

Gardsman

IP SECURITY SYSTEM

CTC-1241GT IP Panel
Web Installation
Guide

.....

.....

.....

.....

25-MAR-2010

For THIRKILD DENMARK

Table of Contents

| | |
|--|-----------|
| 1. INTRODUCTION | 1 |
| 2. SYSTEM REQUIREMENTS | 1 |
| 3. GETTING STARTED | 2 |
| 3.1. HARDWARE INSTALLATION FOR CTC-1241 | 2 |
| 3.2. SOFTWARE INSTALLATION FOR CTC-1241 | 2 |
| 4. CONNECTING TO WEBPAGE | 5 |
| 5. SETTING THE SYSTEM | 7 |
| 5.1. REPORT SETTING | 7 |
| 5.2. MOBILE | 12 |
| 5.3. CENTER | 14 |
| 5.4. CODE SETTINGS | 15 |
| 5.5. DYNAMIC DNS | 17 |
| 5.6. ADMINISTRATOR | 18 |
| 6. SENSOR LEARNING & BYPASS | 19 |
| 6.1. ADD SENSOR | 19 |
| 6.2. LEARNING KP-18 IN THE CONTROL PANEL (LOCALLY) | 27 |
| 6.3. BYPASS | 28 |
| 7. PROGRAM THE SYSTEM | 29 |
| 7.1. PANEL CONDITION | 29 |
| 7.2. PIN CODE | 30 |
| 7.3. PANEL SETTINGS | 32 |
| 7.4. DATE & TIME | 35 |
| 8. SURVEILLANCE | 36 |
| 8.1. CAMERAS | 36 |
| 8.2. VIEWER | 39 |
| 8.3. CAPTURED EVENTS | 41 |
| 9. NETWORK SETTING | 43 |
| 9.1. NETWORK | 43 |
| 9.2. WIRELESS SETTING (WI-FI VERSION ONLY) | 44 |
| 9.3. UPNP | 47 |
| 10. SYSTEM MANAGEMENT & HISTORY RECORDS | 48 |
| 10.1. FIRMWARE | 48 |

10.2. FIRMWARE / ALARM (PANEL FIRMWARE UPDATE) _____ 49

10.3. FACTORY RESET _____ 50

10.4. LOG _____ 51

10.5. HISTORY RECORDS _____ 52

1. Introduction

This section covers unpacking your IP Security System with CTC-1241 IP Panel, Security Sensors and CTC-1807 IP Camera (if purchased). Refer to later chapters for information on setting up and configuring the system over the Web Page in more detail.

IP Security System is advanced with fully integrated TCP/IP technology with Ethernet and Radio connectivity, to take full advantage of new advances in IP Home Security, Home Automation and multi-path signalling.

The system can also support up to 4 wired / wireless CTC-1807 IP Cameras. Each CTC-1807 can be assigned to different devices, which will capture burglar images with any trigger.

2. System Requirements

The system requires a TCP/IP network environment. CTC-1241 IP Panel can be attached into your Network.

To install the CD Wizard, your computer must have:

- Microsoft Windows 98, ME, NT4.0, 2000, XP, Vista, or 7 operating system. A Mac or Linux based machine is also compatible.
- Microsoft Internet Explorer 5.x, or later and Mozilla Firefox 1.0 compatible.
- CD-ROM drive
- CPU: Intel Pentium II 266MHz or above
- Memory: 32MB (64MB recommended)
- VGA resolution: 800x600 or above

3. Getting Started

Read this section of the manual to learn how to set up your CTC-1241 IP Panel and program System Settings over the Web page.

With a valid internet connection, this system will bring you the freedom to Monitor / Access / Control your IP Security System anywhere, anytime in the world.

3.1. Hardware Installation for CTC-1241

- Step 1.** Connect an input of one AC power source of 100~240V 50/60Hz to CTC-1241. A short beep will be performed with Power LED lights ON.
- Step 2.** Plug-in the Internet connection cable into the Internet Jack on CTC-1241. Plug-in the other end of the enclosed Internet cable into your Internet Router port.
- **With Wired Connection:** Once the internet set-up is successful, please leave the cable connected.
 - **With Wi-Fi (Wireless) Connection:** Once the internet set-up is successful, you can remove the Internet connection cable to enjoy its wireless operation.
- Step 3.** CTC-1241 Panel features a built-in GSM communication facility to report to the Monitoring Station. The GSM SIM Card Base is situated inside the Power Supply compartment. Please insert the SIM card.
- Step 4.** Hardware installation for CTC-1241 is now complete.

3.2. Software Installation for CTC-1241

※ THIS INSTALLATION IS ONLY REQUIRED FOR FIRST TIME USER ※

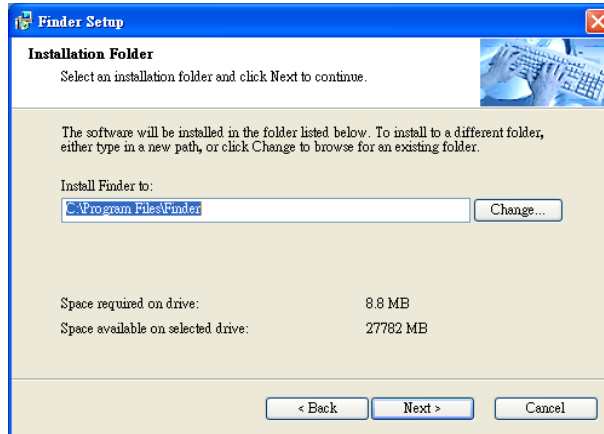
3.2.1. RUNNING THE CTC-1241 FINDER

To install the “CTC-1241 Finder” software:

- Step 1.** Insert the supplied CD-ROM into your CD-ROM drive
- Step 2.** If the installation does not start automatically, use a file explorer application to execute setup.exe in the root folder on the CD-ROM.
- Step 3.** Find the **FinderV1.3** software icon in the CD-ROM.
- Step 4.** Double click on the **FinderV1.3** to initiate the installation.



Step 5. Click **Next** to re-name the shortcut folder. If renaming is not required, please click **Next** to get ready for the installation process.

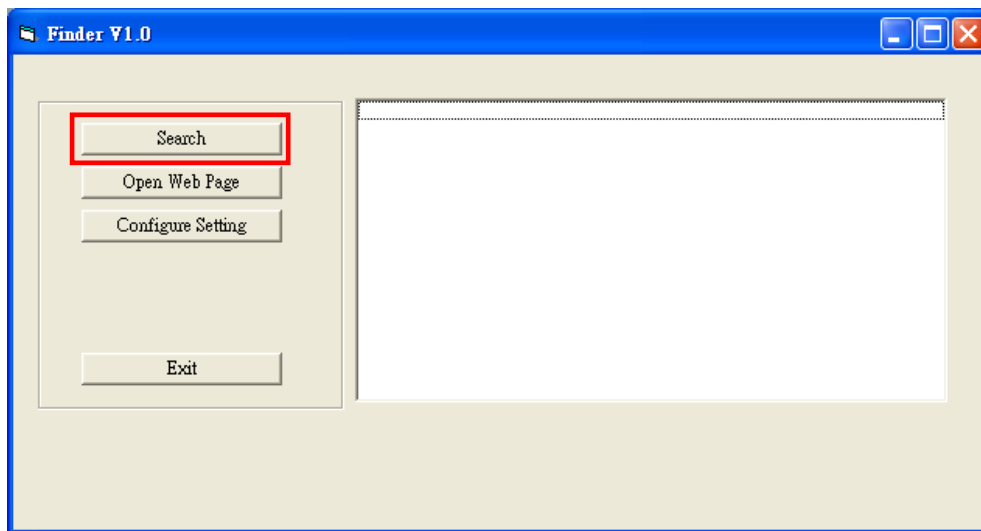


Step 6. Another click on **Next** to begin the Installation; once the installation is complete, click **Finish** to confirm.

Step 7. A new icon will be displayed on your desktop.

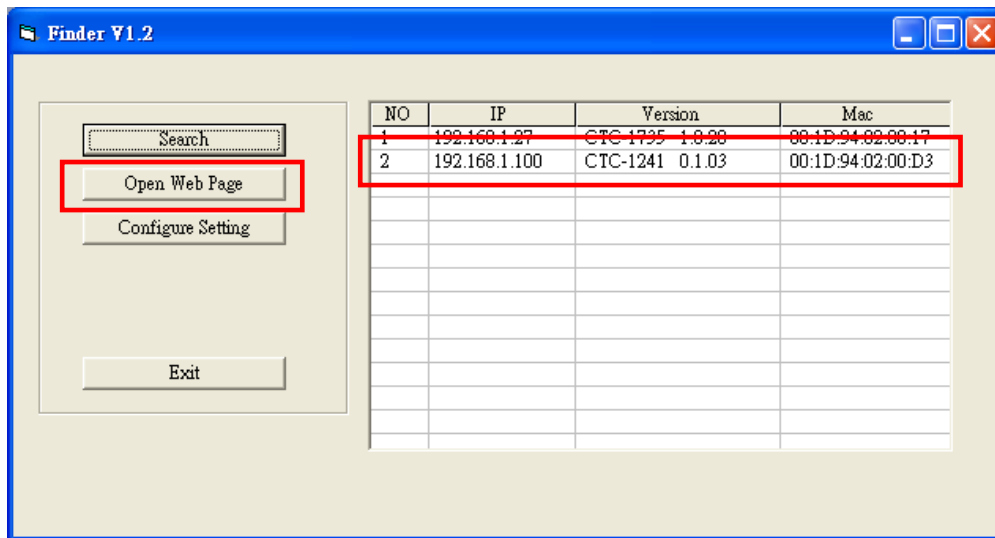


Step 8. Double click on **Finder.exe** to start the installation. The following screen will be displayed:



Step 9. Click on "**Search**", It will start searching for recognized IP address within the Local Network Service.

Step 10. You will be able to locate the current CTC-1241 IP address among the list, displayed with MAC Address and Product name.



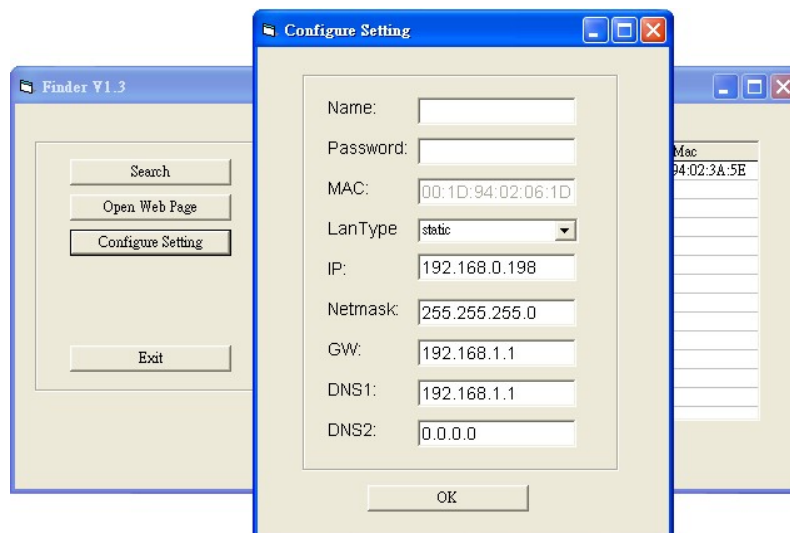
Step 11. Once CTC-1241 is identified, click on **Open Web Page** to be automatically linked to the IP Security System Web page.

Step 12. Software installation for CTC-1241 IP Panel is now complete.

3.2.2. CONFIGURE SETTING

The Configure setting is for you to enter the Internet data manually.

Step 1. Click on **Configure Setting**, the following window will display:



Step 2. Enter the internet data and the CTC-1241's web user name and password.

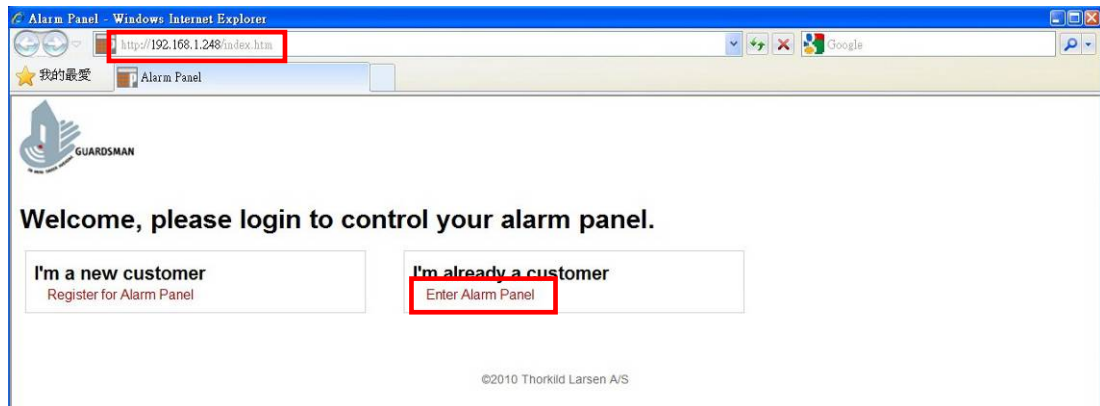
(Default) User Name: **admin**

(Default) Password: **admin1234**

Step 3. Click on **OK** to confirm. When the username and password are correct, a window will display: **Status: Configure success!!**

4. Connecting to Webpage

Step 1. The Webpage can be opened by Finder (please see section 5.1, step 10) or with a valid Internet connection, double click on **Internet Explorer** icon to initial its webpage. Under Address section (highlighted in RED), enter **CTC-1241's IP address** (for example, http://192.168.1.100), and click **GO**. You will enter the welcome Webpage.

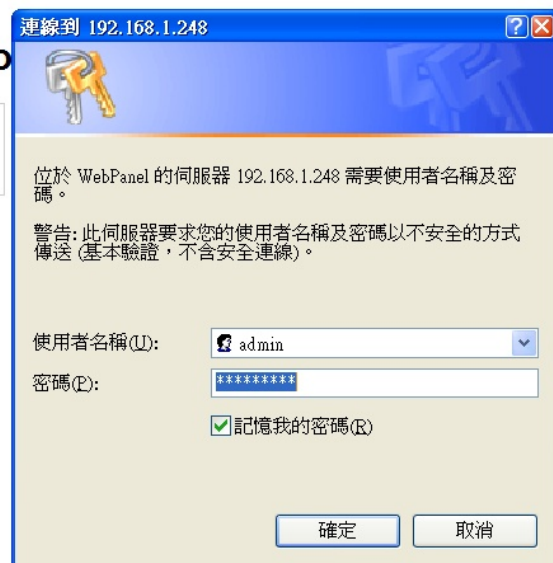


Step 2. Click on **I'm already a customer. Enter Alarm Panel**. It is required to enter the web User name & Password.



Welcome, please login to co

I'm a new customer
Register for Alarm Panel



Step 3. Enter the User name & Password and then click on **OK**.

User Name: **admin**

Password: **admin1234**

The screen enters the home page of the Alarm Panel.



GUARDSMAN

- Home
- Welcome
- Panel Condition
- Bypass
- History Records
- PIN Code
- Panel Settings
- Date & Time
- + Sensor
- + Surveillance
- + Network Settings
- + System Settings
- + System Management
- Logout

Welcome to Alarm Panel!

| | |
|----------------------|-----------------------------|
| Firmware revision: | CTC-1241 1.0.35 GT1241AA25L |
| Public IP Address: | 59.124.123.22 |
| Internal IP Address: | 192.168.1.248 |
| MAC Address: | 00:1D:94:02:3F:6A |

©2010 Thorkild Larsen A/S

5. Setting the System

When CTC-1241 is linked to a Central Monitoring Center, it should do the following set-ups before it can report.

5.1. Report Setting

This menu is for installer to programm/set all requirments for reporting purposes.

- ☞ The reporting via IP connection is always in higher priority than reporting via Tel. Numbers.
- ☞ If BOTH IP & Tel. numbers are set as either First Priority or Second Priority, the reporting will start with IP one first.

Step 1. Click on “**System Setting**” and then “**Report**”, the following screen will be displayed.

GUARDSMAN

- Home
- Welcome
- Panel Condition
- Bypass
- History Records
- PIN Code
- Panel Settings
- Date & Time
- Sensor
- Surveillance
- Network Settings
- System Settings
 - Report**
 - Report SMS
 - Mobile
 - Center
 - Code Setting
 - Dynamic DNS
 - Administrator
- System Management
- Logout

Report Setting

Internet Center Server 1

Server Address: 59.124.123.23
Port Number: 53022
Account Number: 1241
Priority: First Second

Internet Center Server 2

Server Address:
Port Number:
Account Number:
Priority: First Second

PSTN 1

Telephone:
Account Number:
Format: DTMF SMS/Text
Priority: First Second

PSTN 2

Telephone:
Account Number:
Format: DTMF SMS/Text
Priority: First Second

Options

Backup: None 1 2
Report Method: One by One Alternative

©2010 Thorkild Larsen A/S

Step 2. You are then request to enter information for:

- **Internet Center Server #1 & #2**

CTC-1241 IP Panel has GPRS for IP Reporting selection serves as a back-up, when both IP #1 & #2 failed via the Internet connection, then **GPRS** will take over the communication path to IP #1 & #2 of Monitoring Center.

Internet Center Server 1

Server Address

Port Number

Account Number

Priority First Second

Internet Center Server 2

Server Address

Port Number

Account Number

Priority First Second

1. Server Address:

Enter the Monitoring Center IP Server's public IP Address.
For example, 59.124.123.23

2. Port Number:

Enter the Monitoring Center IP Server's Port Number. A maximum of 5 digits can be entered.

3. Account Number:

Enter the Monitoring Center IP Server's Account Number. A maximum of 4 or 6 digits (depend on the Monitoring Center) can be entered.

4. Priority:

(1) First Priority: The system must report to this IP address first (in priority order) and successfully.

If more than one set of Tel. number and/or IP address is set as first priority, all of them must be reported, and all reporting must be successful.

(2) Second Priority: For back-up reporting, the system executes the reporting based on your setting for back-up method (see section **Back-up Method**).

● **PSTN #1 & #2**

PSTN 1

Telephone

Account Number

Format DTMF SMS/Text

Priority First Second

PSTN 2

Telephone

Account Number

Format DTMF SMS/Text

Priority First Second

1. Telephone Number

CTC-1241 IP Panel has GSM Dialer for Reporting selection served as a back-up. A selection of sending CID codes (via DTMF) or SMS text Message to Monitoring Center is available. The maximum length of a number is 30 digits including * & #.

2. Account Number

Enter the Monitoring Center Server's Account Number. A maximum of 4 or 6 digits (depend on the Monitoring Center) can be entered.

Account Number #1 & #2 should be programmed corresponding to Telephone Number #1 & #2.

3. Format

DTMF – CTC-1241 will send Contact ID (CID) codes to Central Monitoring Station (CMS) in DTMF format. **(4- or 6-digit account number must be entered.)** For Example, when the Wrist Transmitter (WTR) or Emergency Pendant is pressed, the Contact ID event code (101) will be sent.

SMS / Text – When 4-digit account number is entered, CTC-1241 will send Contact ID format reporting to CMS SMS Receiver.

If the account number has not been entered, the Control Panel sends SMS text message for reporting. For example, (Area1 Panic Alarm)

4. Priority:

(1) First Priority: The system must report to this Tel. number first (in priority order) and successfully.

If more than one set of Tel. number and/or IP address is set as first priority, all of them must be reported, and all reporting must be successful.

(2) Second Priority: For back-up reporting. The system excutes the reporting based on your setting for back-up method (see section **Back-up Method**).

<IMPORTANT NOTE>

☞ The reporting via IP connection is always in higher priority than reporting via GPRS, then, the Telephone Numbers.

- (a) If all IP, GPRS & Telephone numbers are set as either First Priority or Second Priority, the reporting will start with IP first.
- (b) If IP is set as First Priority and GPRS or Telephone number are set as Second Priority, the reporting will start with IP first.
- (c) If IP is set as Second Priority whereas either GPRS or Telephone number are set as First Priority, and then the reporting will start with First Priority first.

● Report Setting

Options

Backup None 1 2

Report Method One by One Alternative

1. Back-up

This feature is only required if any IP, GPRS and/or Telephone Number are set as **Second Priority** reporting source when they were programmed.

Back-up None (default): The system will not report to any Second Priorities unless all “First Priority” reporting fails.

Back up 1: Rather than only report all the First Priorities, the system is also required to report to one of the Second Priorities before the reporting terminates (with max of 5 retries on each).

Back up 2: Rather than only report the First Priorities, the system is also required to report two of the Second Priorities before the reporting terminates (with max of 5 retries on each).

2. Report Method

The reporting will start with IP reporting first, than the GPRS, then the Telephone Numbers (if they are all set as same priority order).

One-by-one: Each reporting will be retried five times before it moves to the next number until the reporting has been acknowledged.

Reporting Sequence:

■ *IF ALL SET WITH SAME PRIORITY:*

SMS #1 → SMS #2 → SMS #3 → SMS #4
IP/GPRS #1 1st time → ... → IP/GPRS #1 5th time
IP/GPRS #2 1st time → ... → IP/GPRS #2 5th time
TEL #1 1st time → ... → TEL #1 5th time
TEL #2 1st time → ... → TEL #2 5th time (Terminated)

■ *IF ALL SET WITH DIFFERENT PRIORITY:*

All the First Priority Settings will be reported first.

Alternative: Each reporting will be retried one time only before it moves to the next number, a total of 5 cycles of same reporting path will be reached until the reporting has been acknowledged.

Reporting Sequence:

■ *IF ALL SET WITH SAME PRIORITY:*

SMS #1 → SMS #2 → SMS #3 → SMS #4
IP/GPRS #1 → IP/GPRS #2 → TEL #1 → TEL#2
Repeat for 5 cycles (Terminated).

■ *IF ALL SET WITH DIFFERENT PRIORITY:*

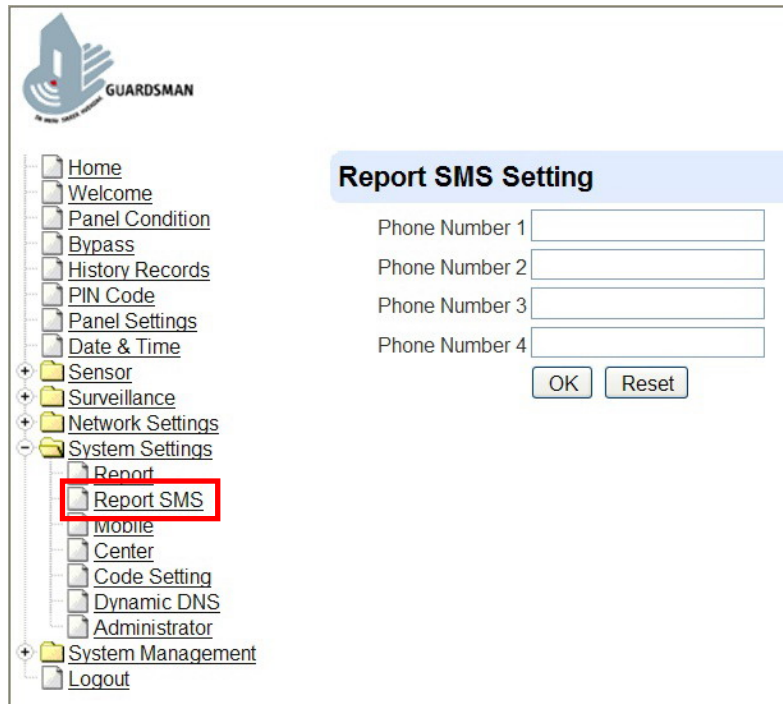
All the First Priority Settings will be reported first.

<NOTE>

- ☞ Each reporting mechanism will be retried for up to 5 times with an interval of 8 sec. between each dialing attempt.
- ☞ The system will not be able to report if no valid Account Number is programmed.

- **Report SMS**

Click on “**System Setting**” and then “**Report SMS**”, the following screen will be displayed.



In an alarm event, panel/sensor fault, and status report, reporting also can be done by sending SMS messages up to the 4 mobile phone numbers programmed at this step. Enter the mobile numbers in the corresponding fields and click **OK** to save.

<NOTE>

- ☞ There is no priority order of the numbers. When a reporting is sent, all numbers entered will be sent altogether.

<EXAMPLE>

- ☞ **acid1 Panel User 01 Area1 Cancel**
 acid1 = SMS Header
 Panel = Device (Control Panel)
 User 01 = User PIN code # 1
 Area 1 = Area 1
 Cancel = Fault/status (alarm cancelled)

- ☞ **acid1 DC Z01 Area 1 Low battery**
 acid 1 = SMS Header
 DC = Device (Door Contact)
 Z01 = Zone 1
 Area 1 = Area 1
 Low battery = Fault/status (low battery)

5.2. Mobile

Step 1. Click on “**System Setting**” and then “**Mobile**” and the following screen will be displayed.

GUARDSMAN

Home
Welcome
Panel Condition
Bypass
History Records
PIN Code
Panel Settings
Date & Time
+ Sensor
+ Surveillance
+ Network Settings
- System Settings
 Report
 Report SMS
 Mobile
 Center
 Code Setting
 Dynamic DNS
 Administrator
+ System Management
 Logout

Mobile Setting

GPRS

APN

User(GPRS)

Password(GPRS)

SMS

SMS Program Keyword

SMS for Area 1

SMS Keyword

SMS Header

SMS for Area 2

SMS Keyword

SMS Header

[Send SMS...](#)

©2010 Thorkild Larsen A/S

Step 2. You are then requested to enter information for:

- **GPRS**

In order to allow GPRS to serve as a back-up IP Reporting method, this section will need to be programmed before reporting.

GPRS

APN

User(GPRS)

Password(GPRS)

1. APN (Access Point) Name

It is the name of an access point for GPRS. Please inquire your service provider for an APN.

When APN is set, the system becomes valid for internet connection.

2. User (GPRS)

It is the Log-in name to input before accessing the GPRS feature. Please inquire your service provider.

3. Password (GPRS)

It is the User Password to input before accessing the GPRS feature. Please inquire your service provider.

<NOTE>

☞ All values will be applied to both Areas 1 & 2.

- **SMS - SMS Program Keyword**

SMS

SMS Program Keyword

Program Keyword is used to recognize the identity of a valid user; and to give authority for Remote Installing (through SMS Text) or Remote Upgrading purposes (through GPRS). This keyword will need to be inserted whenever the Remote Setting or Remote Upgrading is required.

A maximum of 15 characters is allowed.

<NOTE>

☞ All values will be applied to both Areas 1 & 2.

- **SMS for Area #1 & #2**

This feature allows you to set a SMS Keyword and Header for easy recognition. Each Area requires a different Keyword and Header in order to differentiate from each other.

SMS for Area 1

SMS Keyword

SMS Header

SMS for Area 2

SMS Keyword

SMS Header

1. SMS Keyword

Set a personalized Password to allow Remote Controlling (via SMS Text message) feature.

A maximum of 15 characters is allowed.

2. SMS Header

The words, which you edit in SMS Header box will display in the header of each SMS alarm message reported to your mobile phone for easy recognition.

For Example, if you enter your address in the SMS Header box, your address will be sent with SMS alarm message; the format is (your address, Area1 Panic Alarm).

A maximum of 60 characters is allowed.

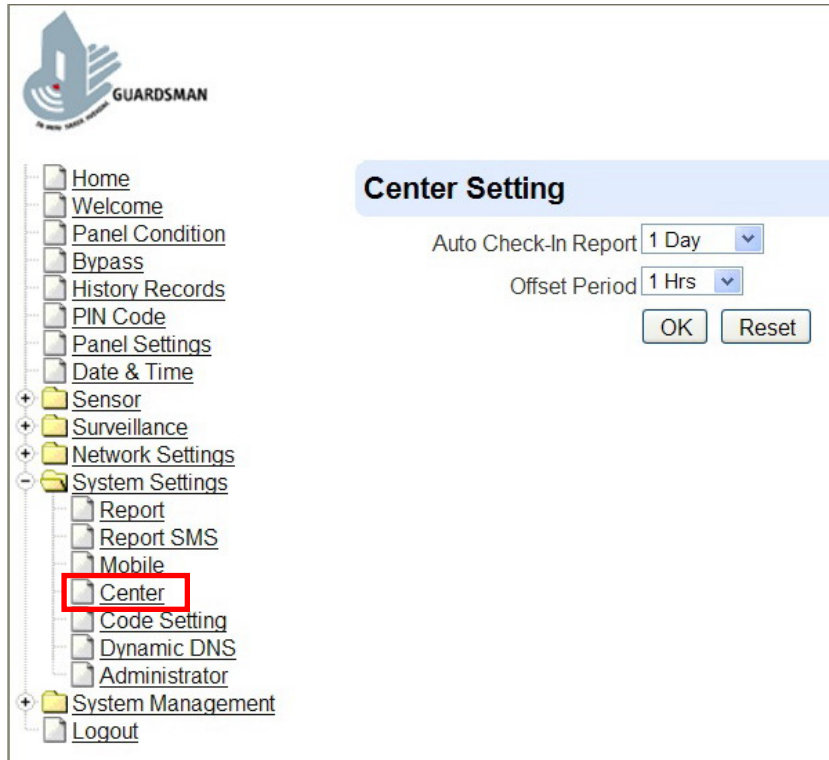
<NOTE>

☞ If no SMS header is programmed, only the SMS alarm message will be sent to mobile phone.

5.3. Center

This is for you to set Auto-Check-in Report & Offset Period.

Step 1. Click on **System Settings** and select the submenu **Center** and the following screen will be displayed.



Step 2. Click on the **V arrow** to select the **Auto Check-in Report** and/or **Offset Period**.

Step 3. Press **OK** to confirm the latest parameter value.

- **Auto Check-in Report**

This is to select whether the Control Panel needs to send check-in reporting to the Central Station automatically, and to select the time interval between check-in reports.

- **Offset Period**

This is to set the time delay before the first **Auto Check-In** report to be made.

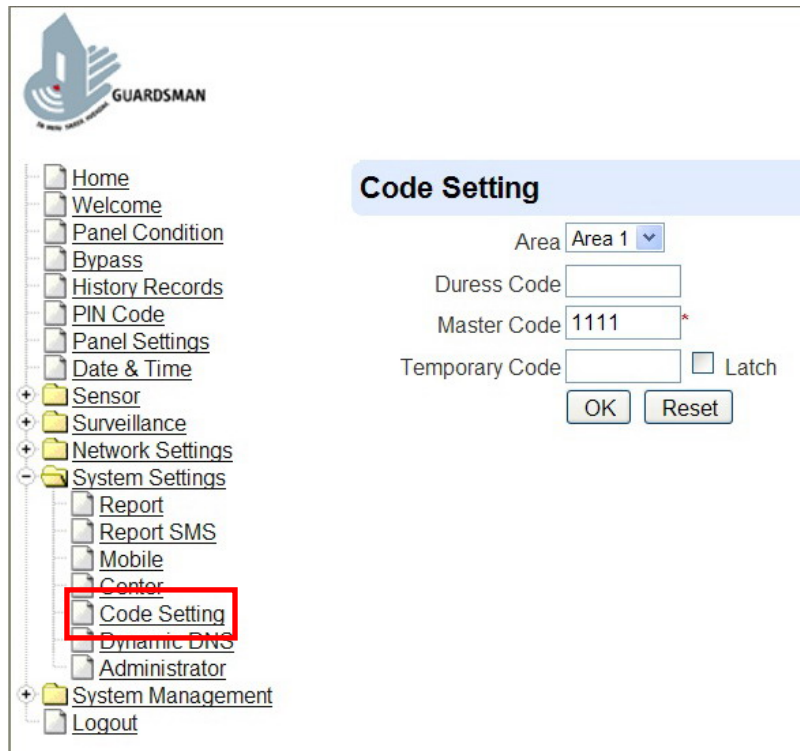
After power is supplied or re-supplied to the Control Panel, a test report will be sent to the Central Monitoring Station (CMS) based on the Offset Period. This is used to test whether the CMS is able to receive the report from the Panel accurately.

After this test report is sent, the Control Panel will then send regular reports based on the setting of the Auto Check-in Report.

For example, if **Offset Period** is set to 2 Hours, and **Auto Check-in Report** is set to 3 Days, the Control Panel will transmit an event code 602 to the CMS after 2 hours, and then report 602 event code periodically at a regular intervals of 3 days.

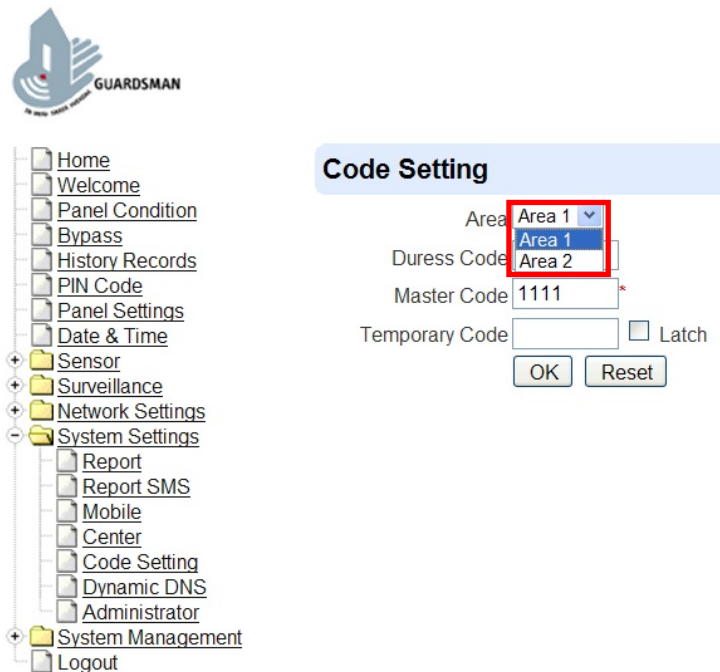
5.4. Code Settings

The Duress Code, Master Code & Temporary Code adds the flexibility of different security level for operation in **Code Settings** menu.



- **Area**

There are two operation areas in the system. Each area can be set / programmed individually. Click on ▼ button to scroll down the selection, you can select area 1 or area 2.



Step 1. Key in your preferred 4 digit **Duress Code**, **Master Code**, and/or **Temporary Code**.

Step 2. You can also choose to have Latch Option On / Off for Temporary Code by tick the Latch Option box.

Step 3. Press **OK** to confirm the uploaded details.

- **Duress Code**

The Duress Code is designed for transmitting a secret & silence alarm.

When Duress Code is used for accessing the system, the Control Panel will report a secret alarm message without sounding the siren to the Central Monitoring Station to indicate of a **Duress Situation in Progress**.

The Duress Code consists of 4 digits and is not activated as default by the factory.

- **Master Code**

The Master Code has the authorization to enter Programming Mode. When you use KP-18 to enter the panel programming mode, the display panel asks you to key in **M-Code**, please enter your Master Code.

Master Code is set to **1111** as factory default. Before you set your own Master PIN code, **1111** has to be keyed in each time it is required.

- **Temporary Code**

Temporary Code is also used to arm/disarm the system, but it is for a temporary user. The temporary Code is **ONLY** valid for one-access per arming and disarming. Afterwards, the Temporary Code will be automatically erased and needs to be reset for a new Temporary user.

The Temporary Code consists of 4 digits and is not activated as default by the factory.

- **Latch Option**

This is to program the Latch Key Reporting feature for Temporary Code. Please click the box to select the options.

Latch → **Latch Report ON** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will transmitt Contact ID code / SMS message / GPRS reporting (according to pre-setting) to notify the Central Monitoring Station.

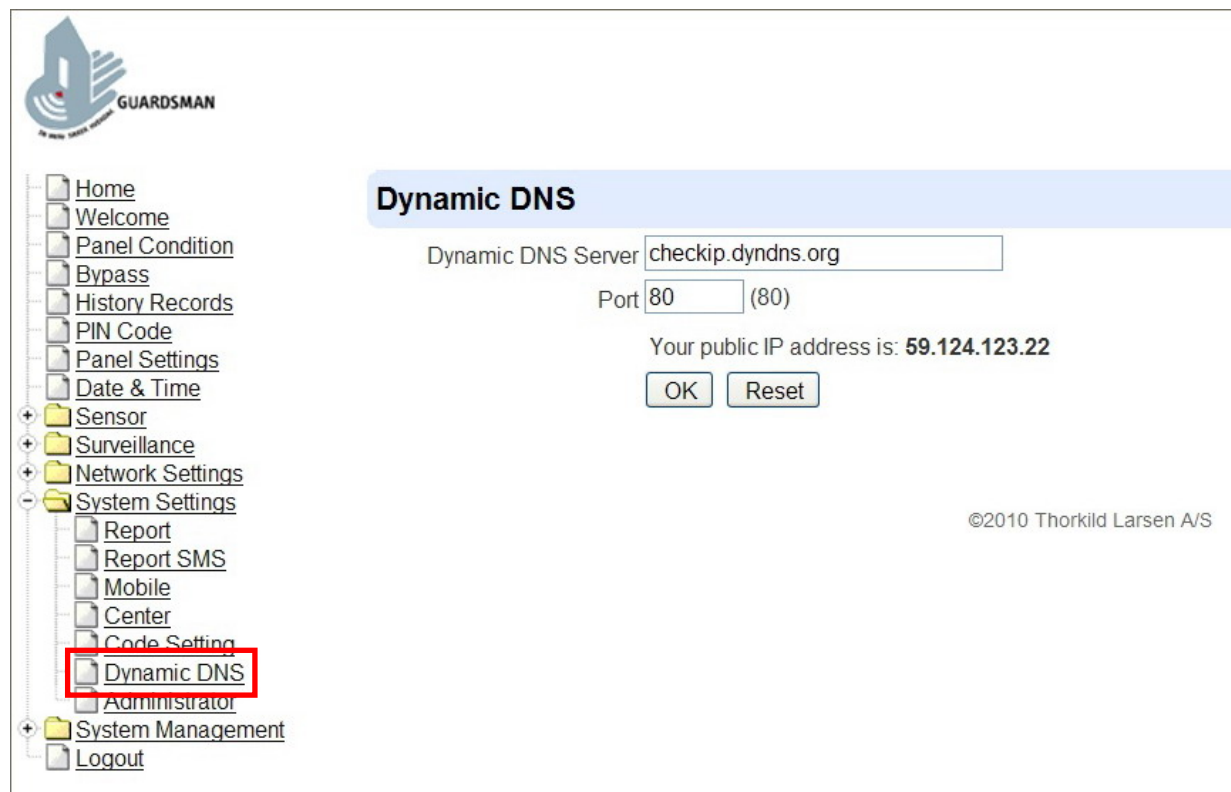
Latch → **Latch Reprot OFF** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will NOT transmit reporting(s) to notify the Central Monitoring Station.

- **Delete**

Except Master Code which can't be deleted in any way, Temporary and Duress Code can be deleted by cleaning the code box and click on OK.

5.5. Dynamic DNS

It is used to get your real public IP address on the internet.



The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with the following items: Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, System Settings (highlighted with a red box), Report, Report SMS, Mobile, Center, Code Setting, Dynamic DNS (highlighted with a red box), Administrator, System Management, and Logout. The main content area is titled "Dynamic DNS" and contains the following information: "Dynamic DNS Server" is set to "checkip.dyndns.org", "Port" is set to "80" (with "(80)" next to it), and "Your public IP address is: 59.124.123.22". There are "OK" and "Reset" buttons below the IP address. A copyright notice "©2010 Thorkild Larsen A/S" is visible in the bottom right corner of the interface.

The information is already pre-set into the system.

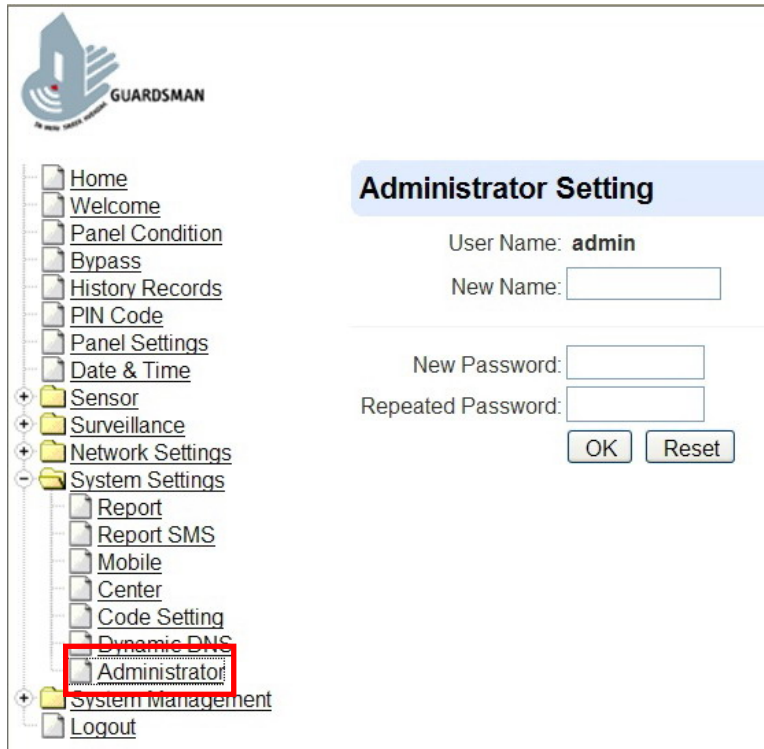
Factory default is:

Dynamic DNS Server: **checkup.dyndns.com**

Port: **80**

5.6. Administrator

It is used to set new Administrator Log-in Name and Password when accessing this web page.



The screenshot displays the GUARDSMAN web interface. On the left is a navigation tree with the following items: Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, System Settings (expanded), Report, Report SMS, Mobile, Center, Code Setting, Dynamic DNS, Administrator (highlighted with a red box), System Management, and Logout. The main content area is titled 'Administrator Setting' and contains the following form fields: 'User Name: admin', 'New Name: [input field]', 'New Password: [input field]', and 'Repeated Password: [input field]'. At the bottom of the form are 'OK' and 'Reset' buttons.

- **New Name**

Set the new Administrator Log-in name for accessing this Web Page.

- **Password:**

Set the new Administrator Log-in name for accessing this Web Page.

To SET the ADMINSTRATOR NAME and LOG-IN PASSWORD:

BEFORE SETTING: Please note the Caps for your Log-in Name and Password.

Step 1. Enter the preferred **Login-in Name**.

Step 2. Enter the preferred **Password** in the “New Password” field, and repeat the same Password in the “Repeated Password” field.

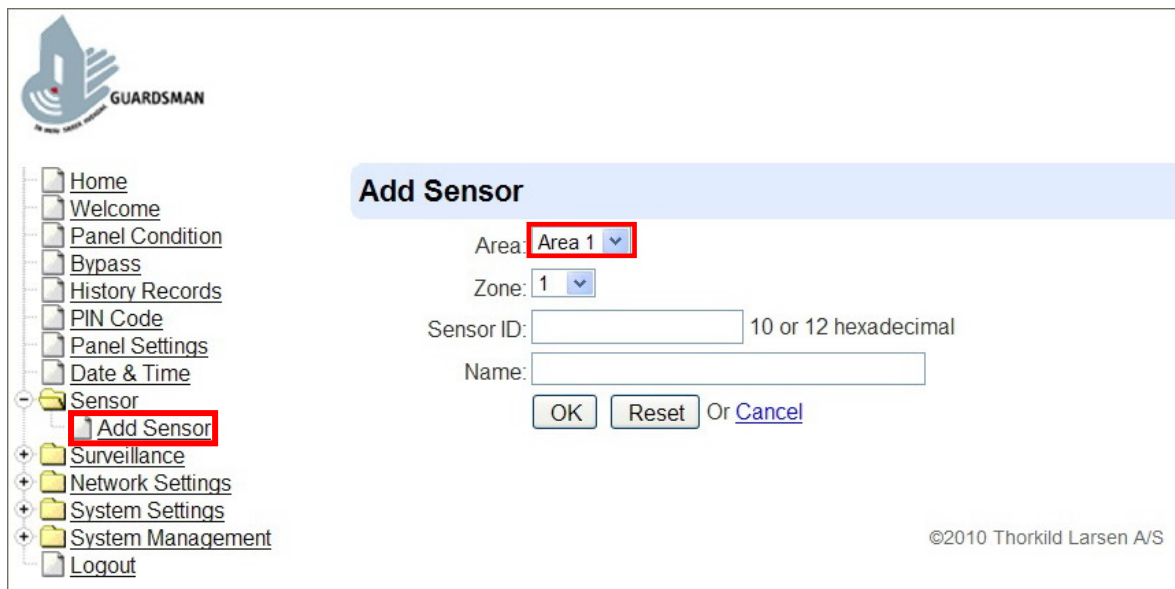
Step 3. Press “**OK**” to confirm the uploaded details.

6. Sensor Learning & Bypass

6.1. Add Sensor

Through Add Sensor Procedure, you can enter the sensor ID manually or by scanner (except KP-18, KP-9/KP-A9 and BX-15).

- Enter the Sensor ID manually



Step 1: Under the Add Sensor menu, move the cursor to **Area** box; then, choose in which area the device should be learnt.

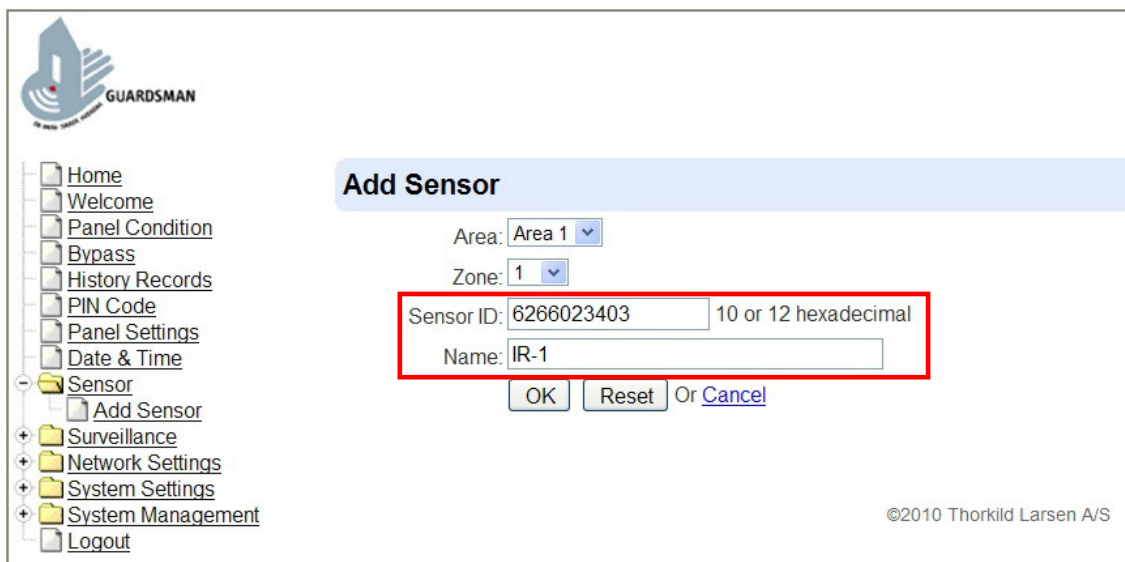
Step 2: Select a **Zone number** for this device.

Step 3: Move the cursor to **Sensor ID** box.

Step 4: Key in the Sensor ID number at the rear side of the device (a series of number underneath Bar code).

Step 5: Enter the preferred name for Sensor (up to 10 letters or numbers).

Step 6: Press **OK** to confirm.



Step 7: If the Learning process is successful, the screen will display the Panel Condition; then, you can check the learnt device.

Step 8: Repeat Steps above to add other sensors, otherwise, the learning procedure is now complete.

- **Enter the Sensor ID with Scanner**

Step 1: Move the cursor to **Sensor ID** box.

Step 2: Scan the Sensor ID bar code at the rear side of the device.

Step 3: The Sensor ID code will be input into the Sensor ID box.

Step 4: Enter the preferred name for Sensor (up to 10 letters or numbers).

Step 5: Press **OK** to confirm.

Step 6: If the Learning process is successful, the screen will display the Panel Condition; then, you can check the learnt device.

Step 7: Repeat Steps 1-5 to add more sensors, otherwise, the learning procedure is now complete.

- For Door Contact, you are requested to select the device attribute from **Burglar, Home Omit, Day Home Omit, Night Home Omit, Home Access, Delay Zone, Away Only, Entry Zone, Away Entry, 24 Hr, Fire, Medical Emergency, Water, Set/Unset, N-Home, or 24h-Special.**
- For PIR Sensor, you are requested to select the device attribute from **Burglar, Home Omit, Day Home Omit, Night Home Omit, Home Access, Delay Zone, Away Only, Entry Zone, or Away Entry.**
- For Remote Controller, you are requested to select the device attribute from **Silent Panic, Personal Attack, Medical Emergency, or Fire.**

<NOTE>

- ☞ If the sensor is learnt-in for a second time, a short beep will be emitted to indicate.
- ☞ Press **Reset** to re-enter all the information.
- ☞ Press **Cancel** to exit the screen and return to Panel Condition Page.

- **Attribute List:**

- ☞ **Burglar (B)**

- When the system is in Away Arm / Home Arm mode, if a **Burglar** DC or IR is triggered, a Burglar Alarm will be activated immediately, an event Code 130 will be reported.

- ☞ **Home Omit (O)**

- When the system is in Away Arm mode (incl. away arm entry), if a **Home Omit** DC or IR is triggered, a burglar alarm will be activated immediately. An event Code of 132 will be reported.
- When the system is in Home Arm mode, if a **Home Omit** DC or IR is triggered, the Control Panel will not respond.

- During the Entry Delay or Exit Delay period, if a **Home Omit** DC or IR is triggered, the Control Panel will not respond.

 **Day Home Omit (DO)**

- When the system is in Away arm / Night Home arm mode, if a **Day Home Omit** Door Contact is triggered, a burglar alarm will be activated immediately. An event Code of 132 will be reported.
- When the system is in Day Home mode, if a **Day Home Omit** Door Contact is triggered, the Control Panel will not respond.
- During the Entry Delay or Exit Delay period, if a **Day Home Omit** Door Contact is triggered, the Control Panel will not respond.

 **Night Home Omit (NO)**

- When the system is in Away arm / Day Home arm mode, if a **Night Home Omit** Door Contact is triggered, a burglar alarm will be activated immediately. An event Code of 132 will be reported.
- When the system is in Night Home mode, if a **Night Home Omit** Door Contact is triggered, the Control Panel will not respond.
- During the Entry Delay or Exit Delay period, if a **Night Home Omit** Door Contact is triggered, the Control Panel will not respond.

 **Home Access (A)**

- When the system is in Away arm mode, if **Home Access** Door Contact is triggered, a burglar alarm will be activated immediately. An event Code of 130 will be reported.
- When the system is in Home arm / Day Home arm / Night Home arm mode, if a **Home Access** Door Contact is triggered, the Control Panel will start an Entry Delay period to give enough time to disarm the system.
- During the Entry Delay or Exit Delay period, if a **Home Access** Door Contact is triggered, the Control Panel will not respond.

 **Delay Zone (D)**

- When the system is in Away arm / Home arm / Day Home arm / Night Home arm mode, if a **Delay Zone** Door Contact is triggered, a burglar alarm will be activated immediately. An event Code of 130 will be reported.
- During the Entry Delay or Exit Delay period, if a **Delay Zone** Door Contact is triggered, the Control Panel will not respond.

 **Away Only (Y)**

- When the system is in Away arm mode, if an **Away Only** Door Contact is triggered, a burglar alarm will be activated immediately. An event Code of 130 will be reported.
- When the system is in Home arm / Day Home arm / Night Home arm mode, if an **Away Only** Door Contact is triggered, the Control Panel will not respond.
- During the Entry Delay or Exit Delay period, if an **Away Only** Door Contact is triggered, the Control Panel will not respond.

 **Entry (E)**

- When the system is in Away arm / Home arm / Day Home arm / Night Home arm mode, if an **Entry** Door Contact is triggered, the Control Panel will start an entry period to give enough time to disarm the system.

- After the delay period is expired and no correct PIN code is entered to disarm the system, the Control Panel will respond with a **Burglar Alarm** after 30 secs and an event code **131** will be reported.
- When the system is in Alarm off mode, if an **Entry** Door Contact is triggered, the Control Panel will make a ding-dong sound for Door Chime (if programmed). To program Door Chime, please refer to section 7.3 Panel Settings.

Away Entry (P)

- When the system is in Away arm mode, if an **Away Entry** Door Contact is triggered, the Control Panel will start an entry period to give enough time to disarm the system.
- After the delay period is expired and no correct PIN code is entered to disarm the system, the Control Panel will respond with a **Burglar Alarm** after 30 secs and an event code **131** will be reported.
- When the system is in Alarm off mode, if an **Away Entry** Door Contact is triggered, the Control Panel will make a ding-dong sound for Door Chime (if programmed).
- When the system is in Home arm / Day Home arm / Night Home arm mode, if an **Away Entry** Door Contact is triggered, the Control Panel will not respond.
- During the Entry Delay or Exit Delay period, if an **Away Entry** Door Contact is triggered, the Control Panel will not respond.

24H (H)

- The **24H burglar** Door Contact is active at all times and does not have to be armed or disarmed. An event code of **133** will be reported.

Fire (F)

- The **Fire** Door Contact is active at all times and does not have to be armed or disarmed. An event code of **110** will be reported.

Medical (M)

- The **Medical** Door Contact is active at all times and does not have to be armed or disarmed. An event code of **100** will be reported.

Water (W)

- The **Water** Door Contact acts as an universal transmitter, and a wired water leakage sensor can be connected to it.
- The **Water** Door Contact is active at all times and will not have to be armed or disarmed. An event code of **154** will be reported.

Set/Unset (S) for Door Contact

- If the Door Contact is set to **Set/Unset**, when the Door Contact is disengaged, the system will enter Arm mode; when the Door Contact is engaged, the system will enter Alarm off mode.

N-Home (NH) for Door Contact

- When the system is in Away arm / Home arm / Day Home arm mode, if an **N-Home** Door Contact is triggered, the Control Panel will start an entry period to give enough time to disarm the system.
- After the delay period is expired and no correct PIN code is entered to disarm the system, the Control Panel will respond with a **Burglar Alarm** after 30 secs and an event code **130** will be reported.

- When the system is in Night Home arm mode, if **N-Home** Door Contact is triggered, a **Burglar Alarm** will be activated immediately. An event Code of 130 will be reported.
- When the system is in Alarm off mode, if an **N-Home** Door Contact is triggered, the Control Panel will not respond.
- During the Entry Delay or Exit Delay period, if a **N-Home** Door Contact is triggered, the Control Panel will not respond.

☞ **24H-Special (SP) for Door Contact**

- The **24H-Special** Door Contact is active at all times and does not have to be armed or disarmed. When a **24H-Special** Door Contact is triggered (both open and close), the Control Panel will report a secret alarm message (both open and close) without sounding the siren to the Central Monitoring Station and sending a SMS message to the mobile phone number (if programmed). An event code of 1150 for Open, and 3150 for Close will be reported.

☞ **Silent Panic (S) for Remote Controller**

If the device attribute is set as **Silent Panic**, when the panic button is pressed & held for 3 seconds or pressed twice within 3 seconds, Control Panel will report a **Silent Panic** alarm, without sounding audible siren. An event code of 122 will be reported.

☞ **Personal Attack (P) for Remote Controller**

Control Panel will give a **Personal Attack** alarm when the panic button is pressed & held for 3 seconds or pressed twice within 3 seconds. An event code of 120 will be reported.

☞ For Alarm Activation by Events and Control Panel Responses, please refer to the following table:

| Alarm attribute | | Disarm | Away Arm | Home Arm | Day Home Arm | Night Home Arm | Away/ Home/Day Home/ Night Home Arm Exit | Away Arm Entry | Home/Day Home/ Night Home Arm Entry |
|-----------------|--------|-------------|-----------------------|-----------------------|-----------------------|-----------------------|--|-----------------------|-------------------------------------|
| Burglar | " B " | No Response | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm |
| Home Omit | " O " | No Response | Instant Burglar Alarm | No Response | No Response | No Response | No Response | Instant Burglar Alarm | No Response |
| D.Home Omit | " DO " | No Response | Instant Burglar Alarm | No Response | No Response | Instant Burglar Alarm | No Response | Instant Burglar Alarm | No Response |
| N.Home Omit | " NO " | No Response | Instant Burglar Alarm | No Response | Instant Burglar Alarm | No Response | No Response | Instant Burglar Alarm | No Response |
| Home Access | " A " | No Response | Instant Burglar Alarm | Start Entry Timer | Start Entry Timer | Start Entry Timer | No Response | No Response | No Response |
| Delay Zone | " D " | No Response | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | No Response | No Response | No Response |
| Away only | " Y " | No Response | Instant Burglar Alarm | No Response | No Response | No Response | No Response | No Response | No Response |
| Entry | " E " | Door Chime | Start Entry Timer | Start Entry Timer | Start Entry Timer | Start Entry Timer | No Response | No Response | No Response |
| Away Entry | " P " | Door Chime | Start Entry Timer | No Response | No Response | No Response | No Response | No Response | No Response |

| Alarm attribute | | Disarm | Away Arm | Home Arm | Day Home Arm | Night Home Arm | Away/ Home/Day Home/ Night Home Arm Exit | Away Arm Entry | Home/Day Home/ Night Home Arm Entry |
|-----------------|---------|----------------------------|--|----------------------------|----------------------------|--|--|--|-------------------------------------|
| 24 HR | " H " | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm | Instant Burglar Alarm |
| Fire | " F " | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm | Instant Fire Alarm |
| Medical | " M " | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm |
| Water | " W " | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm | Instant Water Alarm |
| Set/Unset | " S " | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm | Arm \ Disarm |
| Silent Panic | " S " | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm | Instant Silent Panic Alarm |
| Personal Att | " PA " | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm | Instant Panic Alarm |
| Medical Emg | " M " | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm | Instant Medical Alarm |
| N-Home | " NH " | No Response | Start Entry Timer | Start Entry Timer | Start Entry Timer | Instant Burglar Alarm | No Response | No Response | No Response |
| 24 HR Special | " SP " | Reporting Only | Reporting Only | Reporting Only | Reporting Only | Reporting Only | Reporting Only | Reporting Only | Reporting Only |
| External PIR | " EIR " | No Response | Instant Burglar Alarm (but no reporting) | Warning Beep | Warning Beep | Instant Burglar Alarm (but no reporting) | No Response | Instant Burglar Alarm (but no reporting) | Warning Beep |

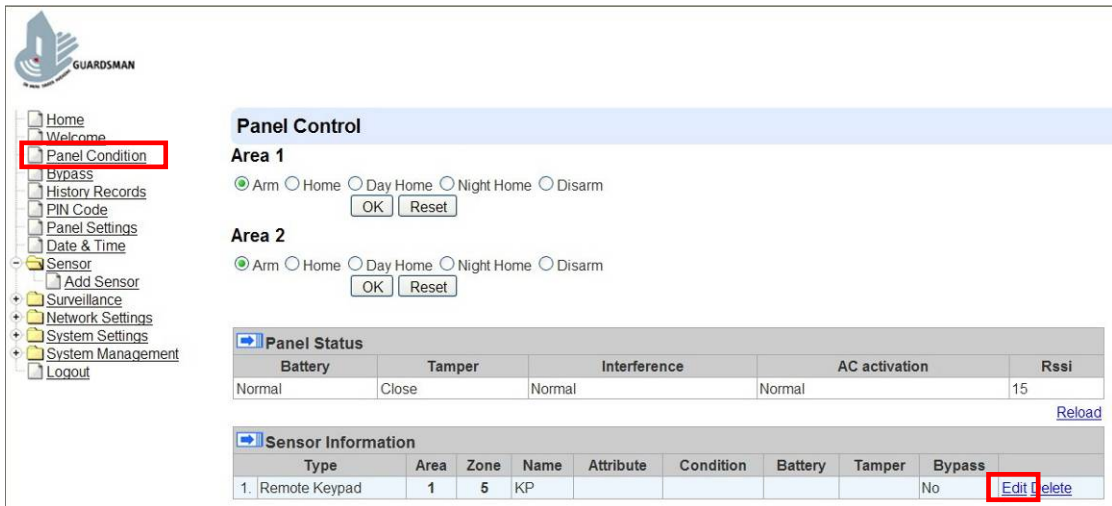
Step 8. When the sensor is learnt-in successfully, the screen will return to Panel Condition Page and newly added sensor will be displayed under the **Sensor Information** section.

<NOTE>

☞ When a sensor is added to the system for a second time (without removing first). An error message will be displayed - **Failed to add a new sensor**. Press **Cancel** to return to Panel Condition Page.

● **EDIT DEVICES**

Step 1. To edit all the devices that have already been installed, choose **Edit** (highlighted in red) under **Sensor Information** section.



Step 2. You are then requested to set a new **Sensor Name & Sensor Attribute**.

Step 3. Press **OK** to save your new changes. The device editing procedure is now successful.

<NOTE>

☞ Press **Reset** to re-enter all the information.

☞ Press **Cancel** to exit the screen and return to Panel Condition Page.

● **DELETE DEVICES**

Step 1. To delete a sensor, choose **Delete** under **Sensor Information** section.

Step 2. A message **Are you sure?** is asked, and press **Yes** if wish to delete the device, Press **No** to return to previous screen.

Step 3. If **Yes** is confirmed, that particular device will be removed from the Sensor Information List, and the undeleted sensors will remain.

6.2. Learning KP-18 in the Control Panel (Locally)

Step 1. Put the Control Panel into **Device +/-** menu and select the **Add Devices** sub menu. The screen on Control Panel will show: **Push button on Device to add.**

Step 2. Apply the AC Power for the KP-18. The KP- LY LCD display will show: **Press “*” key for learning!**

<NOTE>

☞ If KP-18 has been learnt in any Control Panel, the LCD display shows **”connecting...”** after the power is applied. If you would like to re-learn KP-18, press & hold the *** key** on KP-18 for 2 sec, you are required to enter KP Pin Code (default: 0000) for entering KP Test Mode. After entering the test mode, please follow steps 4-6 to relearn KP-18

Step 3. Press & hold the *** Key** on KP-18 for 2 sec to enter the KP test mode.

Step 4. Select **Learning**, and press **OK** key. The KP-18 LCD will show: **Wait leaning Confirm....**

Step 5. Once the control panel receives the learning signal, an acknowledgment, **”Completed”**, will be displayed on KP-18 with 2 beeps emitted.

Step 6. On the other hand, the screen on Control Panel will show: **Detected: OK? KP-18.**

<NOTE>

☞ If KP-18 does not receive the acknowledgement signal, a prompt message **”No response!”** will display on the KP LCD for 2 sec. Then, KP-18 returns to test mode. Please repeat steps 4-6 to try again.

Step 7. Press **OK** key on the Control Panel to confirm. Another prompting message will be displayed for selecting its zone number.

Step 8. Press **OK** key to confirm the zone number and learning process.

<NOTE>

☞ Please refer to CTC-1241 Panel Installation Guide to understand more information and how to learning KP-9/KPA-9, BX-15 and SR-15 in the Control Panel.

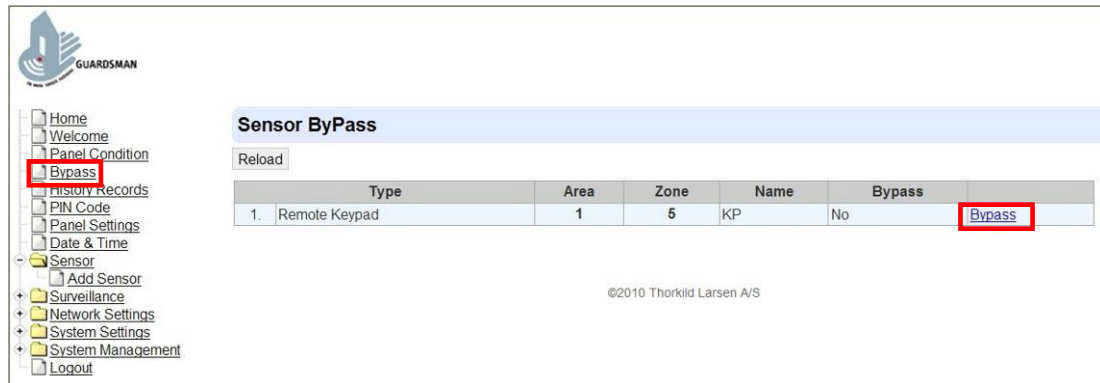
6.3. Bypass

The Bypass function allows the user to deactivate (bypass) any sensors at their own discretion. The bypassed sensor will be deactivated in the followed Away or Home Mode.

- **TO PUT THE SYSTEM INTO BYPASS ARM MODE:**

Step 1. Click on **Bypass** icon and a message **Are you sure?** is asked. Press **Yes** if you wish to bypass the device, or, press **No** to return to previous screen.

Step 2. If Bypass is successful, the **Bypass** icon will be replaced as **Unset** to indicate that device is to be bypassed in next the Away or Home Mode.



<NOTE>

- ☞ If a sensor is bypassed, then the Control Panel will not respond to its triggering in Arm mode.
- ☞ The bypass setting is effective for only one time. Once the system is disarmed, the by-pass setting is cleared automatically.
- ☞ When a sensor is bypassed, the system can be armed directly regardless of its fault situation. However, its fault situation is still being monitored; it will be logged and displayed when you access the **History Records** submenu.

- **TO RESET THE BYPASSED SENSOR:**

Step 1. Click on **Unset** icon and a message **Are you sure?** is asked. Press **Yes** if wish to unset the bypassed device, or press **No** to return to previous screen.

Step 2. If unsetting the bypassed device is successful, the **Unset** icon will be replaced by **Bypass** to indicate that device is not bypassed.

7. Program the System

After the initial set-up, you can then program your system by clicking on the left menu to set them individually.

7.1. Panel Condition

It displays the current **Panel Status & Sensor Information** for the user to view.

Under **Panel Control**, user can also choose to Arm / Home / Day Home / Night Home / Disarm the system mode remotely for both Areas.

A green radio button indicates its current system mode.

Step 1. Click on “**Panel Condition**”, and the next screen will be displayed

The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with 'Panel Condition' highlighted in a red box. The main content area is titled 'Panel Control' and contains two sections: 'Area 1' and 'Area 2'. Each area has radio buttons for 'Arm', 'Home', 'Day Home', 'Night Home', and 'Disarm'. The 'Disarm' option is selected in both areas, indicated by a green dot. Below the radio buttons are 'OK' and 'Reset' buttons. Underneath is the 'Panel Status' section, which contains a table with columns: Battery, Tamper, Interference, AC activation, and Rssi. The values are: Normal, Close, Normal, Normal, and 11. A 'Reload' link is present below the table. Below that is the 'Sensor Information' section, which contains a table with columns: Type, Area, Zone, Name, Attribute, Condition, Battery, Tamper, Bypass, and Edit Delete. The first row shows: 1. Remote Keypad, 1, 5, KP, , , , , No, Edit Delete.

| Battery | Tamper | Interference | AC activation | Rssi |
|---------|--------|--------------|---------------|------|
| Normal | Close | Normal | Normal | 11 |

| Type | Area | Zone | Name | Attribute | Condition | Battery | Tamper | Bypass | Edit Delete |
|------------------|------|------|------|-----------|-----------|---------|--------|--------|-------------|
| 1. Remote Keypad | 1 | 5 | KP | | | | | No | Edit Delete |

To ARM / HOME ARM / DAY HOME ARM / NIGHT HOME ARM / DISARM the system:

Step 1. To Arm / Home / Day Home / Night Home / Disarm each Area, select the corresponding radio button and press **OK** to confirm. The screen on top of Panel Status will be refreshed to show “**Update Successfully**”.

Step 2. The System is now in the chosen mode successfully.

7.2. PIN Code

There are 50 User PIN Codes in total for Areas 1 and 2. You may set any combination within the two areas, as long as they add up to 50. (E.g. 8 PIN in Area 1 + 42 in Area 2, or 30 in Area 1 + 20 in Area 2). Each PIN Code consists of 4 digits. User PIN code #1 in Area 1 and PIN code #2 in Area 2 are always activated by factory default.

User PIN #1 in Area 1

Password: **1234**

User PIN #1 in Area 2

Password: **4321**

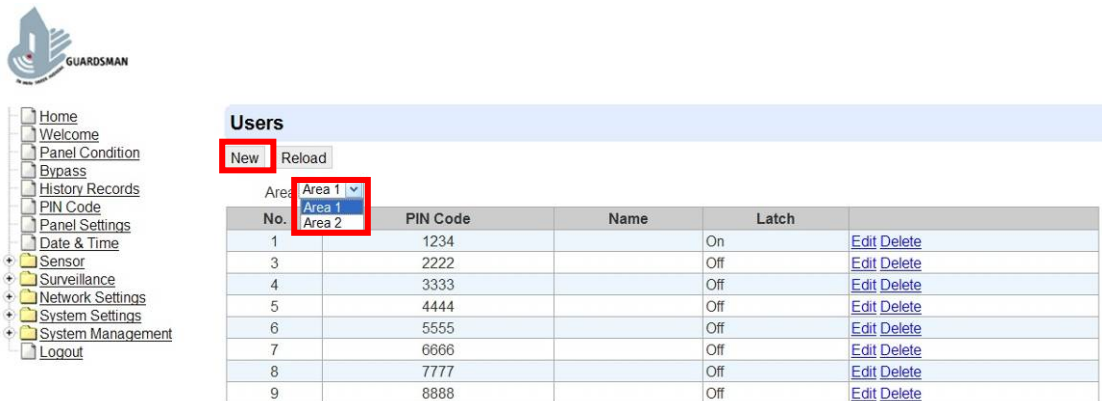
Before you set your own User PIN Code #1 or #2 in each Area, “**factory default code**” has to be keyed in whenever “**Entering Code**” is required by CTC-1241 IP Panel.

User PIN code #3-#50 are deactivated by factory default.

All 50 User PIN Codes are used to regularly arm/disarm the system and are allowed to access the Programming mode accompanied with the Master Code.

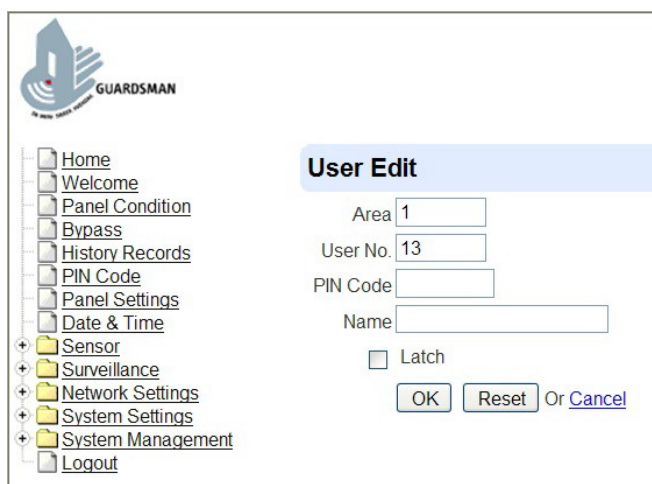
- **TO ADD NEW USER PIN CODE**

Step 1. When setting the User PIN codes, please scroll down the selection to choose between **Areas 1 & 2**, and then click on **New**.



| No. | PIN Code | Name | Latch | |
|-----|----------|------|-------|---|
| 1 | 1234 | | On | Edit Delete |
| 3 | 2222 | | Off | Edit Delete |
| 4 | 3333 | | Off | Edit Delete |
| 5 | 4444 | | Off | Edit Delete |
| 6 | 5555 | | Off | Edit Delete |
| 7 | 6666 | | Off | Edit Delete |
| 8 | 7777 | | Off | Edit Delete |
| 9 | 8888 | | Off | Edit Delete |

Step 2. Assign a User No., enter a new User PIN Code, enter a Name for the user, and check Latch if required. Click on **OK** to save.



- **User No.**

Each individual User can be assigned a number. Enter a desired user number.

- **PIN Code**

Enter a PIN code for this user.

- **Name**

Each individual User can be given a name for easy recognition when understanding system events. User Names can be named when first setting them or by editing them afterwards. The procedure is similar for both situations. Up to 17 alphanumeric characters are allowed per name.

- **Latch Option**

This is to program the Latch Key Reporting feature for all users and any arming/disarming actions of the Remote Controllers of the system. Please click the box to select the options.

Latch → **Latch Report ON** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will transmitt Contact ID code / SMS message / GPRS reporting (according to pre-setting) to notify the Central Monitoring Station.

Latch → **Latch Reprot OFF** = Whenever the system is armed, home/ day home/ night home armed or disarmed, the Panel will NOT transmitt reporting(s) to notify the Central Monitoring Station.

- **TO EDIT USER PIN CODE**

To edit an existing User PIN Code, click on **Edit** and repeat Step 2 as in *TO ADD NEW USER PIN CODE* above.

The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with items like Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, System Settings, System Management, and Logout. The main content area is titled 'Users' and includes 'New' and 'Reload' buttons, and a dropdown menu for 'Area' set to 'Area 1'. Below is a table with columns: No., PIN Code, Name, Latch, and Edit/Delete. The 'Edit' link for User #1 is highlighted with a red box.

| No. | PIN Code | Name | Latch | Edit Delete |
|-----|----------|------|-------|---|
| 1 | 1234 | | On | Edit Delete |
| 3 | 2222 | | Off | Edit Delete |
| 4 | 3333 | | Off | Edit Delete |
| 5 | 4444 | | Off | Edit Delete |
| 6 | 5555 | | Off | Edit Delete |
| 7 | 6666 | | Off | Edit Delete |
| 8 | 7777 | | Off | Edit Delete |
| 9 | 8888 | | Off | Edit Delete |

- **TO DELETE USER PIN CODE**

Except User #1 and #2 can't be deleted in any way, User#3 to 50 PIN codes can be deleted by clicking on **Delete**.

The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with items like Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, System Settings, System Management, and Logout. The main content area is titled 'Users' and includes 'New' and 'Reload' buttons, and a dropdown menu for 'Area' set to 'Area 1'. Below is a table with columns: No., PIN Code, Name, Latch, and Edit/Delete. The 'Delete' link for User #4 is highlighted with a red box.

| No. | PIN Code | Name | Latch | Edit Delete |
|-----|----------|------|-------|---|
| 1 | 1234 | | On | Edit Delete |
| 3 | 2222 | | Off | Edit Delete |
| 4 | 3333 | | Off | Edit Delete |
| 5 | 4444 | | Off | Edit Delete |
| 6 | 5555 | | Off | Edit Delete |
| 7 | 6666 | | Off | Edit Delete |
| 8 | 7777 | | Off | Edit Delete |
| 9 | 8888 | | Off | Edit Delete |

7.3 Panel Settings

Program the **Time Setting** & **Sound Setting** at your discretion.

Step 1. Scroll down the selection to choose between Area 1 or 2.

Step 2. Click on the **V arrow** to select the **Time Setting**, and use the radio buttons to select between **OFF**, **LOW**, or **HIGH** for **Sound Setting**.

Step 3. Press **OK** to confirm all the updated parameter value.

- **Time Setting**

- 1. Entry Delay time for Away Arm:**

When Door Contact (DC) or PIR Detector (IR) is set as **Entry / Away Entry / Home Access** attribute, the system gets into counting down period (Away entry timer) while the DC or IR is triggered under Away arm mode.

During the counting down period, it is allowed to use correct PIN code to disarm the alarm and the alarm reporting is not sent. On the other hand, if the correct PIN code is not entered during the period, Control Panel raises an alarm and sends alarm report.

Options available are **Disable** (alarm immediately), **10 sec**, **20 sec**, up to **70 sec** in 10-sec increments.

- 2. Exit Delay time for Away Arm:**

While the system gets into Away arm mode by Control Panel, Remote controller (RC) or Remote keypad (KP), an Away exit timer starts counting down.

During the counting down period, pressing the Arm Button of the RC can restart the counting. In addition, it is allowed to use correct PIN code or press Disarm Button of the RC to stop the counting and return to disarm mode.

Options available are **Disable** (exit timer prohibited), **10 sec**, **20 sec**, up to **70 sec** in 10-sec increments.

3. Entry Delay time for Home Arm:

When Door Contact (DC) or PIR Detector (IR) is set as **Entry / Away Entry / Home Access** attribute, the system gets into counting down period (Home entry timer) while the DC or IR is triggered under Home / Day home / Night home arm mode.

During the counting down period, it is allowed to use correct PIN code to disarm the alarm and the alarm reporting is not sent. On the other hand, if the correct PIN code has not been entered during the period, Control Panel raises an alarm and sends alarm report.

Options available are **Disable** (alarm immediately), **10 sec**, **20 sec**, up to **70 sec** in 10-sec increments.

4. Exit Delay time for Home Arm:

While the system gets into Home / Day Home / Night Home arm mode by Control Panel, Remote controller (RC) or Remote keypad (KP), an Away exit timer starts counting down.

During the counting down period, pressing the Home Button of the RC can restart the counting. In addition, it is allowed to use correct PIN code or press Disarm Button of the RC to stop the counting and return to disarm mode.

Options available are **Disable** (exit timer prohibited), **10 sec**, **20 sec**, up to **70 sec** in 10-sec increments.

5. Alarm Length:

This is for you to select the built-in siren duration when an alarm is activated. Options are **Disable** (no siren alarm), and **1-min** to **15-min** in 1-min increments.

- If **Disable** is selected, when the Control Panel receives an alarm signal, the panel siren and Bell Box (BX) will not raise an alarm sounding.
- If BX's alarm length is longer than the Control Panel's, the system gives priority to the Control Panel (e.g. when the BX's alarm length is set as 3 mins, and the panel's alarm length is set as 1 min, both alarm siren stop at 1 min when an alarm is triggered. However, the BX's LED keeps flashing until 3 mins is expired.

6. Siren Delay:

This is for you to decide how long should the Control Panel suppress the audible alarms after a Burglar or Entry alarm is reported.

<NOTE>

☞ Some audible alarm will not be delayed (disregard its siren delay setting) when the following conditions are detected:

- ✓ Fire
- ✓ Water
- ✓ Personal panic
- ✓ Medical emergency
- ✓ Tamper

7. Mobility Check:

This function is designed to avoid an accident (e.g. swoon or lost consciousness) happening to the user without anyone notices. Under all modes except Away arm mode, when the system does not detect any user movement within the pre-set mobility period, an inactivity (fault) report will be sent to the monitoring center.

<NOTE>

- ☞ The mobility time re-calculates once one of the following actions occurs:
 - In **Home** mode: whenever any key of Control Panel is pressed, or whenever any **Home Omit / Day Home Omit / Night Home Omit** DC or IR is triggered.
 - In **Day Home** mode: whenever any key of Control Panel is pressed, or whenever any **Home Omit / Day Home Omit** DC or IR is triggered.
 - In **Night Home** mode: whenever any key of Control Panel is pressed, or whenever any **Home Omit / Night Home Omit** DC or IR is triggered.
 - In **Disarm** mode: whenever any of the DC or IR (except **24 Hr, Fire, Medical Emergency and Water**) is triggered, or whenever any keys of the Control Panel / RC / KP is pressed.
- ☞ The mobility function is disabled automatically when the system is set to **Away Arm**.

8. Supervisor:

This option is used to enable system supervision function. When **4/6/8/12 Hrs** is selected, CTC-1241 will be able to receive the check-in signals from the devices to indicate their proper functioning.

The PIR sensor, Door Contact, Water Sensor or Smoke Sensor, after installed, will transmit a periodic supervision signal at intervals between 60 min. to 100 min.

If the Control Panel does not receive the signals transmitted from an individual sensor for a period of 4 Hours, 6 Hours, 8 Hours, or 12 Hours, a **sensor out-of-order** fault event will be detected.

- **Sound Setting**

1. **Door Chime**

This is for you to decide whether the Control Panel sounds a Door Chime (Ding-Dong Sound) while the DC and/or IR is activated in Alarm off mode, and volume sound.

2. **Entry Delay time for Away Arm:**

This is for you to decide whether the Control Panel sounds count-down beeps, and volume of beep during the Away entry timer.

3. **Exit Delay time for Away Arm:**

This is for you to decide whether the Control Panel sounds count-down beeps, and volume of beep during the Away exit timer.

4. **Entry Delay time for Home Arm:**

This is for you to decide whether the Control Panel sounds count-down beeps, and volume of beep during the Home entry timer.

5. **Exit Delay time for Home Arm:**

This is for you to decide whether the Control Panel sounds count-down beeps, and volume of beep during the Home exit timer.

6. **Warning Beep**

This is for you to decide whether the Control Panel sounds warning beeps every 30 seconds when a fault condition is detected, and volume of beep.

7.4. Date & Time

Program the current **Date & Time**. Normally this will automatically synchronize with Network Time Server with a valid internet connection.

The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with the following items: Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, **Date & Time** (highlighted with a red box), Sensor, Surveillance, Network Settings, System Settings, System Management, and Logout. The main content area has three sections:

- Date & Time**: Date is set to 2010/03/25 (with a calendar icon and '(yyyy/MM/dd)' format). Time is set to 15:33 (with '(hh:mm)' format and a 'Now' link). There are 'OK' and 'Reset' buttons.
- Time Zone**: Time Zone is set to '(GMT+08:00) Beijing, Hong Kong, Taipei' (with a dropdown arrow). There are 'OK' and 'Reset' buttons.
- Internet Time**: A checkbox is checked, labeled 'Automatically synchronize with an Internet time server.'. Below it, the Server is set to 'pool.ntp.org' (with a dropdown arrow). There are 'OK' and 'Reset' buttons.

<NOTE>

- ☞ If you do not want the system to automatically synchronize the Date & Time with Internet Time Server, please then untick the check box and the green tick will disappear.
- ☞ Press **OK** to confirm.

Date: This is for you to set the current month & date.

Time: This is for you to program the current time to be displayed (hour & minute).

Time Zone: Choose your time zone, and then the system will calculate the daylight saving time automatically (if necessary).

Internet Time: The system will automatically synchronize with an internet time server. With a tick in the check box to enable the function.

The selectable servers are: pool.ntp.gov, time.mist.gov and tick.usno.navy.mil

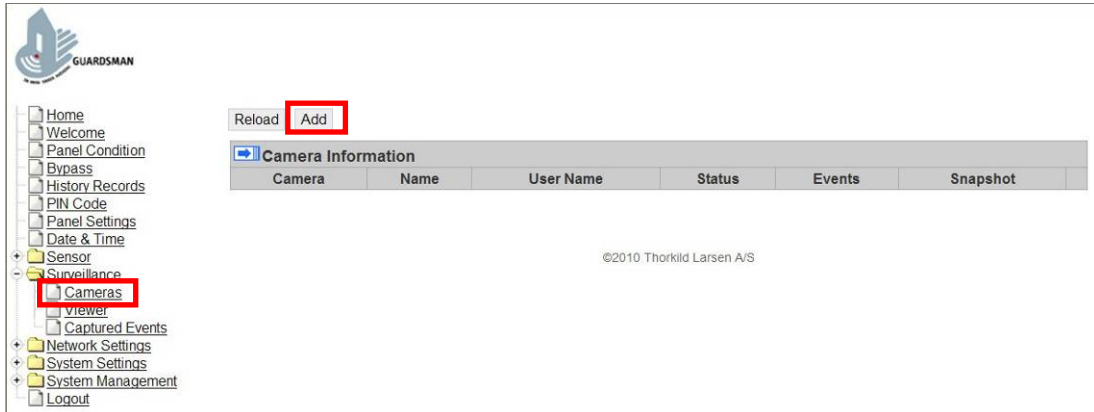
8. Surveillance

※ THIS INSTALLATION IS ONLY AVAILABLE IF CTC-1807 IS PURCHASED ※

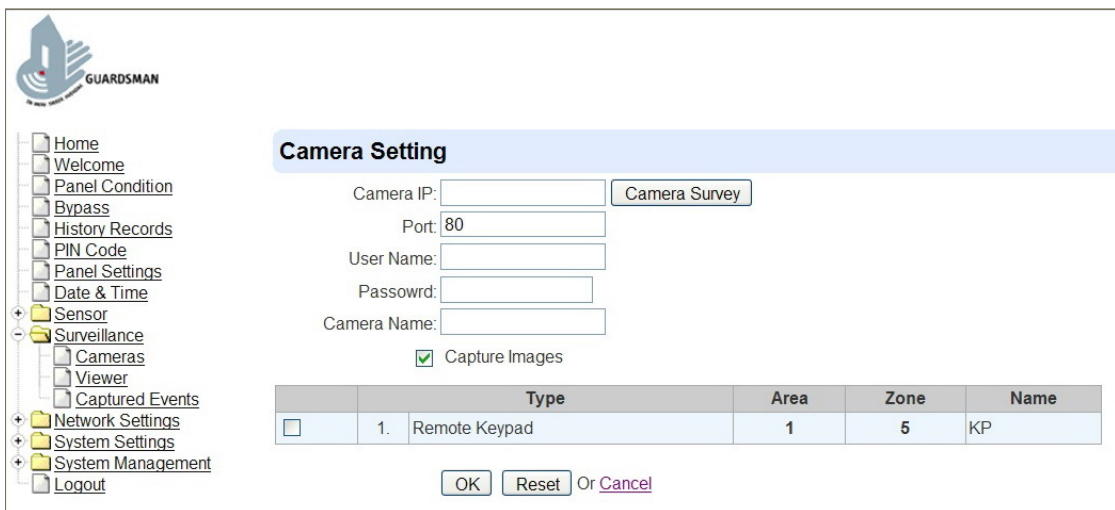
※※ Please make sure your CTC-1807 IP Camera has completed its set up before it can be used with this function ※※

8.1. Cameras

Step 1. On System Web Page, click on **Surveillance**, then **Cameras**. Camera Information will be displayed.



Step 2. Click on **Add** to add a new camera into the system. The following screen will be displayed:



Step 3. Click on **Camera Survey** button to find out all available CTC-1807 IP Address within the LAN. The Camera IP Address will be displayed. Click on **Add** of the corresponding camera to add into the system.



Step 4. Enter the Camera User Name (default: admin), Camera Password (default: admin1234) and Camera Name of the particular CTC-1807 IP Camera that you wish to include.

Step 5. Tick the **Capture Images** check box if you want this camera to capture alarm images once the system has been triggered. If it is not selected, there will be no pre- & post-alarm images available.



| | Type | Area | Zone | Name |
|-------------------------------------|----------------------|------|------|------|
| <input checked="" type="checkbox"/> | 1. Door Contact | 1 | 1 | |
| <input checked="" type="checkbox"/> | 2. IR Sensor | 1 | 2 | |
| <input checked="" type="checkbox"/> | 3. Remote Controller | 1 | 3 | |
| <input checked="" type="checkbox"/> | 4. Wrist TX | 1 | 4 | |

©2008 Solar Denmark A/S

Step 6. Under the **Sensor Type** section, tick the check box in front of each device that you wish to assign the CTC-1807 IP Camera to its corresponding devices. All cameras can be assigned to any learnt-in devices repeatedly (e.g. a Door Contact to be linked to both cameras 1 & 2; a PIR Sensor can be linked to cameras 2, 3, and 4).

Step 7. Press **OK** to confirm the CTC-1807 adding procedure.

<NOTE>

☞ Only one set of pre- & post-alarm images can be stored in CTC-1807 IP Camera (i.e. if an alarm is triggered for a second time, the second pre- &

post-alarm images will not be stored). In order to get the precise captured events when the devices are triggered, users should select the devices located closer to the IP Camera.

- ☞ Users can select different learnt-in devices for one IP Camera (maximum 80 devices), but the selected devices should be set in the same area.
- ☞ The burglar images will be captured in a standard timing of 10 sec pre-alarm & 10 sec post-alarm.

● VIEWING CAPTURE IMAGES

When the alarm is triggered with alarm images captured, click on **View** in the Events column to view all the capture images.

● SNAPSHOT

The system will take real-time snapshots at the speed of 1 image per second. Click on **View** in the Snapshot column to view the images.



The screenshot displays the GUARDSMAN web interface. On the left is a navigation menu with items like Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance (expanded to show Cameras, Viewer, Captured Events), Network Settings, System Settings, System Management, and Logout. The main content area features a 'Camera Information' table with columns for Camera, Name, User Name, Status, Events, Snapshot, and Edit Delete. The 'Events' and 'Snapshot' columns for the first camera entry (192.168.0.97) have 'View' links highlighted with red boxes. Above the table are 'Reload' and 'Add' buttons. A copyright notice '@2008 Solar Denmark A/S' is visible at the bottom of the interface.

| Camera | Name | User Name | Status | Events | Snapshot | Edit Delete |
|-----------------|------|-----------|--------|----------------------|----------------------|-----------------------------|
| 1. 192.168.0.97 | C1 | admin | OK | View | View | Edit Delete |

8.2. Viewer

It is used to support Video stream feature with both **ActiveX mode** (for Internet Explorer users) and **Java mode** (for Internet Explorer and Netscape users).

Step 1. Click on **Viewer** under **Surveillance** to see the 24-Hour live show of each camera.



The screenshot shows the GUARDSMAN web interface. On the left is a navigation tree with the following items: Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance (expanded), Cameras, **Viewer** (highlighted with a red box), Captured Events, Network Settings, System Settings, System Management, and Logout. On the right, there are 'Reload' and 'Add' buttons. Below them is a table titled 'Camera Information'.

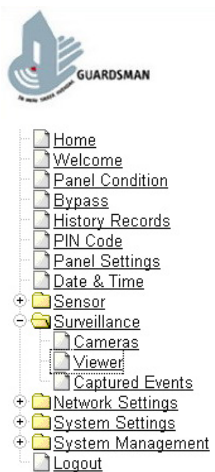
| Camera | Name | User Name | Status | Events | Snapshot | |
|--------|--------------|-----------|--------|--------|----------------------|--|
| 1. | 192.168.0.97 | C1 | admin | OK | View | View Edit Delete |

©2008 Solar Denmark A/S

※ TO USE BELOW FEATURES, PLEASE MAKE SURE YOU HAVE ※
ALREADY INSTALLED JAVA AND ACTIVE-X SOFTWARE

Step 2. Click on **View** in the Java column to watch the real-time video.

Step 3. Click on **View** in the ActiveX column to watch the real-time video.



The screenshot shows the GUARDSMAN web interface. The navigation tree is the same as in Step 1, but 'Viewer' is now selected. On the right, there is a 'Reload' button and a table titled 'Camera Viewer'.

| Camera | Name | Java | ActiveX |
|--------|--------------|----------------------|----------------------|
| 1. | 192.168.0.97 | View | View |

©2008 Solar Denmark A/S

Example:



- Home
- Welcome
- Panel Condition
- Bypass
- History Records
- PIN Code
- Panel Settings
- Date & Time
- + Sensor
- Surveillance
 - Cameras
 - Viewer
 - Captured Events
- + Network Settings
- + System Settings
- + System Management
- Logout

Back

IP Camera Viewer



192.168.0.97

©2008 Solar Denmark A/S

8.3. Captured Events

This screen allows you to see the captured images when an alarm is triggered.

- Step 1.** Click on **Captured Events** to see Burglar images taken by any CTC-1807 IP Camera linked to alarm triggered devices.
- Step 2.** Click on **View** in the View column to see the image gallery.

The numbers in the Status column indicate the number of captured images. The number marked in red represents the number of images captured within 5 sec pre-alarm / post-alarm.

GUARDSMAN

Home
Welcome
Panel Condition
Bypass
History Records
PIN Code
Panel Settings
Date & Time
Sensor
Surveillance
Cameras
Viewer
Captured Events
Network Settings
System Settings
System Management
Logout

Reload Cameras

| Camera | Name | Sensor | Event Time | Status | View |
|--------------|------|--------------------------|---------------------|--------|---|
| 192.168.0.97 | C1 | Area:4, Zone:4, Wrist TX | 2009/12/11 09:49:25 | 25(9) | View Delete |

©2008 Solar Denmark A/S

Example:

GUARDSMAN

Home
Welcome
Panel Condition
Bypass
History Records
PIN Code
Panel Settings
Date & Time
Sensor
Surveillance
Cameras
Viewer
Captured Events
Network Settings
System Settings
System Management
Logout

Reload Captured Events

Surveillance Images

Area:1, Zone:4, Wrist TX
Camera IP: 192.168.0.97
Event Time: 2009/12/11 09:49:25
Time: 2009/12/11 09:49:20

Pages: 1 2

| | | | |
|----------------|----------------|----------------|----------------|
| | | | |
| 12/11 09:49:10 | 12/11 09:49:10 | 12/11 09:49:11 | 12/11 09:49:12 |
| | | | |
| 12/11 09:49:13 | 12/11 09:49:14 | 12/11 09:49:14 | 12/11 09:49:15 |
| | | | |
| 12/11 09:49:16 | 12/11 09:49:17 | 12/11 09:49:18 | 12/11 09:49:19 |
| | | | |
| 12/11 09:49:19 | 12/11 09:49:20 | 12/11 09:49:21 | 12/11 09:49:22 |

Pages: 1 2

<NOTE>



The burglar images will be captured in a standard timing of 10 sec pre-alarm & post-alarm, at the speed of approximately 1 sec per image.

- ☞ The captured time marked in red indicates the picture is captured 5 sec pre-alarm / post-alarm.
- ☞ The speed of image capture will also depend on the numbers of IP Cameras being installed in the system and the speed of your local network connection.
- ☞ Only one set of pre- & post-alarm images can be stored in CTC-1807 IP Camera (i.e. if an alarm is triggered for a second time, the second pre- & post-alarm images will not be stored). You are required to clear the memory before the next set of alarm images can be captured again.
- ☞ To view the full size image, click on the particular image that you wish to enlarge.

- **CLEAR CAPTURED IMAGES**

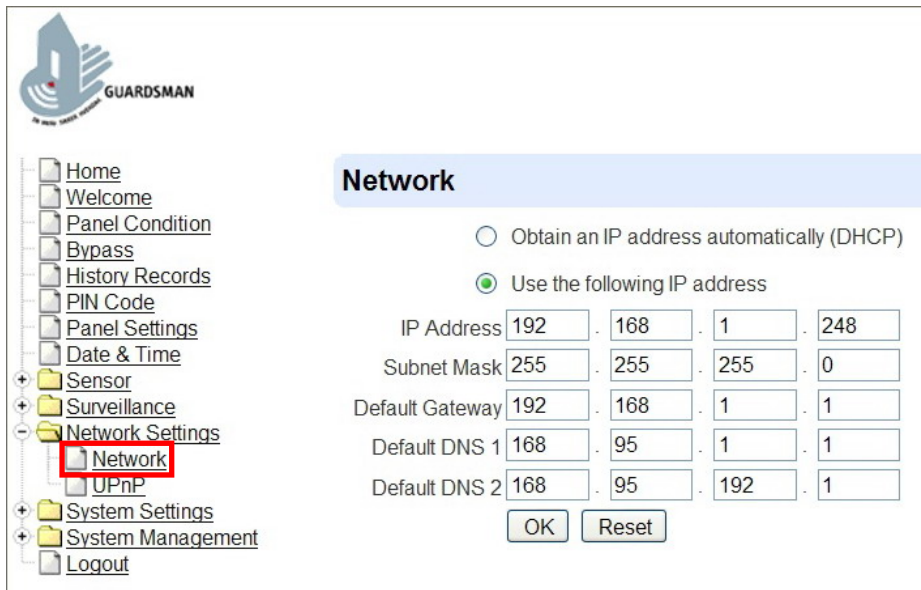
Step 1. Click on **Delete** in the View column to clear the image gallery.

Step 2. A message **Are you Sure?** will be displayed. Press **Yes** to clear the image gallery, or press **No** to cancel and return to Captured Events page.

9. Network Setting

This is for you to program the Network for IP connection.

9.1. NETWORK



- **Obtain an IP address automatically (DHCP)**

If DHCP is selected, the Network will obtain an IP address automatically with a valid Network DHCP Server. Therefore, manual settings are not required.

This is only to be chosen if your Network environment supports DHCP. It will automatically generate all information.

- **Use the IP address**

You can also enter the Network information manually for IP Address, Subnet Mask, Default Gateway, Default DNS 1 and Default DNS 2.

Please make sure that you have obtained all required values according to your Network environment. Please contact your network administrator and/or internet service provider for more information.

9.2. Wireless Setting (Wi-Fi Version Only)

This is for you to enter the Wi-Fi setting of CTC-1241.



The screenshot shows the 'Wireless Setting' page. The SSID is 'WLANAP' and the Security is set to 'None'. There are 'OK' and 'Reset' buttons at the bottom.

Step 1. Key-in your **SSID** name.

Step 2. Select the **Security** Level of your Wi-Fi connection. The available ones are **None**, **WEP**, **WPA** and **WPA2**.

<NOTE>

If you don't know the Wi-Fi SSID and/or Security Level, please contact your network administrator.

- **Security Level set as None**

Select this to disable encryption on CTC-1241.

- **Security Level set as WEP**



The screenshot shows the 'Wireless Setting' page with Security set to 'WEP'. The SSID is 'WLANAP'. The Authentication is set to 'Open System' and the Encryption is set to '64bit'. The Key Type is 'ASCII' and the Key Index is 'Key 1'. There is a 'WEP Key' input field. There are 'OK' and 'Reset' buttons at the bottom.

1. Authentication Type:

Open System: Anyone with the correct SSID can connect to the camera.

Shared Key: Anyone with the correct SSID plus the correct encryption key can connect to the camera, thereby providing a higher level of security..

2. WEP Encryption:

Choose between **64 bits** or **128 bits**.

3. Key Type:

Choose between **ASCII** or **HEX**.

4. Key Index:

You are able to input 4 security keys. This is in case you have more than 1 network that you can connect to. Instead of having to enter the encryption key every time, you can select key 1, 2, 3 or 4. This is especially helpful for 128-bit HEX (52 characters).

5. WEP Key

● Security Level set as WPA

Wi-Fi Protected Access with **Preshared Key**, the key field (Passphrase) needs to be filled out and will support up to 128-bit encryption.



Wireless Setting

SSID:

Security:

Cipher Type: TKIP AES

Passphrase:

1. Cipher Type:

Choose between **TKIP** or **AES**.

2. Passphrase

- **Security Level set as WPA2**



Wireless Setting

SSID:

Security:

Cipher Type: TKIP AES

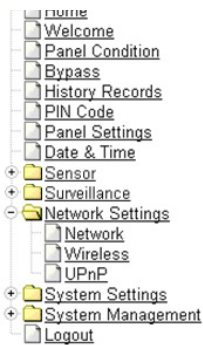
Passphrase:

- 1. Cipher Type:**

Choose between **TKIP** or **AES**.

- 2. Passphrase**

- **Site Survey**



Wireless Setting

SSID:

| Wireless APs <input checked="" type="checkbox"/> | | | |
|--|-------------------|-----|---------------------|
| SSID | MAC | WEP | |
| climaxlab | 00:13:46:C2:48:A4 | Yes | Add |

Security:

Cipher Type: TKIP AES

Passphrase:

- 1. SSID:**

Service Set Identifier is an identifier for the wireless network name that other devices can recognize.

- 2. Site Survey:**

This page will allow you to select a wireless network that CTC-1241 was able to detect upon booting up.

9.3. UPnP

UPnP is Universal Plug and Play, which opens networking architecture that leverages TCP/IP and the Web technologies to enable seamless proximity networking in addition to control and data transfer among networked devices in the home, office, and public spaces.

The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with items like Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, UPnP (highlighted with a red box), System Settings, System Management, and Logout. The main content area is titled 'UPnP' and contains the following settings:

- Enable UPnP Device.
- Enable UPnP Port Redirect.

Port Forwarding

Application: Web Server

Local Port: 80

External Port: 53080

Protocol: TCP

Buttons: OK, Reset

- **Enable UPnP Device:**

CTC-1241 supports UPnP. Once this is selected, you will be able to see this device via any UPnP discovery tool (e.g. Window XP).

- **Enable UPnP Port Redirect:**

The device will try to find an UPnP-supported router and set up the port to redirect to the router.

- **Port Forwarding:**

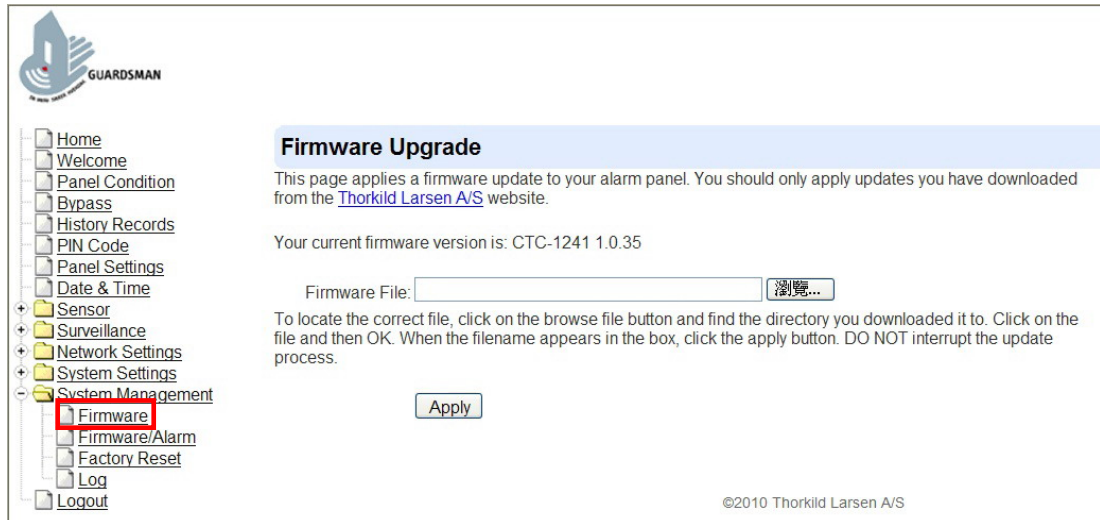
1. **Local Port**
2. **External Port**
3. **Protocol**

10. System Management & History Records

10.1. Firmware

You can upgrade your Web Firmware via Web Page.

Step 1. Click on **Firmware**, the next screen will be displayed:



Step 2. Click on **Browse** and locate the latest Web firmware file in your PC.

Step 3. Click **Apply** to flash to the latest firmware. It will take about 2-5 mins to load the file onto CTC-1241.

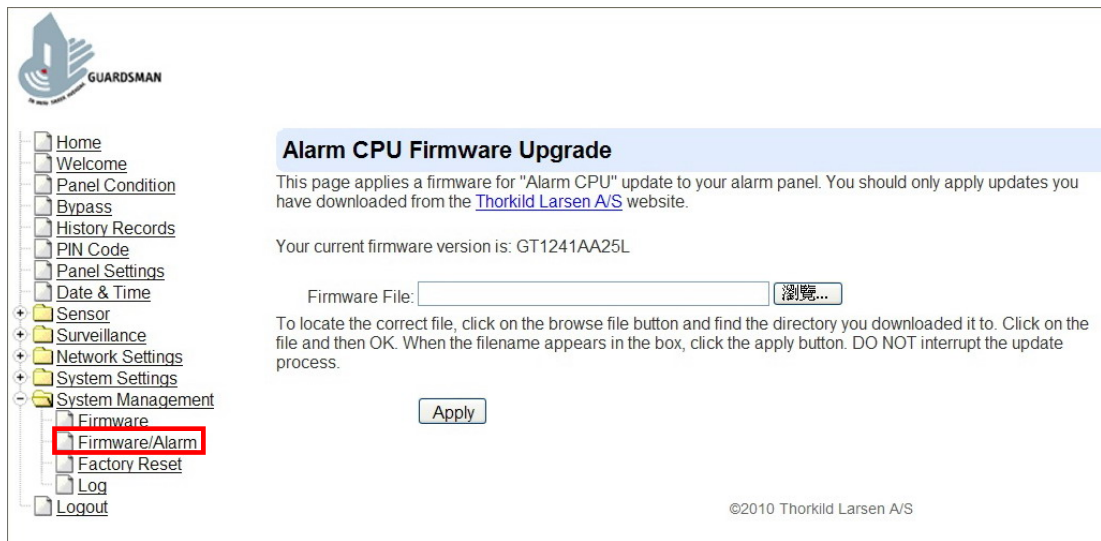
Step 4. Wait for 1 min and do NOT power off during this time.

Step 5. Once Firmware upgrading is complete, it will automatically reboot the CTC-1241 IP Panel.

10.2. Firmware / Alarm (Panel Firmware Update)

You can upgrade your Panel Firmware via Web Page.

Step 1. Click on **Firmware / Alarm**, the next screen will be displayed:



The screenshot shows the GUARDSMAN web interface. On the left is a navigation menu with items like Home, Welcome, Panel Condition, Bypass, History Records, PIN Code, Panel Settings, Date & Time, Sensor, Surveillance, Network Settings, System Settings, and System Management. Under System Management, 'Firmware' is expanded, and 'Firmware/Alarm' is highlighted with a red box. The main content area is titled 'Alarm CPU Firmware Upgrade' and contains the following text: 'This page applies a firmware for "Alarm CPU" update to your alarm panel. You should only apply updates you have downloaded from the [Thorikild Larsen A/S](#) website.' Below this, it states 'Your current firmware version is: GT1241AA25L'. There is a 'Firmware File:' label followed by an empty text input field and a 'Browse...' button. A note below reads: 'To locate the correct file, click on the browse file button and find the directory you downloaded it to. Click on the file and then OK. When the filename appears in the box, click the apply button. DO NOT interrupt the update process.' An 'Apply' button is located below the input field. At the bottom right, the copyright notice '©2010 Thorikild Larsen A/S' is visible.

Step 2. Click on **Browse** and locate the latest Panel firmware file in your PC.

Step 3. Press **Apply** to flash to the latest firmware. It will takes about 2-5 mins to load the file onto CTC-1241.

Step 4. Wait for 1 min and do NOT power off during this time.

Step 5. Once Firmware upgrading is complete, it will automatically reboot the CTC-1241 IP Panel.

10.3. Factory Reset

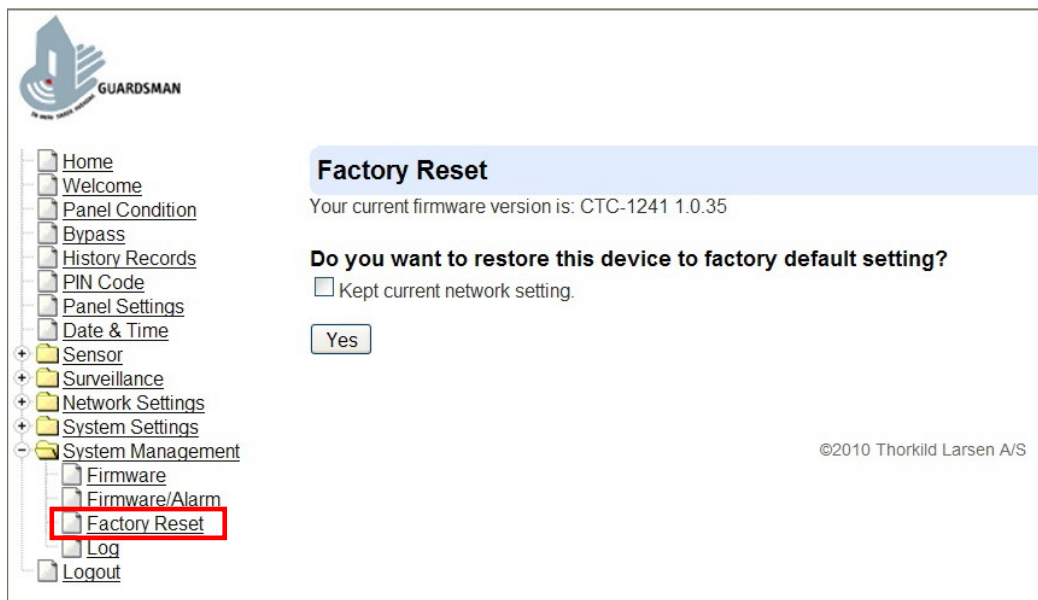
The Control Panel can clear all programmed parameters and reset IP defaults back to Factory Default when either Local Reset or Remote Reset is applied.

Once the **System Reset** is executed, all the programmed data & IP values will returned to its default value, and all the learnt-in devices will be removed. You have to reprogram and learn in the device one by one again.

● LOCAL RESET

- Step 1.** Power down Control Panel and remove the battery
- Step 2.** Apply power while holding down the ▲ key.
- Step 3.** Release the ▲ key when a tone is heard, **Enter Code** will be displayed.
- Step 4.** Enter the following keys sequence: ▲▼▲▼▲▼▲▼, OK
- Step 5.** Press the ⌂ key
- Step 6.** All programmed parameters are reset to factory default setting.
- Step 7.** If more than 17 incorrect keys entered, the unit will revert to normal Alarm On mode.

● REMOTE RESET



- Step 1.** Tick the **Kept current network setting** box to keep the current Network settings. Otherwise, the system will reset its value back to factory default.
- Step 2.** Press **Yes** to continue the Reset procedure.
- Step 3.** Wait for 1 min and do NOT power off during this time.
- Step 4.** Once reset is complete, it will automatically reboot the CTC-1241 IP Panel.

10.4. Log

You can track all the System Event Logs in the **Log** menu under the **System Management** section.

Log List

Reload


| Date | Time | Priority | Identify | Message |
|--------|----------|----------|------------|--|
| Mar 25 | 15:01:50 | info | webs[153] | Web login:admin from:192.168.1.187 |
| Mar 25 | 15:00:54 | info | webs[153] | Web login users are logout by timeout |
| Mar 25 | 14:24:31 | info | webs[153] | Web login:admin from:192.168.1.120 |
| Mar 25 | 14:24:25 | info | webs[153] | Web login users are logout |
| Mar 25 | 14:21:55 | info | webs[153] | Setup SNTP time success. |
| Mar 25 | 14:16:36 | info | webs[153] | Web login:admin from:192.168.1.120 |
| Mar 25 | 14:16:23 | info | webs[153] | Web login users are logout by timeout |
| Mar 25 | 13:59:34 | info | webs[153] | Web login:admin from:192.168.1.187 |
| Mar 25 | 13:29:43 | info | webs[153] | Setup SNTP time success. |
| Mar 25 | 05:22:30 | info | webs[153] | Web login:admin from:192.168.1.120 |
| Mar 25 | 05:21:10 | info | webs[173] | Setup SNTP time success. |
| Jan 1 | 00:00:32 | info | webs[173] | DDNS success and get public IP 59.124.123.22 |
| Jan 1 | 00:00:14 | info | webs[173] | The alarm CPU status:1 |
| Jan 1 | 00:00:14 | info | webs[174] | Running the alarm reporting thread |
| Jan 1 | 00:00:14 | info | webs[173] | Running the timer thread |
| Jan 1 | 00:00:13 | info | webs[172] | Running the command process manager thread |
| Jan 1 | 00:00:13 | info | webs[153] | The ttyS0 file descriptor:6 |
| Jan 1 | 00:00:13 | info | webs[153] | The ttyS0 baud rate:57600 |
| Jan 1 | 00:00:13 | info | webs[153] | WLAN status: disabled |
| Jan 1 | 00:00:13 | info | webs[153] | Alarm panel started... tty= |
| Jan 1 | 00:00:13 | info | webs[153] | Logger started... |
| Jan 1 | 00:00:10 | info | upnpd[152] | Startup the UPnP basic device at 192.168.1.248 |

512K bytes of event logs will be recorded with **Date** (Month & Date), **Time** (Hour & Minute), **Priority** (Info = General System Information; Warning = Finer System Information; Error = System Error Information), **Identiry**, and **Message**.

- The System Event log includes:
 - ✓ Whenever the WAN IP is changed
 - ✓ Date & Time Sychonised
 - ✓ Whenever the Panel is powered on
 - ✓ Captured Burglar images by IP Camera
- The System logged events are displayed in reverse chronological order (most recent event first).

10.5. History Records

You can track all the Panel Event Logs under **History Records**.



| Date | Time | Sensor/User | Activation |
|-------|-------|-----------------------------------|------------|
| 03/25 | 15:25 | Area 2, Admin | Disarm |
| 03/25 | 15:25 | Area 2, Admin | Disarm |
| 03/25 | 15:25 | Area 1, Admin | Disarm |
| 03/25 | 14:41 | Area 2, Admin | Arm |
| 03/25 | 14:41 | Area 1, Admin | Arm |
| 03/25 | 14:25 | Area 2, Admin | Disarm |
| 03/25 | 14:25 | Area 1, Admin | Disarm |
| 03/25 | 14:21 | Area 2, Admin | Disarm |
| 03/25 | 14:21 | Area 1, Admin | Disarm |
| 03/25 | 14:18 | Area 1, User 1 | Disarm |
| 03/25 | 14:18 | Area 1, Admin | Arm |
| 03/25 | 14:18 | Area 1, Admin | Disarm |
| 03/25 | 14:18 | Area 1, Admin | Disarm |
| 03/25 | 14:18 | Area 2, Admin | Disarm |
| 03/25 | 13:47 | Area 1, User 1 | Disarm |
| 03/25 | 13:46 | Area 2, User 10 | Arm |
| 03/25 | 13:46 | Area 1, User 3 | Arm |
| 03/25 | 13:46 | Area 2, User 10 | Disarm |
| 03/25 | 13:46 | Area 1, User 3 | Disarm |
| 03/25 | 13:46 | Area 1, KP, Remote Keypad, User 3 | Arm |
| 03/25 | 13:46 | Area 1, KP, Remote Keypad, User 1 | Disarm |
| 03/25 | 13:46 | Area 1, KP, Remote Keypad, User 1 | Home |
| 03/25 | 13:46 | Area 1, KP, Remote Keypad, User 1 | Disarm |
| 03/25 | 13:46 | Area 1, KP, Remote Keypad, User 1 | Arm |

A total of 250 Panel event logs will be recorded with **Date** (Month & Date), **Time** (Hour & Minute), **Sensor / User**, and **Activation** (cause of event).

- The Panel alarm log memorizes the last 30 Panel events including:
 - ✓ All Alarm Events with Device ID
 - ✓ All Fault Warning Events from Panel or Device
 - ✓ All Arming And Disarming Events by Panel
- The Panel logged events are displayed in reverse chronological order (most recent event first).