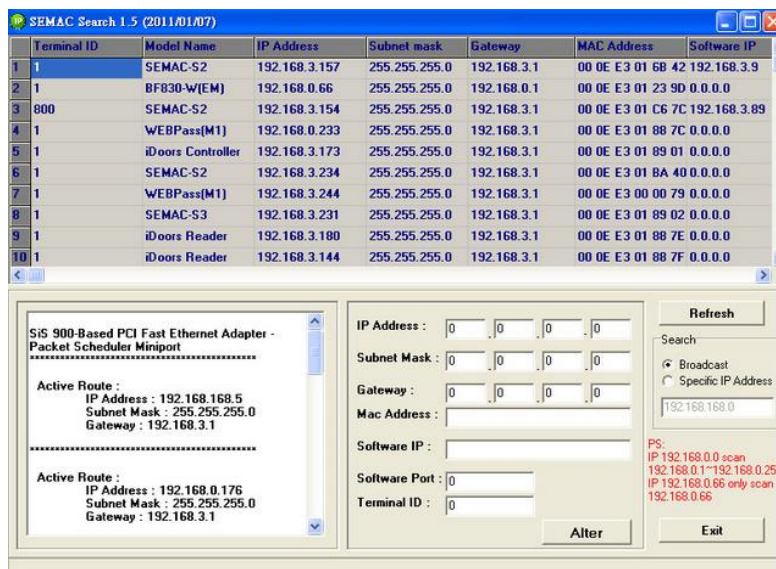
- PC has connected to MX60, and PC and MX60 are situated in the same WAN with power supplied.
- If the default IP address (192.168.0.66 ) is occupied by else device, then it is a must to shut down that device first till the setting is over, and then allocate new IP address to MX60.

## How to search MX60

1、After installation of MX60 and network cable is completed, use MX60's SEMAC Search to search all MX60 in a certain LAN, or download SEMAC Search tool from CHIYU homepage. Desktop icon as below:



2、Click SEMAC Search Picture icon, will display a window, as shown:



Terminal ID	Model Name	IP Address	Subnet mask	Gateway	MAC Address	Software IP
1	SEMACE-S2	192.168.3.157	255.255.255.0	192.168.3.1	00 0E E3 01 68 42	192.168.3.9
2	BF830-W(EM)	192.168.0.66	255.255.255.0	192.168.0.1	00 0E E3 01 23 9D	0.0.0.0
3	SEMACE-S2	192.168.3.154	255.255.255.0	192.168.3.1	00 0E E3 01 C6 7C	192.168.3.89
4	WEBPass(M1)	192.168.0.233	255.255.255.0	192.168.3.1	00 0E E3 01 88 7C	0.0.0.0
5	iDoors Controller	192.168.3.173	255.255.255.0	192.168.3.1	00 0E E3 01 89 01	0.0.0.0
6	SEMACE-S2	192.168.3.234	255.255.255.0	192.168.3.1	00 0E E3 01 8A 40	0.0.0.0
7	WEBPass(M1)	192.168.3.244	255.255.255.0	192.168.3.1	00 0E E3 00 00 79	0.0.0.0
8	SEMACE-S3	192.168.3.231	255.255.255.0	192.168.3.1	00 0E E3 01 89 02	0.0.0.0
9	iDoors Reader	192.168.3.180	255.255.255.0	192.168.3.1	00 0E E3 01 88 7E	0.0.0.0
10	iDoors Reader	192.168.3.144	255.255.255.0	192.168.3.1	00 0E E3 01 88 7F	0.0.0.0

SiS 900-Based PCI Fast Ethernet Adapter - Packet Scheduler Miniport

Active Route :  
IP Address : 192.168.168.5  
Subnet Mask : 255.255.255.0  
Gateway : 192.168.3.1

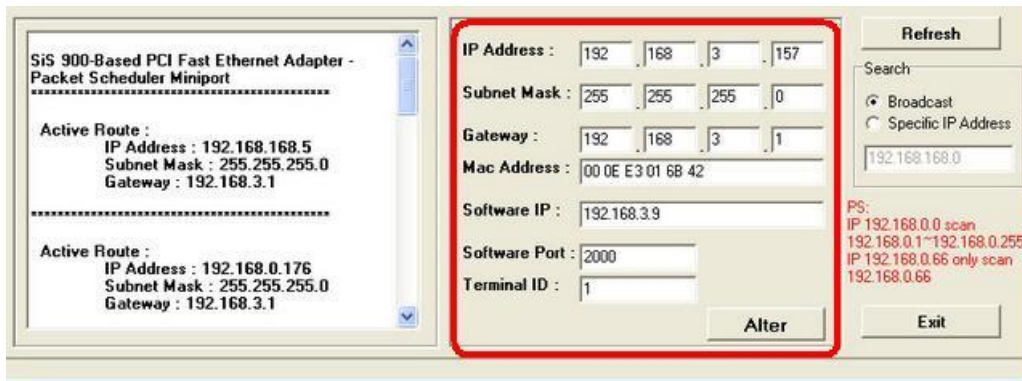
Active Route :  
IP Address : 192.168.0.176  
Subnet Mask : 255.255.255.0  
Gateway : 192.168.3.1

IP Address : [0].[0].[0].[0]  
Subnet Mask : [0].[0].[0].[0]  
Gateway : [0].[0].[0].[0]  
Mac Address :  
Software IP :  
Software Port : [0]  
Terminal ID : [0]

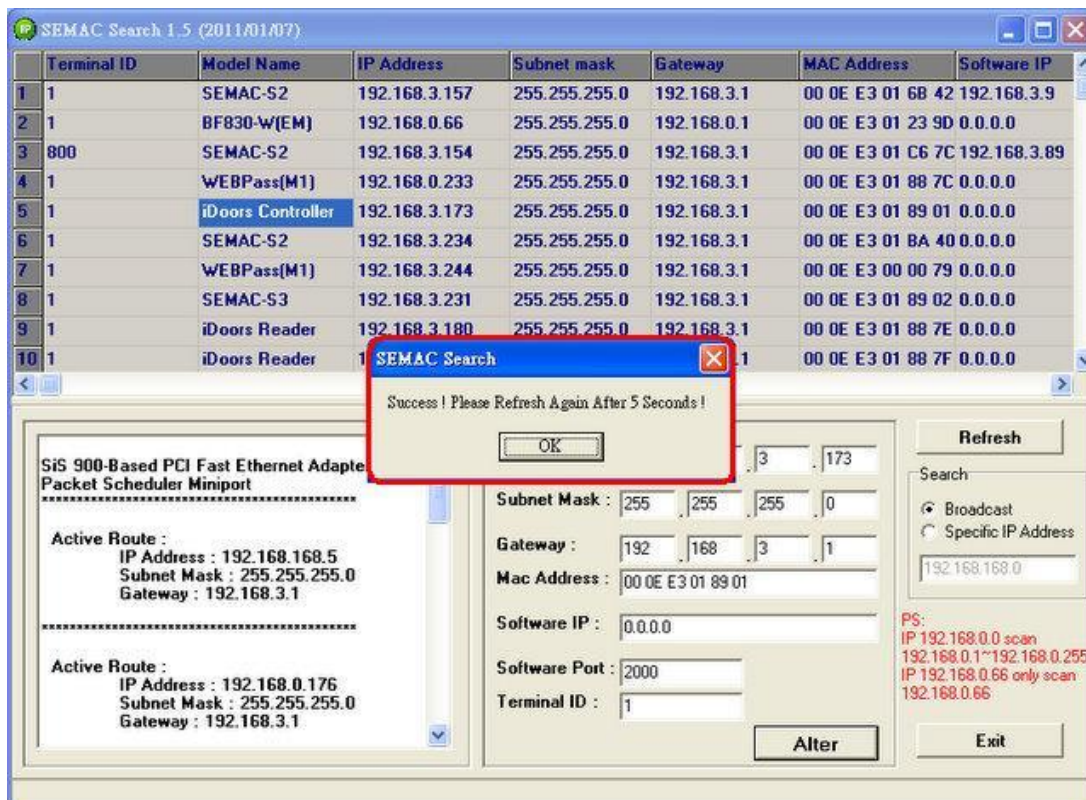
Refresh  
Search  
 Broadcast  
 Specific IP Address  
192.168.168.0  
PS:  
IP 192.168.0.0 scan  
192.168.0.1~192.168.0.255  
IP 192.168.0.66 only scan  
192.168.0.66

Alter Exit

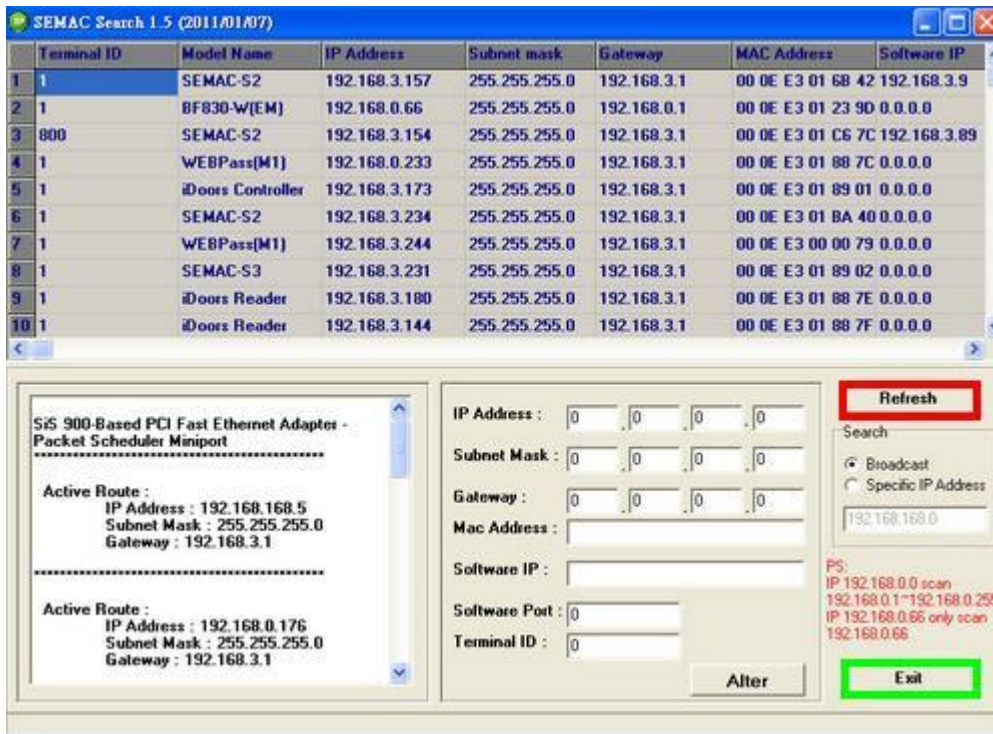
3、While the SEMAC Search window shows up, it will display all MX60 in LAN, and show its Terminal ID, Model Name, IP Address, Subnet Mask, Gateway, Mac Address, Software IP. Select particular MX60, then its related information will appear below the window, as shown:



4、The showed information of MX60 can be revised directly in the window, the part can be modified: IP Address, Subnet Mask, Gateway, Software IP, Software Port, Terminal ID. **After** modification completed ( MAC Address can not modify ),click Alter then it will display the modified information, as shown:



- 5、After modification, if want to confirm whether the modification is correct or not, click Refresh button to refresh and check information ( Fig-1 ), click Exit button to leave.(Fig-2)





- 6、After modification, the IP address of MX60 has matched with its WAN, if want to get access into the Web of MX60, has two methods:

- (1) Open SEMAC Search, select and double click particular MX60, then to enter its webpage.
- (2) While the internet explorer opened, input MX60 IP address to enter its webpage

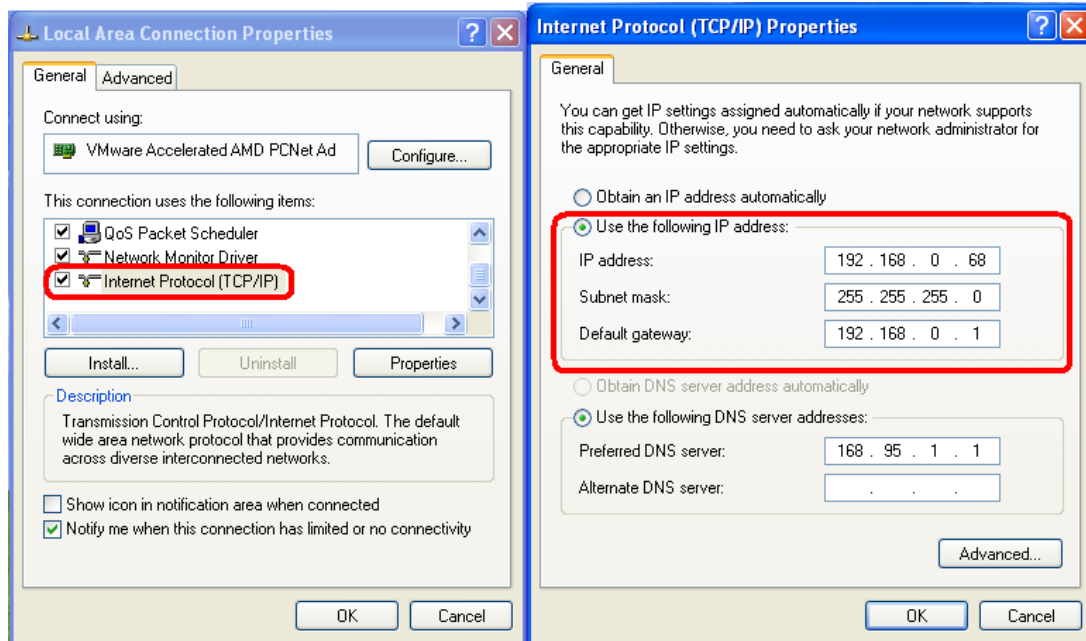
### WINDOWS XP :

《Step 1》

Click WINDOWS XP my computer  , Open Control Panel  Control Panel on the left side, please turn to traditional overview and select network link

《Step 2》

Click LAN, then select content, the link configuration will be shown, click Internet Protocol (TCP/IP) as left figure, then input the same setting as MX60, as right figure:



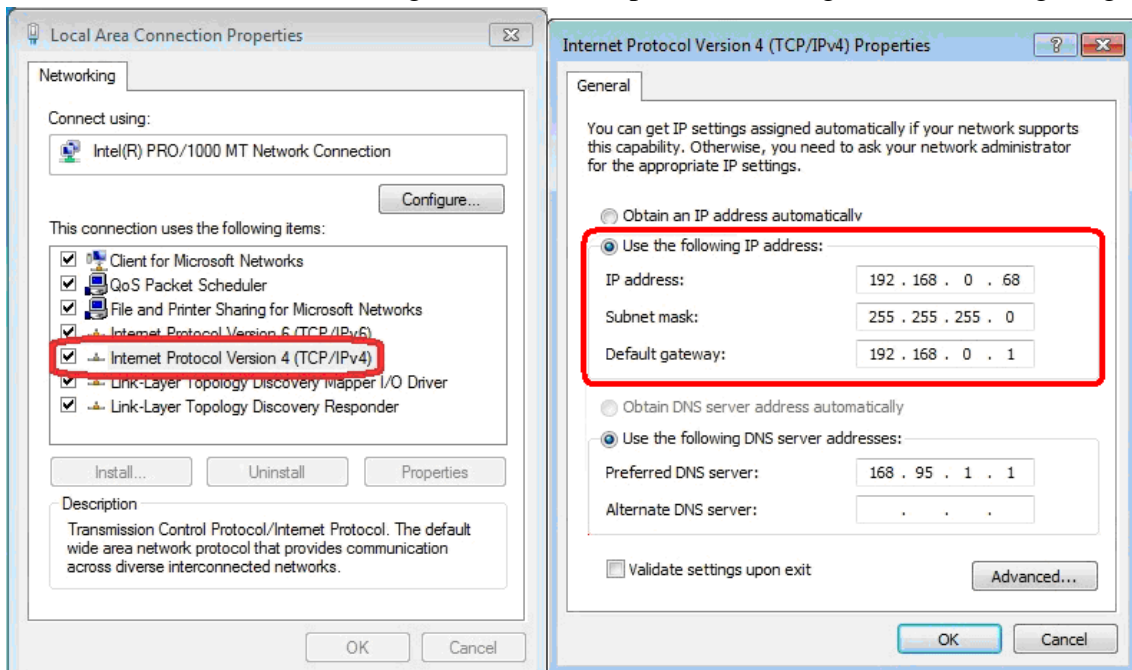
## WINDOWS 7 :

«Step 1»

Click Windows 7 icon,  select  Control Panel , open and search for ,  Network and Sharing Center click Alter Interface Card on the upper-left side.

«Step 2»

Click LAN link, select content, then the LAN settings will be shown, click Internet Protocol(TCP/IPv4), as left figure, click and input same setting as MX60, as right figure.

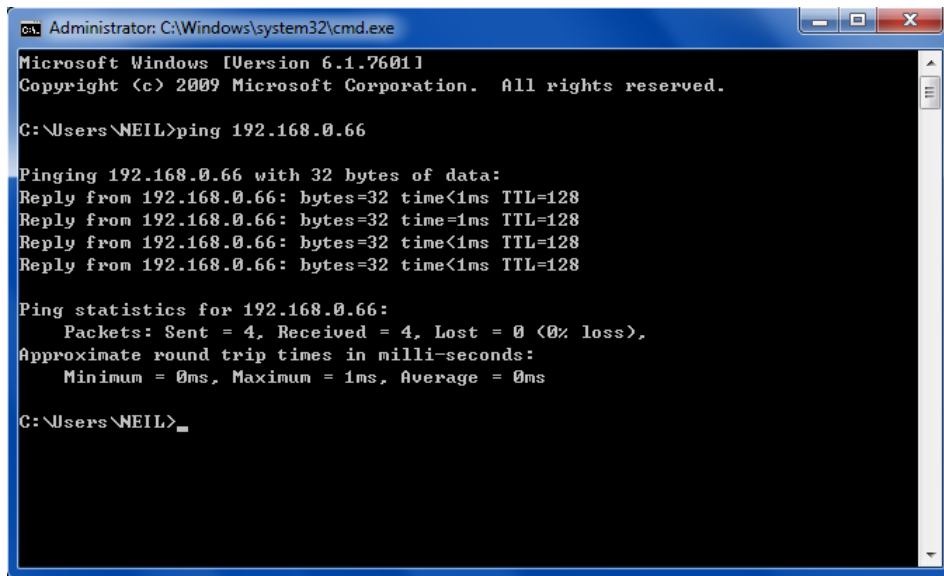


## How to log on to MX60 web browser

1、Start Web browser ( eg: WIN 7 IE ), input MX60 IP Address, for example: use the default MX60 IP Address: <http://192.168.0.66>

2、If connection failed, should check:

- If MX60 installed and its power supplied properly
- To examine the LAN connection, can use start tools→Execute→Input cmd open MS-DOS, Input “ ping” to test MX60 connection, input command: ping 192.168.0.66, as shown below:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NEIL>ping 192.168.0.66

Pinging 192.168.0.66 with 32 bytes of data:
Reply from 192.168.0.66: bytes=32 time<1ms TTL=128
Reply from 192.168.0.66: bytes=32 time=1ms TTL=128
Reply from 192.168.0.66: bytes=32 time<1ms TTL=128
Reply from 192.168.0.66: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.66:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NEIL>_
```

- If no response received, it explains the link has troubles either the connection is not proper or the PC’s IP address can not match with MX60’s IP address
- Set the PC’s IP address with MX60’s IP address with same segment, if the PC uses fixed IP address, the address must be ranged in: 192.168.0.1 ~ 192.168.0.65 or 192.168.0.67 ~ 192.168.0.254 , thus it can be compatible with MX60’s default IP address: 192.168.0.66, the “ Subnet Mask’s setting must be: 255.255.255.0

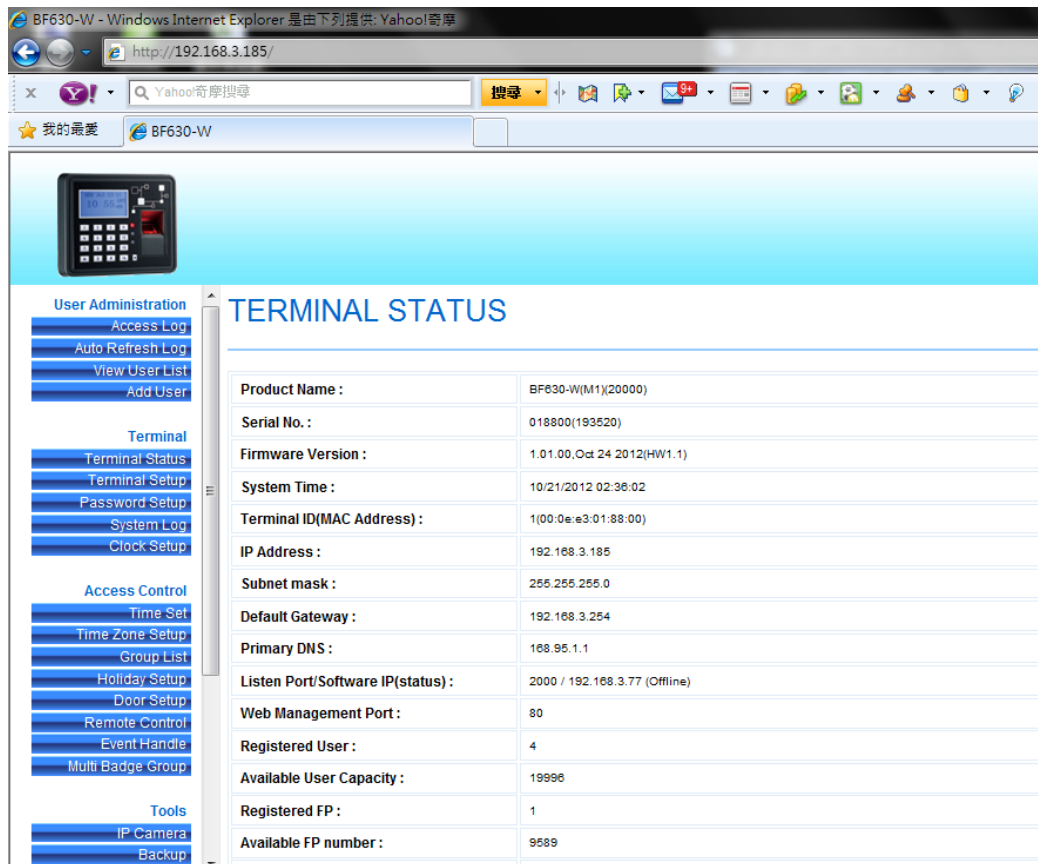
- 3 · If the connection with MX60 is successful, then it will display a message window for User name and Password, the default for user name and Password is: [admin/admin](#), as shown below:



- 4 · While the user name and password entered, a Web setting interface of MX60 will be showed, enter it will then display a “ Quick Setup “ page.

# Terminal Status

When installation has completed and connected with MX60, a Terminal Status window "as below will pop up:



The screenshot shows a web browser window with the address bar displaying `http://192.168.3.185/`. The browser's address bar also shows the text "BF630-W". The page content includes a navigation menu on the left and a main content area titled "TERMINAL STATUS".

**Navigation Menu:**

- User Administration
  - Access Log
  - Auto Refresh Log
  - View User List
  - Add User
- Terminal
  - Terminal Status
  - Terminal Setup
  - Password Setup
  - System Log
  - Clock Setup
- Access Control
  - Time Set
  - Time Zone Setup
  - Group List
  - Holiday Setup
  - Door Setup
  - Remote Control
  - Event Handle
  - Multi Badge Group
- Tools
  - IP Camera
  - Backup

**TERMINAL STATUS Table:**

Product Name :	BF630-W(M1)(20000)
Serial No. :	018800(193520)
Firmware Version :	1.01.00,Oct 24 2012(HW1.1)
System Time :	10/21/2012 02:36:02
Terminal ID(MAC Address) :	1(00:0e:e3:01:88:00)
IP Address :	192.168.3.185
Subnet mask :	255.255.255.0
Default Gateway :	192.168.3.254
Primary DNS :	168.95.1.1
Listen Port/Software IP(status) :	2000 / 192.168.3.77 (Offline)
Web Management Port :	80
Registered User :	4
Available User Capacity :	19996
Registered FP :	1
Available FP number :	9589

【Terminal Status】 — Picture1

## 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>	Instant Access to records Display
<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
<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>Multiple Badge</b>	Set up multiple badge combination for access control purpose. 2~3 user per set, up to 10 combination set support.
▶ Tools	
<b>IP Camera</b>	1. Set up IP address, type, username and password for the IP Camera. 2. Display snapshot picture captured from the IP Camera (only latest one)
<b>Backup</b>	Switch to the “Backup personnel data, terminal data “ screen.
<b>Restore</b>	Switch to the “Restore personnel data, terminal data “ screen.
<b>Reboot</b>	Switch to the “Reboot System“ screen.
<b>Upgrade Firmware</b>	Switch to the “Firmware Upgrade“ screen.
<b>Reset</b>	1. Delete User Data. Access Logs. Group Time Zone. Time Set. Holiday. System Logs 2. Switch to the “Factory Default“ screen.
▶ BUTTON	
<b>Refresh</b>	Refresh the WEB Status.

# User Administration

## Access Log

Select “Access Log” on the Main Window, you’ll see the “Access Log” screen as following picture:

### Access Log/Query and Export

No.	User ID	User Name	Date	Time	IN/OUT	Door	Note.
1.	1(N)	CHIYU	05/25/2011	11:33:29	IN(O)	1	(C)
2.	1(N)	CHIYU	05/25/2011	11:33:28	IN(O)	1	(C)
3.	----	----	05/25/2011	11:33:05	IN	1	(C)UNREG(5354879)

Total 3 Record(s)

<< End of List... >>

### Query and Export

Type  
 user  event

Selection  
 Single  All

Start Date

End Date

User ID

Card No.(DEC)

Export Type  
 Txt  Xls

【Access Log】 — Picture2

## Illustration of Access Log :

<b>No.</b>	Serial Number of Access Logs
<b>User ID</b>	User ID will be showed for the user who has access the door. By clicking “User ID” will direct current screen to “User Record ”page to “Modify User Record” ( picture 4). Should it be not connected, it means the information of the User ID has been deleted. * The figure in the parentheses ( ) after the “User ID” means the user’s level as 1~10.
<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>	IN: Access by WEBPASS OUT: Access by Wiegand Reader ※ APB level will be shown followed the IN/OU
<b>Door No.</b>	It stands for the Door Number Controlled By MX60
<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 Former 10 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.
<b>▶ Query and Export</b>	
<b>Type</b>	1. <b>User</b> : Check the user, can search the user records, and export the file out 2. <b>Event</b> : Check the Event, can search the Event records, and export the file out
<b>User ID or Card Number</b>	1. <b>Single</b> : Can only 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>StartDate/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.
<b>▶ Button</b>	
<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

Select “Auto Refresh Log” will see the “Auto Refresh Log” screen as the following picture:

Auto Refresh Log Fri Feb 25 2011 15:39:14 GMT+0800 (China Standard Time)

No.	User ID	User Name	Date	Time	IN/OUT	Door	Note.
4	1	Chiyu	02/25/2011	15:39:02	IN	2	(C)
3	1	Chiyu	02/25/2011	15:39:00	IN	2	(C)
2	----	----	02/25/2011	15:38:58	IN	2	(C)UNREG(2091082572)
1	----	----	02/25/2011	15:38:25	IN	2	(C)UNREG(1553301682)

【Auto Refresh Log】 — Picture3

## Illustration of Auto Refresh Log :

▶ Auto Refresh Log	
<b>No.</b>	Serial Number.
<b>User ID</b>	Instant Display Access records User ID.
<b>User Name</b>	Instant Display Access records User Name.
<b>Date</b>	Instant Display Access records user enter/out date.
<b>Time</b>	Instant Display Access records user enter/out Time.
<b>IN/OUT</b>	Instant Display Access records user IN/OUT Log
<b>Door</b>	Instant Display Door
<b>Note.</b>	Show up the relative IN/OUT records automatically as Anti-Duress, Fire Alarm.....etc.

# View User List

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

## User List

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

\*Reg Type:F(Finger) ,P>Password) , C(Card)

No.	User ID	Employee ID	User Name	User Type	Active	F	P	C	Bypass Level
<input type="checkbox"/> 1.	<a href="#">1111111</a>			Normal	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 2.	<a href="#">55555</a>			Normal	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 3.	<a href="#">12345</a>			Normal	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	1
<input type="checkbox"/> 4.	<a href="#">1234567890</a>			Normal	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	1

Total 4 User(s)

<< End of List... >>

**Activate, Deactivate or Delete SELECTED Employee**

【User List】 – Picture4

## Illustration of User List :

► Search User	
<b>By “User ID”</b>	Select “User ID” and enter “User ID” in the textbox to search.
<b>By “Card No.”</b>	Select “Card No.” and enter “Card No.” in the textbox to search.
<b>By “User Name”</b>	Select “User Name.” and enter “User Name” in the textbox to search.
<b>By “Employee ID”</b>	Select “Employee ID” and enter “Employee ID” in the textbox to search
<b>Click button ”GO”</b>	Start to search.
Steps :	
1. Enter your “User ID”, “Card No or ” or “User Name” or “Employee ID” in the “blank textbox”.	
2. Click button “GO” to search certain user from database.	
► 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
<b>Employee ID</b>	Display “Employee ID” for user
<b>User Name</b>	Display “User Name” for user
<b>User Type</b>	Types of the system User. Whenever “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 user’s authorization status. Green Light means the user’s authority is activated, otherwise it is not activated.
<b>F</b>	When user’s Fingerprint has registered, green light lit.
<b>P</b>	When user’s Personal Password registered, green light lit.
<b>C</b>	When user’s card registered, green light lit.
<b>Verification mode</b>	Display user’s verification mode: (F: Fingerprint/P: Password/C: Card)
<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 Former 10 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

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

**User Record**  
**Modify User Record**

User ID :

Card No. :

Employee ID :

Name :  (Max 31 chars.)

Expire Date Check :  Disable  Enable

From 2012 (M) 10 (D) 19 (H) 11 (M) 28

To 2012 (M) 10 (D) 19 (H) 11 (M) 28

Status :  Activate  Deactivate

User Type :

Group : 1.  2.  3.  4.

Bypass TZ Level :

Personal Password :  (4 ~ 8 digits.)

Personal Confirm :

Number of Finger : 1

---

【Modify User Record】 — Picture5

## Illustration of Modify User Record in User Record :

▶ 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>Employee ID</b>	User's employee ID. Max at 10 characters.
<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 a 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</b> . The Respective definitions are as below : <b>Super User Card</b> : Super user is free from 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>Group</b>	Each user can be assigned to 4 different groups. All 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 time zone level, the door's " Time Zone" becomes invalid.
<b>Personal Password</b>	4~8 digits are required.
<b>Personal Password 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 as following picture:

**User Record**  
**Add New User**

REG:  Single  Continuous    Amount:

User ID:

Card No.:

Employee ID:

Name:  (Max 31 chars.)

Expire Date Check:  Disable  Enable

From: 2012 (M) 10 (D) 21 (H) 3 (M) 24

To: 2012 (M) 10 (D) 21 (H) 3 (M) 24

Status:  Activate  Deactivate

User Type: Normal User ▼

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

Bypass TZ Level: LV1 ▼

Personal Password:  (4 ~ 8 digits.)

Personal Confirm:

Number of Finger: 0

---

【Add User】 — Picture6

## 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 in a time. You may input required q'ty in the text box of Amount. However, only the continuous serial number is 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>Employee ID</b>	Employee ID for user, max at 10 characters (English)
<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 a 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</b> . The Respective definitions are as below : <b>Super User Card</b> : Super user is free from limitation of 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>Group</b>	Each user can be assigned to 4 different groups. All 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 time zone level, the door's " Time Zone" becomes invalid.
<b>Personal Password</b>	4~8 digits are required.
<b>Personal Confirm</b>	Reconfirm Personal Password.
<b>Fingerprint Template</b>	Registry fingerprint templates amount
▶ Button	
<b>Save</b>	Save User RECORDS.

# TERMINAL

## Terminal Status

Select "Terminal Status" on the Main Window, you'll see the "Terminal Status" screen for Logon. It will display current Terminal Status and relative information of WEB setup as following picture:

### TERMINAL STATUS

Product Name :	BF630-W(M1)(20000)
Serial No. :	018800(193520)
Firmware Version :	1.01.00,Oct 24 2012(HW1.1)
System Time :	10/21/2012 03:29:35
Terminal ID(MAC Address) :	1(00:0e:e3:01:88:00)
IP Address :	192.168.3.185
Subnet mask :	255.255.255.0
Default Gateway :	192.168.3.254
Primary DNS :	168.95.1.1
Listen Port/Software IP(status) :	2000 / 192.168.3.77 (Offline)
Web Management Port :	80
Registered User :	4
Available User Capacity :	19996
Registered FP :	1
Available FP number :	9589
Access/System Log Count :	2/67
Control Mode :	Controller(WG34)
Anti-Pass-Back(Tolerance Timer) :	Disabled(0)
Anti-Duress :	Disabled
Next BF630-W(Status) :	0.0.0.0(Offline)

【Terminal Status】 — Picture7

## Illustration of TERMINAL Status :

▶ TERMINAL STATUS	
<b>Product Name</b>	Model Number of MX60
<b>Serial No.</b>	Serial Number of MX60
<b>Firmware/Hardware Version</b>	Firmware and Hardware Version of MX60
<b>System Time</b>	System Time of MX60
<b>Terminal ID (MAC Address)</b>	Terminal ID and MAC address of MX60
<b>IP Address</b>	IP address of MX60
<b>Subnet Mask</b>	Subnet mask of MX60
<b>Default Gateway</b>	Default Gateway address of MX60
<b>Primary DNS</b>	Primary DNS address of MX60
<b>Listen Port/Software IP(Status)</b>	MX60 and software communication Port number and Software IP address (status between WebPass and software: Online or Offline)
<b>WEB communication port</b>	MX60 WEB communication port number
<b>Registered User</b>	Registered user numbers of MX60
<b>Available User Capacity</b>	Available Capacity of MX60 to register user.
<b>Access/System Log Count</b>	The Sum from access and system logs of MX60
<b>Control Mode</b>	MX60 control mode will be Controller (WG34)
<b>Anti-Pass-Back (Tolerance Timer)</b>	Enable or Disable the MX60 APB (Anti Pass Back) function (including its Tolerance Time).
<b>Anti-Duress</b>	Enable or Disable the MX60 function of Anti Duress.
<b>Next MX60 (Status)</b>	Enable or Disable the MX60 Anti Pass Back function ( including its Tolerance Time)

# Terminal Setup

Select "Terminal Setup" on Main Window, you'll see the "Terminal Configuration "as following picture:

## Terminal Configuration

---

Terminal Setting :	Terminal ID : <input type="text" value="1"/>
	*IP Address : <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="3"/> . <input type="text" value="185"/>
	*Subnet Mask : <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="255"/> . <input type="text" value="0"/>
	*Gateway : <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="3"/> . <input type="text" value="254"/>
	*DNS Server : <input type="text" value="168"/> . <input type="text" value="95"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
Listen Port :	*TCP Port(Software Used) : <input type="text" value="2000"/> *Software IP : <input type="text" value="192.168.3.77"/>
Web Language :	<input type="text" value="English"/> ▼
Anti Pass Back :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Tolerance Timer <input type="text" value="0"/> (Minute, Maximum 65535, 0 means No Tolerance)
Anti Duressed :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
	Password • <input type="text"/> (Max 3 digits,default is 9)
WEB Managemant Port :	Http Port : <input type="text" value="80"/>
Next BF630-W(for APB):	IP Address : <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Fast Reg Card Mode :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Sound for verify card :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Security Level :	<input type="text" value="1/100,000"/> ▼ (Default: Auto Normal)
Illegal FP Access record :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FP auto adjustment :	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Terminal may need to restart after configuration saved.

---

【Terminal Setup】 — Picture8

## Illustration of Terminal Configuration :

▶ Terminal Configuration	
<b>Terminal ID</b>	For setting the Terminal ID of MX60. Default =1, max. 65535, not allowed to duplicated.
<b>IP Address</b>	For setting the IP Address of MX60.
<b>Subnet Mask</b>	For setting the Subnet Mask of MX60.
<b>Gateway</b>	For setting the Default Gateway of MX60.
<b>DNS Server IP Address</b>	For setting the DNS Server IP Address of MX60. Default DNS Server IP Address is 168.95.1.1.
▶ Software	
<b>TCP Port (for Software)</b>	Setting TCP port number for software and MX60 terminal. Default is 2000.
<b>Software IP</b>	For setting the Software IP to communicate with MX60. Default IP is 0.0.0.0.
▶ Web Language	
<b>English</b>	When you choose "English", Web page will be switched to "English" type interface.
<b>Chs</b>	When you choose "Chs", WEB page will be switched to "Simplified Chinese" mode interface .
<b>Others</b>	When you choose "Others", the WEB page will be switched to "Traditional Chinese" mode interface or other language by requested.
▶ 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 Timer</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 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 is 9, max. 3 digits.
▶ WEB Management Port	
<b>HTTP Port</b>	Set your WEB port number for MX60 communication, default value is 80.
▶ Next MX60 (for APB only)	
<b>IP Address</b>	Set your IP address for Next MX60, but only available for the structure of multiple of MX60. Whenever this IP for next MX60 is set up, all the levels settings of original MX60 will be copied to next MX60.
▶ Fast Registry Card Mode	
<b>Enable</b>	Tick this circle to enable the "Fast Registry card mode"
<b>Disable</b>	Tick this circle to disable the "Fast Registry card mode"

<b>Sound to verify card mode</b>	
<b>Enable</b>	Tick to enable “Sound to verify card”
<b>Disable</b>	Tick to disable “Sound to verify card”
<b>Security Level</b>	
Default is “Auto Normal” ( Recommend not to change)	
<b>▼ Illegal FP Access Record</b>	
<b>Enable</b>	Illegal fingerprint access log will be recorded
<b>Disable</b>	Illegal fingerprint access log will NOT be recorded
<b>Fingerprint Auto Adjustment</b>	
<b>Enable</b>	Scan twice for one fingerprint ( two fingerprint templates for one finger will be saved)
<b>Disable</b>	Scan once for one fingerprint (one fingerprint template will be saved)
<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 :  (47 Char. Max)

Administrator WEB Logon Password :  (35 Char. Max)

Operator WEB Logon User Name :  (47 Char. Max)

Operator WEB Logon Password :  (35 Char. Max)

USER WEB Logon User Name :  (47 Char. Max)

USER WEB Logon Password :  (35 Char. Max)

## Entrance Password

---

Common Password :  (4 ~ 8 digits.)

【WEB Logon Setting/Entrance Password】 — Picture9

## Illustration of WEB Logon Setting/ Entrance Password :

▶ WEB Logon Setting	
<b>Administrator User Name</b>	Input the required Administrator's logon user name for WEB management, max. 47 characters, default value: "admin".
<b>Administrator Password</b>	Input the required Administrator's logon password for WEB management, max. 35 digits, default value: "admin".
<b>Operator User Name</b>	Input the required Operator's logon user name for WEB management, max. 47 characters, default value: "user".
<b>Operator Password</b>	Input the required Operator's logon password for WEB management, max. 35 digits, default value: "user".
<b>User Name</b>	Input the required User's logon user name for WEB management, max. 47 characters, default value: "user0".
<b>User 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.

**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" to see the "System Log" screen as following picture:

## System Log

No.	Date	Time	Description
1 .	05/25/2011	09:14:17	System Power ON
2 .	05/24/2011	17:28:11	System Cold Start
3 .	05/24/2011	17:28:10	WEB Image File Upgrade Success via HTTP
4 .	05/24/2011	17:16:26	System Warm Start
5 .	05/24/2011	17:15:25	System Cold Start
6 .	05/24/2011	17:15:25	WEB Image File Upgrade Success via TFTP
7 .	05/24/2011	17:13:56	IP Conflict
8 .	05/24/2011	17:12:50	System Warm Start
9 .	05/24/2011	17:12:22	System Cold Start
10 .	05/24/2011	17:12:22	WEB Image File Upgrade Success via TFTP
11 .	05/24/2011	17:11:59	System Cold Start
12 .	05/24/2011	17:11:58	FW Upgrade Success via TFTP
13 .	05/24/2011	17:10:09	System Cold Start
14 .	05/24/2011	17:10:08	WEB Image File Upgrade Success via HTTP
15 .	05/24/2011	17:09:09	System Cold Start
16 .	05/24/2011	17:09:08	WEB Image File Upgrade Success via HTTP
17 .	05/24/2011	17:05:11	System Cold Start
18 .	05/24/2011	17:05:11	WEB Image File Upgrade Success via TFTP
19 .	05/24/2011	17:04:48	System Cold Start
20 .	05/24/2011	17:04:48	FW Upgrade Success via TFTP

Total 67 Record(s) < [First](#) | [Prev 10](#) | [1](#) [2](#) [3](#) [4](#) | [Next 10](#) | [End](#) >>

【System Log】 — Picture10

## 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.
<b>Export TXT</b>	Export TXT File
<b>Export XLS</b>	Export XLS File
※Max. logs capacity : 1536 entries for checking authorized person(s) only, no logs export provided.	

## Clock Setup

Select "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

time.windows.com

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

Time Zone :

(GMT+08:00) China, Hong Kong, Australia Western

Save

New Date : 02/15/2011 (mm/dd/yyyy)

New Time : 09:16:41 (hh:mm:ss)

Save

【System Clock Setup】 – Picture11

## 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 "mm/dd/yyyy".
<b>New Time</b>	The date of networked PC computer. You may adjust the time to your requirement as the format of "hh:mm:ss".
<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	
-----	---------------	--	-----	---------------	--

---

Time Set :  From  H :  M To  H :  M

【Time Set】 — Picture12

## 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>	Input a time set period, for example : 8:00am to 17:00pm 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 referring to the following picture:

### Time Zone List

---

Time Zone List :

000	Deactivate		001	Any Time	
-----	------------	--	-----	----------	--

---

Time Zone ID :

【Time Zone Setup】 — Picture13

## 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:	000 -- 00:00 ~ 00:00	Time 2:	000 -- 00:00 ~ 00:00	Time 3:	000 -- 00:00 ~ 00:00	Time 4:	000 -- 00:00 ~ 00:00
Time 5:	000 -- 00:00 ~ 00:00	Time 6:	000 -- 00:00 ~ 00:00	Time 7:	000 -- 00:00 ~ 00:00	Time 8:	000 -- 00:00 ~ 00:00
Time 9:	000 -- 00:00 ~ 00:00	Time 10:	000 -- 00:00 ~ 00:00	Time 11:	000 -- 00:00 ~ 00:00	Time 12:	000 -- 00:00 ~ 00:00
Time 13:	000 -- 00:00 ~ 00:00	Time 14:	000 -- 00:00 ~ 00:00	Time 15:	000 -- 00:00 ~ 00:00	Time 16:	000 -- 00:00 ~ 00:00

Save Cancel

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Holiday
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	000 -- 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	000 -- 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	000 -- 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	000 -- 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	000 -- 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	000 -- 00:00 ~ 00:00
Time 7:	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	000 -- 00:00 ~ 00:00
Time 8:	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	000 -- 00:00 ~ 00:00
Time 9:	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	000 -- 00:00 ~ 00:00
Time 10:	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	000 -- 00:00 ~ 00:00
Time 11:	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	000 -- 00:00 ~ 00:00
Time 12:	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	000 -- 00:00 ~ 00:00
Time 13:	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	000 -- 00:00 ~ 00:00
Time 14:	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	000 -- 00:00 ~ 00:00
Time 15:	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	000 -- 00:00 ~ 00:00
Time 16:	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	000 -- 00:00 ~ 00:00

【Time Zone Information】 — Picture14

## Illustration of Time Zone Information :

▶ Time Zone Information Setting																																																									
<b>Weekday (Day)</b>	<p>The “Drop Down Menu ”offers you options from Monday to Sunday and Holiday. Steps : “SET” the “Time Set” on “Time Set” screen→ Select your weekday →Choose your time set(s) of the time zones.</p>																																																								
<b>Time Set 1 ~ Time Set 16 (16 time set per day)</b>	<p>Each day from Monday ~Sunday and Holiday is allowed 16 time sets. However, you have to make some Time Sets on the “Time Set” screen in advance for the options here, otherwise only 2 default Time sets for your choice, referring to the following illustration:</p> <p><u>Step 1 : “Time Set” screen to “SET” some time sets</u></p> <p><b>Time Set</b></p> <hr/> <p><b>Time Set List :</b></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td style="padding: 2px;">000</td> <td style="padding: 2px;">00:00 ~ 00:00</td> <td style="padding: 2px;"></td> <td style="padding: 2px;">001</td> <td style="padding: 2px;">00:00 ~ 23:59</td> <td style="padding: 2px;"></td> </tr> <tr> <td style="padding: 2px;">002</td> <td style="padding: 2px;">08:30~18:00</td> <td style="padding: 2px;"><input type="button" value="DELETE"/></td> <td style="padding: 2px;">003</td> <td style="padding: 2px;">12:00~20:00</td> <td style="padding: 2px;"><input type="button" value="DELETE"/></td> </tr> </table> <hr/> <p style="text-align: center;">Time Set : 004 ▾ From 00 H : 00 M To 23 H : 59 M <input type="button" value="SET"/></p> <p><u>Step 2 : “Time Zone Information” screen for more options than original 2 default time sets</u></p> <p><b>Time Zone Information -- 002</b></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <tr> <td colspan="2"></td> <td colspan="4">Day : Monday ▾</td> </tr> <tr> <td style="padding: 2px;">Time 1:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 2:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 3:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 4:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> </tr> <tr> <td style="padding: 2px;">Time 5:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 6:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 7:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 8:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> </tr> <tr> <td style="padding: 2px;">Time 9:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 10:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 11:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 12:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> </tr> <tr> <td style="padding: 2px;">Time 13:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 14:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 15:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> <td style="padding: 2px;">Time 16:</td> <td style="padding: 2px;">000 ~ 00:00 ~ 00:00 ▾</td> </tr> <tr> <td colspan="2"></td> <td colspan="4" style="text-align: center;"> <input type="button" value="Save"/> <input type="button" value="Cancel"/> </td> </tr> </table>	000	00:00 ~ 00:00		001	00:00 ~ 23:59		002	08:30~18:00	<input type="button" value="DELETE"/>	003	12:00~20:00	<input type="button" value="DELETE"/>			Day : Monday ▾				Time 1:	000 ~ 00:00 ~ 00:00 ▾	Time 2:	000 ~ 00:00 ~ 00:00 ▾	Time 3:	000 ~ 00:00 ~ 00:00 ▾	Time 4:	000 ~ 00:00 ~ 00:00 ▾	Time 5:	000 ~ 00:00 ~ 00:00 ▾	Time 6:	000 ~ 00:00 ~ 00:00 ▾	Time 7:	000 ~ 00:00 ~ 00:00 ▾	Time 8:	000 ~ 00:00 ~ 00:00 ▾	Time 9:	000 ~ 00:00 ~ 00:00 ▾	Time 10:	000 ~ 00:00 ~ 00:00 ▾	Time 11:	000 ~ 00:00 ~ 00:00 ▾	Time 12:	000 ~ 00:00 ~ 00:00 ▾	Time 13:	000 ~ 00:00 ~ 00:00 ▾	Time 14:	000 ~ 00:00 ~ 00:00 ▾	Time 15:	000 ~ 00:00 ~ 00:00 ▾	Time 16:	000 ~ 00:00 ~ 00:00 ▾			<input type="button" value="Save"/> <input type="button" value="Cancel"/>			
000	00:00 ~ 00:00		001	00:00 ~ 23:59																																																					
002	08:30~18:00	<input type="button" value="DELETE"/>	003	12:00~20:00	<input type="button" value="DELETE"/>																																																				
		Day : Monday ▾																																																							
Time 1:	000 ~ 00:00 ~ 00:00 ▾	Time 2:	000 ~ 00:00 ~ 00:00 ▾	Time 3:	000 ~ 00:00 ~ 00:00 ▾	Time 4:	000 ~ 00:00 ~ 00:00 ▾																																																		
Time 5:	000 ~ 00:00 ~ 00:00 ▾	Time 6:	000 ~ 00:00 ~ 00:00 ▾	Time 7:	000 ~ 00:00 ~ 00:00 ▾	Time 8:	000 ~ 00:00 ~ 00:00 ▾																																																		
Time 9:	000 ~ 00:00 ~ 00:00 ▾	Time 10:	000 ~ 00:00 ~ 00:00 ▾	Time 11:	000 ~ 00:00 ~ 00:00 ▾	Time 12:	000 ~ 00:00 ~ 00:00 ▾																																																		
Time 13:	000 ~ 00:00 ~ 00:00 ▾	Time 14:	000 ~ 00:00 ~ 00:00 ▾	Time 15:	000 ~ 00:00 ~ 00:00 ▾	Time 16:	000 ~ 00:00 ~ 00:00 ▾																																																		
		<input type="button" value="Save"/> <input type="button" value="Cancel"/>																																																							
▶ Button																																																									
<b>Save</b>	Save the“ Time Zone Information”.																																																								
<b>Cancel</b>	Cancel or Modify the “Time Zone Information”.																																																								
<p>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.</p>																																																									

## Group List

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

### Group List

Group List :

000	Disallowed Group		001	Free Time Group	
-----	------------------	--	-----	-----------------	--

Group ID :

【Group List】 — Picture15

## 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"
<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

---

Allowed Door :	Time Zone ID :
<input checked="" type="checkbox"/> 1.	001 Activate ▾

---

【Group Information】 — Picture16

## Illustration of Group Information :

▶ Allowed Door	
<b>Door</b>	Tick the box of Door , then the user(s) of this Group can access Door 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 and Click "Holiday Setup" on the left side of the Main Window, you'll see the "Holiday setup" screen referring to the following picture:

### Holiday setup

---

01  Month / 01  Date

---

**Holiday List :** -

---

【Holiday setup】 — Picture17

## 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 left side of the Main Window, you'll see the "Door Setting" screen as below:

**Door Setting**

	IN		OUT
L9 First Admin FP IN Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L8 Multiple Badge FP Time Zone :	000 Deactivate ▾	Double ▾	000 Deactivate ▾ Double ▾
L7 Multiple Badge Time Zone :	000 Deactivate ▾	Double ▾	000 Deactivate ▾ Double ▾
L6 Card+FP+Admin Password Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L5 FP+Admin Password Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L4 Card+Personal Password or Card+FP Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L3 Password or FP Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L2 Card Only Time Zone :	000 Deactivate ▾		000 Deactivate ▾
L1 Card or Password or FP Time Zone :	001 Any Time ▾		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)
Lock Release Time :	10	Sec ( 1 - 65535, 10 = default )	
Door Open Delay Time :	10	Sec ( 1 - 65535, 10 = default )	
Access Log :	Recorded ▾		
Door Sensor Mode:	N/A ▾		
Door Relay Energized:	<input type="radio"/> None	<input checked="" type="radio"/> 1 Relay	<input type="radio"/> 2 Relay

SET

【Door Setting】 — Picture18

## Illustration of Door Setting :

▶ Door Setting	
<b>L9 First Admin FP Time Zone</b>	<p>Set First Admin FP Time Zone for door (default for IN/OUT is 000 Deactivate). All users can only access at door with their own Card, Fingerprint or Personal Password when First Admin user has identified by MX60 at the door.</p> <p>When L9 bypass time zone is chosen, user can access door 1 by Card only. When Lock Release Time zone has chosen, user can access door freely.</p>
<b>L8 Multiple Badge FP Time Zone</b>	<p>Set Multiple Badge FP Time Zone for door (default is 000 Deactivate). Multiple Badge combination should be firstly configured with 2~3 user accounts before set up Multiple Badge FP Time Zone. (No verification order needed to the multiple badge group members)</p> <p>When L8~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>
<b>L7 Multiple Badge Time Zone</b>	<p>Set Multiple Badge FP Time Zone for door (default is 000 Deactivate). Multiple Badge combination should be firstly configured with 2~3 user accounts before set up Multiple Badge FP Time Zone. (No verification order needed to the multiple badge group members)</p> <p>When L7~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>
<b>L6 Card+FP+ Admin Password Time Zone</b>	<p>Set up door with L6 Time Zone (default 000 Deactivate). All user should access door with their own card +fingerprint+ Admin password (without order).</p> <p>When L6~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>
<b>L5 FP+Admin Password Time Zone</b>	<p>Set up door with L5 Time Zone (default 000 Deactivate). All user can access door with their own fingerprint and input admin password without order.</p> <p>When L5~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>
<b>L4 Card+Personal password or Card+Fingerprint Time Zone</b>	<p>Set up door with L4 Time Zone (Default 000 Deactivate). All user can access door by card+personal password or by card+fingerprint. (Terminal will indicate the identification procedure: press * for 1:1 verification mode, or input personal password) without identification order.</p> <p>When L4~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>
<b>L3 Password or Fingerprint Time Zone</b>	<p>Set up door with L3 Time Zone (Default 000 Deactivate). All user may access door by input personal password or identify fingerprint.</p> <p>When L3~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.</p>

<b>L2 Card Time Zone</b>	Set up door with L2 Time Zone (Default 000 Deactivate). All user may access door by scan card. When L2~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.
<b>L1 Card or Password or Fingerprint</b>	Set up door with L1 Time Zone (Default 001 Anytime). All user may access door by card or personal password or common password or fingerprint. When L2~L9 bypass time zone is chosen, user may access door by card. When Lock Release Time Zone has chosen, user can access door freely.
<b>Lock Release Time Zone</b>	When door set up with Lock Release Time Zone (Default 000 Deactivate). All user may access door without identification. When First card is chosen, lock will be released only a legal card identified first.
<b>Exit Button Time Zone</b>	Set up door with Exit Button Time Zone. Support only Out direction (inside of door). Default is 001 Anytime
<b>Anti Pass Back In/Out</b>	Set up door with APB mode by 0~255 level
<b>Door Close Delay Time</b>	Set up door with “Door Close Delay” alarm time, default is 10 seconds
<b>Door Open Delay Time</b>	Set up door with “Door Open Delay Time”, default is 10 seconds.
<b>Access Log</b>	Record or not record access log (Default is record)
<b>Door Relay Energized</b>	Selection for door relay trigger mode: None: No Trigger 1 Relay: Trigger door relay only 2 Relay: Trigger all relays including door relay : a. Without BF20/BF-50: Trigger another relay b. With BF20/BF50: Trigger Relay no.2 to drive BF20/BF-50 (Event Handle configuration to Hard Alarm and Soft Alarm should NOT be duplicated)
<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.
<b>► Button</b>	
<b>Set BF-50 Card</b>	Input 50 set of card numbers to BF-50. When main controller is disconnected to BF-50, BF-50 will check the card number with the input card number list to open the door.
<b>Update BF-50 Card</b>	Input card number to BF-50 then tap the update button to update card numbers to BF-50

## Set up BF-50 with card list

Select "Door Setup" to configure "BF-50 Card" with card list. Support up to 50 card IDs can be recorded to BF-50. When system disconnected will still secure door will be opened open by the legal cards that have programmed in to the BF-50 Card list.

### BF50 CARD

No.	Card No.	No.	Card No.	No.	Card No.	No.	Card No.	No.	Card No.
1	0	2	0	3	0	4	0	5	0
6	0	7	0	8	0	9	0	10	0
11	0	12	0	13	0	14	0	15	0
16	0	17	0	18	0	19	0	20	0
21	0	22	0	23	0	24	0	25	0
26	0	27	0	28	0	29	0	30	0
31	0	32	0	33	0	34	0	35	0
36	0	37	0	38	0	39	0	40	0
41	0	42	0	43	0	44	0	45	0
46	0	47	0	48	0	49	0	50	0

Set cancel

【BF-50 Card】 — Picture18-1

## Illustrations of BF-50 Card :

▶ BF-50 Setting	
<b>NO</b>	Total from 1~50 card number can be set
<b>Card No</b>	Enter BF-50 User Card
▶ Button	
<b>Set</b>	Save data

# Remote Control

Select "Remote Control" to configure "Door Status Monitoring/Security Bypass" status as below:

## Door Status Monitoring

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

Door

Door State	<input checked="" type="radio"/>
Webpass/BF50 Status	X
Fire Alarm Detection	off

## Security Bypass

State

【Door Status Monitoring】 — Picture19

## Illustrations of Door Status Monitoring/Security Bypass :

▶ Door Status Monitoring	
<b>Door Status</b>	Display the updated status of Door 1 and Door 2. 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>MX60/BF-50</b>	Display MX60/BF-50 update status. LED gray : No Response Green light: Door is closed Yellow light: Door is opened Red light: Abnormal status (circuit short, circuit open, intrude, door open too long ..etc)
<b>Fire Alarm Detection</b>	Display whether the “Fire Alarm Detection ”enabled or not.
▶ Security Bypass	
<b>Status</b>	There are three “Security Bypass Status”of the doors: Normal/Force Open/Force Close.
<b>Pulse Open Door</b>	Click button to open the door(s) remotely. The function works when the Security Bypass status is in 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 status(s) of all the door(s) ticked will display Force Close even a valid card have flashed thru the reader, user may not access the door(s).
<b>Back to Normal</b>	Click this button to restore all the ticked door(s) 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>Fire Alarm Detection ON</b>	Click this button to activate the “Fire Alarm Detection” function and the door(s) status will display “ON”.
<b>Fire Alarm Detection OFF</b>	Click this button to deactivate the “Fire Alarm Detection” function and the door(s) status will display “off”.
<b>Alarm OFF</b>	Click this button to deactivate the Alarm triggered.

# Event Handle

Select "Event Handle" to configure "Event Handle" mode:

## Event Handle

E-mail Alerts		Hard Alarm	Soft Alarm1	Soft Alarm2	IP Camera	E-mail Alerts
Location :	<input type="text" value=""/> (max59)	0	0	0	0	0
SMTP Mail Server :	<input type="text" value=""/> (max47)	<b>Event</b>				
Mail from :	<input type="text" value=""/> (max47)	Unregistered User	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
SMTP Server Requires Authentication :	username : <input type="text" value=""/> (max45)	Deactivated User	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	password : <input type="text" value=""/> (max29)	Not Allowed Door	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mail To :	<input type="text" value=""/> (max47)	Time Zone Violation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Mail Cc :	<input type="text" value=""/> (max47)	Expired User	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input type="button" value="Set"/>		Anti Pass Back Violation	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Door open too long	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Tamper Switch Breakdown	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Door Intruded	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Duress Alarm On	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
		Fire Alarm On	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

【Event Handle】 — Picture20

## Hard Alarm

Latched Time  (sec,Max 65535 : 0 means unlimited)

Unregistered User   
  Deactivated User   
  Not Allowed Door   
  Time Zone Violation   
  Expired User  
 Anti Pass Back Violation   
  Door open too long   
  Tamper Switch Breakdown   
  Door Intruded   
  Duress Alarm On  
 Fire Alarm On

## Soft Alarm1(BF20/50 Only)

Latched Time  (sec,Max 65535 : 0 means unlimited)

Unregistered User   
  Deactivated User   
  Not Allowed Door   
  Time Zone Violation   
  Expired User  
 Anti Pass Back Violation   
  Door open too long   
  Tamper Switch Breakdown   
  Door Intruded   
  Duress Alarm On  
 Fire Alarm On

## Soft Alarm2(BF20/50 Only)

Latched Time  (sec,Max 65535 : 0 means unlimited)

Unregistered User   
  Deactivated User   
  Not Allowed Door   
  Time Zone Violation   
  Expired User  
 Anti Pass Back Violation   
  Door open too long   
  Tamper Switch Breakdown   
  Door Intruded   
  Duress Alarm On  
 Fire Alarm On

---

## IP Camera

---

- Unregistered User     Deactivated User     Not Allowed Door     Time Zone Violation     Expired User  
 Anti Pass Back Violation     Door open too long     Tamper Switch Breakdown     Door Intruded     Duress Alarm On  
 Fire Alarm On

## E-mail Alerts

---

- Unregistered User     Deactivated User     Not Allowed Door     Time Zone Violation     Expired User  
 Anti Pass Back Violation     Door open too long     Tamper Switch Breakdown     Door Intruded     Duress Alarm On  
 Fire Alarm On

## Illustration of Event Handle :

► Event Type	
<b>Unregistered User</b>	<ol style="list-style-type: none"> <li>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.</li> <li>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 :</li> </ol>
<b>Deactivated User</b>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu”. When it’s selected and the user card has been deactivated then a Deactivated status will be recorded to Access Log screen. If Event Handle level is equaled to or higher than the “Alarm Trigger Level”, the Relay will be triggered then sent and alert E-mail to the account which has been configured.</li> <li>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.</li> </ol>
<b>Not Allowed Door</b>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu”. When it’s selected and the user’s “Group” setting is different than the Door’s group settings, then a“Disallowed door” message will be recorded on the “Access Log ”screen; if the event handle level is equaled to or higher than the“Alarm Trigger Level”, the Relay will be triggered and an E-mail will be sent out if any email account has been configured.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</li> </ol>
<b>Time Zone Violation</b>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu. When it’s selected and the user’s Time Zone Group setting is different from the Door Group Time Zone settings, one Open Time Error message will be recorded on the Access Log ”screen; If the event handle level is equaled to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and an E-mail will be sent out to the account which has been configured</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking Alarm OFF button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</li> </ol>

<p><b>Expired User</b></p>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu”. When it’s selected and the user’s “Expiry Date” overdue one “EXPIRED ”message will be recorded on the Access Log ”screen. If the event handle level is equaled to or higher than the“ Alarm Trigger Level, the relay will be triggered and an E-mail will sent to an email account which has been pre-configured.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</li> </ol>
<p><b>Anti Pass Back Violation</b></p>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu”. When it’s selected and the doors with “Anti Pass Back Level ”configuration, one “Anti_PB Rej ”message will be recorded on the Access Log ”screen. If the event handle level is equaled to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and an alert E-mail will be alert to an account which has been pre-configured.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0. * Only 1 Door (2 way) is supported</li> </ol>
<p><b>Door open too long</b></p>	<ol style="list-style-type: none"> <li>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’s card flashed, one “Open too long ”message will be recorded on the Access Log ”screen. If the event handle level is equaled to or higher than the“ Alarm Trigger Level”, the Relay will be triggered and an alert E-mail will be alert to an account which has been pre-configured.</li> <li>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.</li> </ol>
<p><b>Tamper Switch Breakdown</b></p>	<ol style="list-style-type: none"> <li>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. if the event level equals 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.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 0.</li> </ol>

<b>Door Intruded</b>	<ol style="list-style-type: none"> <li>1. It will be listed in the “Drop Down Menu”. When it’s selected and the door is accessed forcibly and abnormally, one “ DOOR INTRUDED ” message will be shown on the Access Log ”screen ; if the event level equals 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.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 4.</li> </ol>
<b>Duress Alarm On</b>	<ol style="list-style-type: none"> <li>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” then press “ENT ”before flashing users card) then an “ANTI DURESS” message will be shown on the Access Log ”screen; if the event level equals 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.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 4.</li> </ol>
<b>Fire Alarm On</b>	<ol style="list-style-type: none"> <li>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 shown on the Access Log ”screen; if the event level equals 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.</li> <li>2. When the “Latched Time : 0”, the alert can only be stopped by clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function, default level = 5.</li> </ol>
<b>Latched Time</b>	The “Latched Time” can be set up to 65535 seconds. When the “Latched Time : 0”, means the latched status will never be restored until the alert be stopped by manually clicking “ Alarm OFF ”button on the “Door Status Monitoring/Security Bypass” screen of “Remote Control” function.
<b>Hard Alarm</b>	Set up event handle type for MX60 I/O relay trigger
<b>Soft Alarm 1</b>	BF-50 relay 2 will be triggered by certain event types that configured to the system
<b>Soft Alarm 2</b>	BF-50 relay 3 will be triggered by certain event types that configured to system
<b>E-Mail Alarm</b>	Select event types to trigger email alert
<b>IP Camera</b>	Select event types to trigger IP Camera to take photo

▶ E-mail Alarm	
<b>Device Name</b>	Enter the device name for alarming.
<b>SMTP Mail Server</b>	Enter the Mail Server address of sending Alarm E-mail.
<b>Mail from</b>	Enter location of senders email
<b>SMTP Server Identification</b>	Set mail server User id and Password
<b>Alarm to 1st E-mail Address</b>	Enter the 1st one Alarm E-mail address.
<b>Carbon copy to E-mail Address</b>	Enter the 2nd one Alarm E-mail address.
<b>“Set”( button )</b>	Save the configured information.

# Tools

## IP Camera

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

IP Camera(IP)	PORT	TYPE	username (30 Char. Max)	password (30 Char. Max)
<input type="text" value="192.168.3.97"/>	<input type="text" value="80"/>	<input type="text" value="VIVOTEK IP7133/7330"/>	<input type="text"/>	<input type="text"/>
		<input type="button" value="SET"/>	<input type="button" value="Refresh"/>	

Door IN

Chiyu,UID=1,05/31/2011,15:05:43



【IP Camera】 – Picture22

## Illustration IP Camera :

▶ IP Camera	
<b>IP Camera</b>	Enter the IP address of IP Camera to be lined.
<b>PORT</b>	Enter the PORT IP Camera number, default is 80
<b>Type</b>	Select Enter IP Camera Type , with VIVOTEK IP7133/7330/7131 and ACTi TCM/ACM series , SoftWell WE1612H can select , default VIVOTEK IP7133/7330
<b>ID</b>	Enter IP Camera Logon
<b>Password</b>	Enter IP Camera Password
<b>Door</b>	Display Picture entrances and exits latest sensor
<b>Set(Button)</b>	Save all the configurations.
<b>Refresh(Button)</b>	Refresh the WEB page of IP Camera.

# BACKUP

Select "Backup" on the Main Window, you'll see the "Backup System" screen as below:

## 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

【BACKUP】 — Picture23

## Illustration of Backup :

▶ Backup	
<b>Database (database.cfg)</b>	Backup Project Terminal Setup, Password Setup, Time Set, Time Zone Setup Group List, Holiday Setup, Dorr Setup.
<b>User Data(userdata.cfg)</b>	Backup Project User ID, Card No, Name, Expire Date Check, Status, User Type, Group, Bypass TZ Level, Personal Password.
<b>User List (userlist.txt)</b>	Backup Project User ID, Card No, Name, User Type, Group.

※UserData.cfg 、 UserList.txt two different backup

# RESTORE

Select "Restore" on the Main Window, you'll see the "Restore System" 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.)

【Restore】 – Picture24

## Illustration Restore :

▶ Restore	
<b>Database (database.cfg)</b>	Restore Project Terminal Setup, Password Setup, Time Set, Time Zone Setup Group List, Holiday Setup, Dorr Setup.
<b>User Data(userdata.cfg)</b>	Restore Project User ID, Card No, Name, Expire Date Check, Status, User Type, Group, Bypass TZ Level, Personal Password.
<b>User List (userlist.txt)</b>	Restore Project User ID, Card No, Name, User Type, Group.

※UserData.cfg and UserList.txt are two different backup mode

# Reboot

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

## Reboot System

REBOOT

【Reboot】 -25

## Illustration of Reboot :

### ▶ Button

<b>Reboot</b>	Reboot the MX60, similar to warm start a computer
---------------	---

## Upgrade Firmware

Select “Upgrade Firmware” on the Main Window, you’ll see the “Firmware Upgrade” screen as below:

### FIRMWAVE UPGRADE

**Warning: Upgrade must NOT be interrupted**

Please select a file to upgrade :

【Firmware Upgrade】 — Picture26

## Illustration of Upgrade Firmware :

### ▶ Steps

Press Button “BROWSE” to search your Firmware to be Upgraded.  
Press Button “Upgrade” to execute the Firmware Upgrade.

### ▶ Note

Please Upgrade the “System Code” First then Upgrade “WEB Code”.

# Reset

Select “Reset” on the Main Window, you’ll see the “Reset” screen as below:

## Reset All

---

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

---

**Reset System to Factory Default** -

---

【Reset】 – Picture27

## Illustration of Reset :

▶ Data Reset	
<b>User Data</b>	Tick the box before “User Data” and Click “DELETE” to delete all the User Data.
<b>Access Log</b>	Tick the box before “Access Log” and Click “DELETE” to delete all the Access Logs.
<b>Group</b>	Tick the box before “Group” and Click “DELETE” to delete all the Group.
<b>Time Zone</b>	Tick the box before “Time Zone” and Click “DELETE” to delete all the Time Zone.
<b>Time Set</b>	Tick the box before “Time Set” and Click “DELETE” to delete all the Time Set.
<b>Holiday</b>	Tick the box before “Holiday” and Click “DELETE” to delete all the Holiday
<b>System Logs</b>	Tick the box before “System Logs” and Click “DELETE” to delete all the System Logs
▶ Button	
<b>SELECT ALL</b>	Tick the box to select all boxes in a time
<b>DELETE</b>	Delete ticked item(s)
<b>Steps :</b>	
1. Tick the item(s) to be deleted.	
2. Click button “DELETE”.	
▶ Reset System to Factory Default	
<b>Factory Default</b>	Execute command to restore the system to the factory default

## Appendix

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
Unregister	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.
Security defense	Security On(Based on software)	Apply software or scan security type card to release the security status
Security off	Security off (Based on software)	N/A
Tamper switch close	Tamper switch closed after tamper switch breakdown	N/A
Illegal time zone	Access door with card out of time zone	Check time zone for door
Lock release time zone start	Unlock time zone start	Check lock release time zone. Change the time zone to be none to release the status
Lock release time zone end	Unlock time zone end	N/A
Warm start	Tap Reboot to warm start terminal (power on status), system display with Warm start message	N/A
Cold start	Power on after power breakdown. System log displays "System power on".	N/A
Backup battery	Backup battery is being used when power off	Check power status
Normal power on	Power on after power breakdown (with backup battery)	N/A
BF50 on line	BF-50 On line	N/A
BF50 off line	BF-50 Off line	Check RS485 or BF50 status
Door sensor circuit short	Door sensor circuit short	Check door sensor circuit

Door sensor circuit open	Door sensor circuit open	Check door sensor circuit
Password invalid	Password error when user input	Check password
Emergency open	Tap Emergency open button remotely	Tap All door then click Back to normal
Emergency close	Tap Emergency close button remotely	Tap all door then click Back to normal
Fire alarm detection on	Fire alarm detection is activated from remote site	N/A
Fire alarm detection off	Fire alarm detection off from remote site	N/A
Force open	Tap Force open button from remote site	N/A
Manually alarm release	Alarm relay is triggered when a certain event tolerance time set to "0". Alarm relay will be off when Alarm off is selected.	N/A
Auto alarm off	Event trigger tolerance time set to other than "0", alarm relay will be triggered.	N/A
IP Conflict	IP confliction over two terminals	Modify IP for one terminal
Keypad invalid	System allows password to be input for 3 times or keypad will be blocked	Check password
Keypad valid	Keypad will be valid again when 30 seconds	N/A
MX60 on line	SEMAC detected a connection of MX60	N/A
MX60 off line	SEMAC detected disconnection of MX60	Check network status or a Sub-controller mode has granted