

# USER MANUAL

## FLASH SETUP

for

## RAMOS MINI A, B, C

**Tel** +420 261 219 182  
**Fax** +420 261 219 192  
**E-mail** [conteg@conteg.com](mailto:conteg@conteg.com)

**Company ID** 25701843  
**VAT ID** CZ25701843  
**Web** [www.conteg.com](http://www.conteg.com)



**Contents**

**Flash Setup ..... 3**  
**General ..... 4**  
**General Setup ..... 5**  
**SNMP Setup ..... 10**  
**Sensors Setup ..... 12**  
**Email & SMS Setup..... 15**  
**Log & Time ..... 17**

## Flash Setup

---

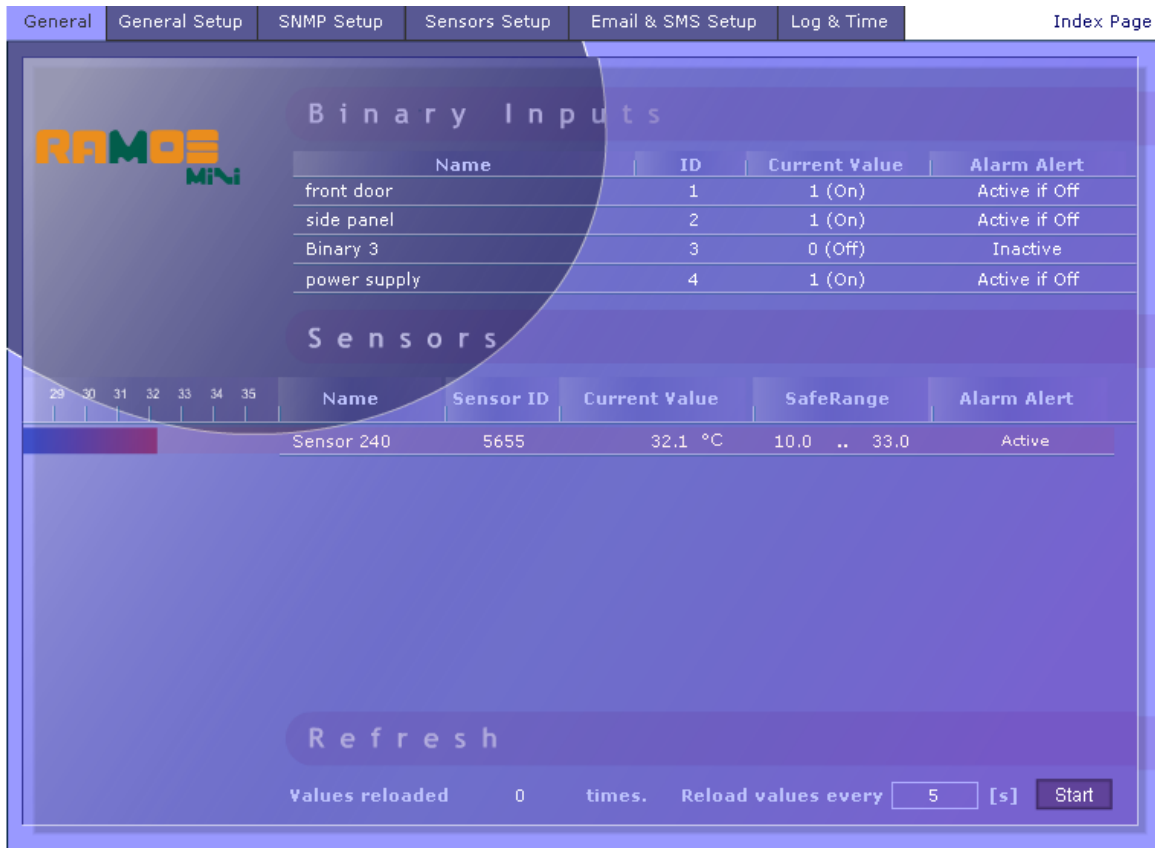
*The Ramos Flash Setup graphical interface is designed for user-friendly device configuration. The user can access the Flash Setup by clicking the **Web Configuration: Flash Setup** link at the bottom of the main web page.*

The concise and user-friendly graphic interface consists of 6 tabs:

- GENERAL
- GENERAL SETUP
- SNMP SETUP
- SENSORS SETUP
- EMAIL & SMS SETUP
- LOG & TIME

## General

The **General** tab contains basic information about the connected sensors. In addition to numeric values, temperatures are indicated graphically at the left-hand side of the page. The page reloads with the specified frequency.



General | General Setup | SNMP Setup | Sensors Setup | Email & SMS Setup | Log & Time | Index Page

**RAMOS MINI**

### Binary Inputs

| Name         | ID | Current Value | Alarm Alert   |
|--------------|----|---------------|---------------|
| front door   | 1  | 1 (On)        | Active if Off |
| side panel   | 2  | 1 (On)        | Active if Off |
| Binary 3     | 3  | 0 (Off)       | Inactive      |
| power supply | 4  | 1 (On)        | Active if Off |

### Sensors

| Name       | Sensor ID | Current Value | SafeRange    | Alarm Alert |
|------------|-----------|---------------|--------------|-------------|
| Sensor 240 | 5655      | 32.1 °C       | 10.0 .. 33.0 | Active      |

Refresh

Values reloaded 0 times. Reload values every 5 [s] Start

- **Values reloaded X times** – shows how many times were the readings reloaded
- **Reload values every X [s]** – frequency of reloading the readings in seconds
- **Start/Stop** button – enable/disable periodic reloading of readings from the Ramos unit

## General Setup

Network settings of the device: Network parameters, trusted IP address range, temperature units, output states, etc.



The screenshot shows the 'General Setup' page for a 'Ramos Mini C' device. The interface is divided into several sections:

- Output Settings:** BinOut 1 is set to 'Off' and BinOut 2 is set to 'On when any alarm'.
- Security:** IP Access Filter table:

| Access to | IP Address Value | IP Mask Range |
|-----------|------------------|---------------|
| HTTP      | 0.0.0.0          | 0.0.0.0       |
| SNMP      | 0.0.0.0          | 0.0.0.0       |

User Passwords table:

| Name | Password | Access Type  |
|------|----------|--------------|
|      |          | Read Only    |
|      |          | Read & Write |

HW Security Protection: Disabled
- Network Settings:** Device Name: Ramos Mini C; Device IP Address: 192.168.161.99; Network Mask: 255.255.255.0; Gateway: 192.168.161.1; HTTP Port: 80; TCP Telnet Setup: 99.
- DNS Settings:** DNS Primary: 0.0.0.0; DNS Secondary: 0.0.0.0.
- Other Settings and Informations:** Display temperature in: Celsius [°]; Flash Setup Version: 2.8.1; Device FirmWare: 3.0.3 (with Update FW button).

An 'Apply Changes' button is located at the bottom right of the form.

### Output Settings

Controls binary outputs. The setting is valid only until the device is restarted. Available options:

- **On** (logic H)
- **Off** (logic L)
- **On when any alarm**  
Output is controlled locally by the Ramos unit. When no sensors (including dry contact inputs) are in the alarm state, the output is set low (Off). When at least one output is in the Alarm state, the output is set high (On).
- **Off when any alarm**  
Output is controlled locally by the Ramos unit. Whenever at least one output is in the Alarm state, the output is set low (Off).

## Security

Security settings. Properties of individual modes are shown in the following table. Lines indicate the method of accessing the device over IP, columns specify the restrictions resulting from the respective security settings.

|                 | No restrictions | HW protection<br>DIP = On | User Password |                |              | IP Access filter |        | SNMP communication |         |
|-----------------|-----------------|---------------------------|---------------|----------------|--------------|------------------|--------|--------------------|---------|
|                 |                 |                           | Read only     | Read + Outputs | Read & Write | HTTP             | SNMP   | Comun1             | Comun2  |
| Web index       | R               | R                         | R             | R              | R            | Access           |        |                    |         |
| Flash setup     | R/W             | R                         | R             | R/W**          | R/W          | Access           |        |                    |         |
| Values.xml      | R               | R                         | R             | R/W**          | R            | Access           |        |                    |         |
| Setup.xml       | R/W             | R                         | R             | R              | R/W          | Access           |        |                    |         |
| SNMP get (next) | R               | R                         |               |                |              |                  | Access | R*                 | R*      |
| SNMP set        | R/W             | R                         |               |                |              |                  | Access | [R*/]W*            | [R*/]W* |
| Modbus/TCP      | R/W             | R                         |               |                |              |                  |        |                    |         |
| TCP setup       |                 | Disabled                  | R             | R              | R/W          | Access           |        |                    |         |
| UDP config      | R/W             | R                         |               |                |              | R                | R      |                    |         |

\* R and/or W must be enabled on the SNMP Setup tab by checking appropriate boxes.

\*\* Only the values of outputs can be written, nothing else. Output mode cannot be changed.

**Note:** The “**No restrictions**” column reflects the default configuration (also shown on the screenshots presented here). That is, HW protection DIP=Off, no password set, IP Access filter set to 0.0.0.0/0.0.0.0.

- **HW Security Protection**

A DIP switch that prevents any changes in the device configuration.

- **OUTPUTS:** You can change values of outputs.
- **CONFIGURATION:** No changes are permitted.

The protection status is displayed in the bottom left-hand corner. When the HW Protection is active, any configuration changes, including changes of the output states, are ignored. This mode is useful when connecting the Ramos to a publicly accessible network.

- **User Passwords**

Two separate user accounts (username and password) can be set up for SNMP and HTTP access.

- Account types:
  - ‘**Read Only**’ – can only read values and configuration settings
  - ‘**Read Only + Outputs**’ – can read values and set outputs, cannot change configuration settings (not even sensor names)
  - ‘**Read & Write**’ – can perform any changes

- The “Read Only” account only has read access to values, cannot perform any configuration changes. The “Read&Write” account can change configuration settings.
  - After setting up a username and a password, you will be asked to log in every time you try to open the Flash interface.
  - Passwords also apply to access to the values.xml and setup.xml files – see the table.
  - In case of “Read Only” HTTP access, you will no longer be able to change configuration settings in Flash setup.
  
- **IP Access Filter**  
 Allows you to define a range of trusted IP addresses that are allowed to access the Ramos over HTTP and SNMP. The trusted IP range is configured separately for each protocol.

To set up the filter, specify the base IP address and the mask that define the trusted range. Access is granted if the following condition is true (AND represents bitwise multiplication):

$$(\text{IP trying to access AND IP Mask Range}) = \text{IP Address Value}$$

| IP Filter settings |                 | Access granted to  |                               |
|--------------------|-----------------|--|-------------------------------|
| IP Address Value   | IP Mask Range   | From – To  |                               |
| 192.168.1.2        | 192.168.1.2     | 192.168.1.2  | Only one IP trusted           |
| 192.168.1.87       | 192.168.1.87    | 192.168.1.87   | Only one IP trusted           |
| 192.168.1.0        | 192.168.1.224   | 192.168.1.0 – 192.168.1.31   | 32 trusted addresses          |
| 192.168.1.0        | 192.168.1.0     | 192.168.1.0 – 192.168.1.255  | All 256 addresses 192.168.1.x |
| 192.168.0.2        | 192.168.254.255 | 192.168.0.2 and 192.168.1.2  | One address on two networks   |
| 192.168.0.0        | 192.168.252.240 | 192.168.0.0 - 192.168.0.15<br>192.168.1.0 - 192.168.1.15<br>192.168.2.0 - 192.168.2.15<br>192.168.3.0 - 192.168.3.15 | 4 x 16 addresses can access   |

- **SNMP community (passwords)**  
 Two different password can be configured. For each of them, it is possible to allow R or R/W access, or temporarily disable it.

Most SNMP programs use the following (default) settings. For security reasons, we highly recommend to change the R/W access password.

- R (get, get next) “public”

- R/W (set) "private"

**Note:** SNMP Access settings are available at the *SNMP Setup* tab.

## What to do if you forget your password

- Restore the factory-default configuration of the device by one of the following methods:
  - Use the **UDP Config** utility (must run on the same network segment). Right-click the line corresponding to the device and select "Load defaults" from the pop-up menu.
  - Use the **DIP Load defaults** feature. Toggle the DIP1 switch several times during the first 5 seconds after powering up the device.
  - Connect to the **Serial Setup** (RS-232) and execute the **Load Defaults** function from the terminal menu. The menu is equivalent to that of Telnet Setup.  
To enter the menu: 9600/8N1, DIP1=1, restart the device.

## Device Name

Name assigned to a particular device. The name is shown in all lists along with the IP address (UDP Config); it is used as the sysname variable in SNMP.

## Network Settings

This block configures the main network parameters for Ethernet communication:

- **Device IP address**  
IP address of the unit. After a change, the device needs to be restarted.
- **Network mask**  
Local network mask. After a change, the device needs to be restarted.
- **Gateway**  
Default gateway. After a change, the device needs to be restarted.
- **HTTP port**  
Port for communication over the HTTP protocol. Default is **80**.
- **TCP Telnet Setup**  
Port for the terminal telnet setup mode. Default is **99**.

## DNS Settings

Primary and secondary DNS server settings. Gateway needs to be set correctly for correct operation.

A DNS server is necessary for converting domain names to IP addresses. Without a correctly configured DNS server, the following functions will not work:

- Time sync (SNTP), used in e-mails and SNMP traps to timestamp events
- E-mailing (SMTP)
- Logging of values with timestamps

**Note:** *The DNS server is often the same as the gateway. Sometimes, the local firewall only allows access to a specific local DNS server. Please contact your network administrator for details.*

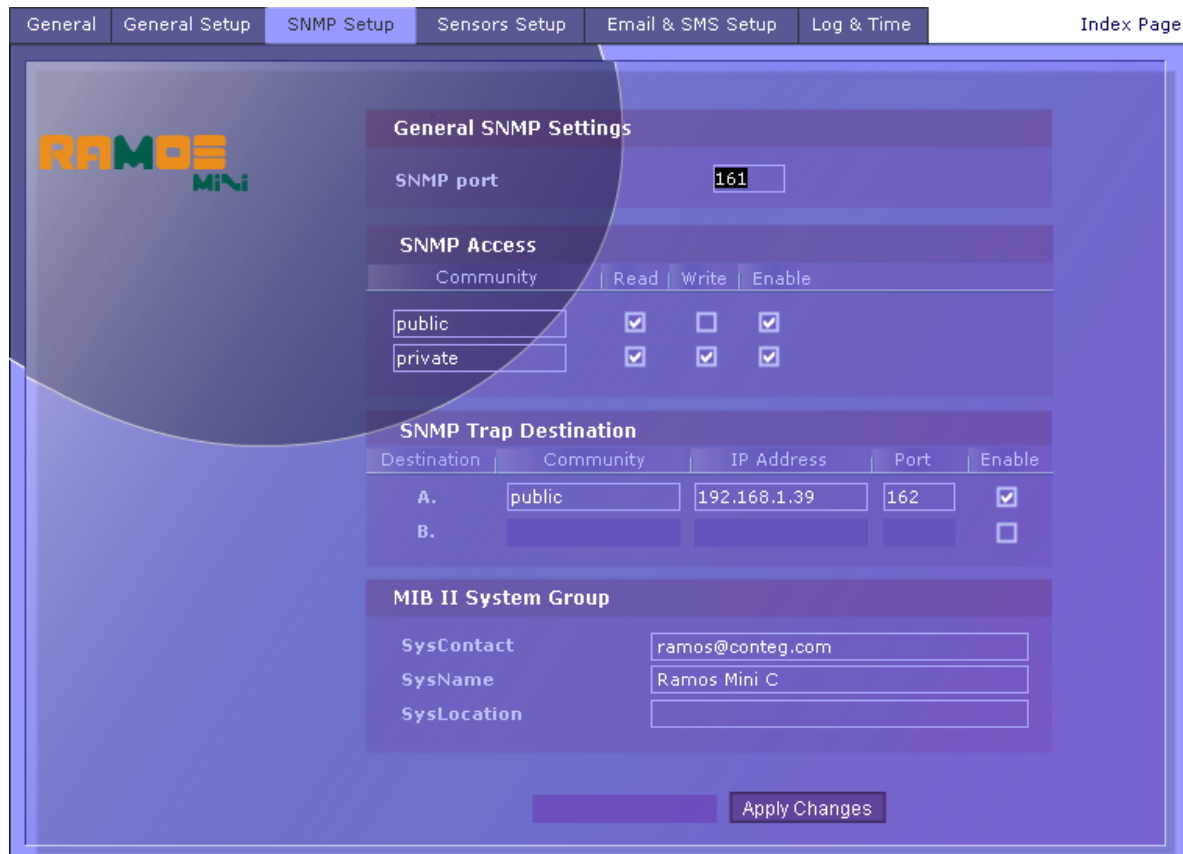
## Other Settings and Information

- **Display temperature in**  
Specifies the unit of temperature (C – Celsius / centigrade, F – Fahrenheit, K – Kelvin). The setting only applies to the WWW interface. All other interfaces and protocols use °C, unless specified otherwise in the interface description.
- **Flash Setup Version** – Version of the graphic interface
- **Device FirmWare** – Version of the device firmware
- **Update FW** button  
Updates the firmware over the WWW. The link to the update page is available at the main page, too. Firmware update erases the current device configuration.

**Note:** *Any changes must be confirmed by clicking the Apply Changes button. A successful change is indicated by an animation in the status bar next to the Apply changes button.*

## SNMP Setup

The SNMP Setup tab allows you to configure the settings for communication with the device using the SNMP protocol.



General | General Setup | **SNMP Setup** | Sensors Setup | Email & SMS Setup | Log & Time | Index Page

**RAMOS MINI**

### General SNMP Settings

SNMP port:

### SNMP Access

| Community | Read                                | Write                               | Enable                              |
|-----------|-------------------------------------|-------------------------------------|-------------------------------------|
| public    | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| private   | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

### SNMP Trap Destination

| Destination | Community | IP Address   | Port | Enable                              |
|-------------|-----------|--------------|------|-------------------------------------|
| A.          | public    | 192.168.1.39 | 162  | <input checked="" type="checkbox"/> |
| B.          |           |              |      | <input type="checkbox"/>            |

### MIB II System Group

SysContact:   
SysName:   
SysLocation:

### General SNMP Settings

- **SNMP port**  
Communication port to use for the SNMP protocol (default is **161**).

### SNMP Access

Defines names and access rights for user groups that can work with the Ramos unit.

- **Community**  
Textual name of the authorized group (usually **Public** and **Private**)
  - **Read** – The community is authorized to read variables over SNMP
  - **Write** – The community is authorized to write values to variables over SNMP
  - **Enable** – Enables or disables the group (community)

## SNMP Trap Destination

Define target destinations A and B for sending SNMP traps.

- **Community** – Textual name of the group for the SNMP trap being sent
- **IP address** – Destination address where the SNMP traps are sent
- **Port** – Destination port where the SNMP traps are sent
- **Enable** – SNMP traps are sent to this destination

## MIB II System Group

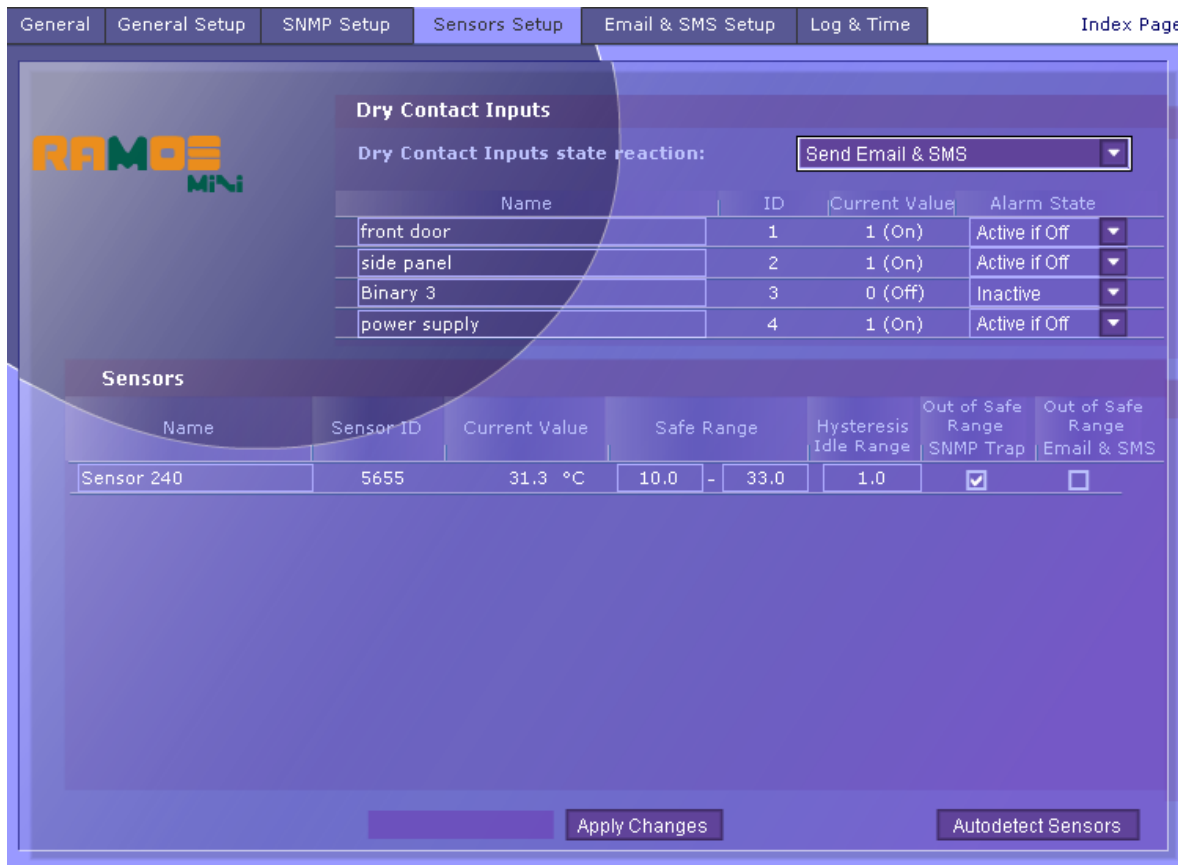
User-defined settings in the standard SNMP header.

- **SysContact** – Contact information of the system administrator, e.g. an e-mail address
- **SysName** – Device name
- **SysLocation** – Location of the unit, e.g. “IT room, floor 2”

**Note:** *Any changes must be confirmed by clicking the Apply Changes button. A successful change is indicated by an animation in the status bar next to the Apply changes button.*

## Sensors Setup

The Sensors Setup tab allows you to configure the settings for all sensors as well as for Dry Contact inputs.



| Name         | ID | Current Value | Alarm State   |
|--------------|----|---------------|---------------|
| front door   | 1  | 1 (On)        | Active if Off |
| side panel   | 2  | 1 (On)        | Active if Off |
| Binary 3     | 3  | 0 (Off)       | Inactive      |
| power supply | 4  | 1 (On)        | Active if Off |

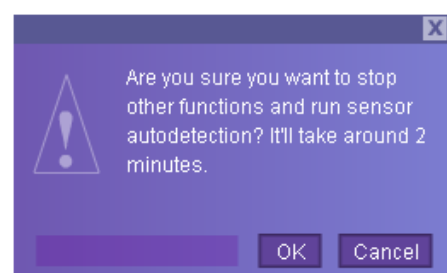
  

| Name       | Sensor ID | Current Value | Safe Range  | Hysteresis Idle Range | Out of Safe Range SNMP Trap         | Out of Safe Range Email & SMS |
|------------|-----------|---------------|-------------|-----------------------|-------------------------------------|-------------------------------|
| Sensor 240 | 5655      | 31.3 °C       | 10.0 - 33.0 | 1.0                   | <input checked="" type="checkbox"/> | <input type="checkbox"/>      |

### Autodetect Sensors

Starts the automatic detection of connected sensors.

When you click the button, a pop-up dialog asks you whether you want the device to stop all other tasks and start detecting sensors automatically. Click OK to stop all activity and start the autodetection. The process can take a long time, even 2 minutes.



When the detection completes, a dialog informs you about the results. After a successful autodetection, all sensors are ready to measure.

**Note:** For a faster autodetection with a more detailed output, see the TCP Setup section.

## Dry Contact Inputs

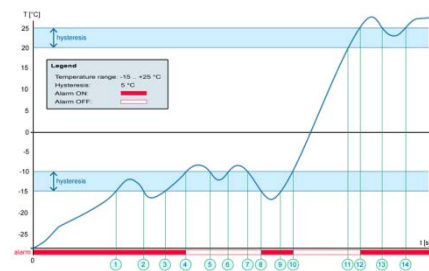
Configuration parameters for the binary (dry contact) inputs.

- **Name** – Name of the input, up to 12 chars (e.g. “left door”, “smoke room 1”)
- **ID** – Unique ID of the input variable within the device
- **Current Value** – Current state of the inputs – “0 (Off)” / “1 (On)”
- **Alarm State** – Alarm state definition for each input
  - **Active if On** – Alarm is active whenever the input is in 1 (On)
  - **Active if Off** – Alarm is active whenever the input is in 0 (Off)
  - **Inactive** – Input has no alarm state defined
- **Dry Contact Inputs state reaction**  
Alarm activation/deactivation response, common for all Dry Contact inputs
  - **Inactive** – Ramos does not react to alarm from Dry Contact inputs
  - **Send SNMP Trap** – SNMP trap is sent upon alarm activation and deactivation
  - **Send Email & SMS** – E-mail and SMS are sent upon alarm activation/deactivation
  - **Send SNMP Trap + Email & SMS** – Both the SNMP trap and the e-mail (or SMS) are sent upon alarm activation or deactivation

## Sensors

Configuration of detected sensors. The sensors must be detected first with Autodetection.

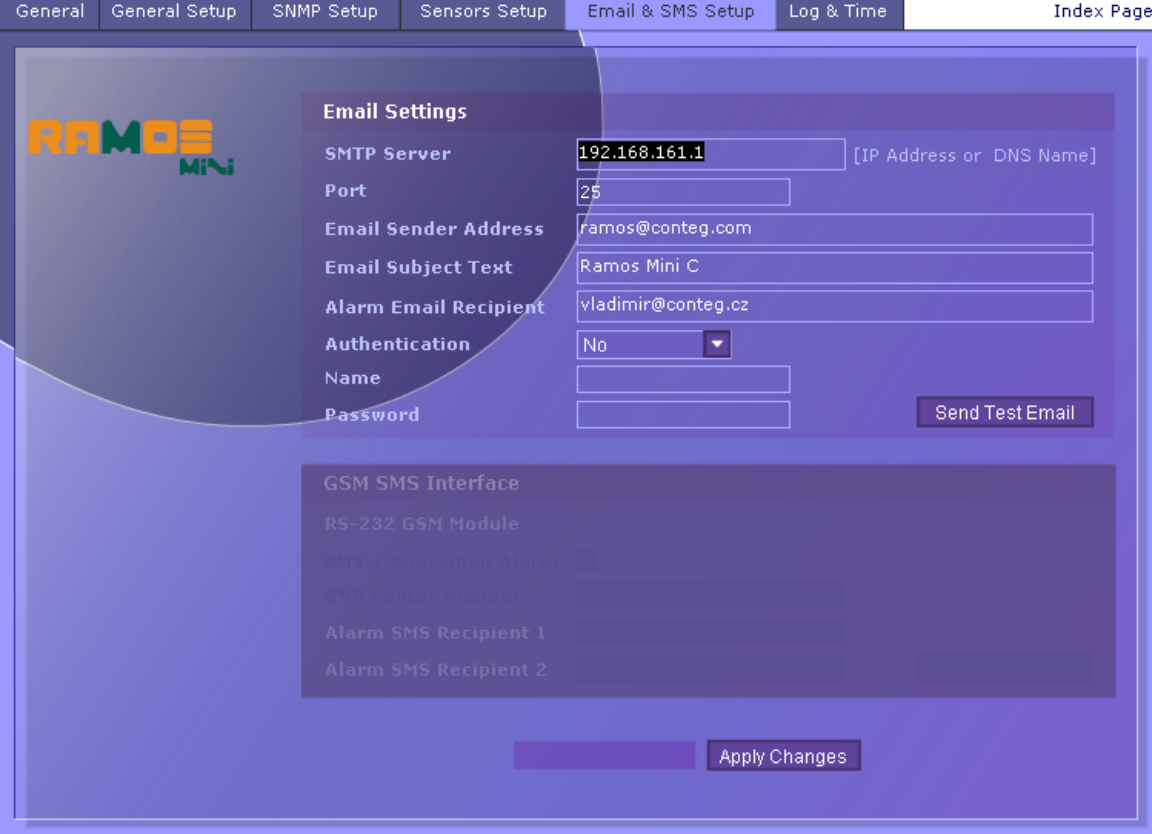
- **Name** – Name of the input, up to 12 chars (e.g. “above door”, “area1 humid”).
- **ID** – Unique sensor identifier, specifies its address on the bus. For more details about sensor IDs, see *Overview of the Ramos product line or Supported interfaces*.
- **Current Value** – Current sensor reading. Sensors that are not found or not working read as “-999.9”.
- **Safe Range** – Range of values which are considered to be OK. When the reading is outside of this safe range, alarm is activated.
- **Hysteresis Idle Range**  
Defines a tolerance range to prevent raising multiple alarms if the value fluctuates near the threshold.  
See the detailed description in the *Sensor Hysteresis* section.
- **Out of Safe Range**  
Defines the response if a value is outside of its safe range:



- **SNMP Trap** – Enables sending a SNMP trap upon alarm activation/deactivation
- **Email & SMS** – Enables sending an e-mail and a SMS are sent upon alarm activation/deactivation  
Enables or disables sending an e-mail or SMS in case of exceeding the safe range


## Email & SMS Setup

This tab contains e-mailing settings the Ramos unit.



The screenshot displays the 'Email & SMS Setup' configuration page. At the top, there are navigation tabs: 'General', 'General Setup', 'SNMP Setup', 'Sensors Setup', 'Email & SMS Setup' (selected), 'Log & Time', and 'Index Page'. The main content area is divided into two sections: 'Email Settings' and 'GSM SMS Interface'. The 'Email Settings' section includes fields for 'SMTP Server' (192.168.161.1), 'Port' (25), 'Email Sender Address' (ramos@conteg.com), 'Email Subject Text' (Ramos Mini C), 'Alarm Email Recipient' (vladimir@conteg.cz), 'Authentication' (No), 'Name', and 'Password'. A 'Send Test Email' button is located at the bottom right of this section. The 'GSM SMS Interface' section includes a 'RS-232 GSM Module' field and two 'Alarm SMS Recipient' fields. An 'Apply Changes' button is located at the bottom center of the page.

### Email Settings

- **SMTP Server** – Host name or IP address of the SMTP server
- **Port** – Port for communication with the SMTP server (**25** by default)
- **Email Sender Address** – E-mail address shown in the “From:” field
- **Email Subject Text** – Subject of the e-mails sent
- **Alarm Email Recipient** – E-mail address of the recipient
- **Authentication** – Enables username/password authentication if the SMTP server requires it
  - **Name** – Username for authentication with the SMTP server
  - **Password** – Password for authentication with the SMTP server
- **Send Test Email** button – Sends a test e-mail 

**Tip:** *It is not always necessary to configure a **SMTP Server** in order to send e-mails. The Ramos can work as SMTP server itself and deliver the e-mails directly to the user's mailbox. However, always test this mode in your particular environment – the e-mails sent in this mode are often blocked by various spam filters due to missing reverse MX records.*

## Received e-mail example:

- E-mail subject: **Table1**
- E-mail is sent upon every alarm activation and deactivation.

```
29.05.2007 13:28:24 Ramos 192.168.005.114
-----
ID      Name                Value  Unit  ALARM      Safe Range
-----
ALARM state:
-----
      2 Contact Input 2    OFF   if OFF
      3 Contact Input 3    ON    if ON

Sensors:
-----
      1 Contact Input 1    OFF   if ON
      2 Contact Input 2    OFF   if OFF
      3 Contact Input 3    ON    if ON
61423 Sensor 1 - Temp    23.2 °C  Enabled  10.0 .. 28.0
      74 Sensor 2 - Temp    25.4 °C  Enabled  10.0 .. 28.0
      106 Sensor 3 - Humi    36.6 %RH Enabled  10.0 .. 60.0

-----
Ramos 1250 : http://192.168.5.114
-----
```

**Tip:** For detailed description of the e-mail format, see the "Using Ramos units in your programs" section.

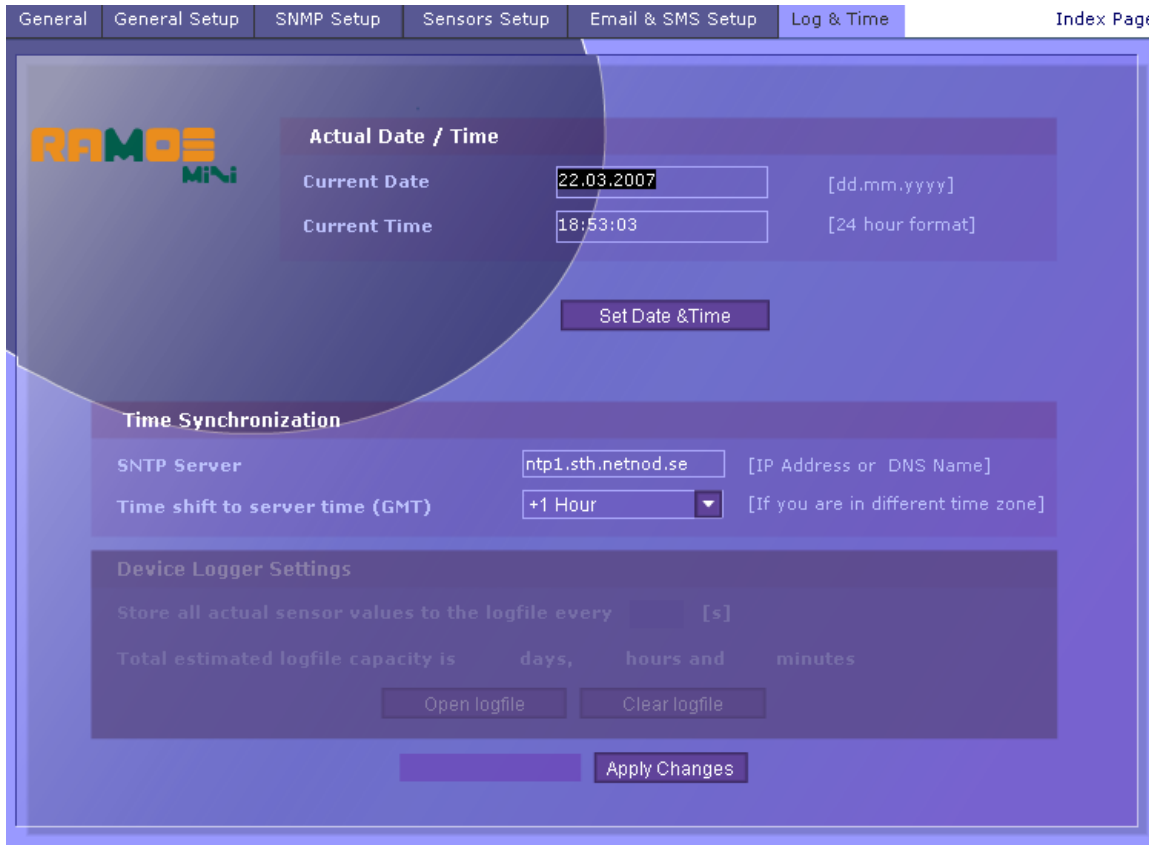
## Sending a test e-mail

Multiple systems need to be configured correctly in order to send e-mails from the device successfully. Therefore, it is advisable to double-check the following parameters:

- **Gateway** for the network connection
- **DNS server** for the network connection
- **SMTP server** and port
- **Authentication** turned on, correct **name** and **password**
- **Spam filter** of your mailbox turned off

## Log & Time

This tab lets you configure the date, time, and logging options (if supported by the particular Ramos model).



### Actual Date / Time

Current date and time settings

- **Current Date** – Date in the [dd.mm.yyyy] format, for example: **31.12.2006**
- **Current Time**  
Current time in the 24-hour [hh:mm:ss] format, for example: **17:38:55**. The time updates automatically while the browser window is open. It is only saved when the “**Set Date & Time**” button is clicked.

**Note:** *Date and time changes are not linked to the Apply Changes button and must be confirmed by clicking the Set Date & Time button.*

## Time Synchronization

SNTP server settings for time synchronization. If the time is not set (the date 1.1.1970 is displayed), the device attempts to synchronize the time approximately once per hour until successful.

- **SNTP Server**  
IP address or host name of the SNTP server to synchronize the time with.  
Preconfigured server is **ntp1.sth.netnod.se**
- **Time shift to server time (GMT)**  
Configure the offset of your timezone with respect to that of the SNTP server. SNTP servers use UTC time, which is nearly equivalent to GMT (London time). Hence, for Paris, Berlin, Prague, and other locations within the same time zone, set +1 hour.

**Note:** *The clock does not run when the device is powered off. The unit contains no battery. After a power failure, the time will be synchronized with the SNTP server.*

## Data Logger Settings

Configuration parameters for logging values to a circular buffer within the internal flash memory. When the buffer is full, the oldest values are overwritten with the newest ones. This function is supported only by certain Ramos models, for example the **Ramos 2251**.

- **Store all actual sensor values to the logfile every**  
Frequency of storing all readings to the log file
- **Total estimated logfile capacity is**  
The capacity estimate is given in days, hours and minutes. The Ramos calculates the capacity based on the number of sensors detected.
- **Open logfile** button  
Stores the current log file to disk by calling the external **/spilog.txt** file.
- **Clear logfile** button  
Clears all values from the logfile by calling the external **/spilog.del** file.

**Note:** *Any changes must be confirmed by clicking the Apply Changes button. A successful change is indicated by an animation in the status bar next to the Apply changes button.*