LS-20

The Universal Box

HOME MANAGEMENT GATEWAY

OPERATION MANUAL V1.03

Table of Contents

INTRODUCTION

Thank you for purchasing the LS-20 the Universal Home Management Gateway.

By adopting modern embedded system and Cloud Server technologies, the LS-20 is designed to provide all the most advanced features to meet your security and home management requirements through Internet.

The LS-20 not only provides you a secure life but also a convenient living environment that allows you to control remote switches through a cloud server, mobile App. or PC by using **HyperSecureLink** software from all over the world. With different environmental sensors, the LS-20 also plays as an environmental monitor center to collect all the environmental data and control corresponding appliances to save your energy consumption automatically.

As your requirements grow and you become more familiar with the system, you can expand and accessorize the LS-20 to meet your specific needs. Simply call your local dealer; trained professionals can answer any questions you have regarding additional accessories.

Main Features:
- High performance wireless Smart Home Management Gateway with security, environment monitoring, automation control and energy saving suitable for Web Based Service.
- Setting, controlling and download/ upload system parameters and events through USB or Ethernet interface, all commands are compatible to LS-10/30.
- Report any activity through Internet in real time with fast response and saving user's communication expenses.
- Built-in detailed 512-event log.
- 4 LED display for Away/ Home/ Disarm and Data transmission indication.
- Voice prompt and warning message to inform user about the status. (optional)
- GSM/GPRS module for spare communication and alarm report if Internet fails. (option)
- Can accommodate 288 sensors and control 15 programmable switches.
- RF signal quality monitoring and jamming detection.
- Robust multi-million RF coding and special transmission timing design to avoid interferences.
- Responds to panic, burglary, fire, medical alarm and environmental hazards.
- Burglar zones with supervised sensors, door and window open/ close detection.
- Special Monitoring mode to record all the activities in the protected area without triggering the alarm.
- Inactivity monitoring to take care of the elderly or physically challenged at home.
- 9 independent partial arm zones, one LS-20 can operate as 10 independent burglar alarm systems.
- Scheduled switch operation for a whole week automatically.
- 8 switch and operation scenes controlled by Keypad.
- 3 external wire sensor inputs and alarm siren control output.
- Battery backup for operation up to 16 hours.

● 1. BASE UNIT

1.1 Display
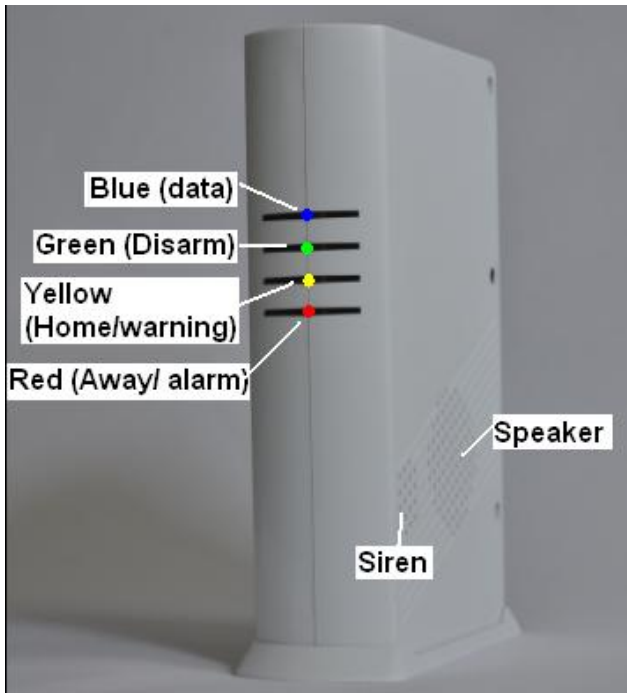
The Blue LED flashes when there is data sending out from the LS-20.

Three LEDs in green, yellow and red colors represent the system operation mode and alarm/ warning status as listed in the following table.

State LED	Red	Yellow	Green (Flash rate slows down while AC loss.)
DISARM	OFF	OFF	Flash
HOME	OFF	Flash	OFF
AWAY	Flash	OFF	OFF
DISARM with Warning Message	OFF	ON	Flash
DISARM with Alarm Message	ON	OFF	Flash
DISARM with Warning & Alarm Message	ON	ON	Flash
HOME with Warning Message	OFF	ON	OFF
HOME with Alarm Message	ON	Flash	OFF
HOME or AWAY with Warning & Alarm Message	ON	ON	OFF
AWAY with Warning Message	Flash	ON	OFF
AWAY with Alarm Message	ON	OFF	OFF

1.2 Rear Panel:
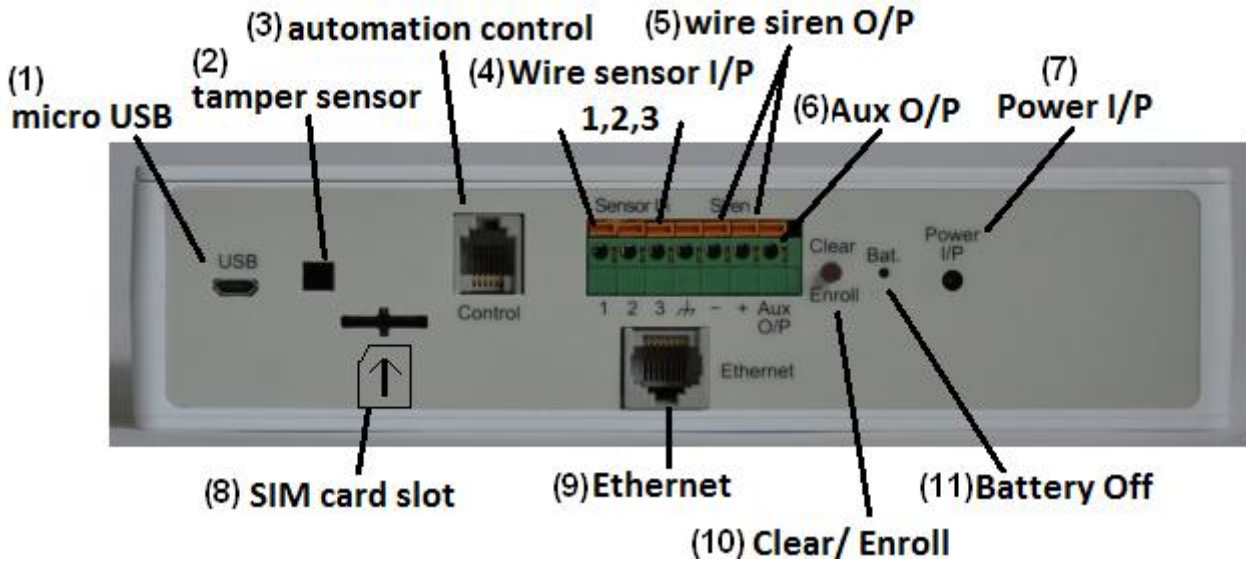
(1). micro USB: Connect to PC for accessing from HyperSecureLink software.

(2). tamper sensor: for tamper detection (Only for wall mounting bracket.)

(3). automation control: RJ-9 connector for X-10 control interface.

(4). 3 wire sensor input terminals.

(5). wire siren output terminals.

(6). Aux output: for Arm/Disarm indication (only driver LED)

(7). Power Socket: 7V DC power input.

(8). SIM Card slot: For GSM SIM card (only for the GSM/GPRS version)

(9). RJ-45 Ethernet Socket: Connect to the Ethernet network.

(10). Clear/Enroll Button:

     Clear LED Status: Press the button for about 0.2 sec. to clear the alarm and warning LED status.

     The LED status also can be cleared from HyperSecureLink command.

     Device Enroll: Press the button for about 3 sec. the LS-20 enters into Enroll Device State for 30 seconds. (Buzzer beeps and Green, Yellow, Red LEDs flash)
Please refer to Section 4.1.

(11). Battery Off: Stick in a straightened paper clip to turn off the battery when the main power input has been removed. (Note: The back-up battery starts to charge automatically while power on.)

1.3 Mounting Bracket:

LS-20 can sit on a stand vertically or put in a wall mounting bracket as below.

Base Unit Stand   Wall Mounting Bracket (option)

1.4 Beeps & LED indication (without audio board)

Status	Beep	LED			Remark
		G	Y	R	
PWR On (OK)	Beeps on operation mode	B			
Disarm	1L	B			
Monitor	1L	B			
Home	2S		B		
Away	4S			B	
Clear (OK)	1L				
Entry Delay	M-M-M--(>10sec.) S-S-S--- (< 10sec.)				
Exit Delay	M-M-M--(>10sec.) S-S-S--- (< 10sec.)				
Open Detect	5sec. continuous		O		
Alarm delay	M-M-M--- (30sec.)			O	
Panic alarm (Siren On)	L-L-L--- (as Alarm Action Time)			O	
Burglar alarm (Siren On)	L-L-L--- (as Alarm Action Time)			O	
Fire alarm	L-L-L--- (as Alarm Action Time)			O	
Medical alarm	L-L-L--- (as Alarm Action Time)			O	
Environment sensor alarm	L-L-L--- (as Alarm Action Time)			O	
Device Enroll	M-M-M--- (30sec. or till success)	B	B	B	
Device Enroll succeed	3S				
Device Enroll failed	1L				
Siren test	1S				
Door Bell	1S+1M				

Beep

S (Short Beep): 0.25sec. On / 0.25sec. Off

M (Medium Beep): 1~ 0.75sec. On / 1~ 0.75sec. Off

L (Long Beep): 2sec. On / 2sec. Off

LED

O: On

B:Blink

2, External Control and Indicator Connection Diagram
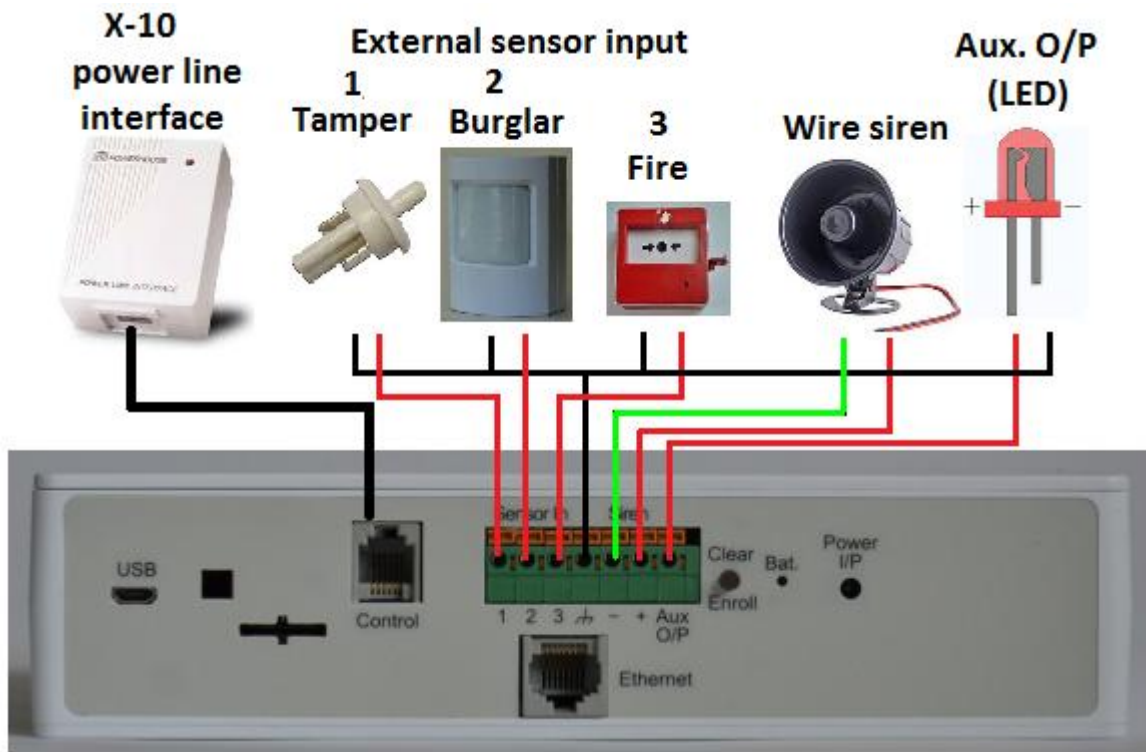
3, Working Scenario:

LS-20 can work standalone with Free HyperSecureLink software, third party's Mobile App (MyHome) or connect to a cloud server to enjoy much more service from the provider.

## 3.1 Programming the LS-20 through USB to connecting to GSM network.

Note: For the LS-20 with only GSM communication module, please use USB and HyperSecureLink software to set the operation parameters.
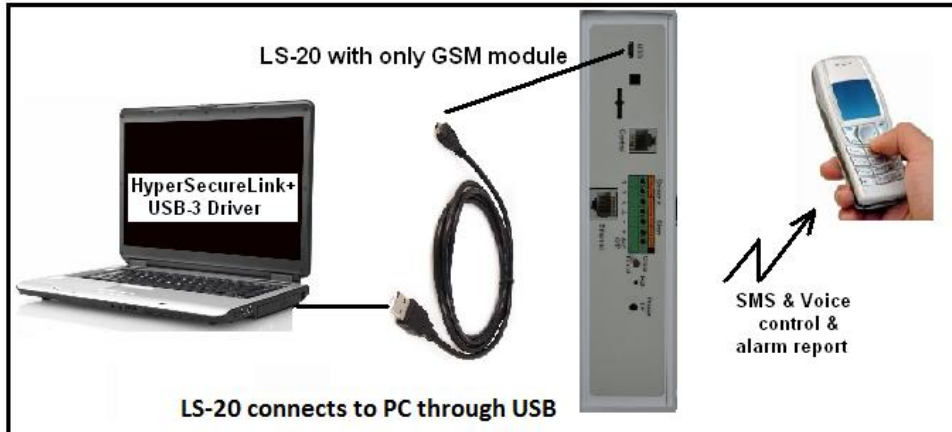
Note: When the USB interface is connected to PC, the Base Unit can't be controlled through Ethernet but data sends out from Ethernet interface is still available.

Please refer to HyperSecureLink user guide also.

3.1.1   Install the USB driver on PC.
3.1.2   Connect the USB port to PC.
3.1.3   A new COM port (Ex. COM4) shows on the HyperSecureLink software.
3.1.4   Select the new COM port then work with HyperSecureLink software.
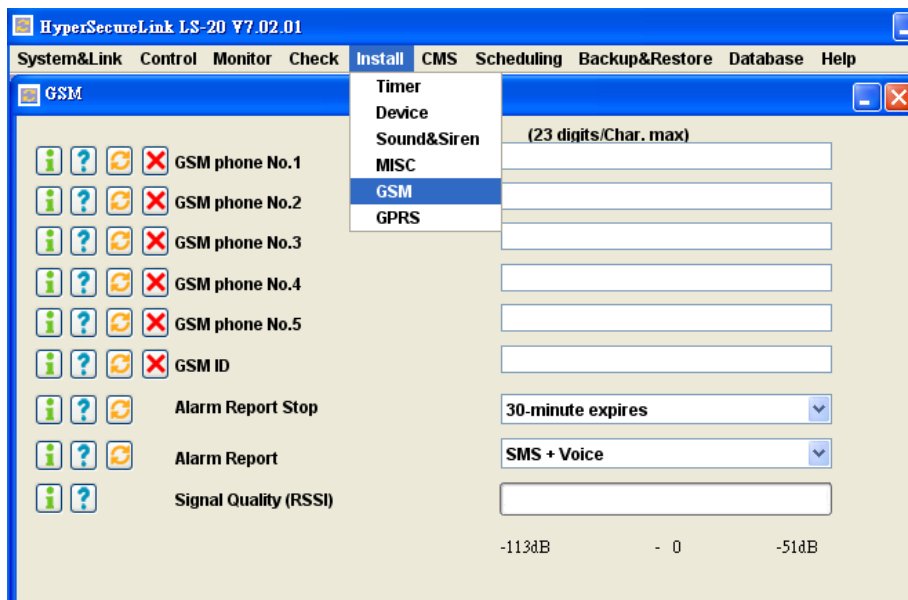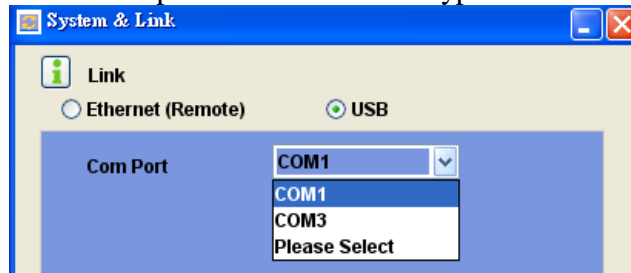
3.2 Access LS-20 by HyperSecureLink software or Mobile App. from local network.
Note: LS-20 must be set as a server.
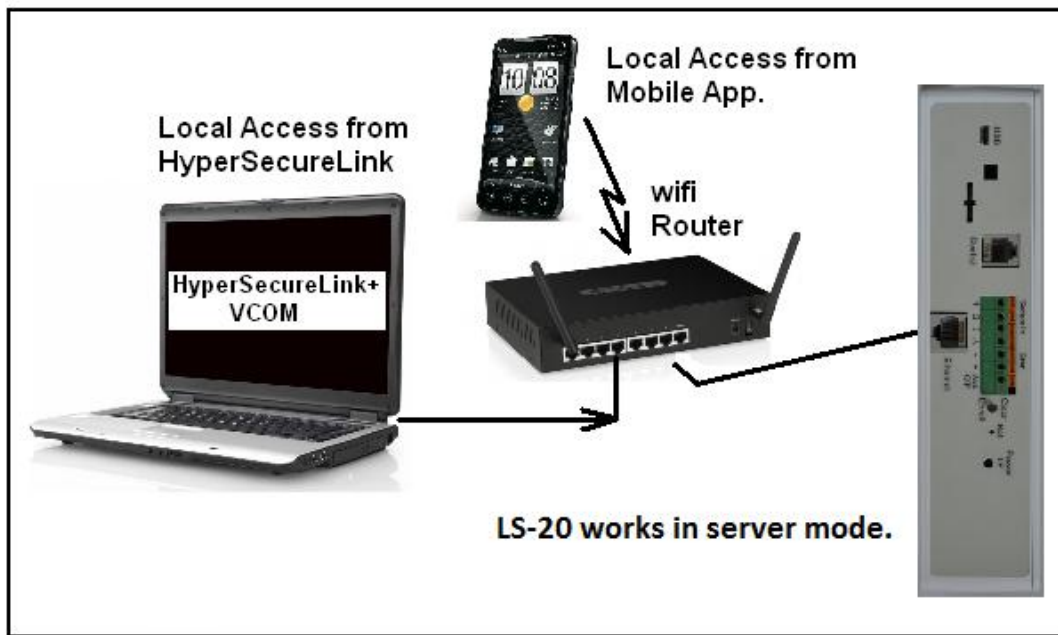
Connecting the LS-20 to a router to be accessed by Mobile App. (MyHome) or HyperSecureLink software locally.

Find the LS-20 address by VCOM and set LS-20 as a server from its web page.

Access the LS-20 by HyperSecureLink software or Mobile App. from local.

3.3 Works with HyperSecureLink software or Mobile App. (MyHome) from Internet.
Note: LS-20 must be set as a server.
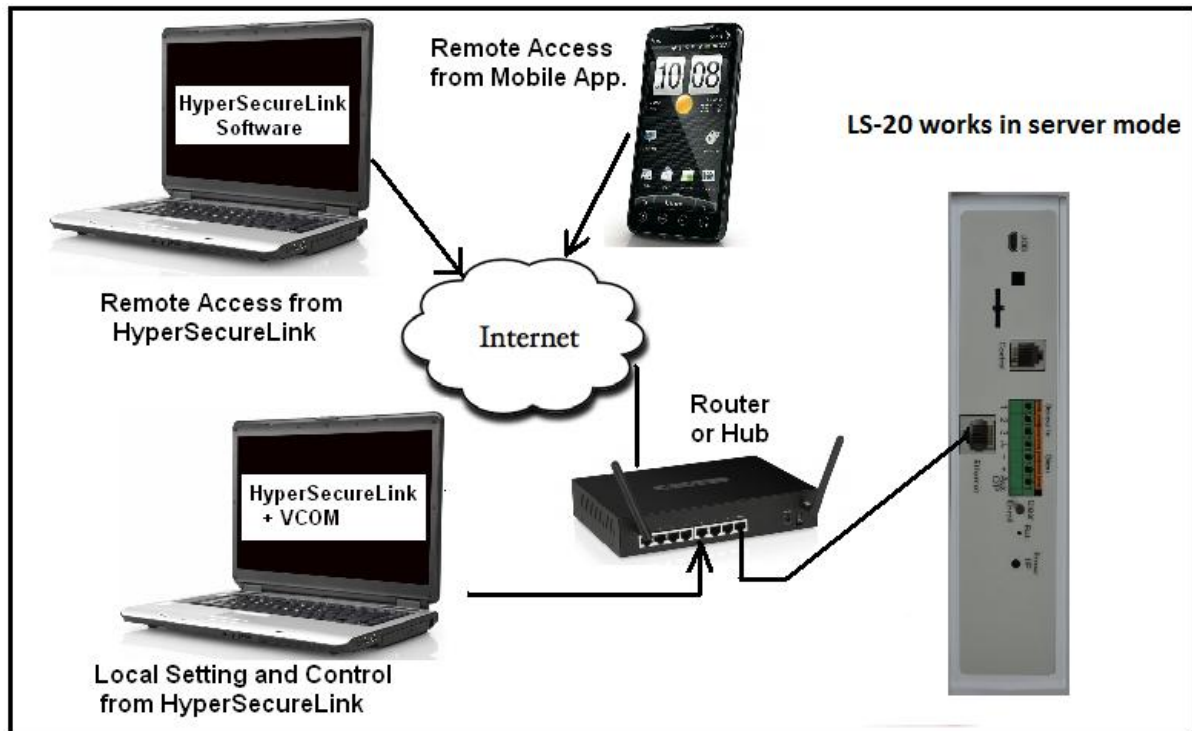
Note: 1, To be accessed from the Internet, the Router needs a fixed IP address or a domain name. A dynamic domain name can be got from www.dyndns.org, www.no-ip.com (free) or other dynamic domain name service provider. Some router manufacturers provide free domain name service if you use their router such as DLINK. Please refer to the web site: http://support.dlink.com/Emulators/dcs3415/setup_dns.html for more information.

2, The LS-20 has to be mapped to a TCP port that can be accessed from Internet by virtual server or port forwarding function in the router.
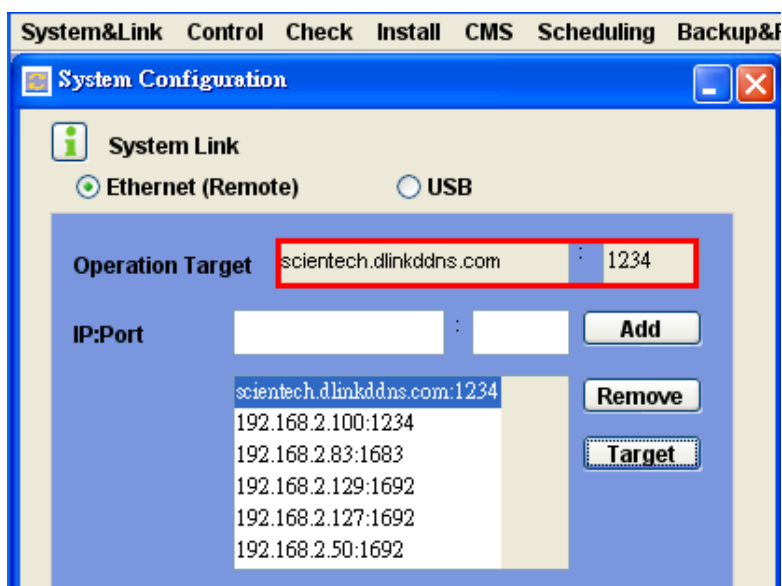
(Ex: Using the free Domain Name Service from the router manufacturer DLINK and 192.168.2.100 is mapped as Virtual Server Port 1234 in the router.)

3.4 Connects to a Cloud Server to Get Full Home Management Service.
Note: LS-20 must be set as a client.
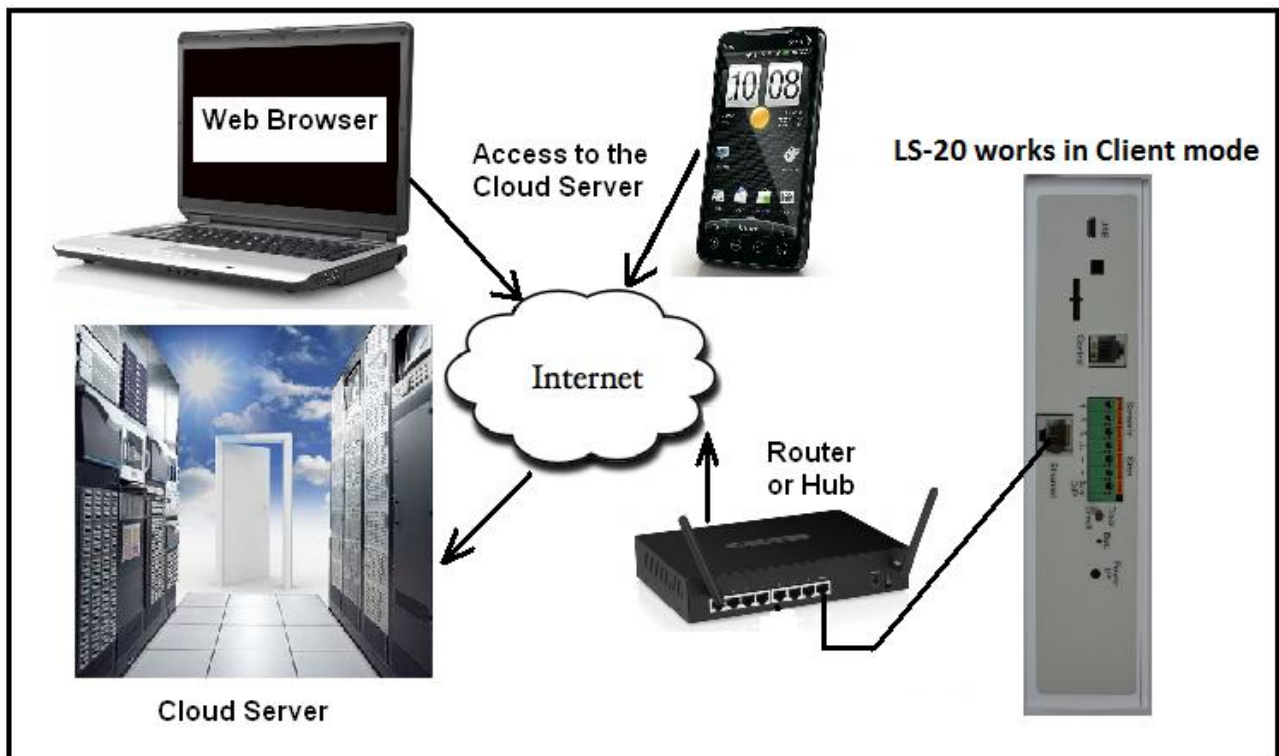
TCP Control

Item	Value
Telnet Server/Client	○ Server ● Client ○ Disable
Port Number	1692
Remote Server IP Address	gateway.livingpatternco.com
Client mode inactive timeout	20 minute (1~99,0=Disable)
Server mode protect timeout	60 minute (1~98,0=Disable,99=Can't replace)
	Update

Ex.: Assign LS-20 to the Livingpattern cloud service.
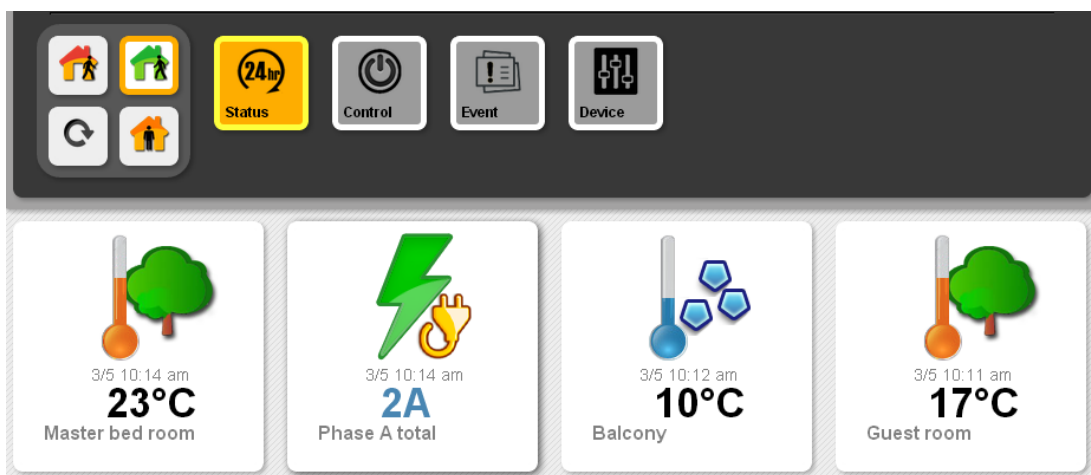
Service example from Livingpattern cloud server.

3.5 Connects to a Central Monitor Station to Get Alarm Service.
Before connecting to a CMS service provider, please consult your distributer first.

Note: LS-20 must be set as a client.

CMS monitoring software example from a service provider.

4, Installation

4.1 Device Enroll

The first step to start the operation of LS-20 is to enroll all the sensor/controller devices into the Base Unit one by one.
(Please refer to the User Guide of the devices to be enrolled as well.)

*Press the Clear/Enroll button for 3 seconds, the LS-20 enters into Enroll Device State for 30 seconds. (Buzzer beeps and Green, Yellow, Red LEDs blink simultaneously)

* Trigger the target device to send RF signal in 30 seconds.
Note: Beware of not to activate any other sensors during the 30 seconds Device Enroll time.

*Activate the target device again after a successful enrollment to confirm the device by checking the "Device Status" from HyperSecureLink software or web server.

Device Enroll

① Press the Key for 3 sec. (Green, Yellow, Red LED blink + buzzer beeps.) Device Enroll starts and lasts for 30 sec.

③ Success: Three short beeps. Failure: One Long beep after 30 sec.

② Trigger the Target Device to send RF signal in 30 sec.

④ Activate the Target Device again to confirm the enrollment was successful.

4.2 Placement of the Base Unit and Sensors

It is important for the Base Unit to have a good reception quality for the RF signals transmitted from all the sensors and controllers.

● Place the Base Unit near the central of your home or business if possible.

● Keep the Base Unit away from large appliances and other metal objects.

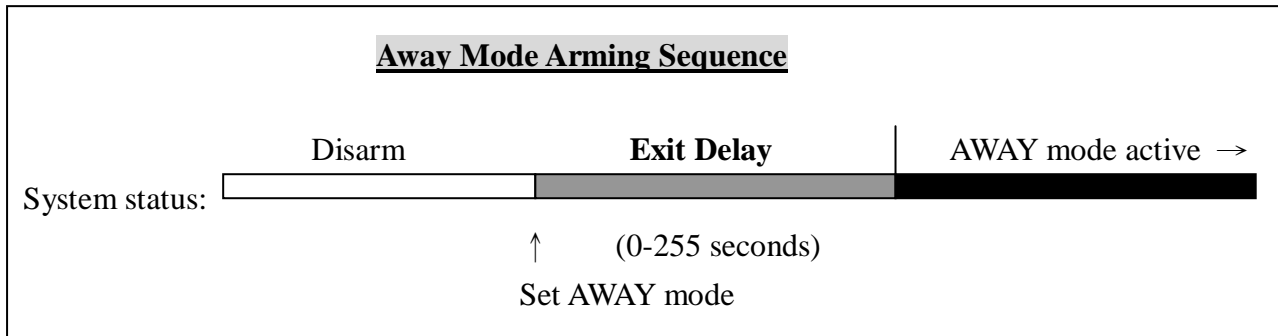● Locate the Base Unit near a power outlet and the router.

Install all the sensors according to your site planning.

Check the radio signal quality from the CS ("Current Status" in "Device Status") reading from the HyperSecureLink software or signal bar from Cloud server or Mobile App. (MyHome) by pressing the test button on the sensors or trigger the sensor's action. Relocate the sensors/Base Unit to get the best signal strength if necessary.

If the dB number is less than 40dB or without bar indication then you should consider to adjust the location of the sensors/Base Unit or add a RF Repeater to the system to extend the RF operation range. (Do not attach the transmitter on a metal surface, this will shrink the RF signal effective range seriously.)

5. OPERATION MODE

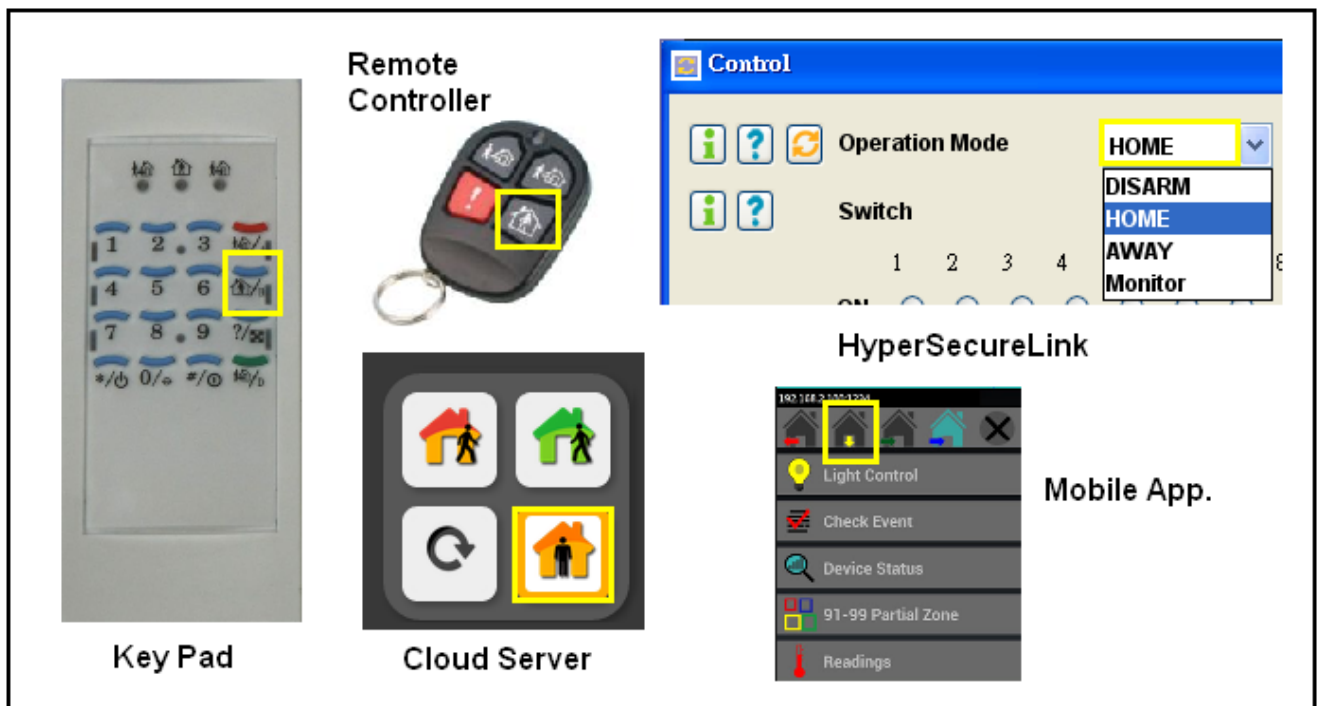**5.1 AWAY Mode:** When you leave your home or business, set the system into Away Mode.

<div>

Away Mode Arming Sequence

System status:

	Disarm	**Exit Delay**	AWAY mode active →

↑   (0-255 seconds)

Set AWAY mode

</div>

Note: When you set the LS-20 in AWAY Mode, the Base Unit clears any previous alarm and warning status on the LED and check the state of the Door Magnet sensors. If any of the sensors is still open (for example, you forgot to close the back door before you leave), the Base Unit will issue a 5 sec. long beep and insert 20 seconds Exit Delay automatically if no Exit Delay has been set to remind you to check the house again.
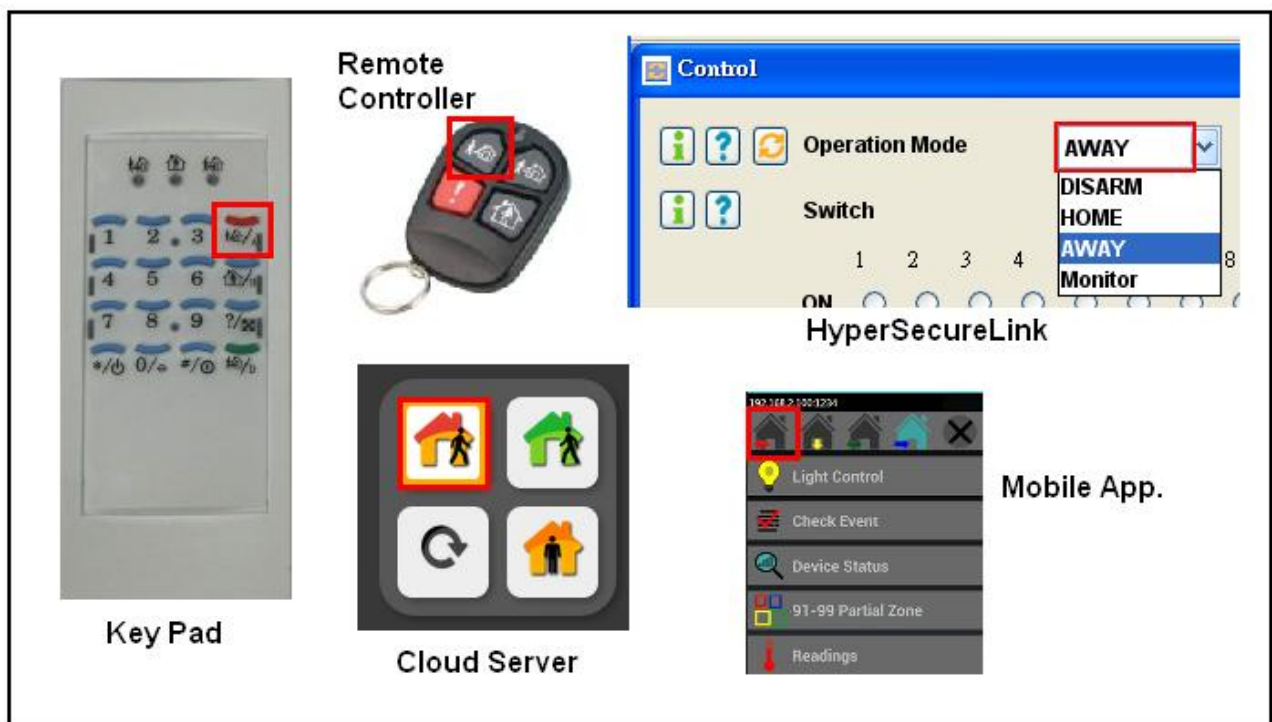
Enter into "AWAY" Mode from different devices or services.

5.2 HOME Mode: In this operation mode, those burglar sensors with their **Enable State – "24-Hour Zone" or "Guard in Home Mode" = Yes,** will still be on alert and offer the protection you need while at home.

Note: When you set the LS-20 in Home Mode, the Base Unit will check the status of the Door Magnet sensors. If any of the sensors is still open (for example, you forgot to close the back door), the Base Unit will keep a "Protection Loop Open" in the Event Log.

The Base Unit will clear any previous alarm and warning status on the LED when the Home Mode is entered from the Disarm Mode.

Enter into "HOME" Mode from different devices or services.

**The Burglar sensor's "Guard in Home Mode" is enabled.**

5.3 DISARM/ MONITOR Mode: The LS-20 will not issue any alarm for Burglar sensors, but 24-Hour sensors, Fire sensors, Panic, Medical Buttons and Environment sensors still work all the time.
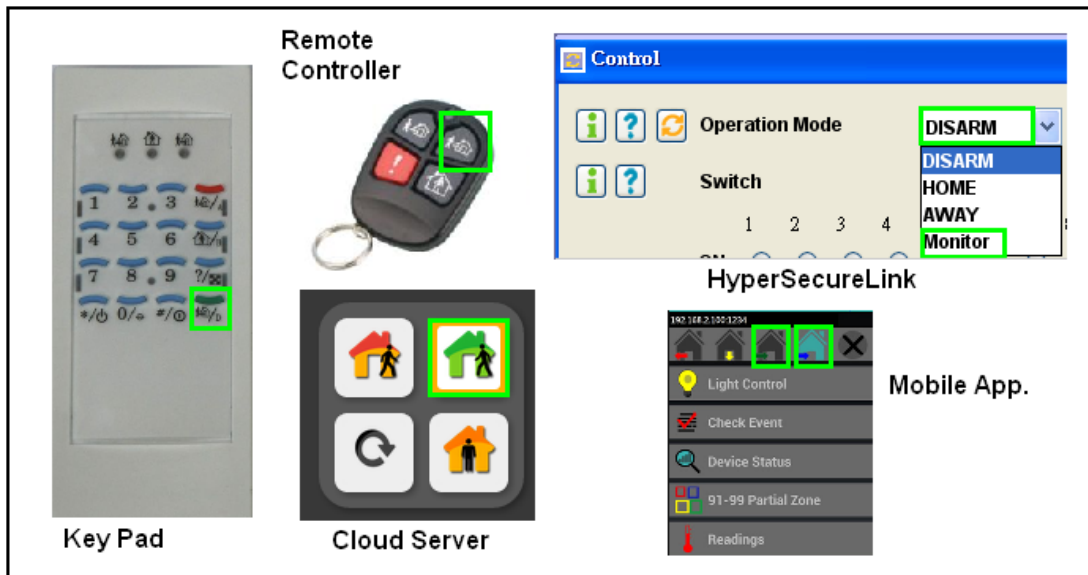

Enter into "DISARM" or "MONITOR" Mode from different devices or services.

Monitor Mode: In this mode all the trigger signals from the **Burglar Sensors** (not including the sensors assigned in Group number 91-99 Partial Arm Zones) will be recorded in the Event Log as trigger events only; no alarm will be issued. The purpose of this mode is for the recording of all activities in the protected area while in Disarm Mode.

5.4 Reaction of LS-20 to Burglar Alarm
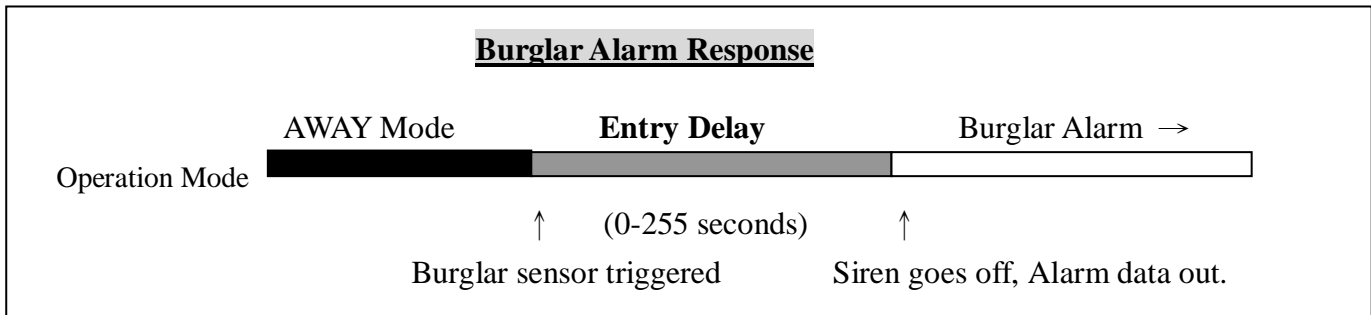
Burglar alarms can only be issued when the system is in AWAY or HOME mode or with the sensors assigned as a 24-Hour Zone device, while Fire, Panic, Medical and Environment alarms can be triggered anytime, regardless of the system operation mode.
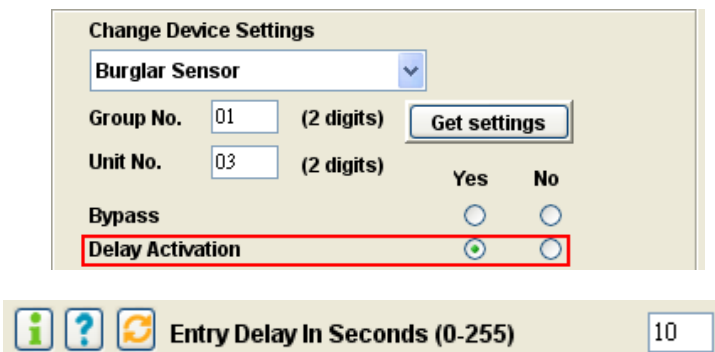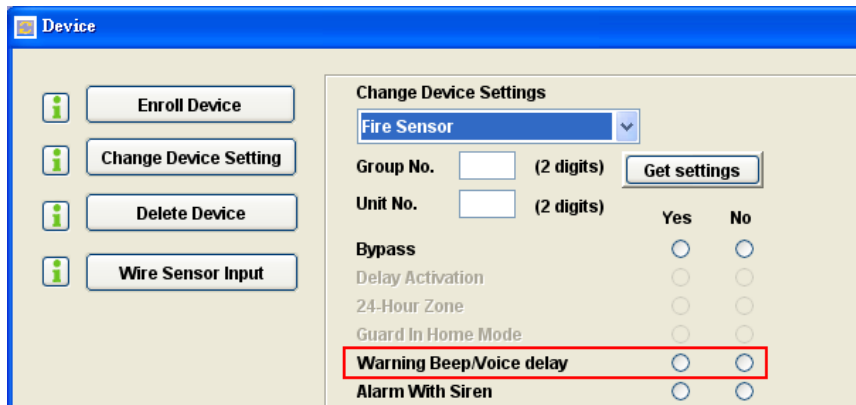

The siren can be stopped by disarming the system.

5.5 Reaction of LS-20 to Other Alarms except Burglar Alarm
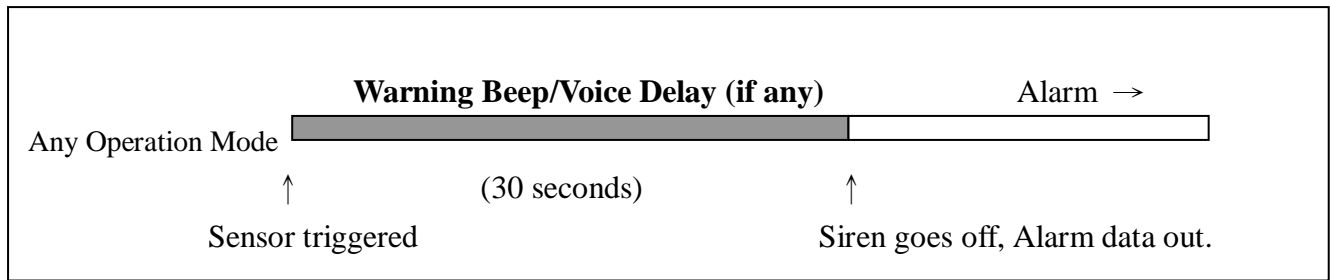
Warning Beep/Voice Delay (if any)   Alarm →

Any Operation Mode

↑   (30 seconds)   ↑

Sensor triggered   Siren goes off, Alarm data out.

Fire, Panic, Medical and Environment alarms can be triggered anytime, regardless of the system operation mode.

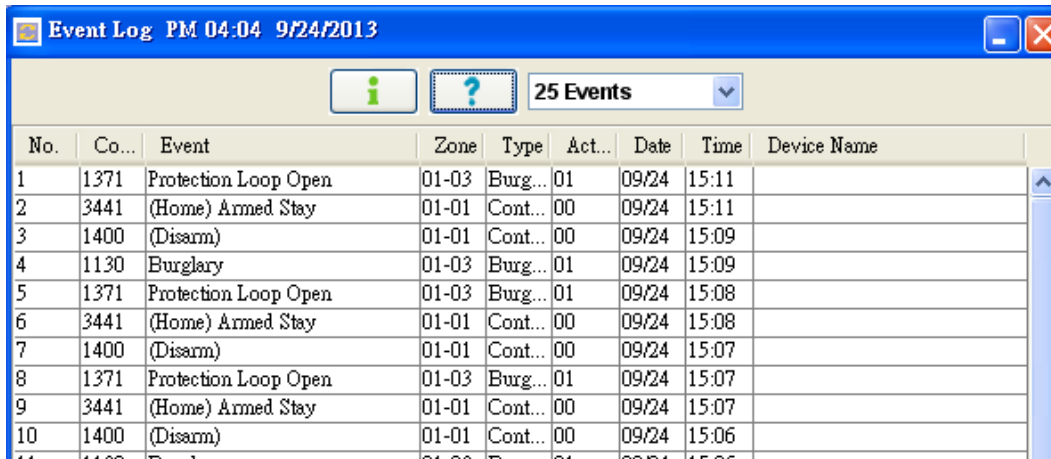The "Warning Beep/Voice Delay" is fixed at 30 seconds.

The siren can be stopped by disarming the system.

6. SYSTEM CHECK

6.1 Event Log: The Base Unit can store 512 event records in its memory. These events can be checked from HyperSecureLink Software or Mobile App (MyHome).

If user applies a Cloud Service then much deeper Event Log can be recorded.
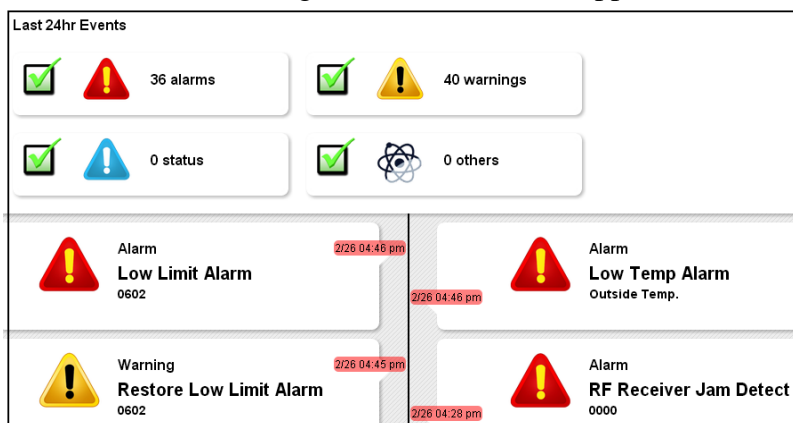
Event Log read from HyperSecureLink software

Event Log read from a mobile App.
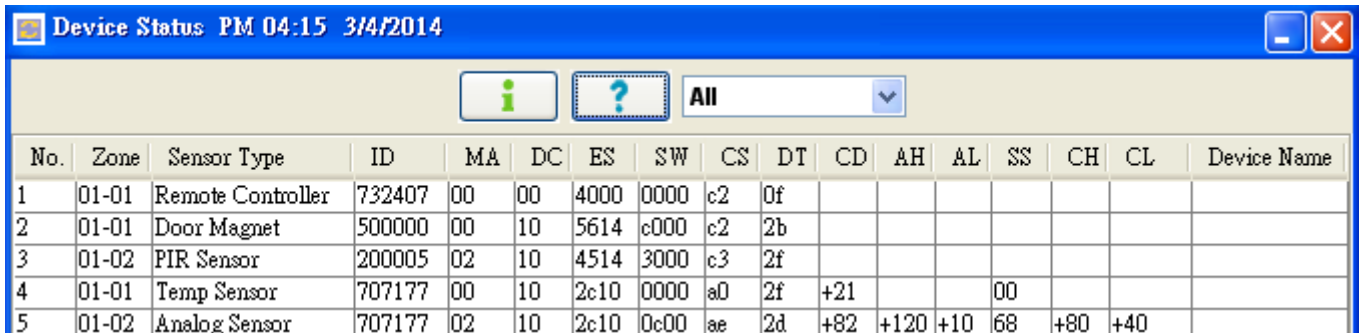
Event Log read from a cloud server.

6.2 Device Status: The latest state of the sensors including, signal strength and readings can be checked by device status from the HyperSecureLink Software or Mobile App (MyHome).

If user applies a Cloud Service then each device can be named for easy identification and Environment readings or activities can be show in graphics.

No.	Zone	Sensor Type	ID	MA	DC	ES	SW	CS	DT	CD	AH	AL	SS	CH	CL	Device Name
1	01-01	Remote Controller	732407	00	00	4000	0000	c2	0f							
2	01-01	Door Magnet	500000	00	10	5614	c000	c2	2b							
3	01-02	PIR Sensor	200005	02	10	4514	3000	c3	2f							
4	01-01	Temp Sensor	707177	00	10	2c10	0000	a0	2f	+21			00			
5	01-02	Analog Sensor	707177	02	10	2c10	0c00	ae	2d	+82	+120	+10	68	+80	+40	

Device Status read from HyperSecureLink software

Device Status read from a Mobile App.

Cloud server allows user to assign a name to each device for user to identify the sensor much easier.
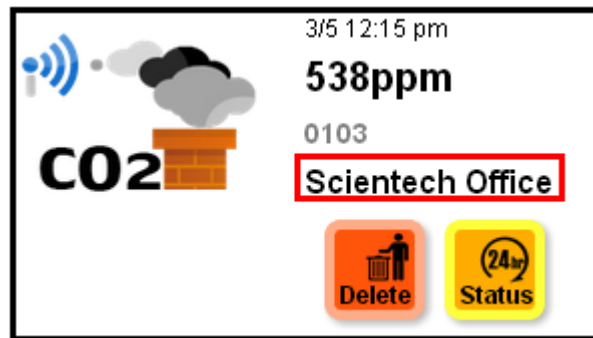
Device Status read from a Cloud Server.
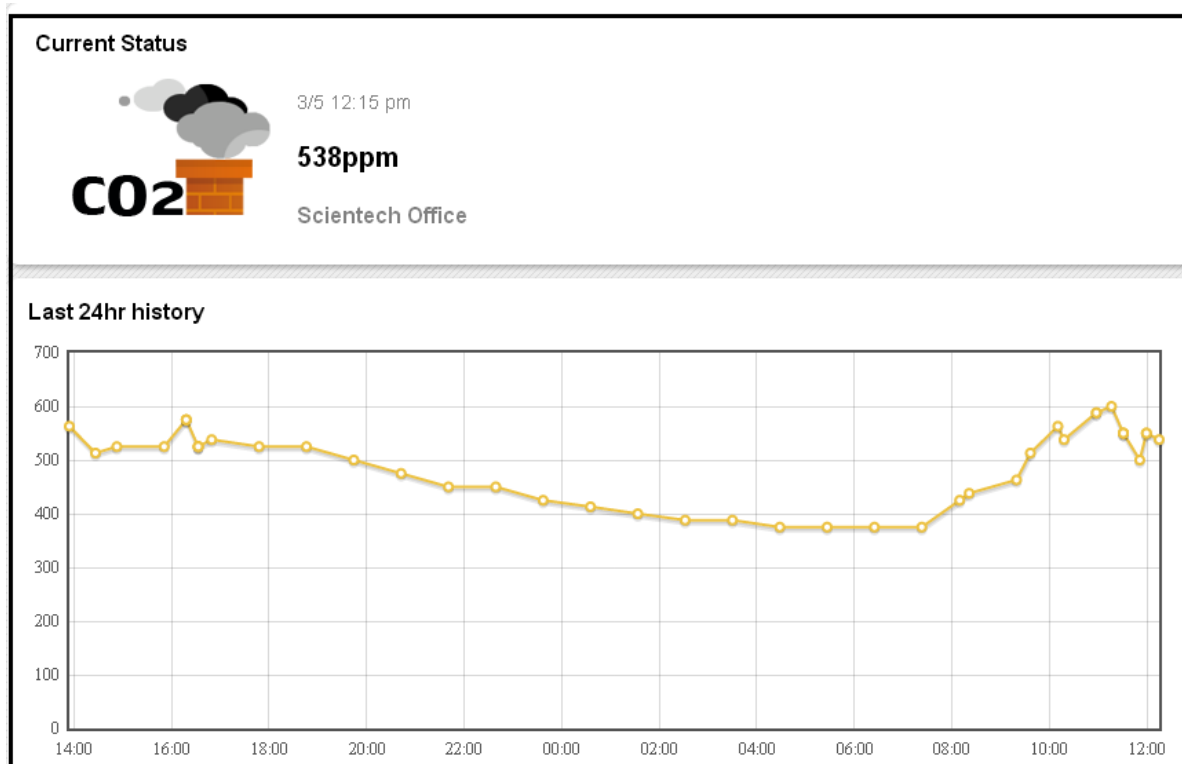
24 Hours history of a CO2 sensor shown from a Cloud Server.

7. HOME AUTOMATION CONTROL

There are 16 (#1~#16) X-10 switches and 8 (#1~#8) RF switches can serve as alarm indications or home appliances control purpose.

These switches can be controlled by Remote Controller, Keypad locally, HyperSecurelink software, mobile App (MyHome) or Cloud Server remotely.

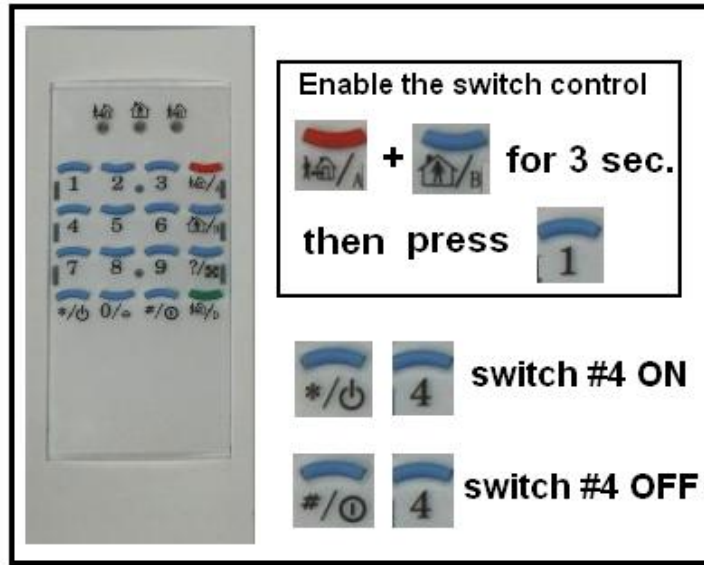**Note:** Switch #16 is for Arm/ Disarm indication, please refer to **8.9, #16 SW Assignment.**

7.1 Switch setting by HyperSecureLink software to be controlled by Remote Controller.
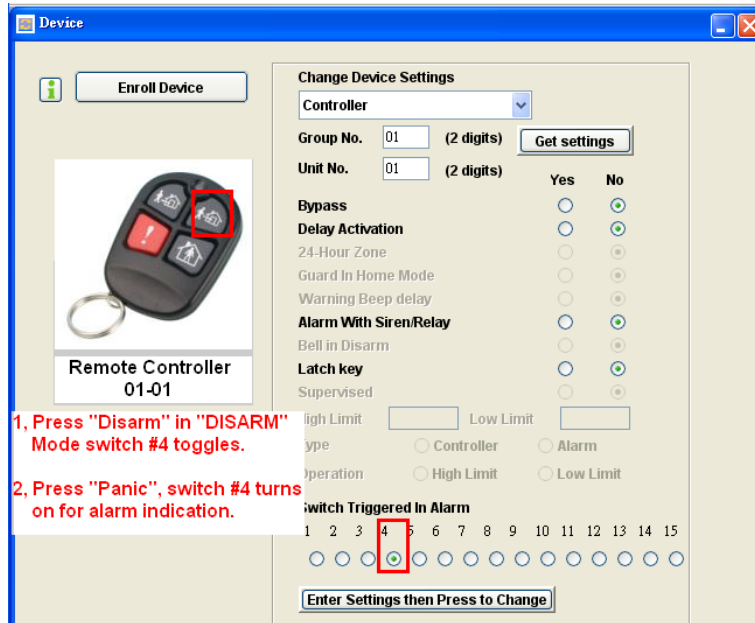
7.2 Directly control from HyperSecureLink software, Mobile App (MyHome) or cloud service.
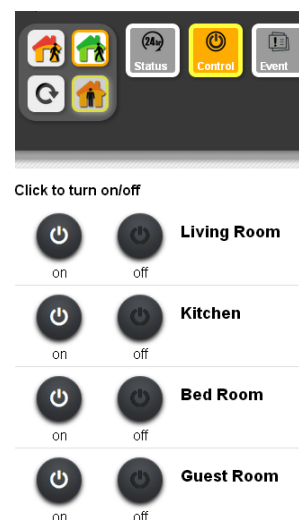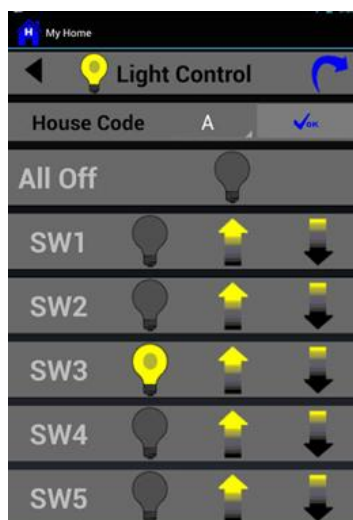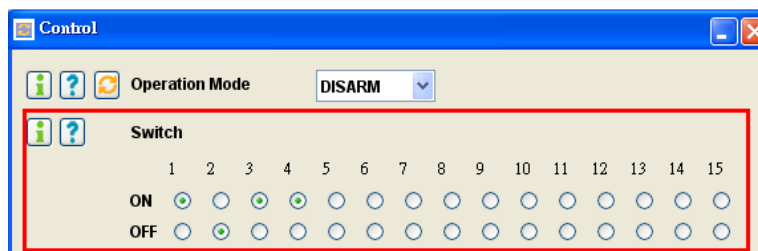
7.3 Switch control from Keypad. (Please refer to the KP-3S User Guide for more information.)

7.4, Automatic controlled by Burglar Sensors with "Home Automation=Yes" in Disarm Mode.

Ex. Below settings will turn the switch #3 on for 10 minutes when the Burglar Sensor 01-02 was triggered in Disarm Mode.

(For PIR sensor, it will turn off till the "Motion Stop" signal was received as well.)

7.5 Automatic control by the Special Sensors with their "High/Low" limit settings.

Ex, Below settings will turn on switch #3 when reading is above "28" and turn off switch #3 when reading is below "26".

(Note: "High Limit" Control is for cooler, and "Low Limit" Control is for Heater)

7.6 Automatically switch control scheduled by HyperSecureLink software.

Ex: The switch #1 will turn on at 19:00 and turn off at 07:05 everyday.

The switch #2 will turn on at 07:15 and turn off at 09:00 everyday.

8. CONTROL AND PARAMETER SETTINGS

8.1 Control

* Siren Test: This test will activate the beeper, external alarm siren and send an Activate signal to the Remote Siren (if a remote siren is installed) immediately.

(HyperSecureLink)   (Livingpattern Cloud Service)

* Clear Status: To Clean the alarm/ warning LED and stop the alarm/ warning reaction.


(HyperSecureLink)   (Livingpattern Cloud Service)   (MyHome App.)

* Device Test: Enter into Device Test Mode for 5 minutes. Any trigger signal (not including the control signal from Remote Controller) in this time will be treated as a test signal. After 5 minutes, the system will exit from this mode automatically.

* External Alarm Siren: On: turn on the wire siren circuit on the rear panel**.**

Off: turn off the wire siren circuit on the rear panel**.**
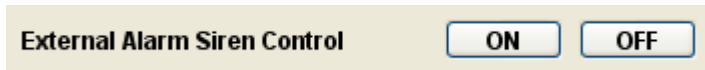
* Control Command Password: (default = Disable)
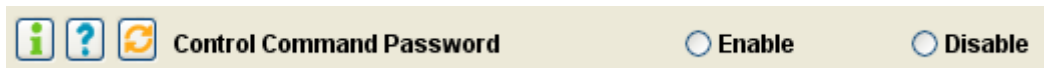
Disable: No password needed for the control commands.

Enable: Password must be attached to the control commands.

(If "Enable" then the password must be set and submitted when running the HyperSecureLink software as below.)
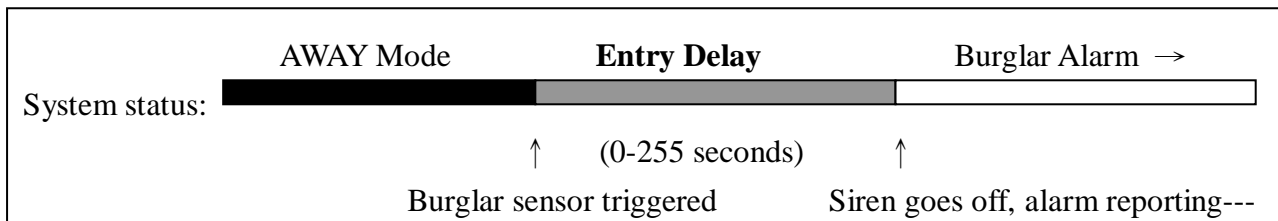
8.2 Settings for Timers

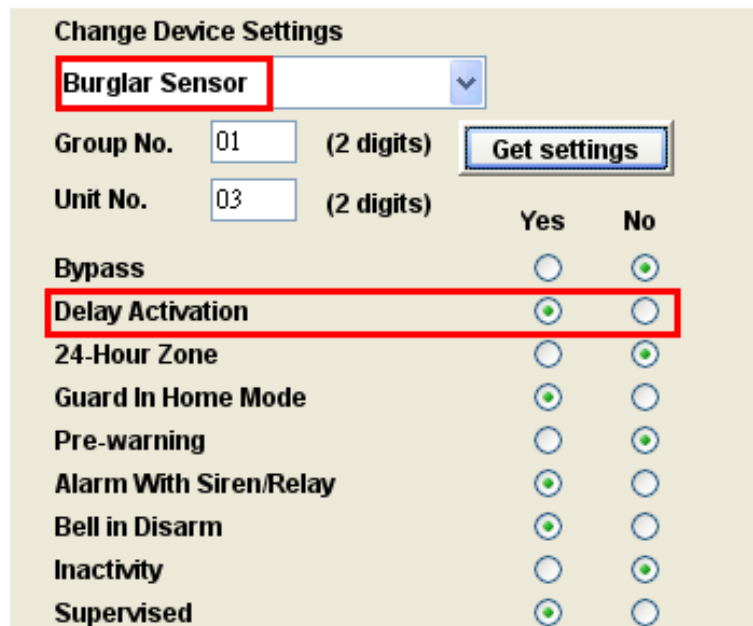### *Entry Delay (For Burglar Sensor only, 0-255 seconds, default =10 sec.)

This setting is the time between any burglar sensor triggers and the alarm action procedure starts. When you return home and open the door, the Base Unit will issue warning beeps (if the **Delay Activation = On**) to remind you that the system is still in the Arm state and you should disarm the system within this time.

   For the system controlled by Wireless Keypad, this timer should be set more than 20 seconds.

This Delay only works on the Burglar Sensor with its Delay Activation= Yes, see below.

*Exit Delay (for Controller only, 0-255 seconds, default =10 sec.)

This setting is the time between selecting the "AWAY" mode and when the "AWAY" arm becomes effective. During this time, the Base Unit will issue warning beeps to remind the people still in the house to leave as soon as possible.

Since the Door Open signal may last for 10 seconds, so add 10 seconds to the time you need to leave the house as the Exit Delay. (Ex. you need 20 seconds to leave the house, set Exit Delay=30s)

For the system controlled by Wireless Keypad, this timer should be set more than 20 seconds.

System status:	Disarm	**Exit Delay**	AWAY ARM effective →

↑ (0-255 seconds)

Set AWAY mode
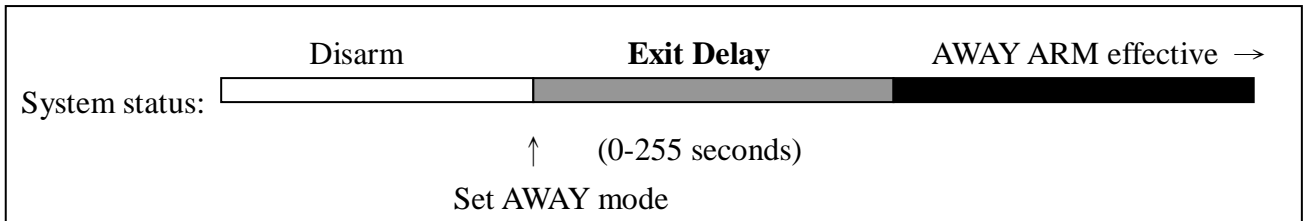
This Delay only works on the Controller with its Delay Activation = Yes, see below.

Change Device Settings

Controller ⌄

Group No.	01	(2 digits)	Get settings		
Unit No.	01	(2 digits)		Yes	No

	Yes	No
Bypass	○	◉
Delay Activation	◉	○
24-Hour Zone	○	◉
Guard In Home Mode	○	◉
Warning Beep delay	○	◉
Alarm With Siren/Relay	○	◉
Bell in Disarm	○	◉
Latch key	○	◉
Supervised	○	◉

* Inner Siren Time: 0-255 seconds (default = 60 sec.)

Inner siren Time In Seconds (0-255) 60

The time of the Inner Siren sounds when the alarm trips.

*Alarm Siren Action Time: 0 second to 120 minutes (default = 60 sec.)

Alarm Siren Action Time In Seconds(0-120) ⌄ 60

The activation time of the external Alarm Siren sounds (on the rear panel) when the alarm trips.

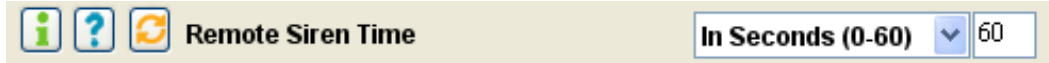***Sensor Supervise Time: 0-24 Hours (default = 12 Hours)**

Sensor Supervise Time 12 Hours ⌄

The LS-20 is a supervised RF wireless system, meaning supervised sensors send "heartbeat" RF signals to the Base Unit at a certain time interval. If the Base Unit does not receive the RF check signal from a supervised sensor within the **Sensor Supervise Time,** the LS-20 considers this sensor to be missing and issues a warning message.

This time can be set from 0 to 24 hours (0 hour means that the system will not check the "heartbeat" signal.

Please note, the time shorter than 4 hours would increase sensor "RF Loss" possibility.

*Remote Siren Time: 0 seconds to 30 minutes (default = 60 sec.)

The time of the wireless Remote Siren sounds when the alarm trips. (Remote Siren is an Option.)

* Pre-warning Time: 0-30min.   (default = 2 min.)
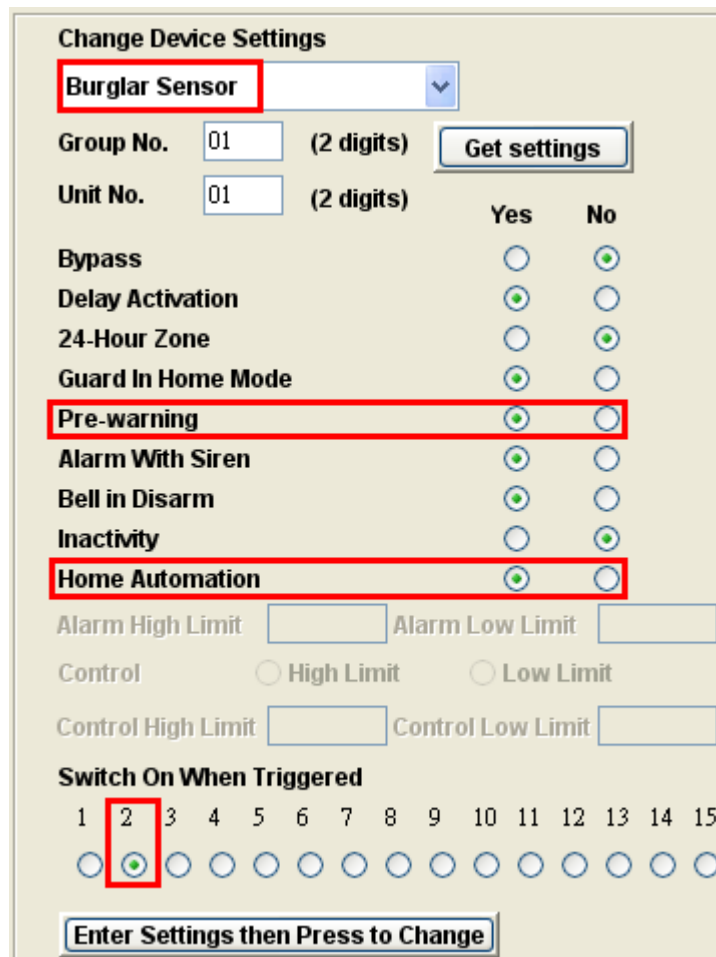

The switch action time when triggered by a Pre-warning Burglar sensor.

*Home Automation Time: 0-30min.   (default = 10 min.)

The switch action time when triggered by a Burglar Sensor in "Disarm" mode with "Home Automation=Yes".

(Please refer to 8.4 "Device Status Settings".)

8.3 Setting for Sound & Siren

* Record /Playback Voice: After an alarm call connects successfully, the LS-30 will play the prerecorded voice message that corresponds to the alarm type.
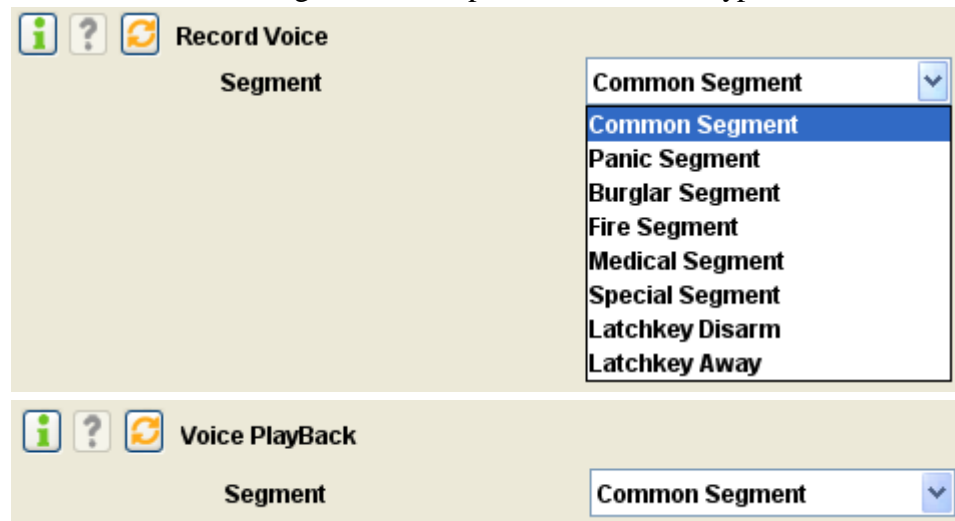
The messages should be recorded in their specified segments.

Common Segment (13 seconds): The voice to be played during all alarm types. This segment should contain your name, address and telephone number.

        Ex: "This is ---, I live at---, phone number is---."

Panic Segment (4 seconds): The voice to be played during a Panic alarm.

        Ex: "Break-in! Break-in! Calling for emergency help."

Burglar Segment (4 seconds): The voice to be played during a Burglar alarm.

        Ex: "Burglar! Burglar! Calling for emergency help."

Fire Segment (4 seconds): The voice to be played during a Fire alarm.

        Ex: "Fire! Fire! Calling for emergency help."

Medical Segment (4 seconds): The voice to be played during a Medical alarm.

        Ex: "Heart patient! Calling for emergency help."

Special Segment (4 seconds): The voice to be played during a Special alarm.

        Ex: "High temperature in the building! Calling for an alert."

Latchkey Disarm (4 seconds): The voice to be played when a latchkey user disarms the system.

        Ex: "I'm home."

Latchkey Away (4 seconds): The voice to be played when a latchkey user sets the system in AWAY mode.

        Ex: "I'm out."

*Door Bell (default = ON):

    The Base Unit will issue a doorbell beep in Disarm Mode when receiving a triggering signal from a Burglar sensor with its "Bell in Disarm = ON".

> **Note:** The Bell function only works for the Burglar Sensor with "Bell in Disarm = Yes".

*Tamper Siren In Disarm: (default = Off)

Some of the sensors (Door Magnet, PIR, Keypad) have a Tamper sensor inside, if it was detached from the wall or the case was opened then the sensor would issue a "Tamper" signal to the Base Unit.

Tamper Siren In Disarm=On: The Siren will go off for 10 seconds, if the Base Unit receives a Tamper signal from a sensor or controller in Disarm Mode.

* Entry Delay Warning: Beep/Voice/Off (default, OFF)

(Please refer to 8.2 "Entry Delay")

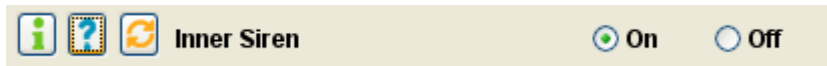**Beep :** The Base Unit will generate beeps during the Entry Delay interval and the beeping speed will get faster until the end of the delay time.

Voice : The Base Unit will generate the voice of "Away Mode" during the Entry Delay interval until the end of the delay time.

OFF: No beeps during the Entry Delay interval.

* Inner Siren: ON/OFF (default, ON)

    Inner Siren On: Enable the Inner Siren.

    Inner Siren Off: Switch off the Inner Siren. (The Siren keeps silent in alarm and warning states.)

<u>**The conditions for the Inner Siren to go off when alarm trips:**</u>

1. The Inner Siren is enabled.

2. The Alarm With **Siren** attribute of the sensor is "Yes".

3. The Inner Siren Time (8.2) has been set.

* Mode Change Chirp: ON/OFF (default, OFF)
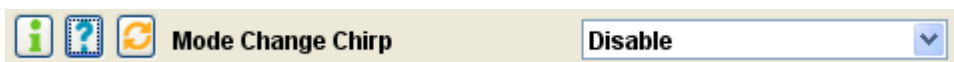
    Mode Change Chirp On: The Sirens sound short chirps (Disregard the Inner Siren status) when the operation mode changes by Remote Controller or Wireless Keypad.

        (Disarm: 1 chirp, Away: 2 chirps, Door Open warning: 5 chirps).

    Mode Change Chirp Off: The Sirens will keep silent when the operation mode changes.

8.4 Device Status Settings:

*Device Bypass (default= No): (For all devices)

　　Bypass = Yes: The system will ignore the trigger signal from this sensor.

*Delay Activation(default= Yes): (For Controller & Burglar sensor)

　　Delay Activation =Yes: (Refer to **Exit Delay/Entry Delay**.)

　　　　For the Remote Controller, the **Exit Delay** time will be imposed on the Away command from this controller.

　　　　For the Burglar sensor, the **Entry Delay** time will be imposed on the Burglar alarm signal from this sensor.

　　Delay Activation=No: The trigger signal or command from this device will be processed immediately, regardless of the Exit/Entry Delay Time.

*24-Hour Zone (default = NO): (For Burglar sensor)

24-Hour Zone=YES: This Burglar sensor's trigger signal will be processed all the time regardless of the system's operation mode, either in Arm or Disarm.

24-Hour Zone=NO: This Burglar sensor's trigger signal will only be processed in Arm Mode.

*Guard in Home Mode (PIR default = No, Door Magnet default = Yes): (For Burglar sensor)

Home Mode =Yes: This Burglar sensor will trigger an alarm in Home Mode operation.

Home Mode=No: This Burglar sensor will not trigger an alarm in Home Mode operation, it will only trigger an alarm in Away Mode operation.

*Pre-warning (default = No): (For Burglar Sensor)

Pre-warning=Yes: When this device is triggered in Arm Mode, it only turns on the corresponding switches those set by this device for the time set in the **"Prewarning Time"** to warn the person who approaching the protected area. (If 24-Hour Zone set, the switches will turn on anytime when this device is triggered.) but won't trigger burglar alarm.

*Warning Beep/Voice Delay (default = Yes): (For Fire, Medical and Special sensors)

Warning Beep/Voice Delay=Yes: If this sensor triggers an alarm, there will be a 30-second warning beep from the Base Unit before the alarm report procedure starts.

Warning Beep/Voice Delay=No: There is no beep warning. The Base Unit reports the alarm immediately when there is an alarm triggered by this device.

*Alarm with Siren (default= Yes, only No for Controller): (For all devices)

Alarm Siren=Yes: The External Alarm Siren and Wireless Remote Siren will go off when there is an alarm triggered by this sensor after the Delay time passes.

Alarm Siren=No: The sirens will keep silent when there is an alarm triggered by this device.

*Bell In Disarm (default = No): (For Burglar sensor)

Bell In Disarm=Yes: In Disarm Mode, the Base Unit will issue a bell beep when receiving a trigger signal from this sensor if the "Door Bell" setting is set to "ON".

Bell In Disarm=No: Doorbell beep will not sound when receiving a trigger signal from this sensor.

Suggestion: This state should be switched on for the Door Magnet sensors on the front and back doors.

Note: The "Door Bell" must also be turned on.
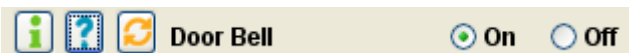
*Inactivity (default = No): (For Burglar Sensor, disabled in "Away" mode)

Inactivity=Yes: This Burglar Sensor is assigned as an **Inactivity Sensor** to monitor the activity of an elderly or physically challenged person. If no activity has been detected during the preset

Inactivity Time (refer to **Inactivity Time**), the **Inactivity Alarm** (medical) will be issued.

Note: "Inactivity" function will be disabled in "Away" mode automatically and will issue alarm   if the Inactivity sensor is triggered.

Inactivity=No: This is a normal Burglar Sensor.

*Supervised: (Automatically set by the sensor itself, refer to **Sensor Supervise Time**.)

    Supervised =Yes: System will check the "heartbeat" signal from this sensor.

    Supervised =No: System will not check the "heartbeat" signal from this sensor.

8.5 Special Settings for Environment Sensor:

Alarm High Limit/Alarm Low Limit: Set the High/Low alarm limits for the sensors with readings, like temperature sensor. (please refer to **the manual of the Sensor.**)

    Ex: Reading above 35 will trigger "High Limit Alarm", Reading below "10" will issue "Low Limit Alarm". Empty value will not trigger any alarm.

Control (High Limit/Low Limit):

    High Limit: For the control of **cooler type device**, it means when the reading is above the

"Control High Limit" then the corresponding switches will turn on and when the reading is below the "Control Low Limit" the corresponding switches will turn off.

Low Limit: For the control of **heater type device**, it means when the reading is below the "Control Low Limit" then the corresponding switches will turn on and when the reading is above the "Control High Limit" the corresponding switches will turn off.

Control High Limit/Control Low Limit: Set the High/Low limits for the control of the corresponding switches. Empty value will not activate any switches.

8.6 Wire Sensor Input Settings

Trigger Open/Close (default, Trigger = Close):

    Alarm will be triggered by close (grounded) or open (>3V) the sensor input contact (or voltage).

Away Open/Close (default, Away = Close): (For Wire Sensor input assigned as a Controller only)

    System will enter Away or Disarm Mode by close (grounded) or open (>3V) the sensor input contact (or voltage).

8.7 Switch On When Triggered: Select the switches that will be activated when this sensor is triggered.

Note: Switch #16 is not allowed for this purpose as this switch has been assigned as the indicator of the Arm/ Disarm Status. **(refer to 8.9, #16 SW Assignment.)**

X-10 Switch

As many as 15 X-10 switches and 8 RF smart sockets can be controlled by each system. For settings of the X-10 switches, refer to the instructions of the X-10 device manual. Only switch 1 to switch 8 can be assigned as RF switches.

Note: For a **Remote Controller**, if you press the DISARM button in DISARM Mode, the switches that have been assigned as active switches will be turned ON or OFF alternatively.

8.8 MISC. Settings

* Deny Arm If Not Ready: (default, No)

If set "yes" then **s**ystem will not enter into "Away" or "Home" Mode if not all the
Door/window Magnet s are closed.
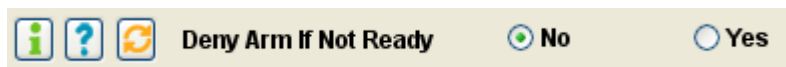
**Note: If "Away" or "Home" control is remotely issued by command from HyperSecureLink,
App. , or Cloud then system will not care about this setting and enter the Arm Mode
immediately.**

*RF Jamming Warning: (default, Disable) Enable or disable the RF jamming warning.
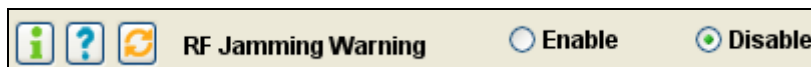
*Reset To Factory Default:

All the settings in the Base Unit will be returned to factory default.

*Inactivity Function: (default, Disable)

Inactivity Enable with time (0-72 hours):

    1, Treats the Inactivity signal from the Wireless Medical Button as a Medical Alarm.
      (The Medical Button will send Inactivity signal if no activity has been detected in 12 hours.)
    2, If no activity has been detected during this time from any Inactivity Sensor (please refer to
      8.4 Device Status Setting-Inactivity) the system will issue the Inactivity Medical Alarm
      (with zone number as **00-06**).

Inactivity Disable: Ignore the Inactivity signal from the Wireless Medical Button and don't
    check the Inactivity Timer.
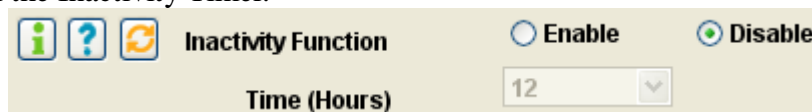
*#16 SW Assignment: (default, ARM=ON): Set the #16 switch as an Arm/Disarm status indicator.

    Arm= On: The #16 switch will be turned on in **Away and Home** Mode.

    Disarm= On: The #16 switch will be turned on in **Disarm and Monitor** Mode.
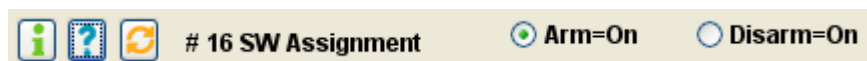
* X-10 House Code <A-P>: (default <A>)

      This code should be the same as the House Code set on the X-10 switches, user can select
      from A to P.

8.9 CMS Settings: LS-20 can report to two CMS phone numbers and TCP/IP CMS/Server.

> For the user to subscribe the CMS/Cloud services please consult with the service provider first.

* CMS User Account Number:

> The user account (8 digits Max.) number for CMS IP Alarm Report.

CMS User Account No.   12345678

* **Mode Change Report: Enable /Disable (default=Disable, for phone number CMS only.)**

Mode Change Report Enable: The LS-20 will report to the CMS phone number if the operation mode (Away/Home/Disarm) has been changed.

* Auto Link Check Period: Disable to 30 days. (default = Disable, for phone number CMS only.)

The LS-20 will send a Loop Check signal to the CMS phone number periodically.

* 2 Way Audio: Enable/Disable (default=Disable, for phone number CMS only.)

2 Way Audio ON: The Base Unit will enter into 2-way voice communication mode after sending the alarm report to the CMS.

(This function only works with a digital receiver using Contact ID and has 2-way voice capability.)

* CMS Report: (default, Report One)

Report All: Report to CMS1, CMS2 and Internet service centers.
Report One: Stop further CMS report if any one of the above reports is successful.

* TCP/IP Alarm Report (default=no)
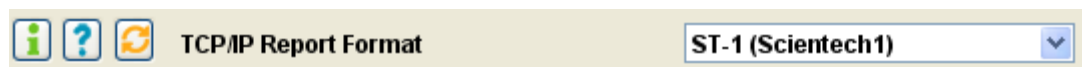
TCP/IP Alarm Report   ○ Yes   ⊙ No

TCP/IP Alarm Report = Yes: If there is no acknowledgement from the CMS or Cloud server within 30 seconds after the alarm issued then the alarm report will be resent max. for 3 times.
> **Note: Since robust TCP/IP protocol is used in alarm data transmission, the fail of transmission is almost impossible.**

*TCP/IP Report Format

TCP/IP Report Format   ST-1 (Scientech1) ▾

The data format used for reporting to the Cloud Server or Internet CMS Server. Please check with your service provider first. When you connect the LS-20 to the server, most of the service providers will set this parameter automatically.

8.10 Scheduling.

> *Auto Switch: In every weekday user can program the On/Off time for each switches, total 20
> items can be assigned. (Please refer to 7.6)

> *Auto Operation: In every weekday user can program the Arm/Disarm time for the system, total
> 20 items can be assigned.

*Switch Scene: 8 switch scenes can be set and controlled by KP-3S Keypad.
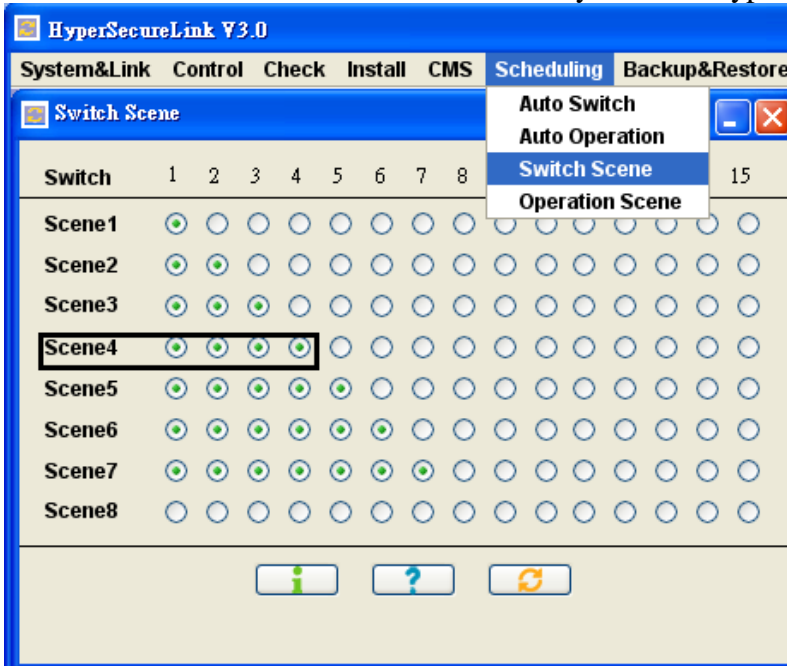
Ex.: If Scene 4 is selected by KP-3S then switch 1 to 4 will be turned on.

*Operation Scene: 8 operation scenes can be set and controlled by KP-3S Keypad
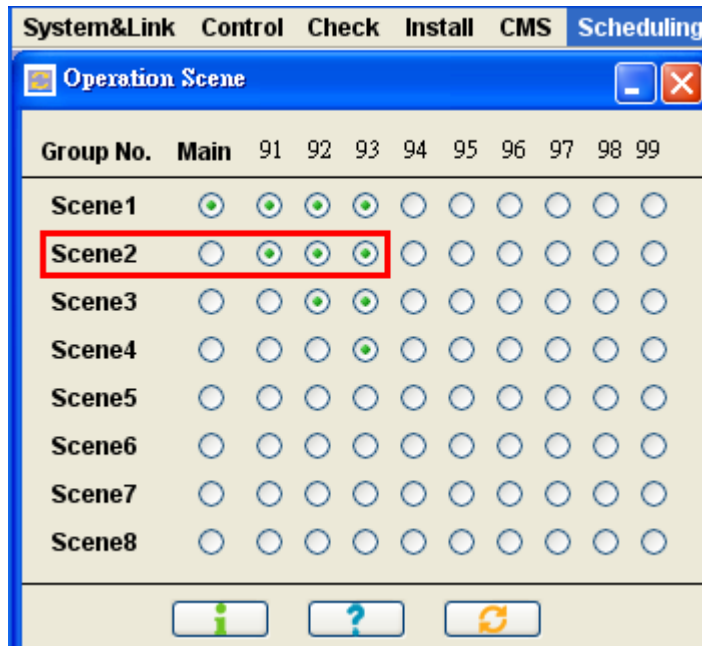
Ex.: If Scene 2 is selected by KP-3S then Partial Zone 91, 92, 93 will enter into "Away Mode".

SPECIFICATIONS

Input Power: 7V DC or Micro USB input.

Standby Current: About 280mA (LS-20E), 320mA (LS-20EG)

RF : (Follows local regulations, other frequencies as requested)

    Receiving Frequency: 915MHz (For FCC), 868MHz (For CE), 433MHz.

    Transmission Frequency: 433MHz

    Data Modulation: OOK (On Off Key).

    Power: less than 10mW.

    Range: about 100m to 300m or more @open field, 25℃ (Depends on sensors and Hardware version).

Receiver Type: super heterodyne.

RF Security Code: 16,777,216 combinations with check sum for each type of sensors.

                More than 4 billion combinations in total.

Communication Link: Ethernet, wifi (Option), GSM (Option), GPRS (Option).

Event Log: max. 512 records.

Display: 4 LEDs (Away/Home/Disarm/Data).

Sensor Zones: total 288 zones. (Burglar zones x 128, Fire zones x 64, Controller zones x 32,

                          Medical zones x 32, Special sensor zones x 32)

Power: NiMH rechargeable battery, back-up time 6~16 hours depends on battery capacity.

Delay Activation Time: 0- 255 seconds programmable.

Digital Interfaces : micro USB socket.

Internet Interface: RJ45, wifi (Option), GPRS (Option).

Automation Switch control: RJ11 6-pin

      Control of 16 units X-10 switches or (XRM-01) Relay Modules.

Wireless Socket: SW#1~SW#8.

Internal siren for Alarm warning.

Internet CMS protocol: Proprietary Scientech Protocol (ST-I, ST-II), CSV and SIA ADM-CID (2007) IP

      Alarm protocol.

Wire Sensor Input: x3 can be assigned as Panic, Burglar, Fire, Medical, Tamper or Controller.

Alarm Out: Open collector transistor output with 10 Ohm protection resistor, for 5V external siren or

      other alarm device, 300mA max.

Clock Accuracy: within 5 seconds daily.

Operation Temp.: -10℃~40℃.

Storage Temp.: -20℃~55℃.

Humidity: 10-95%RH.

Size: 203x120x48 mm. (Main body)

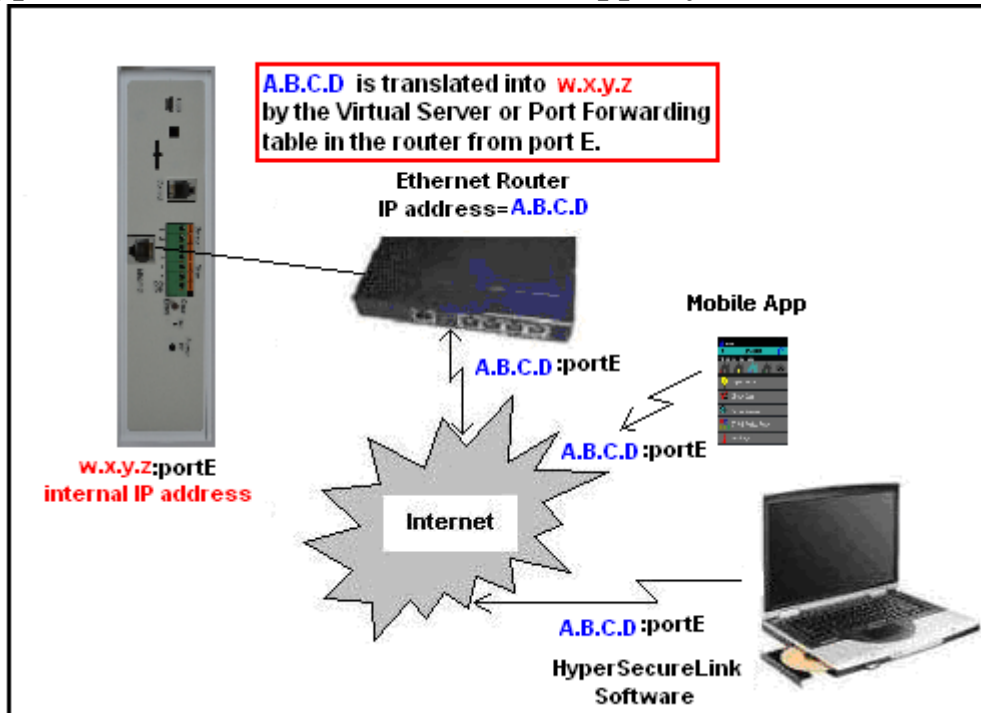Weight: about 550 g. (Main body)

      (The manufacturer reserves the right to change the specifications without prior notice)

Appendix A: Ethernet Interface Settings

Ethernet Interface can be configured as a server to be accessed remotely by the proprietary HyperSecureLink software or mobile App MyHome. It also can be configured as a client to send poll/alarm signal to a web server or CMS (Central Monitoring Station) service provider.

A1, System connection diagram for LS-20 as a server to be accessed by the HyperSecureLink Software or mobile App MyHome from Internet.
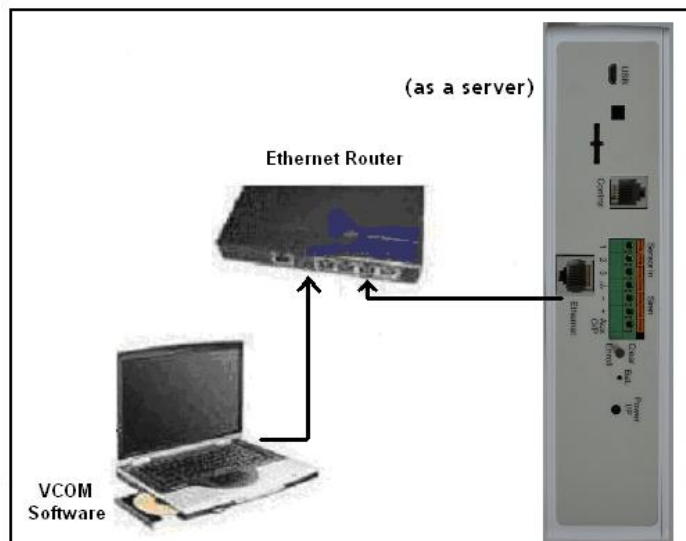

Note: Mobile App MyHome is from third parties and are not free, please refer to the web sites:

https://play.google.com/store/apps/details?id=com.uioo.uioomyhome

https://itunes.apple.com/app/id946734736

A1.1, Ethernet Interface sets up as a server.

Connect the devices as below, please make sure you have installed the **VCOM** software in your PC first.

A1.2, Configure the Router.

The following example is for Fixed IP address application. But if you have no Fixed IP address then you can apply some free DDNS service from the internet.

For example D-Link provides free DDNS service for their routers.

http://support.dlink.com/emulators/wbr2310/tools_ddns.htm

Enter the setup menu of your Ethernet Router and find the setting of **Virtual Server.**

Select a proper internal IP address and corresponding port number for the TCP/IP communication protocol.

Ex: The internal IP address of **192.168.0.90** and port number **1690** is assigned in the Virtual Server table.
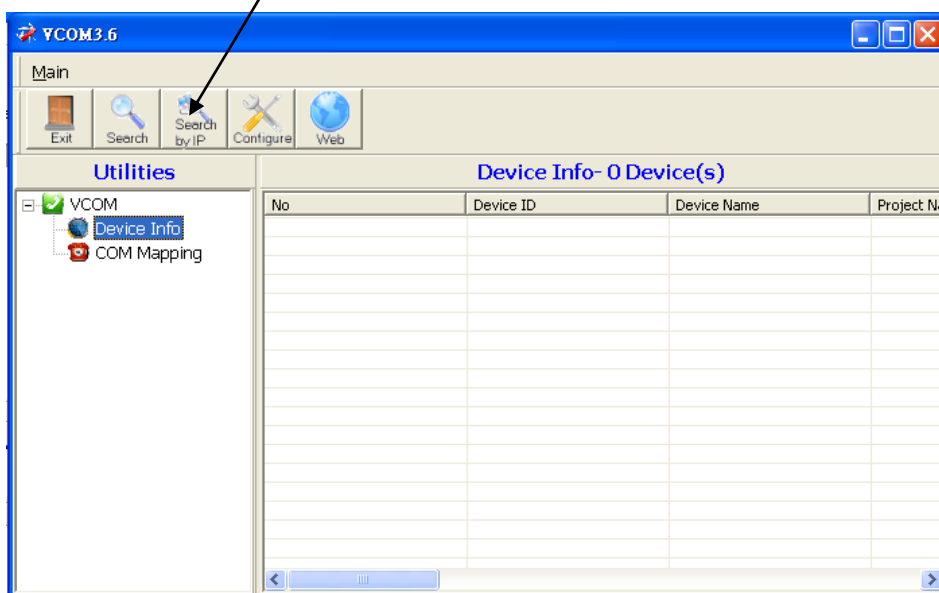
(This IP address and port number will be used to communicate with the LS-20 by HyperSecureLink program or mobile Apps.)
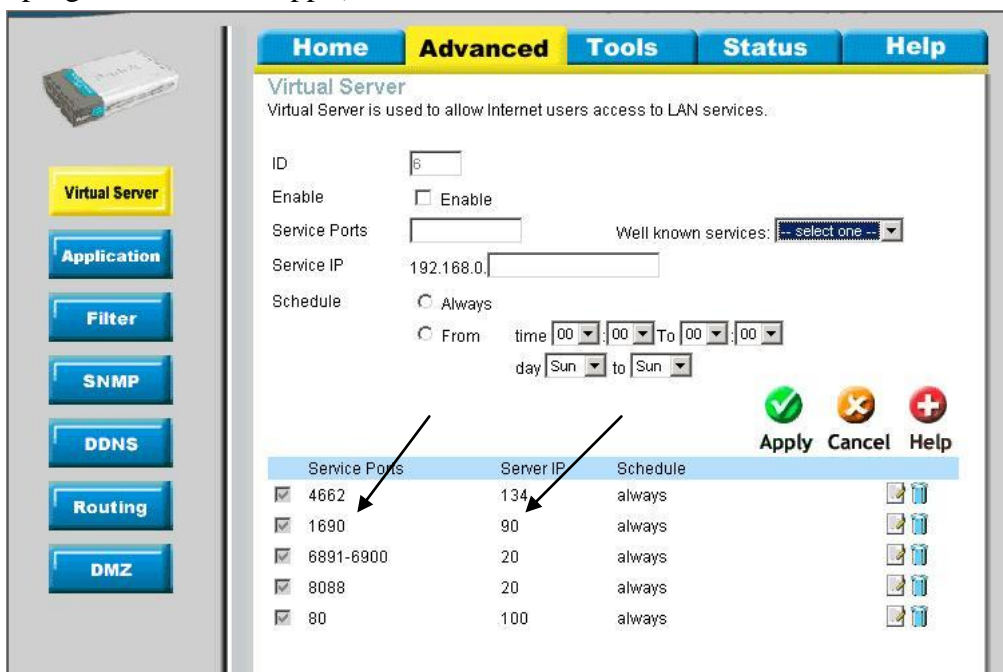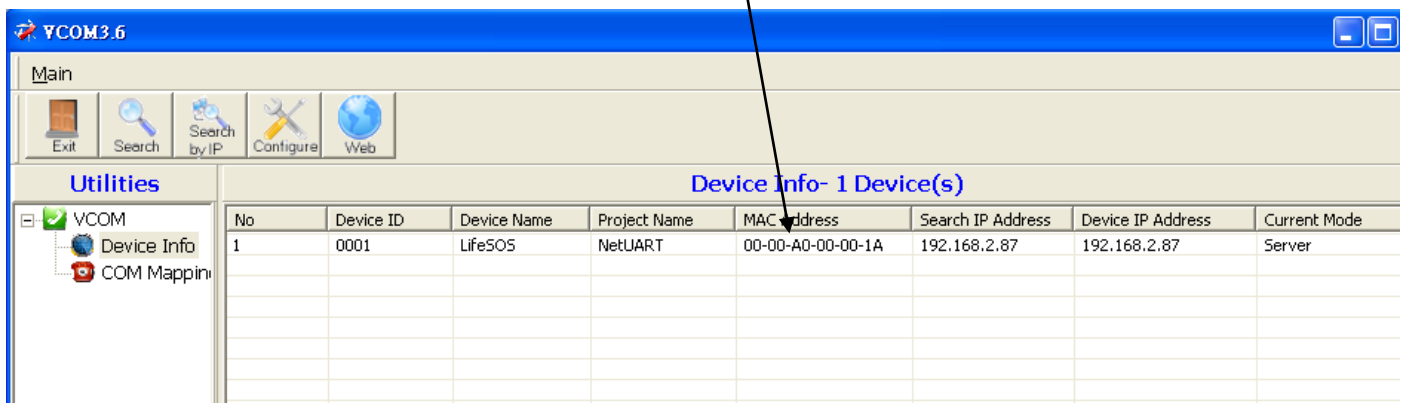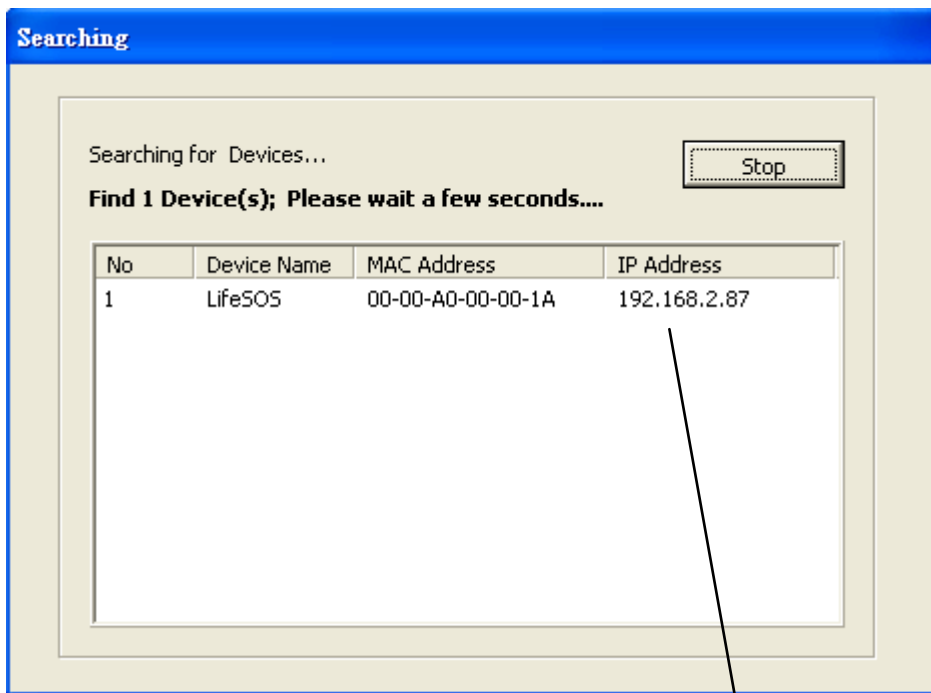
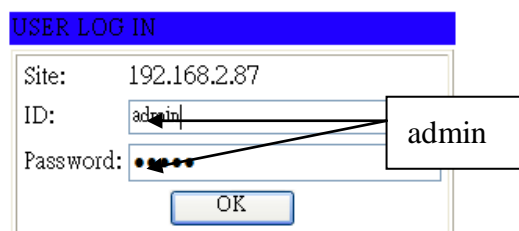## A1.3, Configure the Ethernet Adaptor
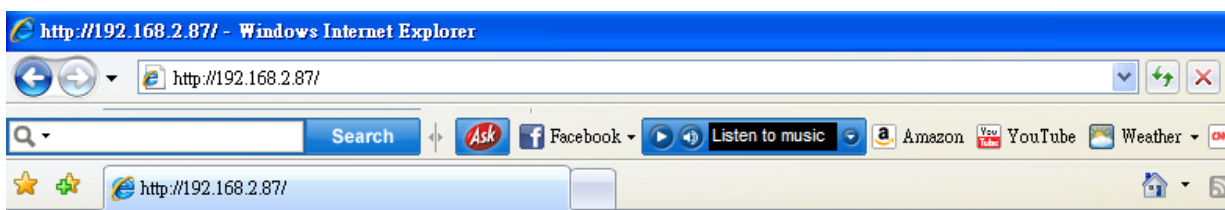
* RUN the VCOM program on your PC**.**

Click the Search

* The **VCOM** software searches in the network for the LS-20 Ethernet Interface and shows the findings on the screen.

* Open the Internet browser you are using and enter the IP address.

* Enter User Name and Password. (Default User Name: **admin**, default Password: **admin.**

* The setup menu of **Administrator Setting** will be shown on the screen and change the parameters according to your network environment.

Nickname: Name or location of the system.

IP Address: As the setting of the Virtual Server in the Ethernet Router.

Subnet mask: 255.255.255.0

**Gateway**: Please enter the gateway address of your Ethernet Router.

DNS: Please get this address information from your ISP.

IP Configure: To operate as a server, Static must be selected

Password Setting: Enter new User Name and Password.

Note: If you change the User Name and Password, please make sure that you write them down on a paper otherwise if you forget the new User Name and Password then this adaptor will not be accessed any more.

* If any of the settings has been changed then double click the Update to update the settings.
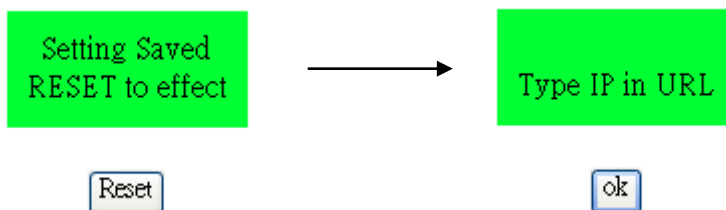
Then Click the Reset to save the settings.

If the IP address has been changed then enter the new IP address and User Name/ Password to access the Ethernet Adaptor setup web page again.

(You can use VCOM software to locate the new IP address.)

* Select **TCP Mode** and change the settings according to your network environment:

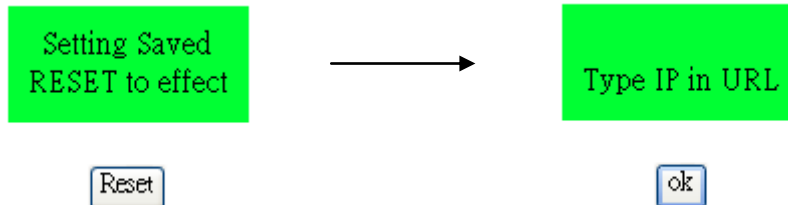Telnet Server/Client: Select **Server**.

Port Number: As the setting of the Virtual Server in the Ethernet Router.

Remote server IP Address: Don't care.

Client mode inactive timeout: 20 minutes (default).

Server mode protect timeout: 60 minutes (default).

* If any of the settings has been changed then double click the Update to update the settings.

Then Click the Reset to save the settings.

* Select **UART** to check if the settings are the same as below.

Mode: RS-232.

Baudrate: 9600.

Character Bits: 8.
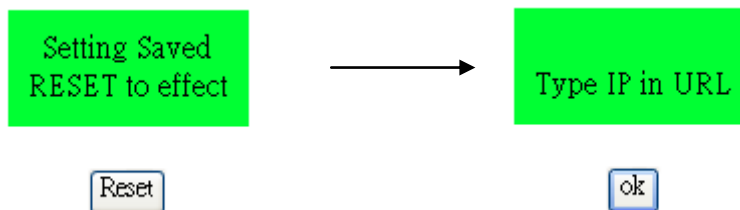
Parity Type: None

Stop Bit: 1.

Hardware Flow Control: None.

Delimiter: No need

* If any of the settings has been changed then double click the Update to update the settings.


Then Click the Reset to save the settings.

● **The setting is completed here.**

About the **HyperSecureLink** software please refer to the **HyperSecureLink user guide.**

A2, System connection diagram for LS-20 as a client to send signal to a cloud server or Central Monitoring Station through Internet.

(This setting is only valid for the user who has CMS or cloud services. User has to know the IP address and port number of the CMS or cloud server before setting the Adaptor.)
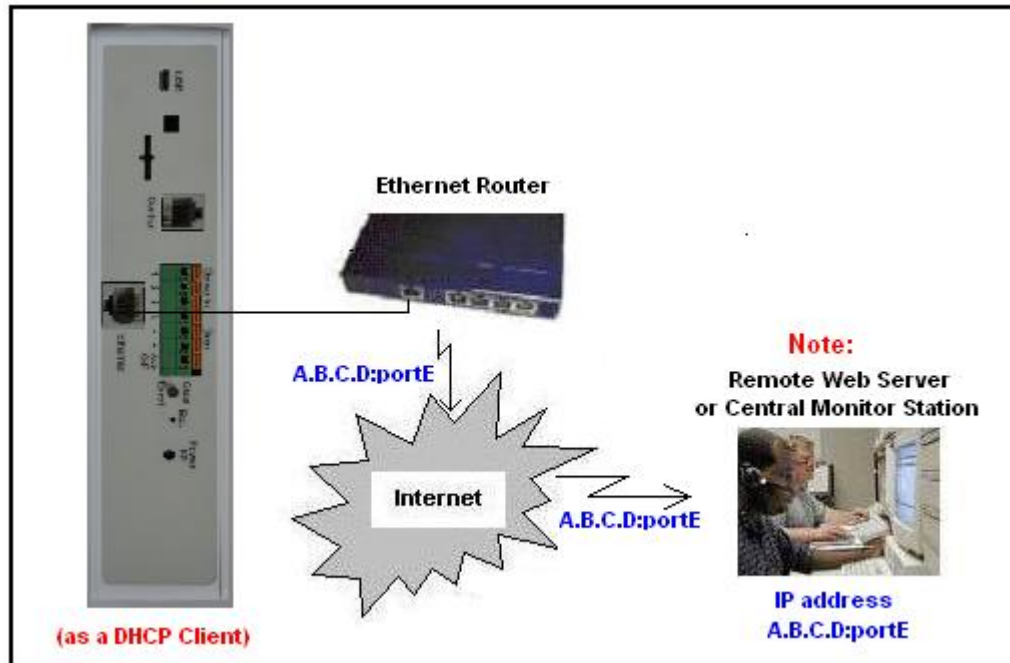
Note: For the cloud services or Central Monitor Station please refer to web sites:

Cloud Services: www.livingpattern.co or www.abell-security.com

Central Monitor Station: www.iklomp.com

A2.1, Ethernet Adaptor sets up as a client.

Connect the devices as below, please make sure you have installed the **VCOM** software in your PC first.
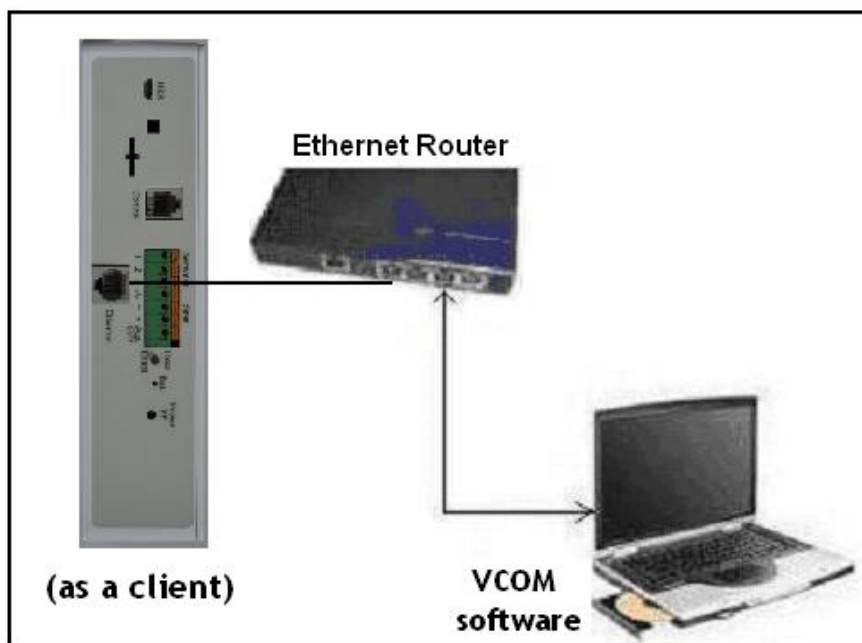
A2.2, Configure the Ethernet Adaptor

* RUN the VCOM program on your PC, check "Device Info"**.**

Click the Search

* The **VCOM** software searches in the network for the LS-20 Ethernet Interface and shows the findings on the screen.
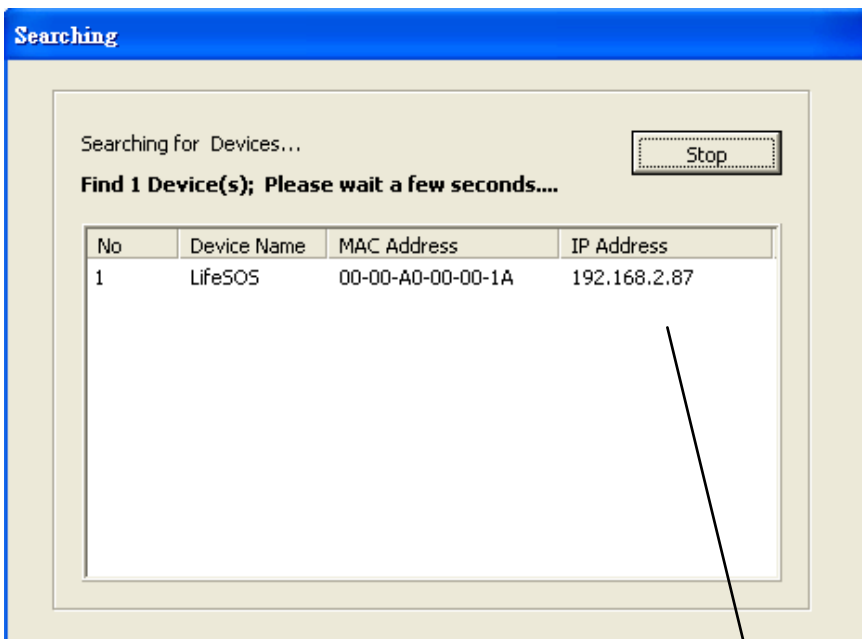
* Open the Internet browser you are using and enter the IP address.
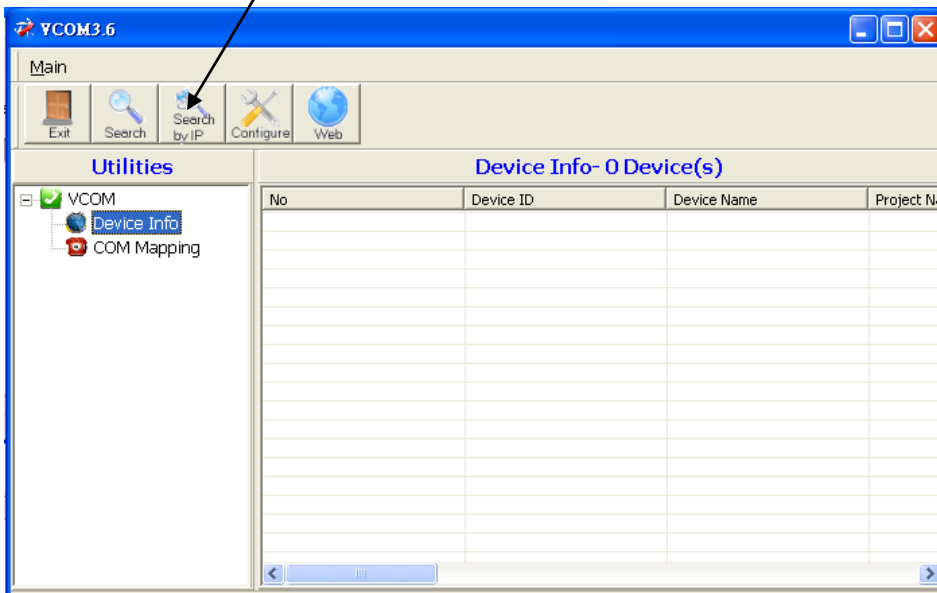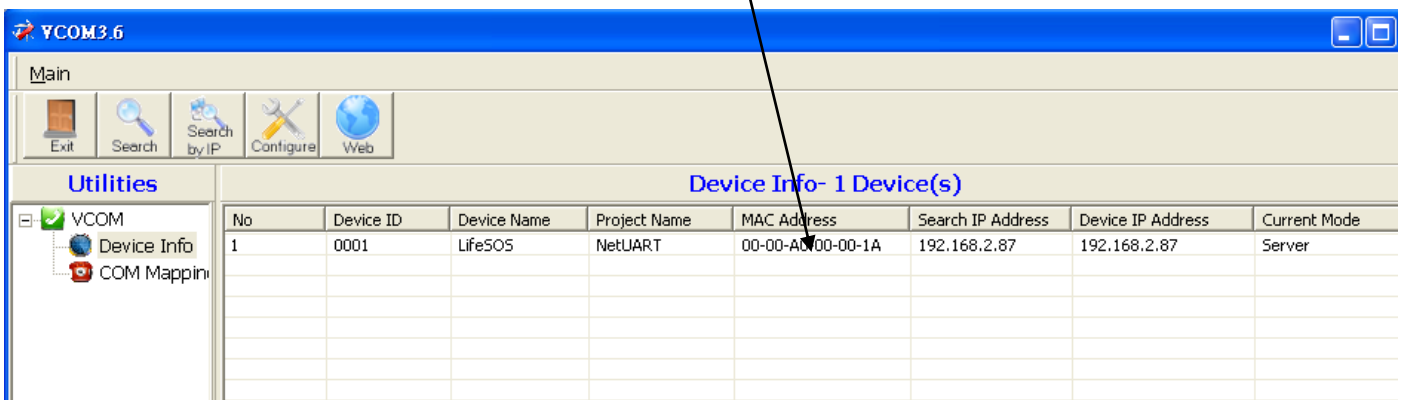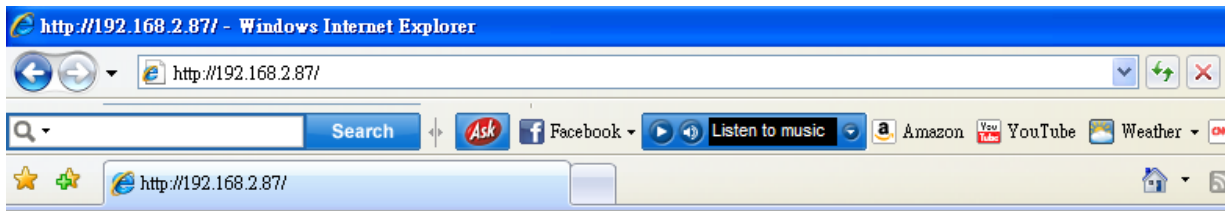

*   Enter User Name and Password.

    (Default User Name: **admin**, default Password: **admin.**

*   The setup menu of **Administrator Setting** will be shown on the screen and change the "IP Configure" to "DHCP".

Nickname: Name or location of the system.

IP Address: Don't care

Subnet mask: 255.255.255.0

Gateway: Don't care.

DNS: Don't care.

IP Configure: To operate as a client, **DHCP** must be selected

Password Setting: Enter new User Name and Password.

Note: If you change the User Name and Password, please make sure that you write them down on a paper otherwise if you forget the new User Name and Password then this adaptor will not be accessable any more.
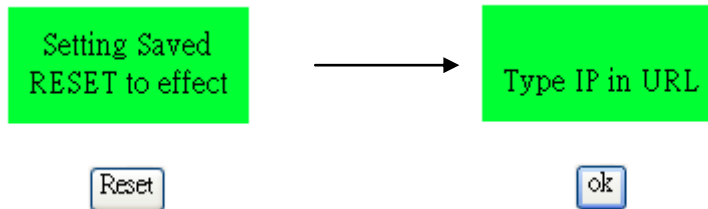
* If any of the settings has been changed then double click the **Update** to update the settings.

Then Click the Reset to save the settings.

Use VCOM software to locate the new IP address and enter the Ethernet Interface setup web page again.
* Select **TCP Mode** and change the settings according to the information from the web server or CMS service provider.

Telnet

Server/Client: Select **Client**.

Port Number: Please check with your web server or CMS service provider for this information.

Remote server IP Address: Please check with your web server or CMS service provider for this information, either IP address or domain name.

Client mode inactive timeout: 20 minutes (default).

Server mode protect timeout: 60 minutes (default).

* Double click the **Update** to update the settings.

Then Click the Reset to save the settings.

* Select **UART** to check if the settings are the same as below.

Mode: RS-232.

Baudrate: 9600.

Character Bits: 8.

Parity Type: None

Stop Bit: 1.

Hardware Flow Control: None.

Delimiter: No need

* If any of the settings has been changed then double click the Update to update the settings.

Then Click the Reset to save the settings.

● The setting is completed here and check with your web server or CMS service provider if they can receive the report from your system.

Appendix B: Wifi Interface Settings

> Location of the LS-20
>
> Since the wifi Interface needs to communicate with your wifi router, please locate the LS-20 near your wifi router to keep good signal quality.

B1, Search all the wifi networks in your environment from PC, tablet or mobile phone. You will find a network SSID as " **lifesosxxxxx**".

Connect to this wifi network by the Password of "**12345678**".

> Note: wifi Interface only can be connected to one browser, if you can see the SSID but can't connect to it then check if it has been connected to other device.
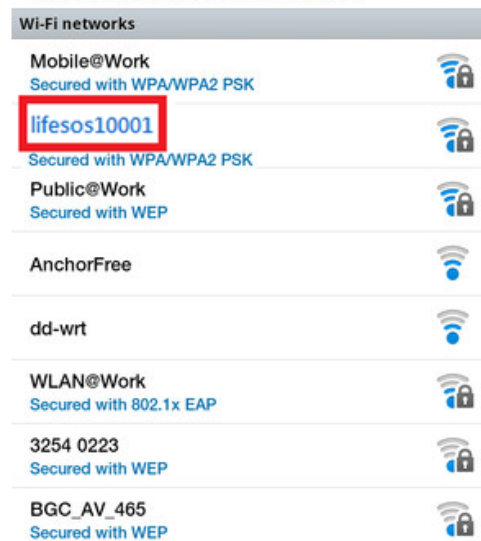
B2, You can run the command prompt "cmd.exe" on your PC and enter "ipconfig" to find the Gateway address of the wifi Interface is "10.10.100.254".

B3, Open the browser and enter http://**10.10.100.254**

Use **admin/admin** to enter the wifi Adaptor setting web page.
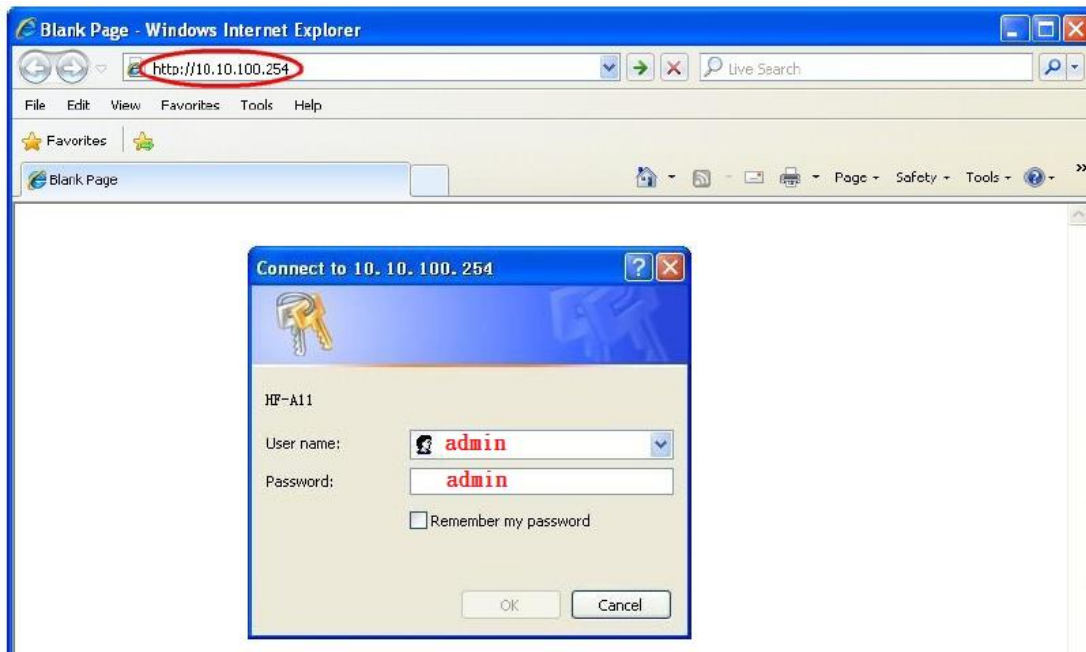
Note: If you change any setting below, only "Restart" the wifi Adaptor after all the changes of the setting had been saved.

B4, Skip this Setting.
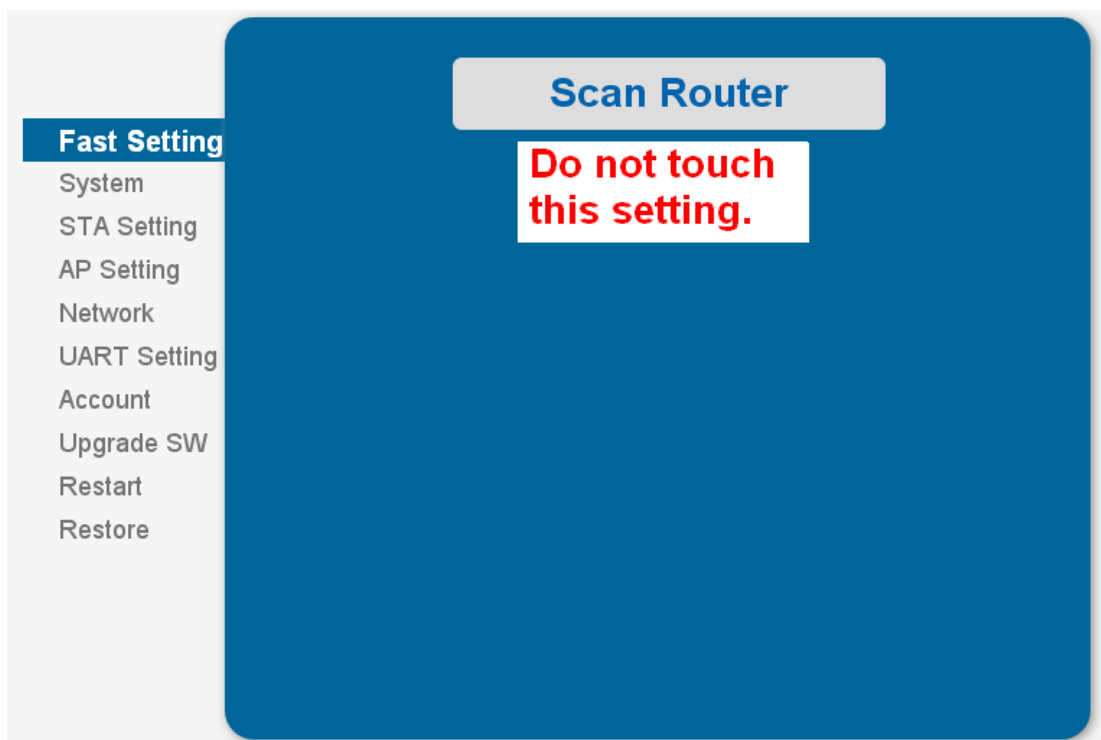
B5, Click "System" to show the settings in the wifi Adaptor.

B6, Click "STA Setting", it should be like the screenshot below, otherwise change the settings then click "Scan".

Select your router and enter the parameters needed for the wifi Adaptor to connect to your router then click "Save".

Do not click "Restart"

B7, Click "AP Setting", it should be the same as the screenshot below, otherwise change the setting as below then click "Save".
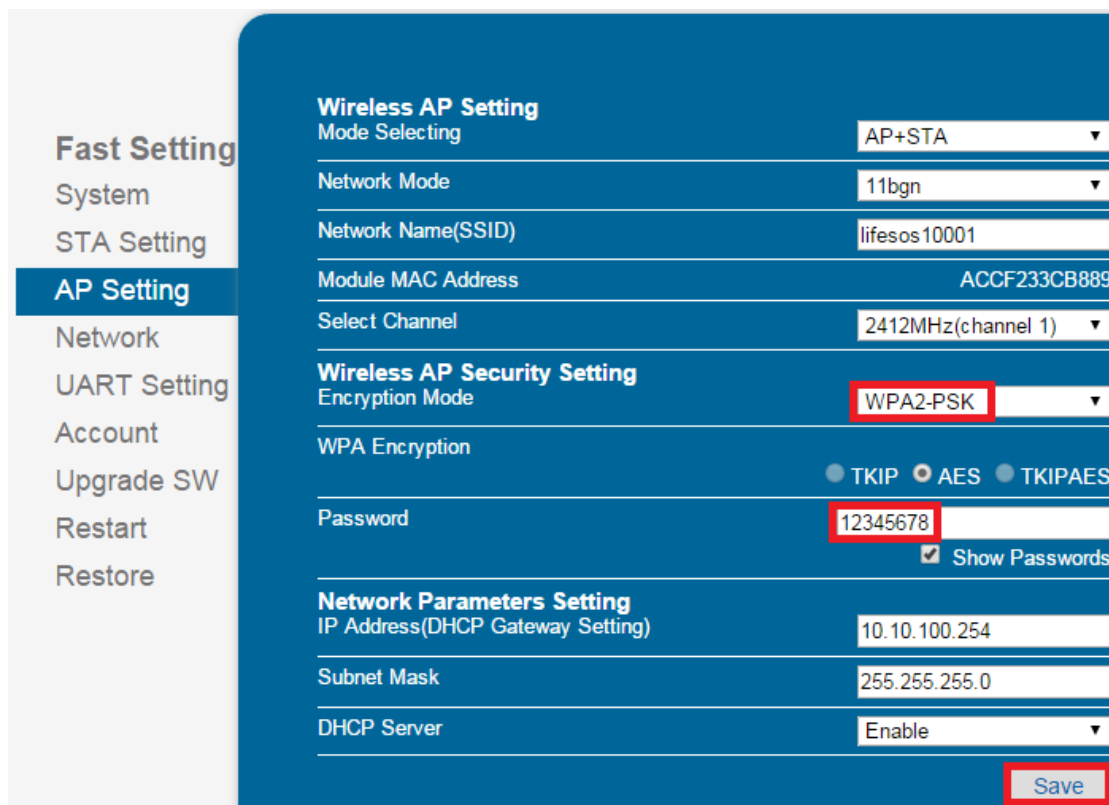
B8, Click "Network", select the protocol and set the Port ID number and Server Address as required then click "Save".

Below example is for the linking to "Livingpattern" cloud services.

TCP-Server: To work with HyperSecureLink software or MyHome App, only port ID is needed.

TCP-Client: To link to Cloud server like Livingpattern or Webehome, both Port ID and Server Address are needed.

B9, Click "UART" Setting, it should be the same as the screenshot below, otherwise change the setting as below then click "save" and then click **"Restart".**

B10, After successfully restart the wifi Adaptor don't forget to restore the wifi setting on your PC or tablet back to your router.

If you can't access the system from cloud after changing any parameter, please wait for about 10 minutes for the server to locate the new connection socket from the system again.

Appendix C: The GSM/GPRS setting in LS-20EG/LS-20GV

The GSM module in LS-20EG/LS-20GV can work in either GSM mode or GPRS mode upon request, but you need to specify when you place the order.

C1, Work in GSM mode

    C1.1 Turn off the PIN code of the SIM card on other mobile phone before using it in LS-20EG/LS-20GV.

    C1.2 Disconnect the power adaptor and use a straightened paper clip to stick in the hole of "Bat." to turn off the backup battery.

    C1.3 Insert the SIM card to the slot then turn on LS-20EG/LS-20GV power.

        SIM card slot

    C1.4 Connect the LS-20EG/LS-20GV USB port to your PC, use supplied HyperSecureLink software to set GSM and/or PSTN numbers at GSM phone No. 1~ 5. In addition, you can enter text in the GSM ID for easier identification when the SMS is received.
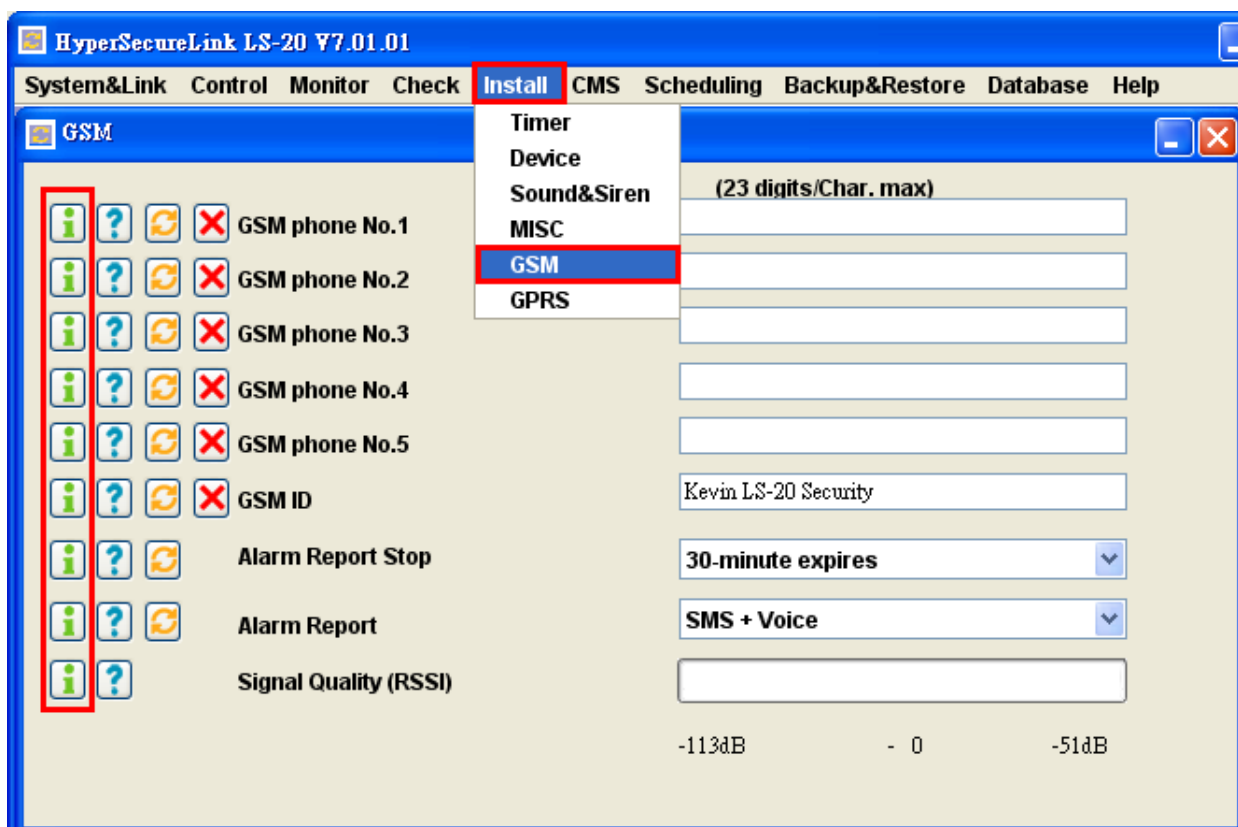
      Note: User will not receive the SMS message if the PSTN phone number is entered.

* Alarm Report Stop: (default, 30-minute expires)

[i] [?] [↻] **Alarm Report Stop**	30-minute expires ▼
	30-minute expires
	Made Successful CMS Report
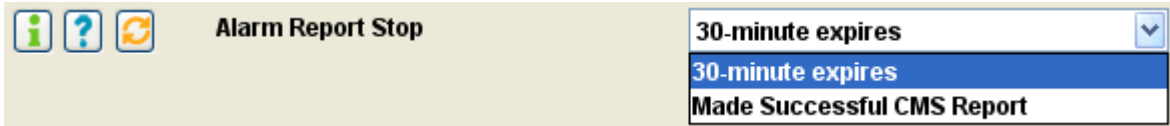
User can select when the GSM calls should stop, either 30 minutes expired or the CMS calls were successfully made if the system connects to CMS also. (Please refer to the CMS settings.)

* Alarm Report: (default SMS+Voice)

[i] [?] [↻] **Alarm Report**	SMS + Voice ▼
	SMS + Voice
	SMS only
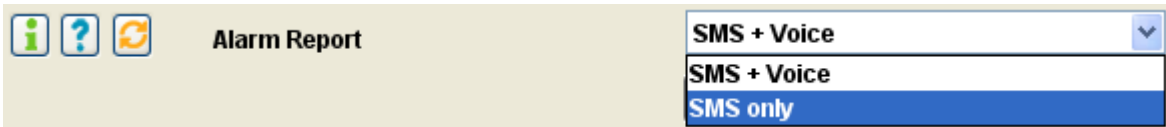
User can select the GSM calls are SMS plus Voice Call or send SMS only.

Note: To select SMS+Voice, LS-20 will sends all SMS messages first then dial the voice call one by one.

You can click the [i] icon to see the explanations; as the screen shots below.

The explanation of "GSM phone No.1"
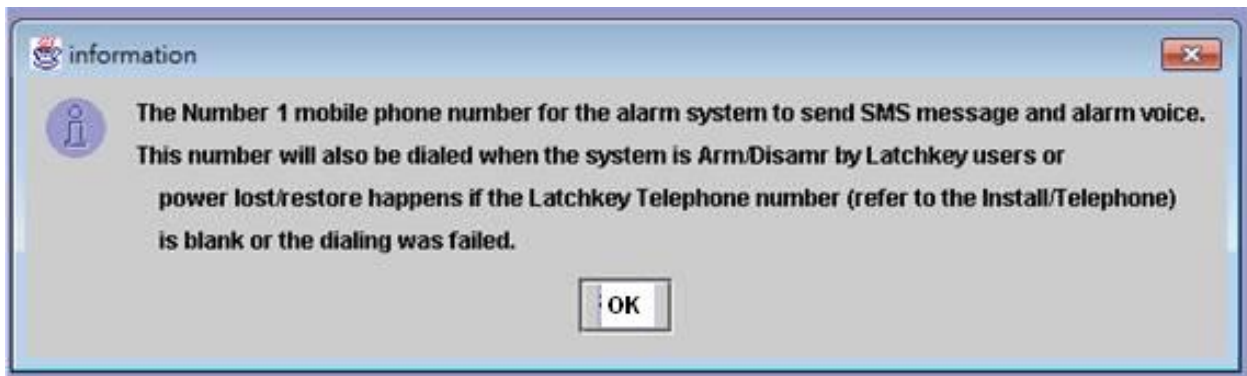
The explanation of "GSM ID"
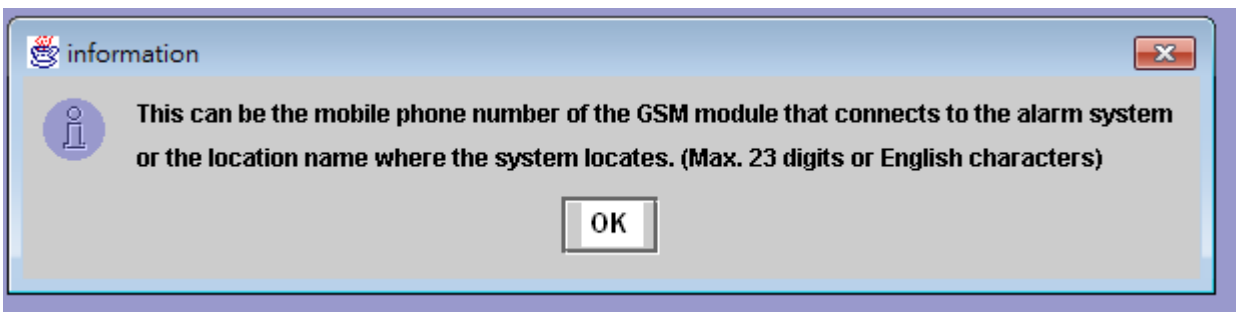
C1.5 To record the voice that will be heard in the voice call. After click the icon, please keep about 20 cm away from LS-20EG/LS-20GV microphone and speak clearly.

Likewise, you can click the to show the explanation and examples as below.
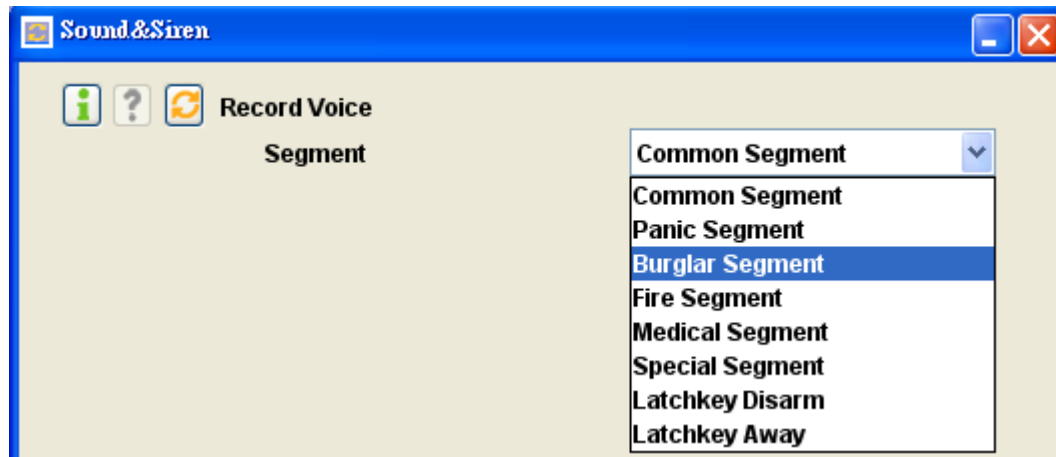
explanation and examples as below.
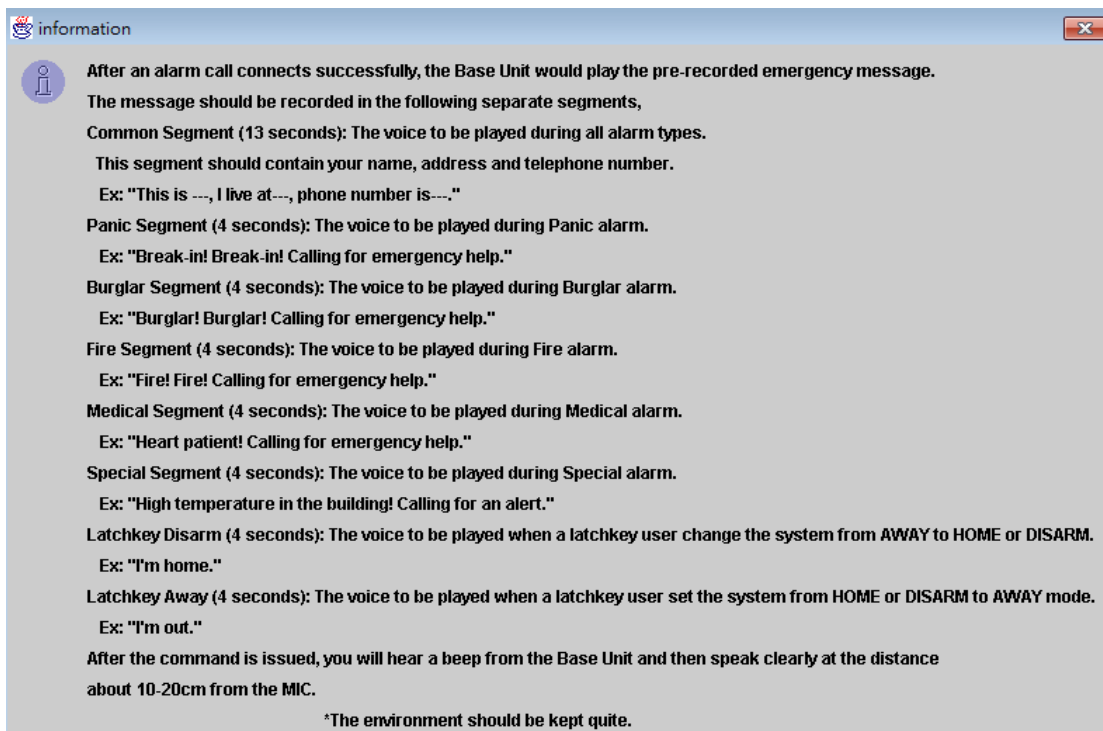
Note: after setting is completed, the USB cable has to be removed from the base unit; otherwise, the LS-20EG/LS-20GV can't connect to the cloud server.

C 1.6 How to answer alarm call from LS-20.

When you receive a call from LS-20, you can follow the procedures below to communicate with the system.

● You will hear the prerecorded message twice, which tells you what event happened to the system.
● After the announcement, the LS-20 enters into monitoring and 2-way half-duplex communication mode for 60 seconds. You can hear any sound picked up by the microphone on the Base Unit or talk to the people inside the house. During these 60 seconds, you can also control the system by pressing specific key on mobile/telephone keypad.
● If you don't press any key during this period, the first 30 seconds will be listen-only and then -after two beeps- the system will enter into 2-way half-duplex communication mode automatically. At 10 seconds before the call termination, one beep will be delivered to remind the receiver.

Press 0 : The system disconnects the call also stops siren immediately and stops any further dialing.
Press 1 : The system disconnects the call also stops siren immediately and dials the next number,
Press 3 : Enter into speak-only mode. (The microphone on the base unit is disabled.)
Press 8 : Enter into listen-only mode.
Press any other key: The system will extend the connection for another 60 seconds.

Note: The sound of the siren or noise from the environment may interrupt the decoding of the input key tone, so keep pressing the key until the command becomes effective.
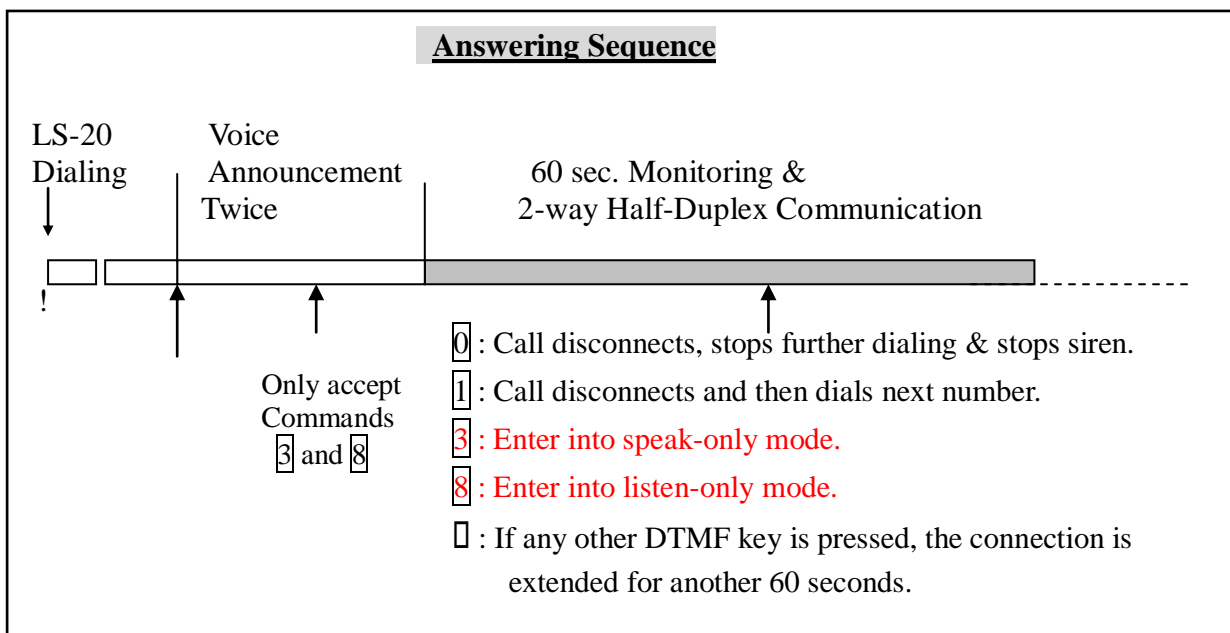
C2, Work in GPRS mode (Note: GPRS only can play the role as a "Client".)

C2.1 Turn off the PIN code of the SIM card on other mobile phone before using it in LS-20EG/LS-20GV.

C2.2 Disconnect the power adaptor and use a straightened paper clip to stick in the hole of "Bat." to turn off the backup battery

C2.3 Insert the SIM card to the slot then reconnect the power.

SIM card slot

C2.4 Connect the LS-20EG/LS-20GV USB port with USB cable to your PC; use HyperSecureLink to set GPRS APN, GPRS Remote Server IP: Port and CMS1&Server.
Note: after setting is completed, the USB cable has to be removed from the base unit; otherwise, the LS-20EG/LS-20GV can't connect to the cloud server.

C2.4.1 GPRS APN varies with the mobile operators, please consult your local mobile operators or refer to the link below
http://www.hw-group.com/products/HWg-Ares/HWg-Ares_GSM_APN_en.html
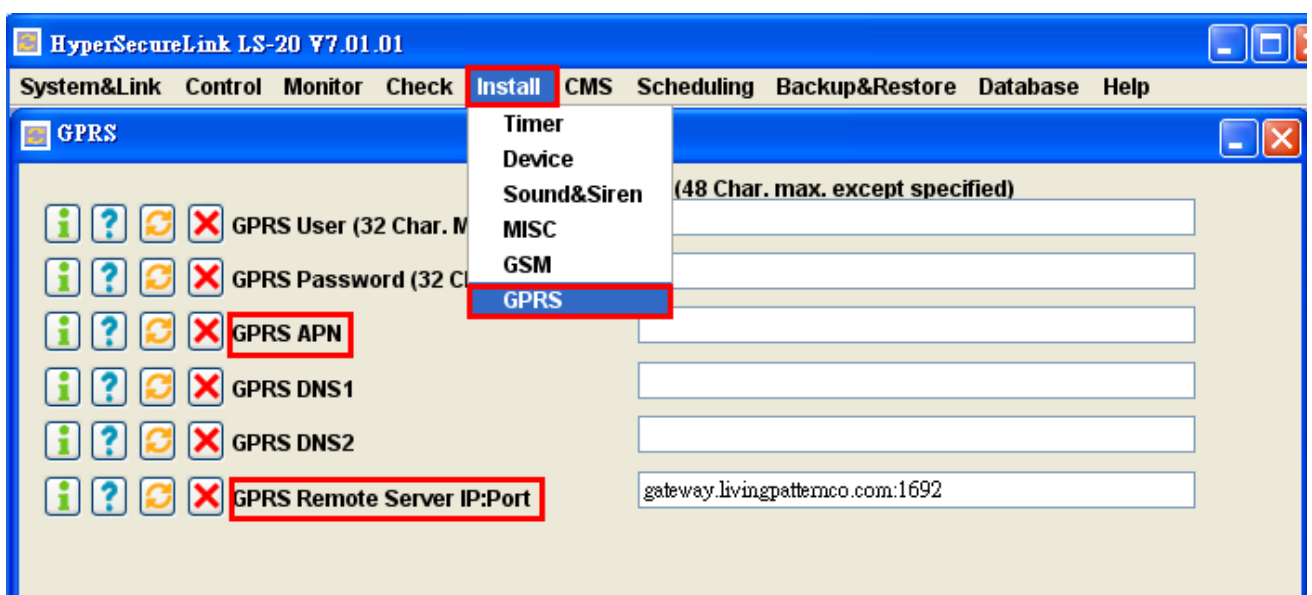
C2.4.2 Select the "CMS Report" and "TCP/IP Alarm Report" as below.
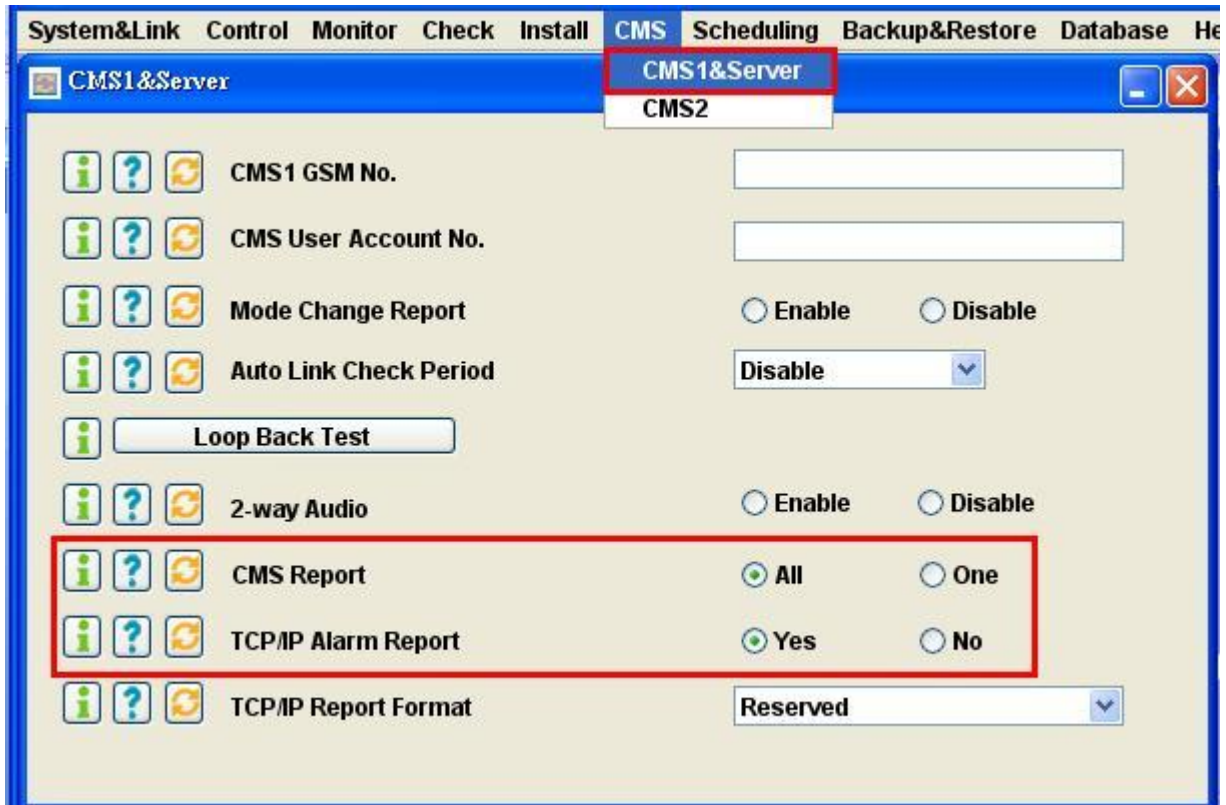
C2.5 Register the LS-20EG/ LS-20GV to the cloud server and connected the Ethernet cable. Please press "Clear" button on the base unit and open the web page of the cloud server from your PC to check if the connection to the server is successful.

C2.6 LS-20EG/LS-20GV will connect to the server through Ethernet first, if it finds the Ethernet is not working then it will switch to the GPRS channel automatically.
Switching from Ethernet to GPRS takes about 3~5 minutes depends on the network service provider, if the switching is successful then you will hear "OK" from the LS-20EG/LS-20GV.

Note: To test this switching action, just remove the Ethernet cable and wait for 3~5 minutes.

C2.7 When the LS-20EG/ LS-20GV is using GPRS to transmit data, by pressing the "Clear" button on the rear panel, it will switch from GPRS back to Ethernet.
At 00:00:00 midnight every day, the LS-20EG/LS-20GV will check if it is using GPRS service and then switch back to Ethernet to save the communication cost.

Appendix D: HyperSecureLink User Guide:

D1, Hardware Installation:

D1.1, Connect by USB cable in local setting.
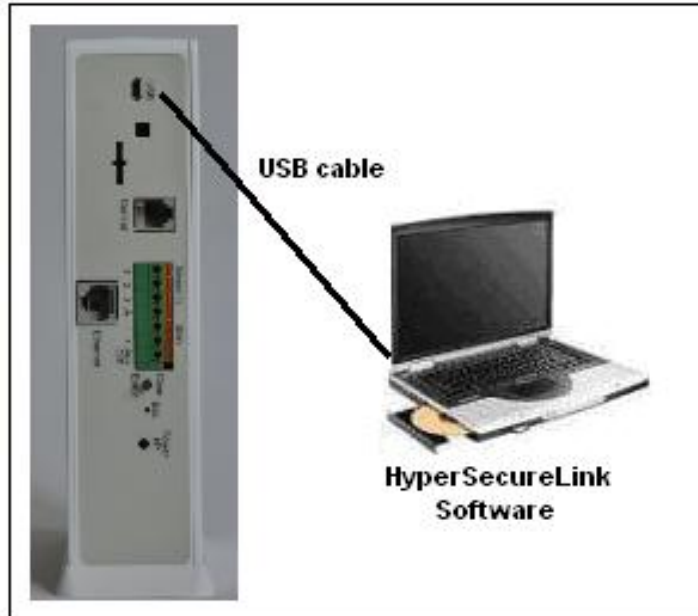
D1.2, Connection Diagram for Internet Remote Access
(For the setting of the Ethernet Interface please refer to Appendix A 1.1~1.3)
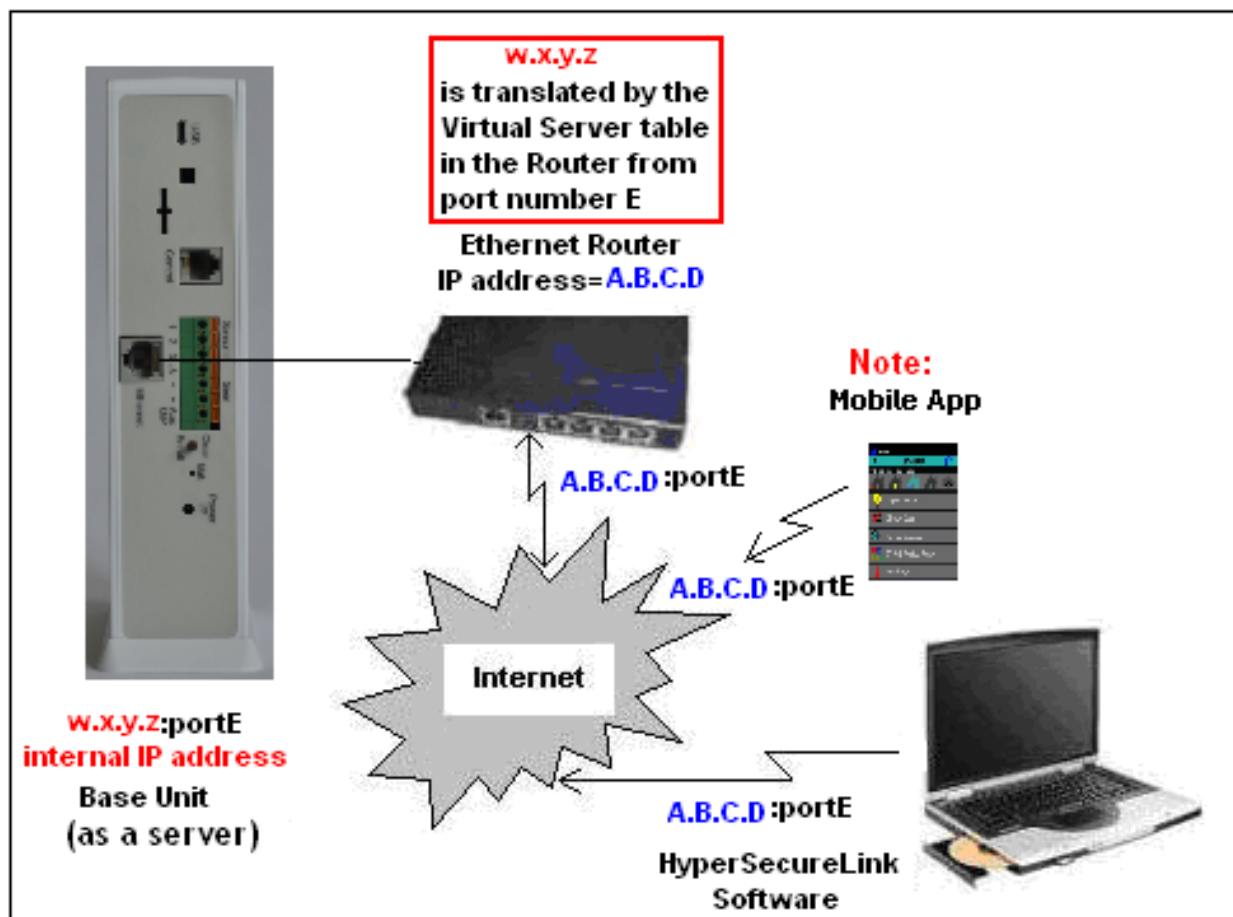
D2, Software Installation:

HyperSecureLink software can run on Windows PC or Apple Mac.
For Windows PC, please open the HyperSecureLink-winxxx-SetupFiles and run the setup file.
For Apple Mac, please open the HyperSecureLink-macxxx-SetupFiles and run the setup file.

Follow the wizard to complete the setup.
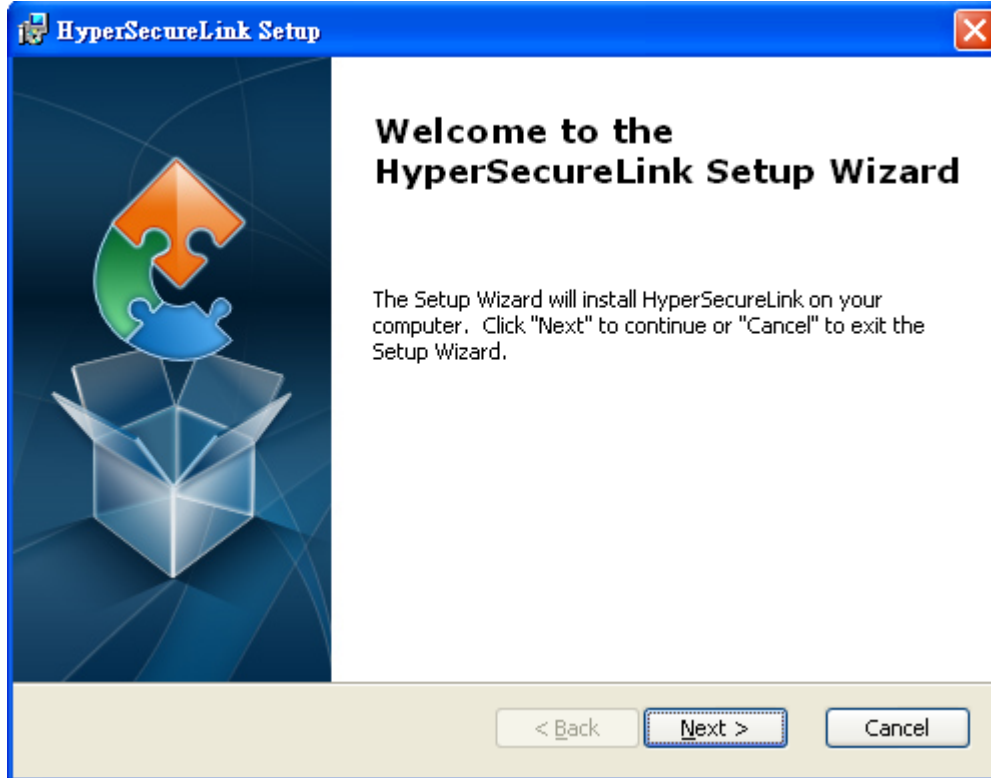
Then run the program

D3, Select Link

D3.1 Using USB interface to access the LS-20.

Select USB .
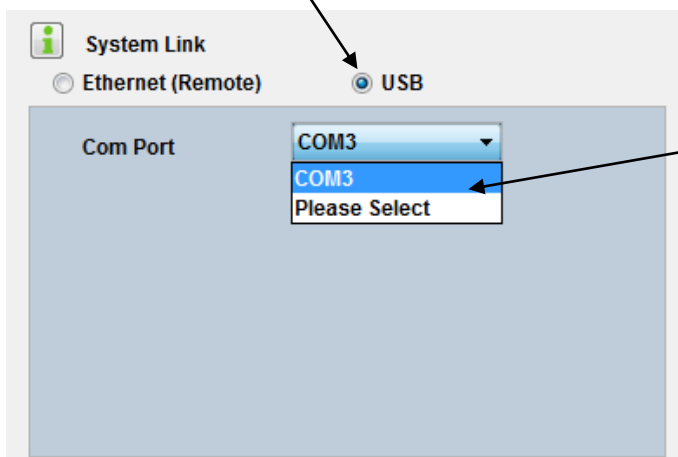
The software will scan the USB ports that are available in your PC. Select the correct one to use.

D3.2 Using Ethernet interface to access the LS-20

D3.2.1, Select Ethernet (Remote) .

D3.2.2, Enter the IP address or domain name and the Port number of the LS-10 and click Add.

IP address or Domain Name and port number
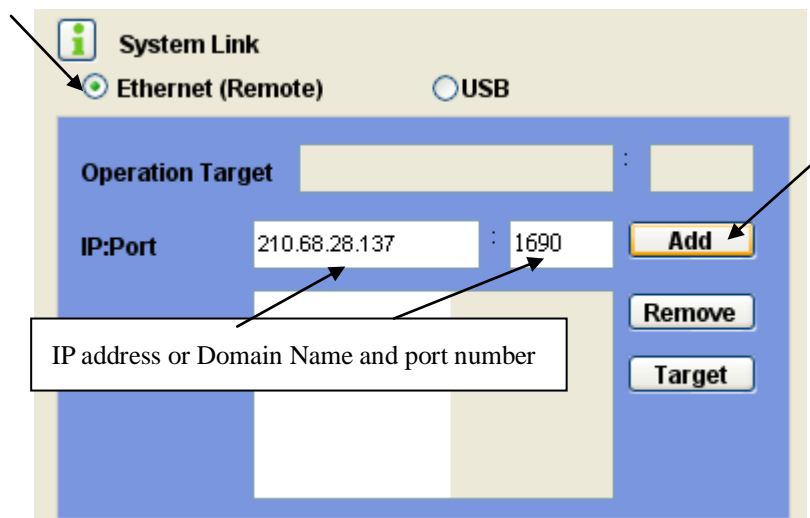
D3.3.3, Mark the IP address and click the Target to assign this address as the operation target.
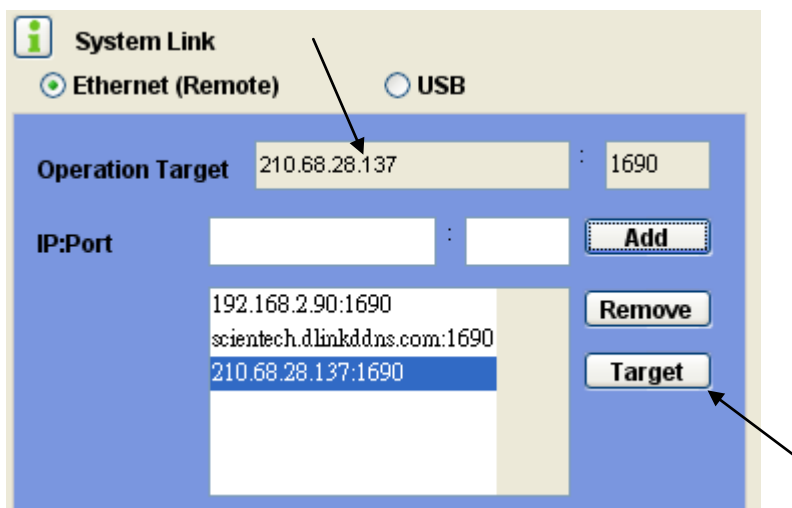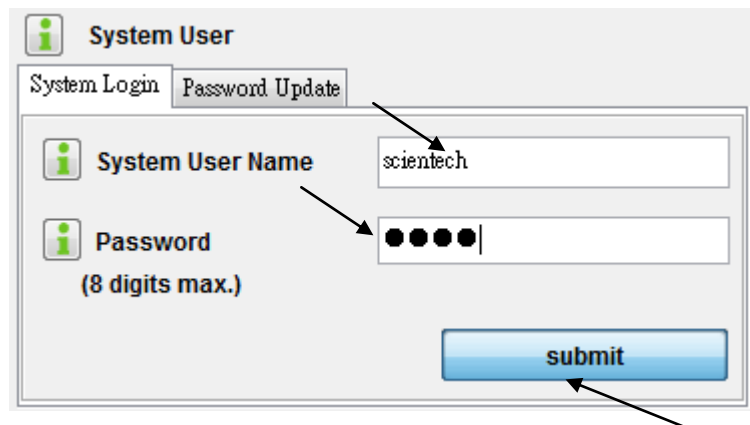
D4, Database User Name and Password

(These two settings are not necessary if you don't use the "**Database"** or the **"Control Command Password=Disable"** on LS-20.)

Device Database:

Please refer to the "**6. Device Name Data Base Management**".

User can assign a device name to each sensor/controller. When the Event Log, Device Status or Special Sensor Reading are recalled, the software will match the "User Name/ Device Type/ Zone Number" under in the Data Base and show the corresponding device name on the table.

Password:

If the setting of the LS-20 Base Unit **" Control Command Password = Enable"** then you should enter the passwords.

D5, Operation

Select the function from the Menus bar.

* Click down arrow to select the options.

* Update the setting of the LS-20 Base Unit by clicking ⟳ .

* Read the status from the LS-20 Base Unit by clicking ❓ .
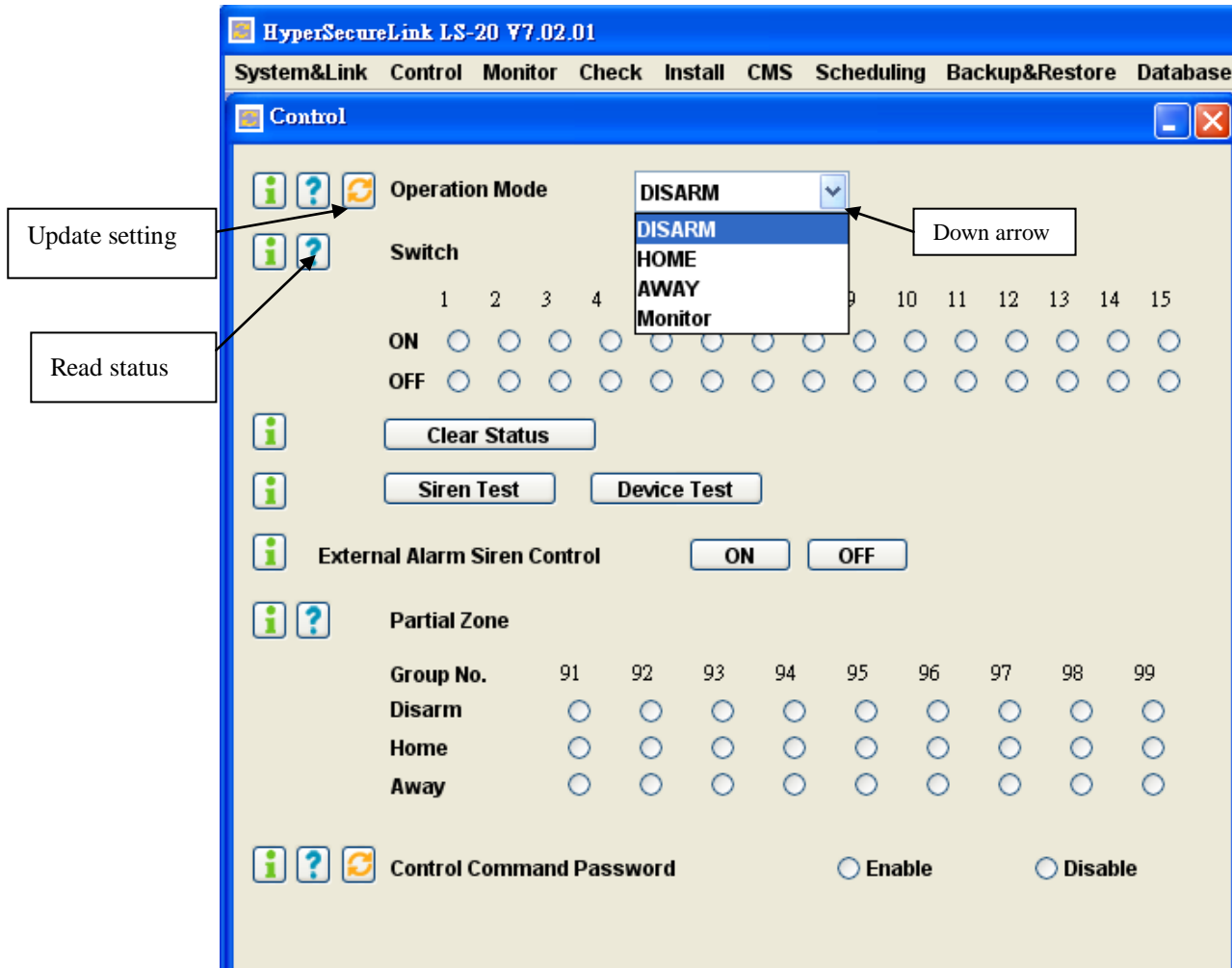
* Checking the function and the operation of the command by clicking ℹ️ .
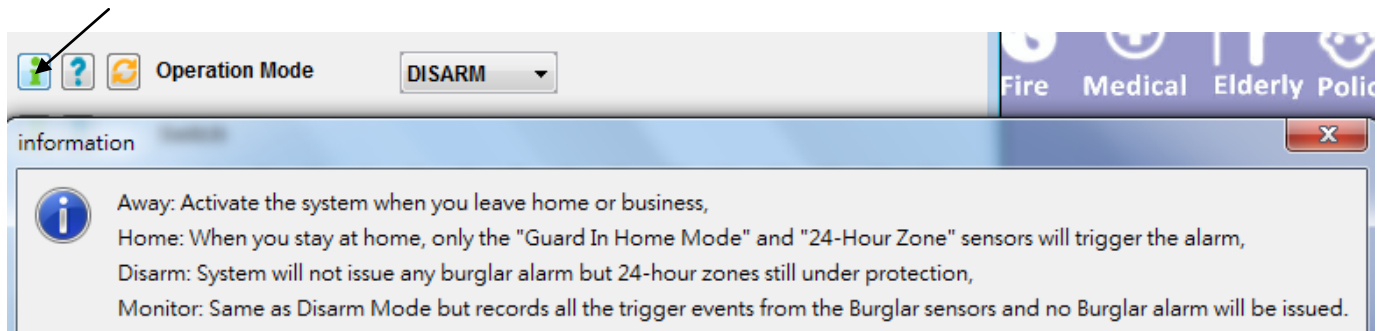
 *Monitor: This function will check the Event log in every 30 seconds and update Device Status in every 5 minutes automatically after start. If you want to change the event read number or another device type then you have to stop the reading first.

Save to File: Press this button will save the reading results under the directory you assigned for further analysis.

* Check: This function will give user a more detailed Event Log and Device Status than the Monitor function.

Device Status AM 11:27 2/1/2016

All

No.	Zone	Sensor Type	ID	MA	DC	ES	SW	CS	DT	CD	AH	AL	SS	CH	CL	Device ...
18	01-07	Remote Siren	99316a	00	10	1410	0000	bd	00							
19	01-08	Remote Siren	9933d7	00	10	1410	0000	bb	10							
20	01-09	Door Magnet	000011	00	10	1730	0006	99	0e							
21	11-15	Glass Break Detector	1a4c92	00	10	1410	0000	83	00							
22	11-16	PIR Sensor	9b1705	00	10	0410	0000	a1	10							
23	11-18	PIR Sensor	60634a	00	10	0410	0000	bf	00							
24	11-19	PIR Sensor	606351	00	10	0410	0000	ab	0f							
25	11-20	PIR Sensor	200005	02	10	0410	3000	b4	00							
26	11-21	Door Magnet	000079	11	10	5410	0000	68	10							
27	01-02	Smoke Detector	4b3071	00	00	0c00	0000	c2	0f							
28	01-03	CO Detector	000001	00	10	0c10	c000	8e	00							
29	01-04	CO Detector	005102	00	00	0c00	0000	a2	0f							
30	11-06	Gas Detector	1030e6	00	10	0c10	0000	66	00							
31	01-01	Medical Button	406005	00	00	0c00	4000	38	0f							
32	02-01	Temp Sensor	209779	00	10	2810	8000	66	00	+21	+30	+10	40	+18	+12	
33	01-06	Light Detector	777079	00	10	2c10	4000	66	00				40	+0	+0	
34	01-07	Temp Sensor	411011	00	10	2c10	0000	6e	00	+27	+26		40	+0	+0	
35	01-08	Humid Sensor	411011	00	10	2c10	8000	54	00	+68	+40		00	+0	+0	
36	02-17	Analog Sensor	800068	00	10	2810	2000	be	00	+100		+50	00	+0	+0	
37	02-18	Temp Sensor	800068	00	10	2c10	0000	c2	00	+28	+26		00	+0	+0	
38	04-06	Temp Sensor	813001	00	10	2c10	0000	8c	00	+19	+28	+26	00	+0	+0	
39	05-01	3-phase AC Meter	813001	00	10	2c10	4000	8c	00	+41	+25	+10	00	+23	+12	
40	05-02	3-phase AC Meter	813002	00	10	2c10	0000	88	00	+0			00	+0	+0	

Save to File

D6. Device Name Data Base Management

User can assign a device name to each device and zone. When the Event Log, Device Status or Special Sensor Reading are read, the software will match the **User Name, Device Type and Zone Number** in the Data Base and show the corresponding device name on the table.

For example, if you installed two systems, one in your company (name: scientech) and the other one in your home (name: John), and they both have the Door Magnet Burglar Sensor at Zone 01-01.

The device name of the Burglar Sensor 01-01 in the office is "Front Door".

The device name of the Burglar Sensor 01-01 at your home is "Living Room".

The software uses different User Name to identify the two different devices although they have the identical Device Type and Zone Number.

* Creating the Device Name in Database:
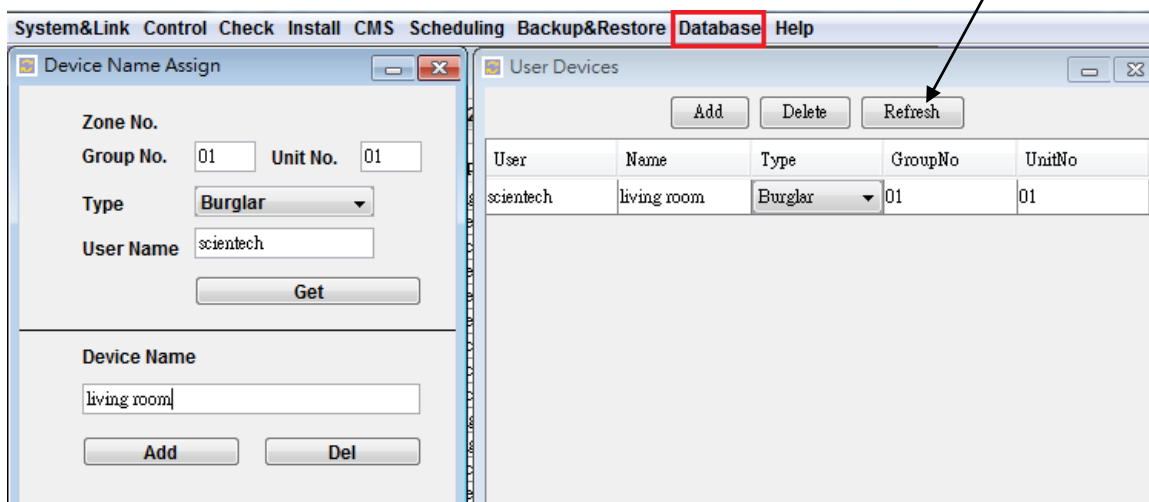
l Device Name to the Data Base

   1, Enter Group Number.

   2, Enter Unit Number.

   3, Select Device Type.

   4, Enter User Name.

   5, Enter Device Name.

   6, Press "Add".

* Click the Refresh to check the new device entry.

D7. Backup&Restore

  * Backup: User can backup the system settings (not including the password) as a .sav file in the **"Backup"** directory. The file name can be changed to identify different systems and the time of backup file generated.
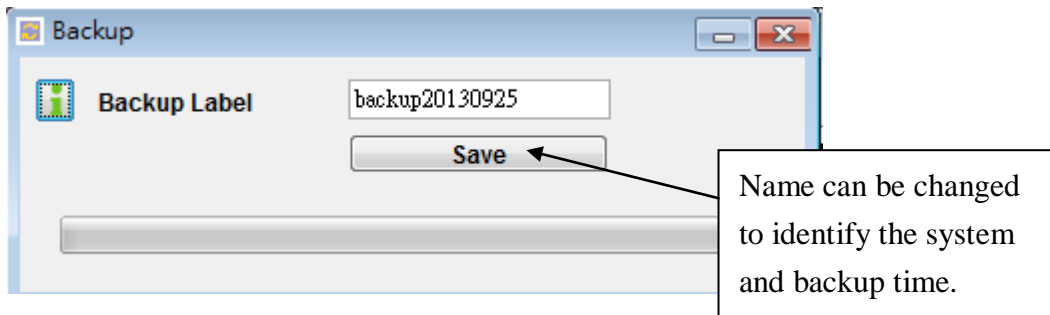
  * Restore: User can restore the system settings from the backup files.
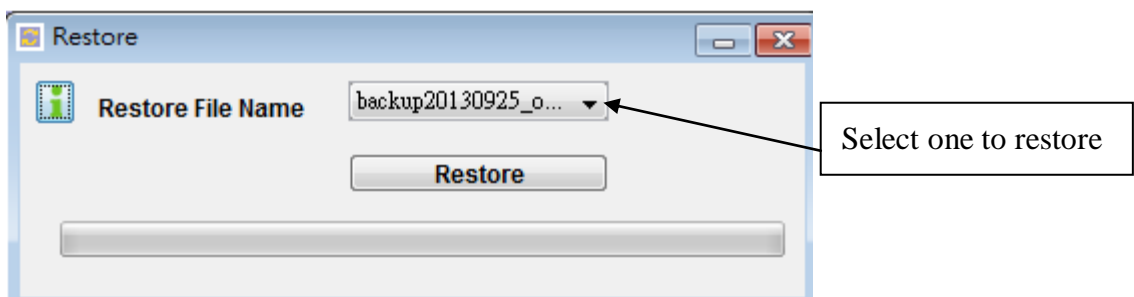
Note: 1, To restore the system settings, user has to enter the "**Password"** in the "**System&Link**".
   2, Check the "Device Status" to make sure all the devices has been restored.

WARRANTY

The Manufacturer warrants its products (hereinafter referred to as the Product) to be in conformance with its own plans and specifications and to be free of defects in materials and workmanship under normal use and service for a period of twelve months from the date of shipment by the Manufacturer. The Manufacturer's obligations shall be limited within the warranty period. At its option, to repair or replace the Product or and part thereof. To exercise the warranty the Product must be returned to the Manufacturer freight prepaid and insured.

This warranty does not apply in the following cases: improper installation, misuse, failure to follow installation and operating instructions, alteration, abuse, accident or tampering, and repair by anyone other than the manufacturer.

This warranty is exclusive and expressly in lieu of all other warranties, obligations or liabilities, whether written, oral, express or implied, including any warranty of merchantability or fitness for a particular purpose, or otherwise. In no case shall the Manufacturer be liable to anyone for any consequential of incidental damages for breach of this warranty or any other warranties whatsoever, as aforesaid.

This warranty shall apply to the Product only. All Products, accessories or attachments of others used in conjunction with the Products, including batteries, shall be covered solely by their own warranty, if any. The Manufacturer shall not be liable for any damage or loss whatsoever, whether directly, indirectly, incidentally, consequentially or otherwise, caused by the malfunction of the Product due to Products, accessories, or attachments of others, including batteries, used in conjunction with the Products.

The Manufacturer shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function.

NOTE: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

$$C\hspace{-0.2em}\epsilon$$