

Defender Smart Alarm Webserver (DSAW)

A device that allow user to check the home status and control the alarm system functionality though a webpage via Ethernet.

1.0 Hardware – Default Factory Setting

MAC Address	- C8:1E:8E:00:00:00
IP Address	- 169.254.1.1
Gateway	- 169.254.1.1
Subnet Mask	- 255.255.0.0
Primary DNS	- 169.254.1.1
Secondary DNS	- 0.0.0.0
Port	- 8088

2.0 Communication between DSAW and home user Router

- Home user Router will automatically assign a Dynamic IP address to DSAW (figure 2.0). Example: TP-LINK ROUTER (TD-W8901G) with DSAW.

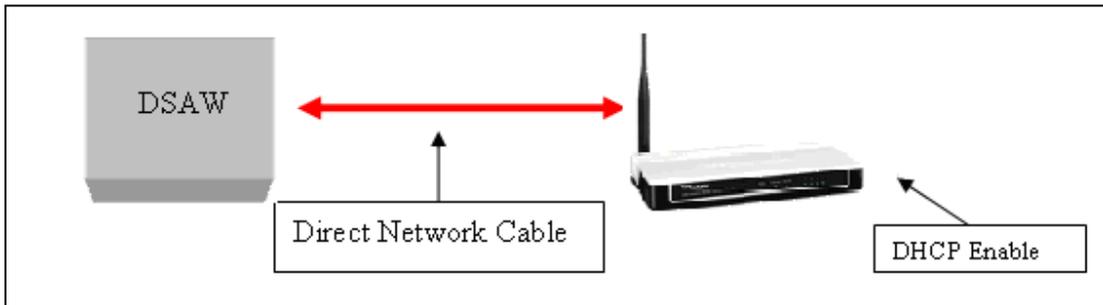


Figure 1.0 Connection between DSAW and Router

TP-LINK®

DHCP IP Pool Summary

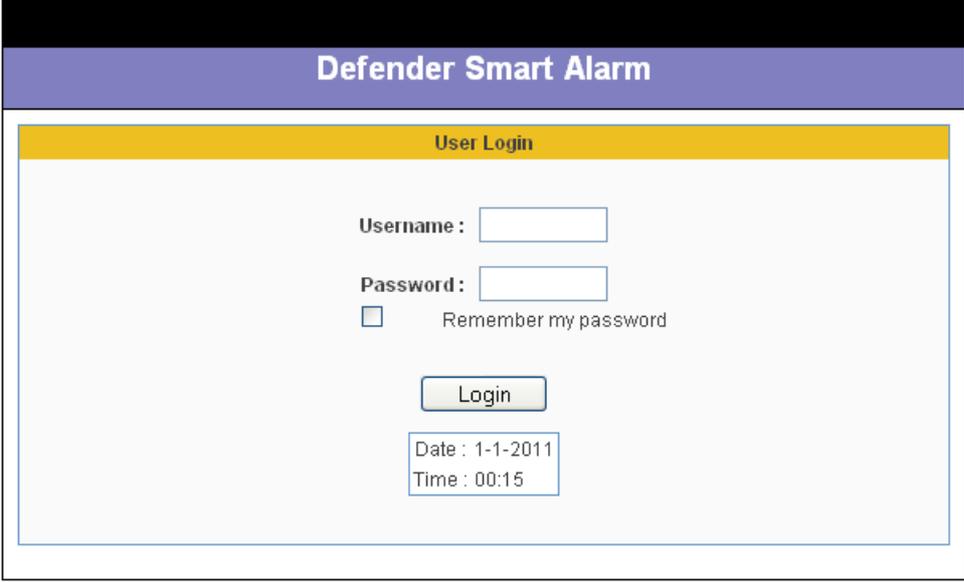
Host Name	IP Address	MAC Address	Expire Time
oem-adc4936ff0a	192.168.1.2	C8-1E-8E-00-00-47	2days, 23:58:45
oem-adc4936ff0a	192.168.1.3	00-E0-4C-77-36-54	2days, 23:53:42

Assign by router

DSA Mac Address

Figure 2.0: DSAW's IP address assigned by TP-link router as 192.168.1.2

- b. Open the browser login to DSAW. Key in <http://defender:8088>. Login page will show as below (Figure 3.0).



The screenshot shows a web browser window displaying the login page for 'Defender Smart Alarm'. The page has a purple header with the text 'Defender Smart Alarm'. Below this is a yellow sub-header with the text 'User Login'. The main content area is white and contains the following elements: a 'Username:' label followed by a text input field; a 'Password:' label followed by a text input field; a checkbox labeled 'Remember my password'; a 'Login' button; and a status box showing 'Date: 1-1-2011' and 'Time: 00:15'.

Figure 3.0 Login Page

3.0 Register for Username

- a. To register username, please enter the IP address as <http://defender:8088/protect/register.htm>. Figure 3.1.

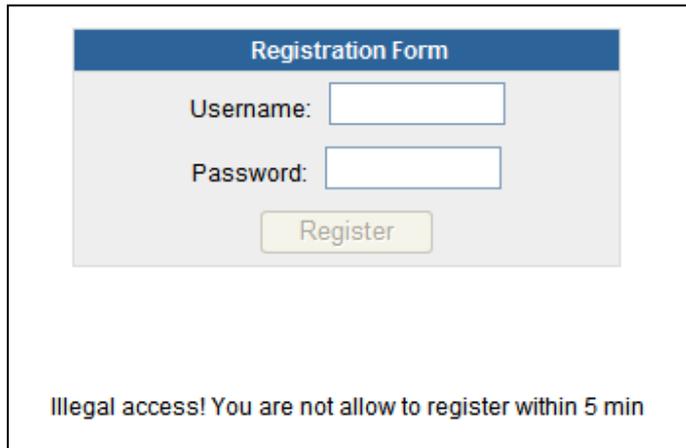


The screenshot shows a web browser window displaying the registration form. The form has a blue header with the text 'Registration Form'. Below the header, there are the following elements: a 'Username:' label followed by a text input field; a 'Password:' label followed by a text input field; and a 'Register' button.

Figure 3.1

- b. Username has to register with **8 characters**.
- c. Username can be register as alphanumeric with uppercase or lowercase.
- d. Password has to same as alarm panel's master password to register.

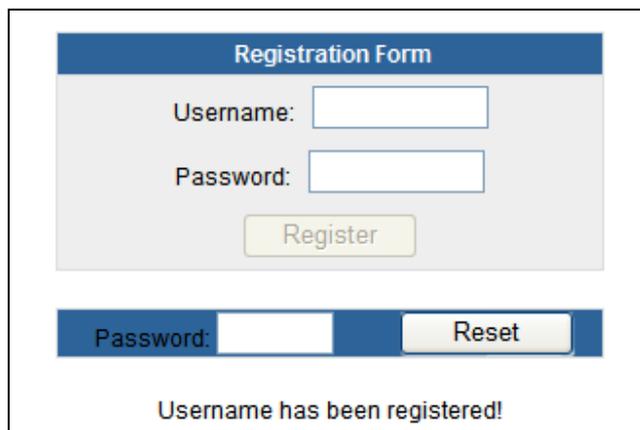
- e. If 5 times wrong password to register, it will no allow registering within 5 minutes (figure 3.2).



The image shows a web form titled "Registration Form" with a blue header. It contains two input fields: "Username:" and "Password:". Below the fields is a yellow "Register" button. At the bottom of the form area, there is a red error message: "Illegal access! You are not allow to register within 5 min".

Figure 3.2

- f. After successfully registered username, it will automatically link to login page (figure 3.0).
- g. If users forget the username, users might register again the username in the same web page. (<http://defender:8088/protect/register.htm>)
- h. If the username has been registered before, below the Registration Form table will appear another new table which is reset username table (figure 3.3).



The image shows the same "Registration Form" as in Figure 3.2. Below the registration form, there is a new section with a blue header. It contains a "Password:" label, an input field, and a yellow "Reset" button. At the bottom of this section, there is a green message: "Username has been registered!".

Figure 3.3

- i. The password to reset the username same as alarm panel's master password.
- j. If wrong password key in, it will immediately stop to reset the username within 5 minutes.

- k. If key in the correct password, the reset username table will disappear and the Registration Form table will enable to register new username (figure 3.1).
- l. After successfully registered username, it will automatically link to login page (figure 3.0).

4.0 8 zones alarm panel status

- a. The status of 8 zones home alarm panel status will shown as below after login (figure 4.0).

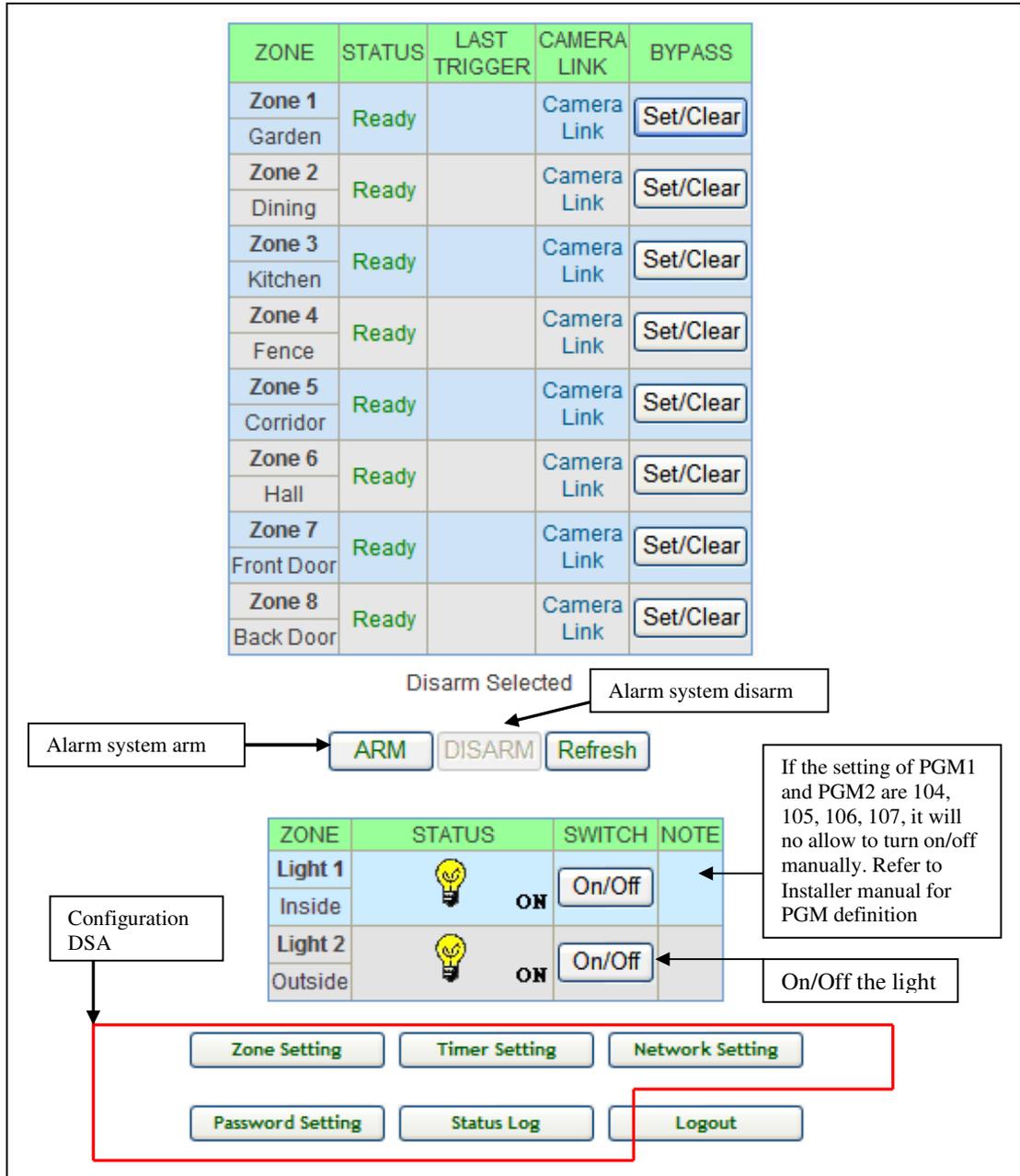


Figure 4.0 Defender 8 zone alarm panel status

- b. Refer to figure 4.0.
- Status – condition for each zone in Arm, Trigger, Ready, Open or Bypass status.
 - Last Trigger – indicate which zone was triggered after disarm.
 - Camera Link – IP camera link for each zone.
 - Bypass – indicate which zones have been bypass.
- c. Functionality of DSAW.
- ARM – to arm the alarm system
 - DISARM – to disarm the alarm system
 - BYPASS – to set or clear the zone bypass
- d. Configuration of DSAW (only master authenticate)
- Zone Setting – to define zone location and IP Camera Link for each zone.
 - Timer Setting – auto arm or disarm the alarm system and auto turn on or off the light follow timer (24 hour format).
 - Network Setting – Configure DSAW's network setting in Dynamic (IP address assign by router) or Static (IP address assign by user) and Port number.
 - Password Setting – change the user's login password (only 4 digits acceptable).
 - Status Log – to indicate who and what activities done on DSAW.
 - Logout – logout the DSAW.

4.1 Configuration DSAW

a. Zone setting (figure 4.1)

- Location – name the location for each zone (max 10 characters).
- Camera Link – IP camera web link for each zone (max 40 characters).

The screenshot displays the 'Defender Alarm Board Configuration' interface. It is divided into two main sections: 'Alarm Sensor Zone' and 'Alarm Light Zone'. The 'Alarm Sensor Zone' section contains a table with 8 rows, each representing a zone with its location and camera link. The 'Alarm Light Zone' section contains a table with 2 rows, representing light zones and their locations. At the bottom of the interface are 'save' and 'cancel' buttons.

ZONE	LOCATION	CAMERA LINK
ZONE 1	Garden	http://www.zonelink1.com.my
ZONE 2	Dining	http://www.zonelink2.com.my
ZONE 3	Kitchen	http://www.zonelink3.com.my
ZONE 4	Fence	http://www.zonelink4.com.my
ZONE 5	Corridor	http://www.zonelink5.com.my
ZONE 6	Hall	http://www.zonelink6.com.my
ZONE 7	Front Door	http://www.zonelink7.com.my
ZONE 8	Back Door	http://www.zonelink8.com.my

LIGHT ZONE	LOCATION
ZONE 1	Inside
ZONE 2	Outside

save

cancel

Figure 4.1 Zone setting

b. Timer setting (figure 4.2)

- Arm/Disarm Timer – set the time to auto arm or disarm the partition 1 or partition 2 of alarm systems (24 hour format).
- Lighting Timer – set the time to auto turn on or off light (24 hour format). If PGM settings are not 064, 065, or 066 (follow timer), the feature of auto timer function will disable. Refer to installer manual for PGM definition.

Defender Alarm Board Configuration

Arm/Disarm Timer

	ARM	DISARM	ENABLE
Partition 1	07 : 00	10 : 00	<input type="button" value="Set"/>
	ARM	DISARM	ENABLE
Partition 2	18 : 00	21 : 00	<input type="button" value="Set"/>

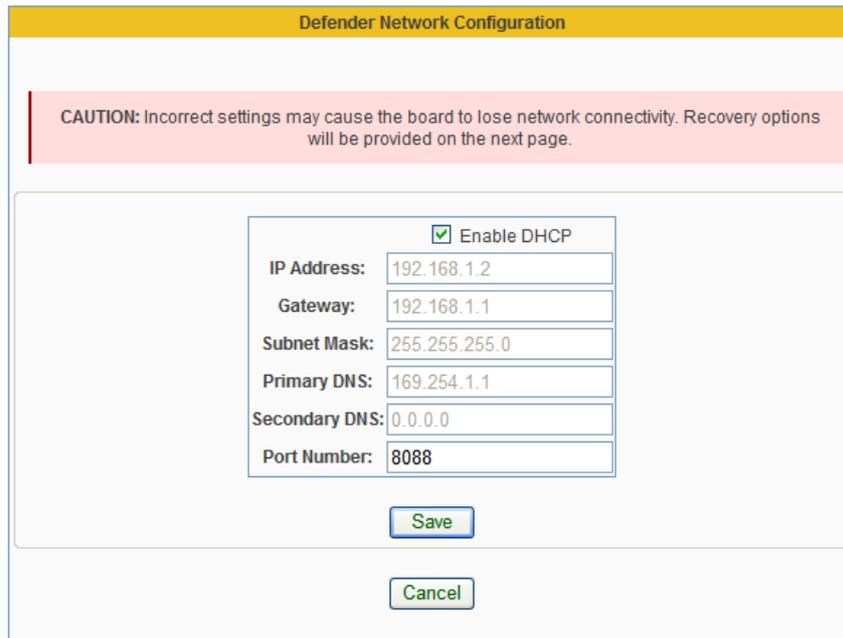
Lighting Timer

24 Hr Format	Light 1	Light 2	Note
Timer 1			To use the auto timer please perform PGM setting
On 18 : 00	X	X	
Off 06 : 30			
Timer 2			
On 19 : 00	X	X	
Off 07 : 00			

Figure 4.2 Timer setting

c. Network setting (figure 4.3)

- For Dynamic DHCP, tick the Enable DHCP. Default is DHCP enable and the port number is 8088.
- For Static refer to step 6.0 for more detail.

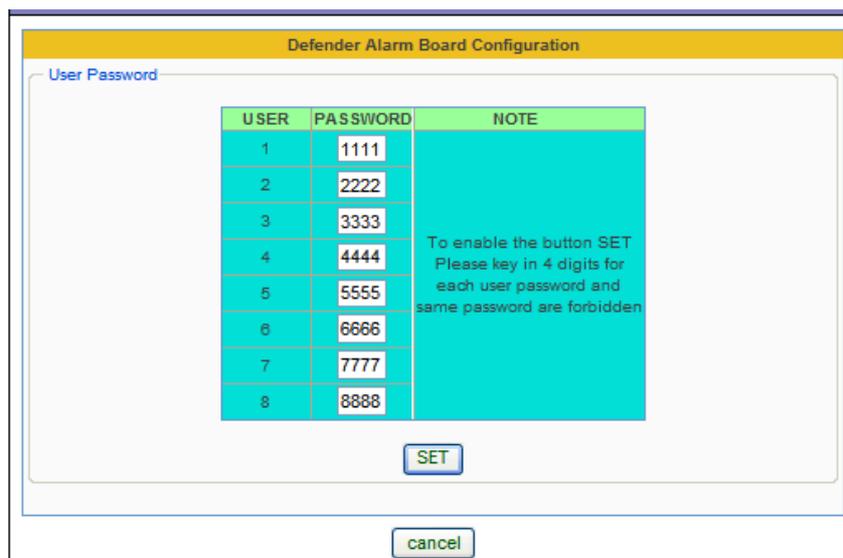


The image shows a web interface titled "Defender Network Configuration". At the top, there is a yellow header bar. Below it, a red warning box contains the text: "CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page." The main configuration area is a white box with a blue border. It contains a form with the following fields: "Enable DHCP" (checked), "IP Address: 192.168.1.2", "Gateway: 192.168.1.1", "Subnet Mask: 255.255.255.0", "Primary DNS: 169.254.1.1", "Secondary DNS: 0.0.0.0", and "Port Number: 8088". Below the form are "Save" and "Cancel" buttons.

Figure 4.3 Network Setting

d. Password Setting (figure 4.4)

- Maximum 4 digits numeric



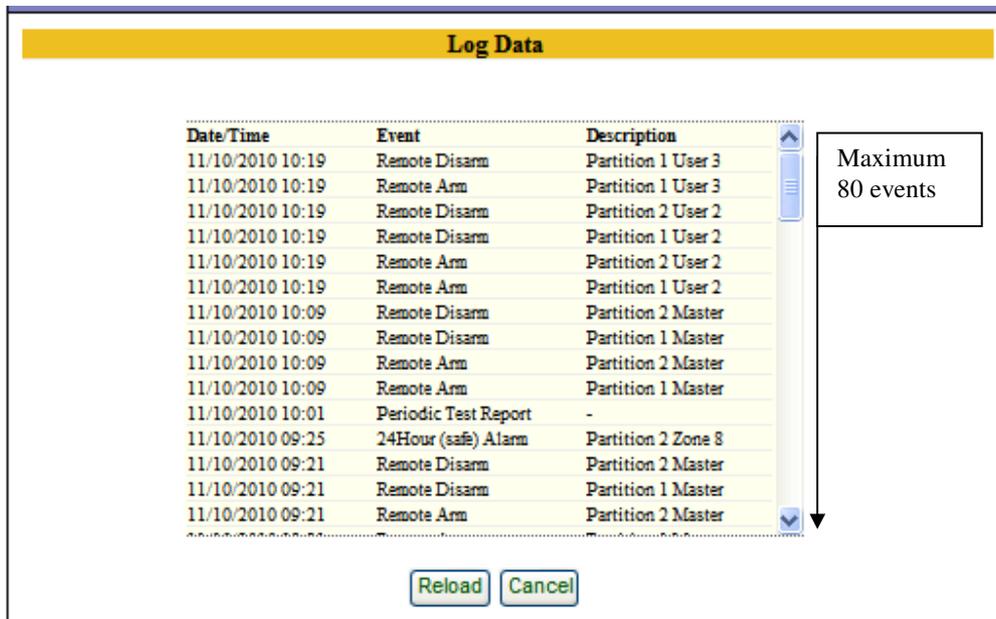
The image shows a web interface titled "Defender Alarm Board Configuration". It features a "User Password" section with a table of user accounts. The table has three columns: "USER", "PASSWORD", and "NOTE". The "NOTE" column contains a message: "To enable the button SET Please key in 4 digits for each user password and same password are forbidden". Below the table are "SET" and "cancel" buttons.

USER	PASSWORD	NOTE
1	1111	To enable the button SET Please key in 4 digits for each user password and same password are forbidden
2	2222	
3	3333	
4	4444	
5	5555	
6	6666	
7	7777	
8	8888	

Figure 4.4 Password Setting

e. Status Log (Figure 4.5)

- Reload button - for reload the latest information. Maximum show 80 events, after 80 events, the next events will show at first location.



The screenshot shows a window titled "Log Data" with a table of events. The table has three columns: "Date/Time", "Event", and "Description". The events listed are:

Date/Time	Event	Description
11/10/2010 10:19	Remote Disarm	Partition 1 User 3
11/10/2010 10:19	Remote Arm	Partition 1 User 3
11/10/2010 10:19	Remote Disarm	Partition 2 User 2
11/10/2010 10:19	Remote Disarm	Partition 1 User 2
11/10/2010 10:19	Remote Arm	Partition 2 User 2
11/10/2010 10:19	Remote Arm	Partition 1 User 2
11/10/2010 10:09	Remote Disarm	Partition 2 Master
11/10/2010 10:09	Remote Disarm	Partition 1 Master
11/10/2010 10:09	Remote Arm	Partition 2 Master
11/10/2010 10:09	Remote Arm	Partition 1 Master
11/10/2010 10:01	Periodic Test Report	-
11/10/2010 09:25	24Hour (safe) Alarm	Partition 2 Zone 8
11/10/2010 09:21	Remote Disarm	Partition 2 Master
11/10/2010 09:21	Remote Disarm	Partition 1 Master
11/10/2010 09:21	Remote Arm	Partition 2 Master

Below the table are two buttons: "Reload" and "Cancel". A callout box on the right side of the table indicates "Maximum 80 events".

Figure 4.5 Status Log

5.0 20 zones alarm panel status (figure 5.0)

ZONE	STATUS	LAST TRIGGER	CAMERA LINK	BYPASS
Zone 1	Ready			Set/Clear
Zone 2	Ready			Set/Clear
Zone 3	Ready			Set/Clear
Zone 4	Ready			Set/Clear
Zone 5	Ready			Set/Clear
Zone 6	Ready			Set/Clear
Zone 7	Ready			Set/Clear
Zone 8	Ready			Set/Clear
Zone 9	Ready			Set/Clear
Zone 10	Ready			Set/Clear
Zone 11	Ready			Set/Clear
Zone 12	Ready			Set/Clear
Zone 13	Ready			Set/Clear
Zone 14	Ready			Set/Clear
Zone 15	Ready			Set/Clear
Zone 16	Ready			Set/Clear
Zone 17	Ready			Set/Clear
Zone 18	Ready			Set/Clear
Zone 19	Ready			Set/Clear
Zone Auto Gate	Ready			Reset
Panic Alarm	Ready			Reset

Alarm system disarm

Alarm system arm

Arm

Disarm

Refresh

Alarm system disarm

ZONE	STATUS	SWITCH	NOTE
Light 1	OFF	On/Off	
Light 2	OFF	On/Off	
Light 3	OFF	On/Off	
Light 4	OFF	On/Off	
Light 5	OFF	On/Off	

If the setting of PGM1, PGM2, PGM3, PGM4 and PGM5 are 130, 131, 132, 133, it will no allow to turn on/off manually. Refer to Installer manual for PGM definition

On/Off the light

Zone Setting

Timer Setting

Network Setting

Password Setting

Status Log

Logout

Figure 5.0 Defender 20 zone alarm panel status

- a. Refer to figure 5.0.
- Zone Auto Gate
 - Zone 20 was used to detect auto gate status. If auto gate no close within 1 min, the keypad / touchpad will beep. Figure 5.0.1 show the zone auto gate status open.
 - If users no close the auto gate or key in master password within 5 min, alarm panel will phone call out to users.
 - Users might switch off the alarm system phone call out and keypad / touchpad beep by press the Reset button through DSAW or phone.
 - Panic Alarm
 - To indicate the Panic status triggered by keypad / touchpad or remote control.
 - Users might switch off panic triggered by press the Reset button through DSAW or phone.

Zone Auto Gate	Open	Reset
Panic Alarm	Triggered	Reset

Figure 5.0.1

5.1 Configuration DSAW

- a. Refer to figure 5.0, for Zone Setting, Network Setting, Password Setting, Status Log and Logout features please refer to 4.1.a, 4.1.c, 4.1.d, 4.1.e and 4.1.f.
- b. Timer Setting (Figure 5.1).
- Arm/Disarm Timer – set the time to auto arm or disarm the partition 1 or partition 2 of alarm systems (24 hour format).
 - Lighting Timer
 - Set the time to auto turn on or off light (24 hour format). If PGM settings are not 080, 081, 082, 083, or 084 (follow timer), the feature of auto timer function will disable. Refer to installer manual for PGM definition.
 - Night Mode Begin Time and Night Mode End Time features are auto turn on the light during night mode begin time and auto turn off during night mode end time.

Defender Alarm Board Configuration

Arm/Disarm Timer

24 HR FORMAT	ARM	DISARM	ENABLE
Partition 1	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="button" value="Set"/>
Partition 2	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	<input type="button" value="Set"/>

Lighting Timer

Night Mode Begin Time : 99:99

Night Mode End Time : 99:99

24 HR FORMAT	ON	OFF	NOTE
Light 1 timer	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	To use the auto timer please perform PGM setting using keypad
Light 2 timer	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Light 3 timer	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Light 4 timer	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	
Light 5 timer	<input type="text"/> : <input type="text"/>	<input type="text"/> : <input type="text"/>	

Figure 5.1 Timer setting

6.0 Instruction to configure DSAW as Static IP

- a. Default DSAW's network setting assigned to DHCP.
- b. Refer to figure 2.0, the DSAW's IP address was assigned by router as 192.168.1.2 in Dynamic DHCP. If users want to assign DSAW as static IP address, please follow below instructions:
 - i. Go to Network Setting, un-tick the ENABLE DHCP and assigned a new IP address (for example: 192.168.1.10) then click Save.

Defender Smart Alarm

Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page.

Un-tick the Enable DHCP

Enable DHCP

Update new IP address

IP Address: 192.168.1.10

Gateway: 192.168.1.1

Subnet Mask: 255.255.255.0

Primary DNS: 169.254.1.1

Secondary DNS: 0.0.0.0

Port Number: 8088

Save

Cancel

Figure 6.0 Network Setting

- ii. The Reboot message was shown in the browser (figure 6.1).

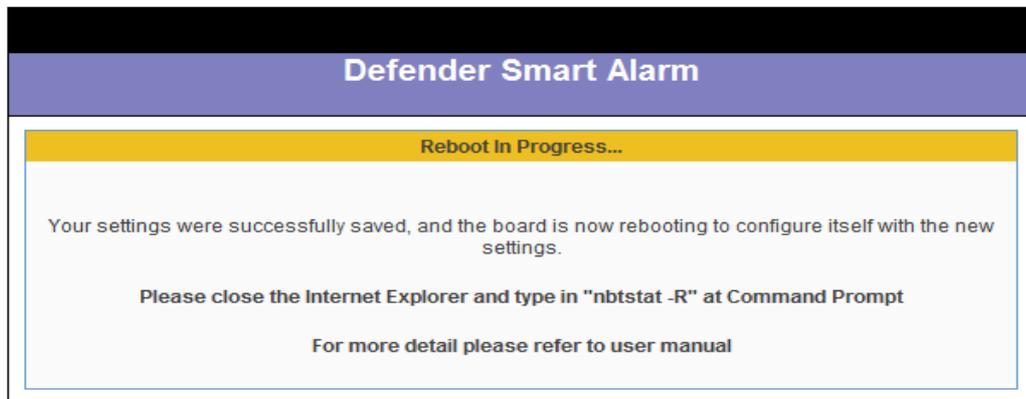


Figure 6.1 Reboot message

- iii. Follow the reboot message, close the browser and open the command prompt. If users used window vista or window 7 (latest OS), please open the command prompt as “**run as administrator**”.
- iv. Key in “**nbtstat -R**” command. “Successful purge and preload of the NBT Remote Cache Name Table” message was shown at figure 6.2.
- v. Key in “**ping defender**” command to ping DSAW. A successfully reply message was shown at figure 6.2 with new Static IP address (192.168.1.10).

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\USER>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.

C:\Documents and Settings\USER>ping defender

Pinging defender [192.168.1.10] with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time=2ms TTL=100
Reply from 192.168.1.10: bytes=32 time=1ms TTL=100
Reply from 192.168.1.10: bytes=32 time=1ms TTL=100
Reply from 192.168.1.10: bytes=32 time=1ms TTL=100

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Documents and Settings\USER>_
```

Figure 6.2 Command Prompt

- vi. DSAW have been successfully configured to static IP address. Open the browser and login to DSAW by key in **http://defender:8088**. (Figure 3.0).
- vii. Go to the Network setting, the updated information was shown at figure 6.3.

Defender Smart Alarm

Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page.

Un-tick because in static

Enable DHCP

IP Address: 192.168.1.10

Gateway: 192.168.1.1

Subnet Mask: 255.255.255.0

Primary DNS: 169.254.1.1

Secondary DNS: 0.0.0.0

Port Number: 8088

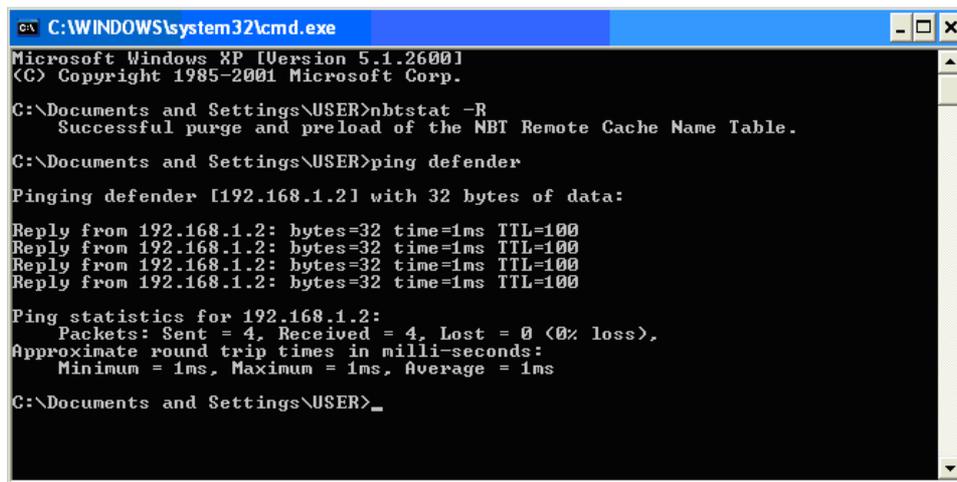
192.168.1.10 - static IP address

Save

Cancel

Figure 6.3 Network Setting

- c. If users want to change back to Dynamic DHCP after Static, just tick the ENABLE DHCP at Network configuration then save.
 - i. The Reboot message was shown in the browser (figure 6.1).
 - ii. Then followed the step 6.0.b.iii to 6.0.b.vii. Successfully result was shown at figure 6.4 and figure 6.5.



```

c:\ C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\USER>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.

C:\Documents and Settings\USER>ping defender

Pinging defender [192.168.1.2] with 32 bytes of data:

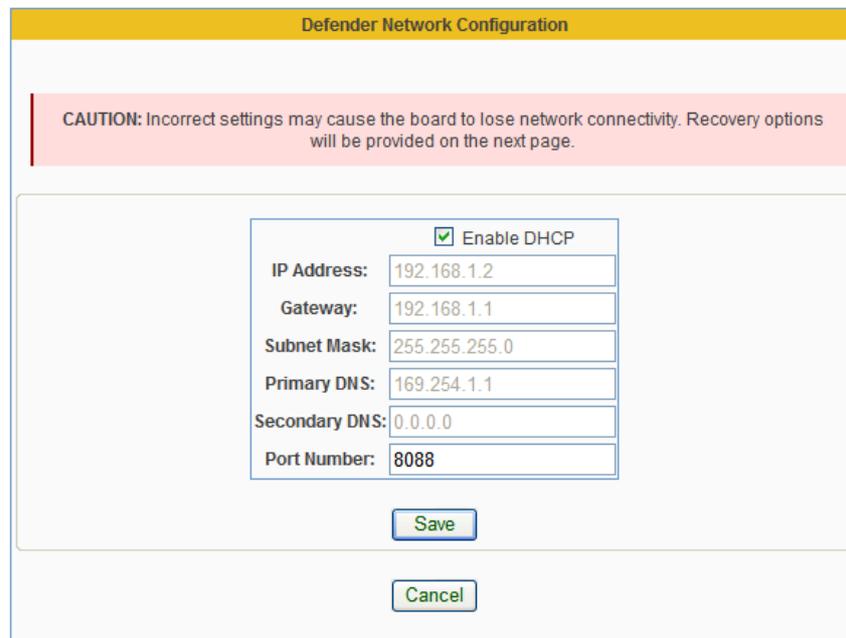
Reply from 192.168.1.2: bytes=32 time=1ms TTL=100

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\USER>_

```

Figure 6.4 Command Prompt



Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page.

<input checked="" type="checkbox"/> Enable DHCP
IP Address: 192.168.1.2
Gateway: 192.168.1.1
Subnet Mask: 255.255.255.0
Primary DNS: 169.254.1.1
Secondary DNS: 0.0.0.0
Port Number: 8088

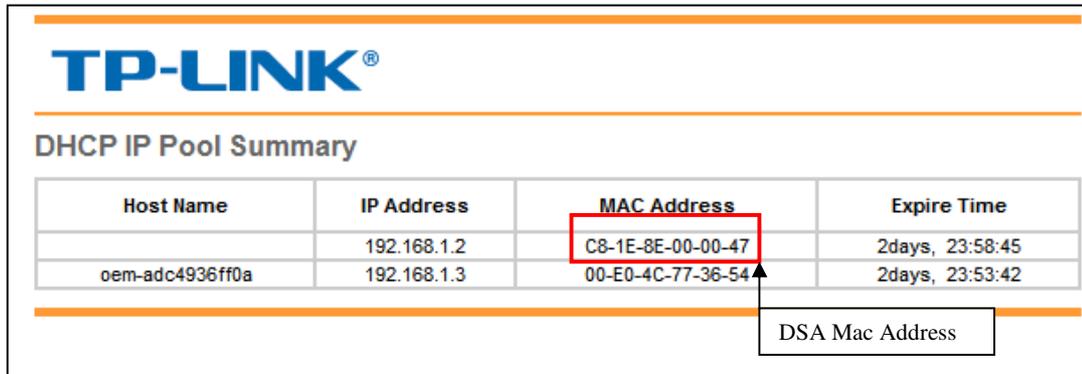
Save

Cancel

Figure 6.5 Network Setting

7.0 Configuration DSAW's Mac Address

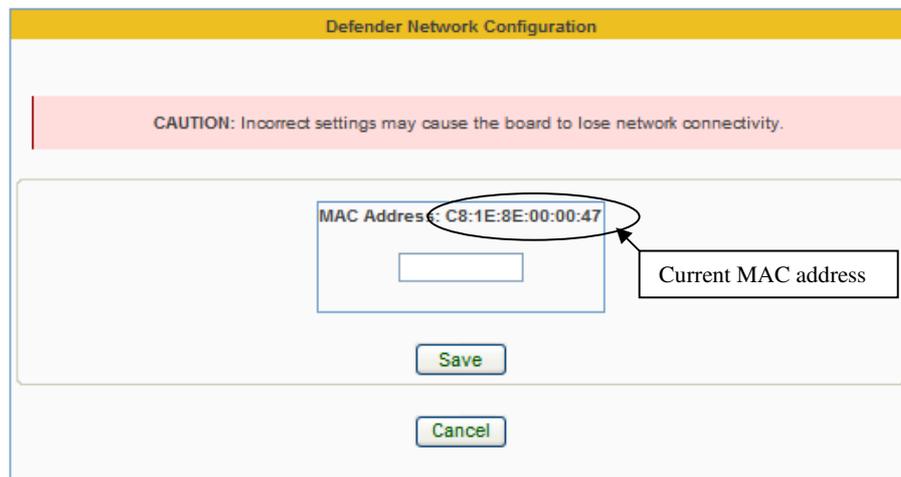
- a. MAC address of DSAW was shown at Router's DHCP table after connected (figure 7.0). For this example, DSAW's IP address assigned as **192.168.1.2** with MAC address **C8:1E:8E:00:00:47**.



Host Name	IP Address	MAC Address	Expire Time
	192.168.1.2	C8-1E-8E-00-00-47	2days, 23:58:45
oem-adc4936ff0a	192.168.1.3	00-E0-4C-77-36-54	2days, 23:53:42

Figure 7.0 DHCP Table

- b. To update the new MAC address, open the browser and key in "<http://defender:8088/protect/mac.htm>". MAC address web page was shown at figure 7.1. The numbers of MAC address only acceptable in numeric and the range from 0 to 16777215 (FF: FF: FF).



Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity.

MAC Address: C8:1E:8E:00:00:47

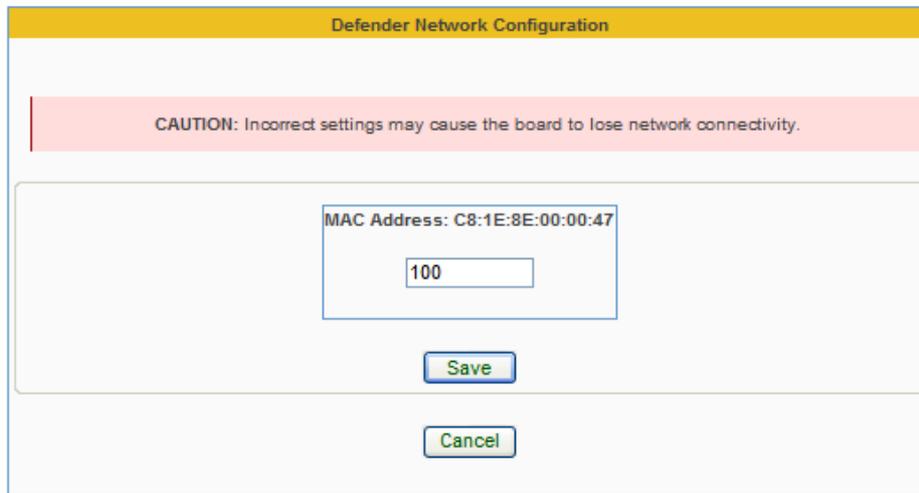
Current MAC address

Save

Cancel

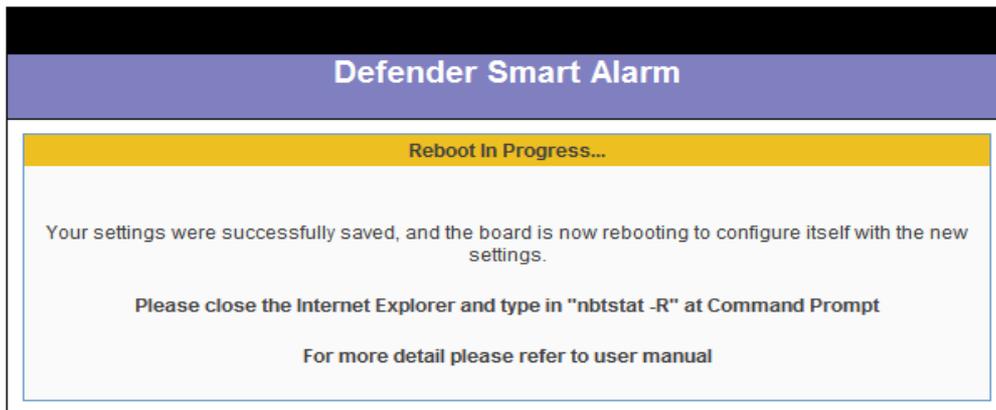
Figure 7.1 MAC Address Setting

- c. For this example, value 100 was saving to update the MAC address (figure 7.2). A reboot message was shown at figure 7.3 after Save button was pressed.



The screenshot shows a web interface titled "Defender Network Configuration". At the top, there is a yellow header bar with the title. Below the header, a pink banner contains a caution message: "CAUTION: Incorrect settings may cause the board to lose network connectivity." The main content area is a light gray box containing a text label "MAC Address: C8:1E:8E:00:00:47" above a text input field with the value "100". Below the input field are two buttons: "Save" and "Cancel".

Figure 7.2 MAC address setting



The screenshot shows a web interface titled "Defender Smart Alarm". At the top, there is a black header bar with the title. Below the header, a yellow banner contains the text "Reboot In Progress...". The main content area is a light gray box containing the following text: "Your settings were successfully saved, and the board is now rebooting to configure itself with the new settings." Below this, it says "Please close the Internet Explorer and type in 'nbtstat -R' at Command Prompt". At the bottom, it says "For more detail please refer to user manual".

Figure 7.3 Reboot message

- i. Follow the reboot message, close the browser and open the command prompt. If users used window vista or window 7 (latest OS), please open the command prompt as "**run as administrator**".
- ii. Key in "**nbtstat -R**" command. "Successful purge and preload of the NBT Remote Cache Name Table" message was shown at figure7.4.
- iii. Key in "**ping defender**" command to ping DSAW. A successfully reply message was shown at figure 7.4 with new IP address (192.168.1.4) assigned by router according the new MAC address.

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\USER>nbtstat -R
    Successful purge and preload of the NBT Remote Cache Name Table.

C:\Documents and Settings\USER>ping defender

Pinging defender [192.168.1.4] with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=1ms TTL=100

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Documents and Settings\USER>

```

Figure 7.4 Command Prompt

- iv. DSAW have been successfully updated the new MAC address with **C8:1E:8E:00:00:64** (figure 7.5).

TP-LINK®			
DHCP IP Pool Summary			
Host Name	IP Address	MAC Address	Expire Time
	192.168.1.2	C8-1E-8E-00-00-47	2days, 23:20:58
oem-adc4938ff0a	192.168.1.3	00-E0-4C-77-38-54	2days, 22:40:52
	192.168.1.4	C8-1E-8E-00-00-64	2days, 23:55:33

Figure 7.5 Router IP Pool List

- v. Open the browser and key in **“http://defender:8088/protect/mac.htm”**, the configuration of MAC address web page was shown at figure 7.6 with new MAC address **C8:1E:8E:00:00:64**. (100 decimal = 64 hex)
- vi. Updated IP address **192.168.1.4** was shown at figure 7.7.

Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity.

MAC Address: C8:1E:8E:00:00:64

Figure 7.6 MAC address setting

Defender Smart Alarm

Defender Network Configuration

CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page.

Enable DHCP

When router detected new MAC address, the IP address automatically updated in DHCP enable

IP Address:

Gateway:

Subnet Mask:

Primary DNS:

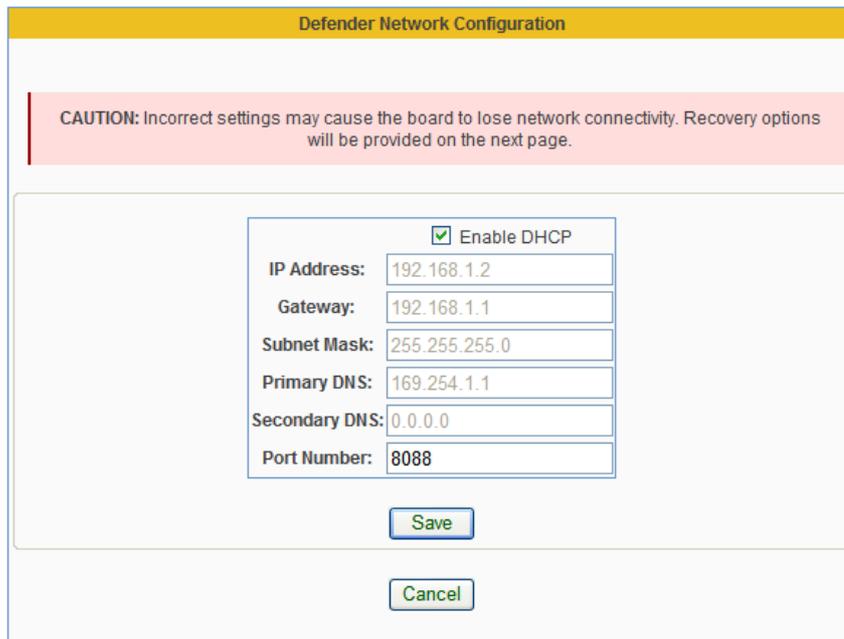
Secondary DNS:

Port Number:

Figure 7.7 Network Setting

8.0 Configuration DSAW's Port number

- a. Refer to figure 8.0, the default DSAW's port number was assigned as 8088.



The screenshot shows a window titled "Defender Network Configuration". At the top, there is a yellow header bar. Below it, a red warning box contains the text: "CAUTION: Incorrect settings may cause the board to lose network connectivity. Recovery options will be provided on the next page." The main configuration area is a light gray box containing a form with the following fields:

- Enable DHCP
- IP Address: 192.168.1.2
- Gateway: 192.168.1.1
- Subnet Mask: 255.255.255.0
- Primary DNS: 169.254.1.1
- Secondary DNS: 0.0.0.0
- Port Number: 8088

Below the form are two buttons: "Save" and "Cancel".

Figure 8.0 Network Setting

- b. To update the new port number, just key in the new port number at Port Number text box (figure 8.1). A reboot message was shown at figure 7.3 after Save button was pressed.
 - i. Follow the reboot message, close the browser and open the command prompt. If users used window vista or window 7 (latest OS), please open the command prompt as "**run as administrator**".
 - ii. Key in "**nbtstat -R**" command. "Successful purge and preload of the NBT Remote Cache Name Table" message was shown at figure 8.2.
 - iii. Key in "**ping defender**" command to ping DSAW. A successfully reply message was shown at figure 8.2.

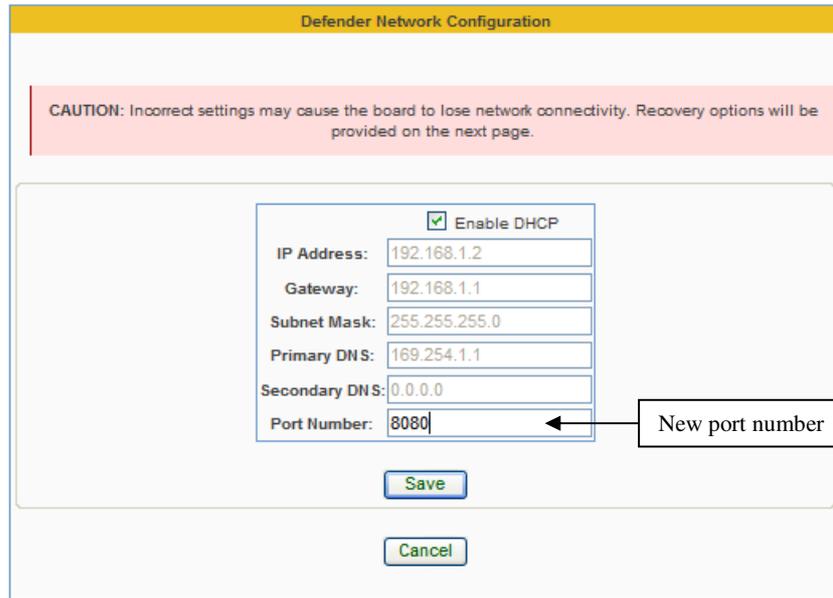


Figure 8.1 Network Setting

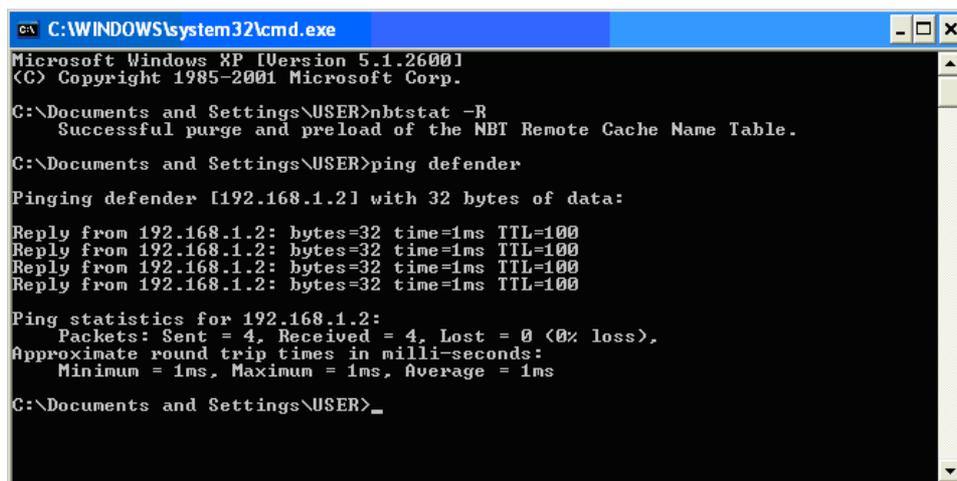


Figure 8.2 Command Prompt

- c. Open the browser and key in **http://defender:8080**. Successfully accessed the login page was shown. Refer to figure 3.0.

9.0 Default factory setting

- a. If any mistake cause the DSAW unable to connect, set to factory default setting is needed.
- b. Off the DSAW power, press the reset button and on the power, continue holding the button until the LED flash then release the button.
- c. After reset, the DSAW network setting was returned to default factory setting and the Username was reset.

10.0 Security of DSAW

- a. For security purpose, the DSAW will auto logout to login page after some time when do some instructions.
- b. If access the DSAW by illegal (without login the username and password), the information of defender smart alarm will hide or automatically return back to login page.

11.0 Hardware Connection

- a. The hardware connection for DSAW with 8 zone alarm panel (figure 11.0).

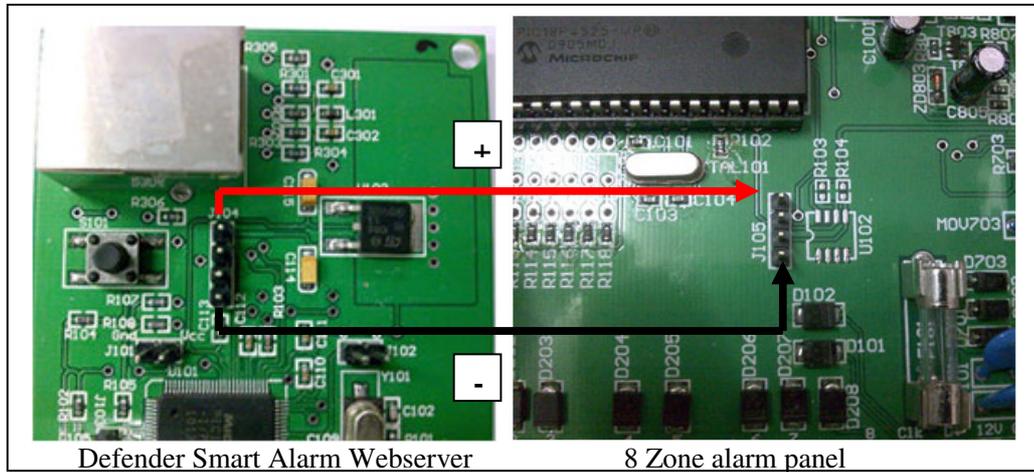


Figure 11.0 Connection between DSAW and 8 zone alarm panel

- b. The hardware connection for DSAW with 20 zone alarm panel (figure 11.1).

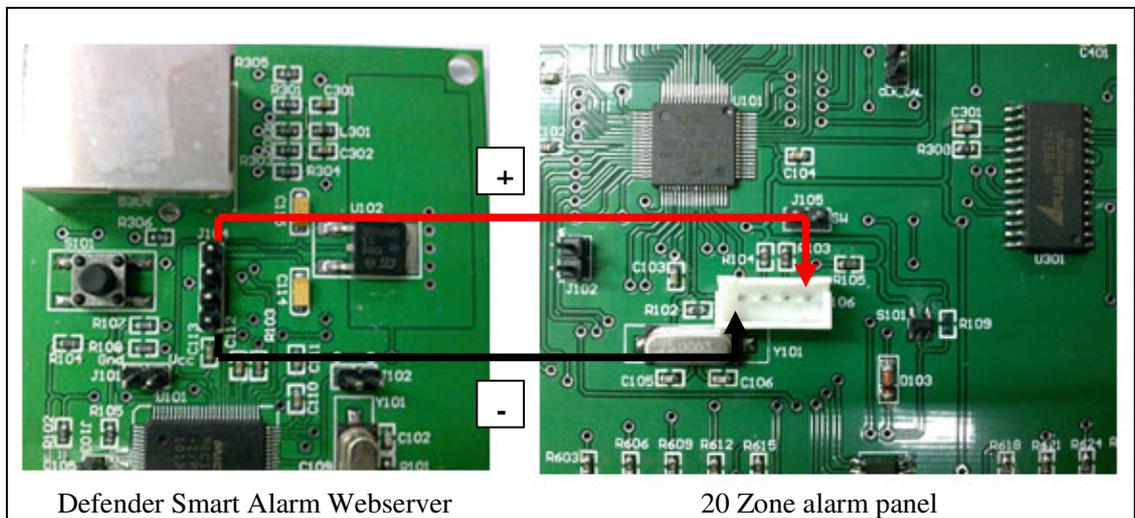
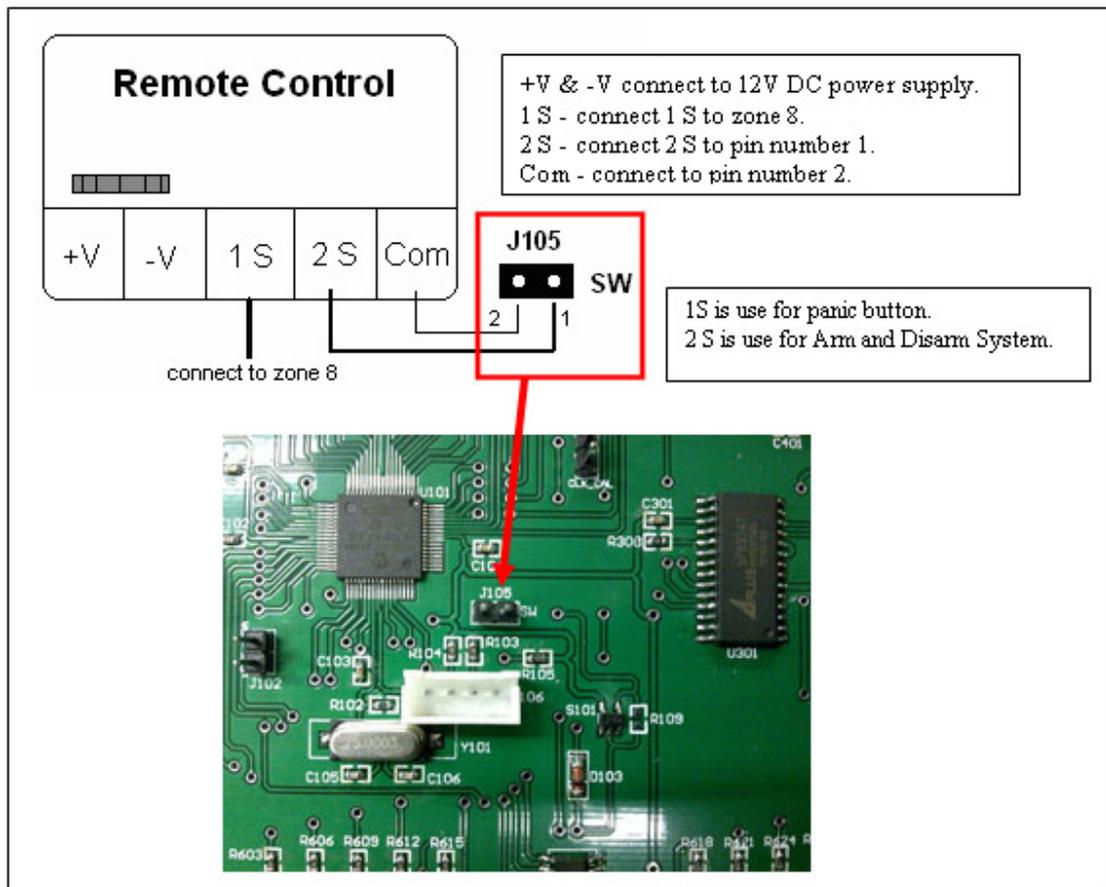


Figure 11.1 Connection between DSAW and 20 zone alarm panel

- c. The hardware connection for arm or disarm and Panic the 20 zone alarm panel by Remote control (figure 11.2).
- i. For Panic feature please follow the step below.
 1. Refer to **ZONE PROGRAMMING** table address 14, remove the zone 8 as 24 Hour zone type.
 - a. Enter Programming Menu,
[*] [0] [Installer code] [Address] [Zone] – [*] [0]
[1397] [14] [8]
 2. Go to address 17 setting, assign zone 8 as Normally Open Zone type.
 - a. Enter Programming Menu,
[*] [0] [Installer code] [Address] [Zone] – [*] [0]
[1397] [17] [8]
 3. Then go back to address 14, assign back zone 8 as 24 Hour zone type.
 - a. Enter Programming Menu,
[*] [0] [Installer code] [Address] [Zone] – [*] [0]
[1397] [14] [8]



- d. The hardware connection for vibration sensor / magnet sensor with 20 zone alarm panel (figure 11.3).

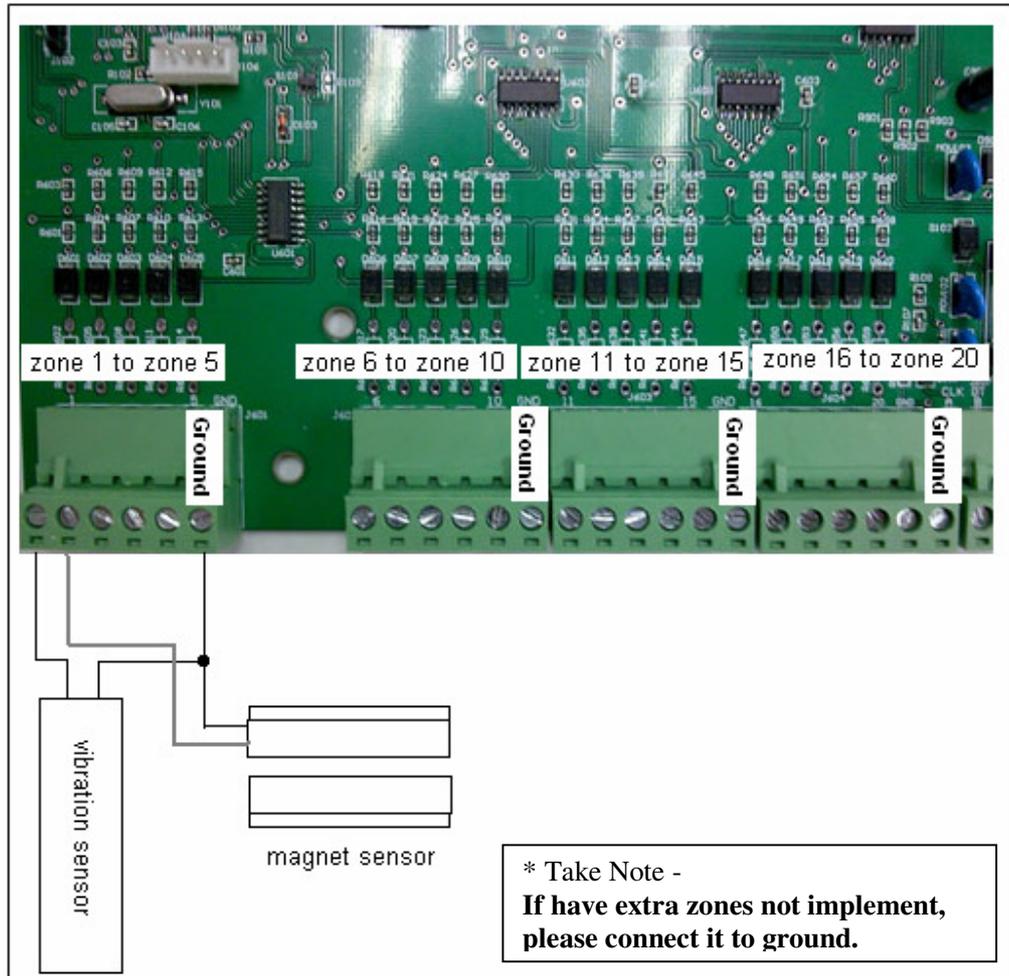


Figure 11.3 Connection between vibration / magnet sensor and 20 zone alarm panel

- e. The hardware connection for touchpad with 20 zone alarm panel (figure 11.4).

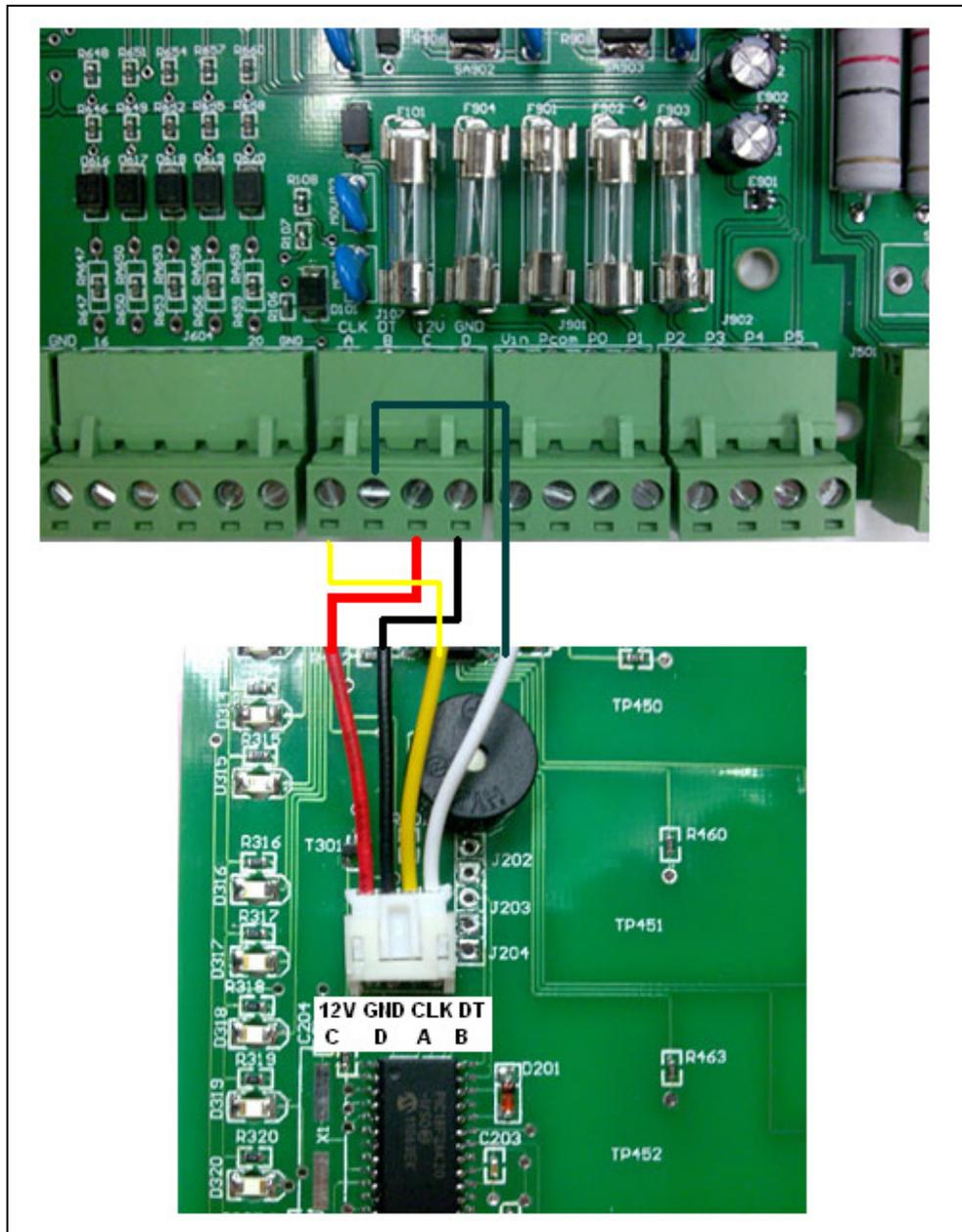


Figure 11.4 Connection touchpad and 20 zone alarm panel

- f. The hardware connection for siren and strobe light with 20 zone alarm panel (figure 11.5).
 - i. For PGM 1 as strobe light, turn on when zone trigger, please follow the steps below.
 1. Refer to **NUMBER PROGRAMMING** table address 51, define PGM1 as 133. (PGM definition: 133 = active when zone trigger, off after disarm.)
 2. Enter Programming Menu,
 - a. [*] [0] [Installer code] [Address] [PGM Definition]
– [*] [0] [1397] [51] [133]

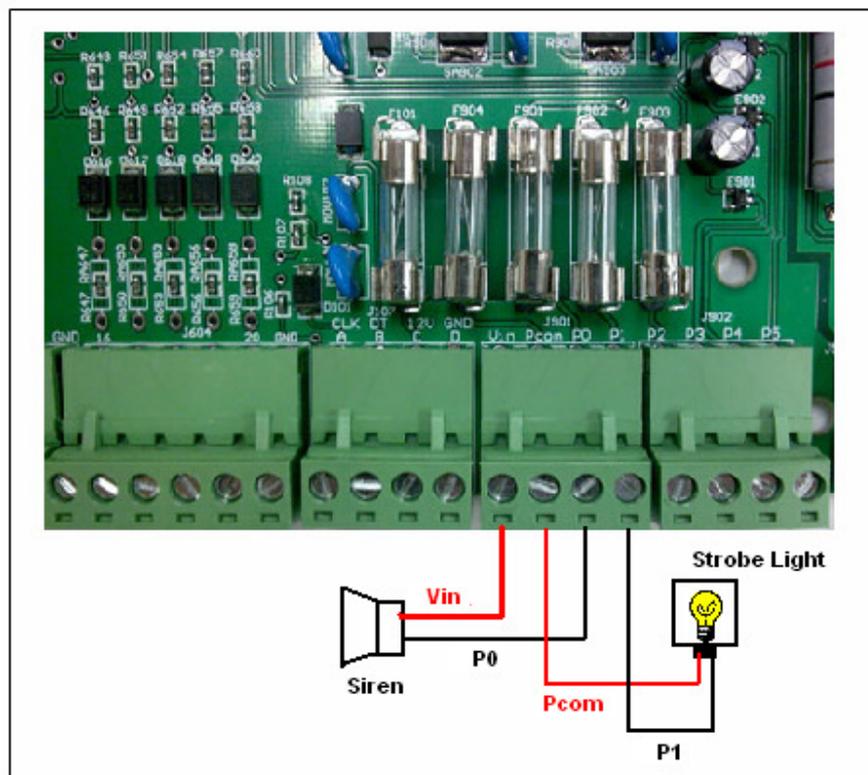


Figure 11.5 Connection between siren and strobe light with 20 zone alarm panel

- g. The hardware connection for auto gate with 20 zone alarm panel (figure 11.6).

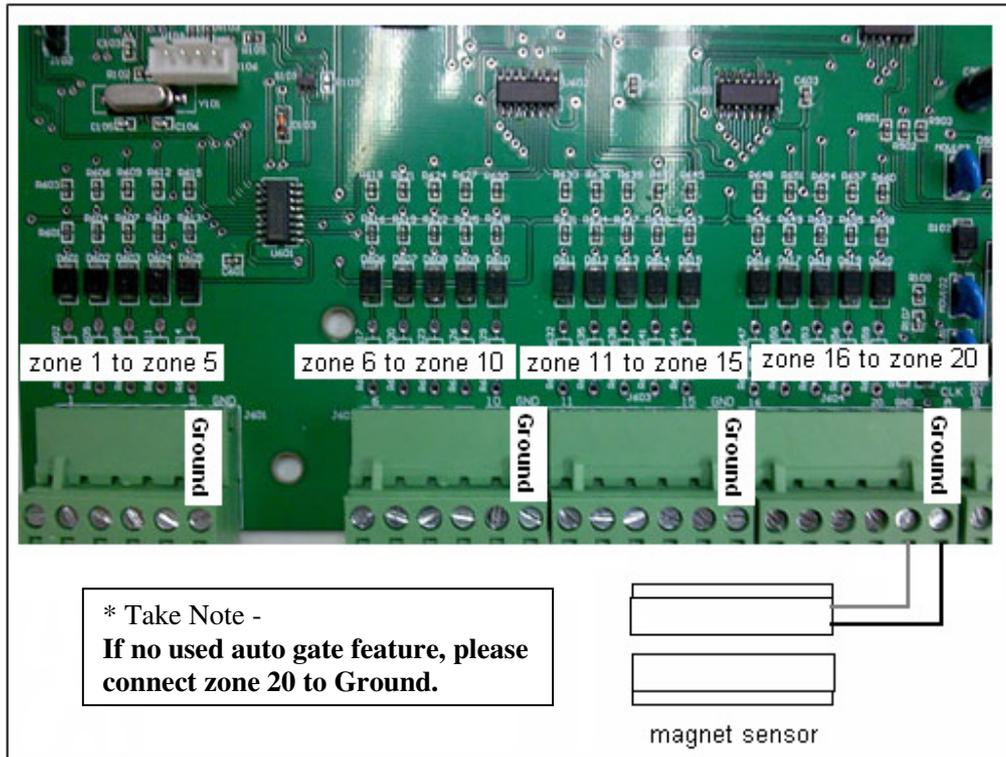


Figure 11.6 Connection between auto gate and 20 zone alarm panel