User Guide

Management Web Interface
Summary

Interface Connection..............................................................................................................................................................................6
Dashboard............................................................................................................................................................................................................7
LoneWorker Security set-up......................................................................................................................................................................12
Smartphone applications and authorizations management..................................................................................................................12
Set up patrols or Start & End of services..........................................................................................................................................................13
Forms Management..................................................................................................................................................................................13
Follow up.............................................................................................................................................................................................................14
Settings..................................................................................................................................................................................................................27
Tags Forms............................................................................................................................................................................................................61
Multi-Accounts........................................................................................................................................................................................................72
Write us.................................................................................................................................................................................................76
Help....................................................................................................................................................................................................................77
Annex.................................................................................................................................................................................................................79
Illustrations Index................................................................................................................................................................................................83
# Table of Contents

- Interface Connection ................................................................. 6
- Dashboard ............................................................................. 7
  - Header .................................................................................. 8
  - Menus .................................................................................. 9
  - Content ............................................................................... 10
    - PUSH Messages ................................................................. 11
- LoneWorker Security set-up ..................................................... 12
- Smartphone applications and authorizations management ...... 12
- Set up patrols or Start & End of services ................................. 13
- Forms Management .................................................................. 13
- Follow up ............................................................................... 14
  - Traces ................................................................................. 14
  - Real Time ............................................................................ 16
- Smartphones .......................................................................... 17
- Remote Monitoring ................................................................ 17
- Connection ........................................................................... 18
- Patrons .................................................................................. 19
- Services ............................................................................... 20
- Forms ................................................................................... 21
- Statistics ............................................................................... 22
  - Events ................................................................................. 22
  - Usage ................................................................................ 23
  - Autonomy .......................................................................... 24
  - LoneWorker Usage .............................................................. 24
  - Number of uses .................................................................... 25
- Beacons ................................................................................ 26
- Settings .................................................................................. 27
  - Company ............................................................................ 27
  - Users .................................................................................. 28
  - Smartphones .................................................................... 31
    - Menu button ...................................................................... 32
      - Main tab ......................................................................... 32
      - NFC tab .......................................................................... 32
      - Menu tab .......................................................................... 33
    - LoneWorker button ............................................................. 34
      - Main tab .......................................................................... 34
Interface Connection

The connection to the management interface requires an ID and a Password. You can access to the connection page from our website neosafe.fr.

1) Click on the Client Access button located on the top right corner

![Client Access button on the website](image1)

**Illustration 1: Neosafe website**

2) You can now enter your connection information: ID (mail) and Password

![Login page](image2)

**Illustration 2: Client Access**
Dashboard

The Dashboard is the main page of this management web interface. It is composed of three separate zones:

1. **Header**
2. **Menus**
3. **Content**

*Illustration 3: Dashboard*
Header

This part is always visible, regardless of the page currently viewed by the user.

1) Account name
   It can be changed from the setting page by clicking on Settings --> Users. By holding the mouse on this part, you can access the account modification or the log off button

2) Pop-up display

3) Refresh button
   Use this one instead of the navigator’s refresh button

4) Switch the language to English

5) Switch the language to French
Menus

Click on a menu show a drop-down list with all the associated sub menus.

Illustration 5: Menus allowing to navigate through the web interface

1) NeoSafe company logo
2) Access to the Dashboard
3) Access to the Follow up functions
4) Access to the Settings functions
5) Access to the patrols, start & end of services and forms functions
6) Access to the Messenger functions
7) Access to the NeoSafe dialog box
8) Access to the FAQ and the technical documents
Content

The Dashboard display a quick review of the many information available on the web interface, in a tiling form.

Illustration 6: Dashbord display

Each tile matches to a specific information, briefly summarized. You can also find a link that lead directly to the linked setting.
PUSH Messages

A PUSH message is a pop-up containing a specific message defined from the web interface that will appear on the chosen smartphone.

1) Receivers selection, you can choose among the LoneWorker smartphones related to this account
2) Message title
3) Message content
4) Message settings

Illustration 7: PUSH messages personalization
LoneWorker Security set-up

The big steps to set up the LoneWorker Security are listed below. Every step is detailed in the linked chapter.

1) **Set up the smartphone configuration** (Settings --> Smartphones --> L.W.)
   This is the set-up of the security equipment
2) **Events management set-up** (Settings --> Events)
   The entire system (smartphone and Neosafe servers) generates a lot of messages called events. The system administrator can define which action set up when a specific event appears.
   For example, a SOS event can trigger a cascade call from a vocal server, or send an e-mail.
3) **Security Instructions establishment** (Settings → Safety)
   The steps is available only if the Remote Monitoring channel is active.

Smartphone applications and authorizations management

1) **Applications authorizations** (Settings --> Smartphones --> MDM --> Apps)
   All the currently installed applications on the phone are showed. The system administrator can choose which are allowed to the user and which are not. If the user try to launch a forbidden app, eSafeMe Pro block it and a pop-up inform the user that is it a forbidden application.
2) **Phone calls authorizations** (Settings --> Smartphones --> MDM --> Calls)
   The system administrator can choose which incoming and outgoing calls are allowed.
3) **Creating a simple and secure user phone interface** (Settings --> Smartphones --> MDM --> Launcher)
   The user will only have access to a specific interface set up by the system administrator.
   All the accessible functions are displays in a pictogram screen.
   This screen is an option available with the Launcher or MAM license.
Set up patrols or Start & End of services

1) **Create Customers** (Tags Forms --> Tags)
   A patrol must be linked to a Customer.

2) **Link Tags to Customers** (Tags Forms --> Tags)
   To link a Tag to a patrol, it must be linked to a Customer first. To save a Tag in the system, a Tag must be "read" by a smartphone. In order to ease this step, the administrator can use the learning function (Tag Forms --> Learning).

3) **Build a patrol** (Tags Forms --> PatROLS)
   You need to indicate which Tags constitute the patrols and the patrol’s operation.
   This step is not mandatory to set up a Start of Services.

4) **Set up a Start of Service** (Tags Forms --> Services)
   This step consist of identifying the specifics Tags that triggers the Start of the Service, and the time slots.
   This step is not mandatory to set up patrols.

Forms Management

1) **Create Customers** (Tags Forms --> Tags)
   A forms must be linked to a Customer.

2) **Build a form** (Tags Forms --> Forms)
   You will actually build a canvas of a form that will be available for the user. The administrator can build here the structure and the content of the form.
Follow up
Here are gathered all the system's information. Each theme is classed by tab. All the data are saved during 90 days on our servers.

Traces
The Traces tab gather all the event generate by the system.

![Illustration 8: Traces]

1) Selection of the viewing date. Its a specific day, not a period
2) Selection of the smartphone to view. They are all selected by default
3) Selection of the event to view. They are all selected by default
4) Data export in .pdf format. This .pdf file includes all the previous events and their location on a map
5) Show on a map the location of the selected event
6) See meta data can show elements like photos or texts when the selected event includes some
7) Filtering button. You can filter the data according to many criteria
8) Sorting button. You can sort the data according to many criteria
9) Data export button. You can export file in many formats: Excel, Word, XML or PDF

The board show the following events:

➔ **Smartphone name**
   Smartphone name when the event appears. A smartphone's name change don't affect the previous events

➔ **Phone**
   Phone number when the event appears

➔ **Type**
   Event type. Around sixty events are available. See the Event list in the annex

➔ **Event date**
   Smartphone date when the event appears

➔ **Date server**
   Neosafe server date when the server recovers the event. A difference between the Event date and the Server date mean that the smartphone did not have a mobile data when the event appears

➔ **GPS date**
   Last localization date of the smartphone

➔ **Tag**
   Name tag read by the smartphone. It can be a NFC tag, geolocalized tag or wifi tag.

➔ **Customer**
   Customer linked to the readed tag

Many row can be selected at the same time by maintain the MAJ or CTRL of the keyboard and by clicking on the desired row. The See on map button can then show the location of all the selected buttons.
Real Time

This function allow you to show the location of many events on a map, depending a specific period. Each new event on the server refresh the map with the new data. All the events are represented by icons.

1) Display settings selection. You can choose the specific date and period of visualization (between 1h and 24h) and the specific smartphone to display. No smartphone is selected by default.
2) Location tracking of the events on the map. You can click on a specific event to have more information.
Smartphones

This tab displays the main smartphone's information about the eSafeMe Pro application. The type of the last event sent to the Neosafe servers and the time since this last event allow to estimate the activity of each smartphone.

![Smartphone display](Illustration 10: Smartphone display)

Remote Monitoring

The Remote Monitoring tab display the follow-up of all the alarm event between our servers and the remote monitoring company, a remote monitoring software or the vocal servers. You can choose the visualization period. The board show the event date, the name of the concerned smartphone, the comment of the event, the state of the event (error or alarm) and the remote monitoring report if available. You can open this report by double-clicking on the icon.

![Remote Monitoring events display](Illustration 11: Remote Monitoring events display)
Connection

This board regroup all the previous connection that happened in the account. The board display the date and hour of the connection as well as the name of the user who connected.

Illustration 12: Connections history
Patrols

A patrol is an expedition to keep watch over an area. It is a course made by the smartphone’s user. During this course, the user can indicate its passage to-specific places identified in the system by reading NFC tags or by GPS localization. The patrols settings is detailed in a dedicated chapter. This page display all the closed patrols.

1) Customer and viewing period choice. A .pdf file that contain the list of all the patrols can be generate
2) Patrol display. All the patrols information are listed: date, duration and status. You can add a comment about the selected patrol by clicking on the "Add comment" button
3) Patrol content. The Number columns shows the number of time that a Tag has been read. As long as a Tag has not been read yet, the Error box is checked. if a the patrol end while an error is still present, the patrol status is Error
4) Comment display previously added by the "Add comment" (2)
5) Tags list read during the patrol that are not attached to the patrols
6) Data export button. You can export file in many formats: Excel, Word, XML or PDF
Services

This page displays all the services history.

The board regroups the following information:

- **Date**
  - Start of service date
- **Tag**
  - Start & End of services Tag. This Tag can be a NFC Tag or a Geolocalized Tag
- **Smartphone**
  - Name of the smartphone used to read the Tag
- **Duration**
  - Service duration
- **Status**
  - Service status
Forms

The system allows the creation of form templates. The user can fill in the form on his smartphone and send them to the server. This tab displays the forms previously filled by the user and exports them in .pdf format.

1) Customer and date of receipt selection
2) Form list
3) Form content

Illustration 15: Forms display
Statistics

Statistics on alert events and smartphone usage can be displayed on this page.

Events

1) Selection of the viewing period and the smartphones to be displayed
2) Selection of information to display
3) Result display area. You can change the display settings for this area with right click
4) Choice of events to display

Illustration 16: Statistics / Events
Usage

1) Selection of the viewing period and the smartphone to be displayed
2) Detail of the area selected in the table (4)
   The information displayed is in the form:
   Smartphone name --> Date - Start time --> Date - Stop time --> Day duration – hour:minutes
3) Result display area
   Each gray area begins when the smartphone starts and ends when the smartphone stops
**Autonomy**
Displays the average battery life of smartphones using eSafeMe Pro. The display of this information can be changed in the same way as the other Statistics tabs.

**LoneWorker Usage**

1) Selection of the duration of use to display
2) Result display area
3) Legend
   - It is possible to hide a section by clicking on it
4) LoneWorker Protection information summary table

You can change the display of this information in the same way as the other Statistics tabs.
Number of uses

1) Selection of the number of uses to display. There is one use when starting the eSafeMe Pro application
2) Result display area
3) Legend
   It is possible to hide a section by clicking on it
4) LoneWorker Protection information summary table

The display of this information can be changed in the same way as the other Statistics tabs.
Beacons

Illustration 20: Beacons display

Displays all information regarding Bluetooth tags such as battery level, date of last reading by a smartphone, etc.
**Settings**

This menu allows access to the interface configuration and LWP protection screens. It is only visible to System Administrators.

**Company**

The Company tab is used to fill in the information fields for the company that owns the account. It is only possible to save the data if all the mandatory fields (marked with a star) are completed. It is possible to modify the NeoSafe logo at the top left with a personalized logo. To do this, the **Browse…** button allows you to choose a specific image. Pay attention to the size of the image, because it is loaded dynamically each time a page of the interface is displayed. A reasonable size is less than 5 KB. A **View** button appears when the replacement file is loaded on the server. Pressing this button displays the selected image displays the image for verification before validation. If the result is not satisfactory, it is possible to delete the selected image by pressing the **Delete** button.

The advantage of using a different logo is not only to present a personalized web interface, but also to integrate this logo into all the reports that can be generated from the system. In addition, a click on this logo automatically launches the associated website (if completed).

*Illustration 21: Company informations*
Users

This section allows viewing, adding or modifying access to the administration web interface. The table displayed by default shows the list of all the users existing on the account, indicating the name, first name, user ID and their access level. A user can be deactivated, which means that the data concerning him is kept on the system but that he can no longer connect to the web interface.

The Add user button brings up a window for entering the data of the new user. Likewise, the Modify button (pencil icon on the right) authorizes the modification of data for an existing user.
The username must be at least 8 characters long and be an email address. This address will be used in the event of a password recovery procedure. The identifier is unique on our servers. If the system indicates that the identifier already exists, a different identifier must be entered.

The password must be at least 8 characters long, with at least one capital letter, one lowercase letter and one number.

The Messaging option gives access to the messaging system with our technical service. The Refresh option allows automatic refresh of the data every minute in the display screens.

Five access levels are available:

- **Administrator**
  Access to all interface features

- **Users**
  Access to the Follow-up and Tags Forms sections only. The other links (Settings, etc.) are no longer accessible

- **Vision only**
  Access to the Follow-up section only

- **Customer**
Access to the history of rounds, Start & End of services and to forms for one or more given customers. When this level is selected, a table appears with the names of the customers created in the system. The selection of clients is made by checking the boxes

➔ **Sites Managers**
Access to the Traceability section and to the settings for rounds, outlets and end of services and forms for one or more given customers. When this level is selected, a table appears with the names of the customers created in the system. The selection of clients is made by checking the boxes
Smartphones

This tab is dedicated to the configuration of portable equipment (telephone, smartphone, etc.).

Illustration 25: Smartphones settings

The board recalls the main information on smartphones.

The configuration is carried out by following the steps:

1) Select the line corresponding to the smartphone to configure. The selected line is grayed out
2) Press one of the **Menu**, **LWP**, **MDM** or **Services** buttons depending on the parameters to be set
3) Set the proposed parameters (see below) then confirm
4) Generate an event from the smartphone, for example by pressing the Test button on the eSafeMe Pro application (on the smartphone) or by plugging the smartphone into its mains charger
Menu button

Main tab

On the left side, the general information of this smartphone is displayed. The frame on the right lists all the other smartphones with the same version number of eSafeMe Pro and on which it is possible to copy the same parameters. Smartphones are selected by checking the smartphone box. The smartphones thus selected will then receive the same parameters.

NFC tab

Currently, only the "NFC Tag Reader" setting is available. You must check this option so that the eSafeMe Pro application supports reading NFC Tags.
**Menu tab**

It is possible to customize the basic menu, visible on the smartphone, via this tab.

1) Main menu as it will appear on the phone
2) The function located on the same line as these options is accessible via two tools: a button or a badge
   - The button is displayed in the eSafeMe Pro application. Depending on the setting, the function is triggered by a single press, a double press or a long press
   - A badge is a pictogram that the user can move at will on the smartphone screen. The main interest is that it is accessible on the lock screen
   - Check box to make the tool visible / invisible on the smartphone screen
3) Enter edit to modify the corresponding button
4) Editing of texts, colors and icons
5) Validation / cancellation of the current edition
6) Validation / menu cancellation
LoneWorker button

This category of parameters concerns elements related to personal security.

Main tab

On the left side, general information on this smartphone is displayed. The frame on the right lists all other smartphones with the same version number of eSafeMe Pro. They can be selected by clicking on the lines and holding the Ctrl or Shift keys on the keyboard. The selected smartphones will receive the settings at the same time.

Illustration 28: LoneWorker settings/ Main tab
Pre-alarm tab

The pre-alarm is a system that allows the user to stop sending an alert in the case of false detection (fall, SOS by shake me, etc.).

![Illustration 29: LoneWorker settings/ Pre-alarm tab](image)

The pre-alarm duration is adjustable. The value is given in seconds, by default it is set to 30. A selection list allows you to choose the sound that will be played by the smartphone. The black button on the right allows you to play the sound on the PC.

The following check boxes activate or deactivate the associated functions:

- The sound of the pre-alarm is broadcast with the maximum volume that can produce the smartphone
- Smartphone vibrates during pre-alarm
- The flash is flashing
**Fall down tab**

The system is able to detect a fall using two methods:

- **Fall detection**
  This choice corresponds to an algorithm developed by NeoSafe. The cursor visible on the right allows you to adjust the detection sensitivity. The value is adjustable between 1 and 10, from "more sensitive" to "less sensitive".

- **Tilt detection**
  Often called "Inclinometer", the latter method detects if the smartphone is oriented at a specific angle to the vertical for a given time. The angle and the duration are configurable.

The text field at the bottom of the window offers the possibility to modify the voice message played by the smartphone when sending the fall event.
**Immobility tab**

- **Immobility enabled**
  Check the box to activate the immobility function

- **Immobility time**
  Indicates the duration during which a lack of movement is considered abnormal. At the end of this period, the alarm is triggered

- **Sensibility**
  Selection of the detection sensitivity threshold. This parameter is adjustable from 1 (sensitive) to 3 (not very sensitive)

- **Ack by move**
  User can stop the immobility pre-alarm by moving the smartphone

- **Active when charging**
  Indicates whether motion detection should be active when the smartphone is connected to the AC adapter. By default, this option is disabled

The text field at the bottom of the window offers the possibility of modifying the voice message broadcast by the smartphone when sending the immobility event.
Solutions pour la protection des personnes et applications métiers innovantes

SOS tab

The user can trigger voluntary alarms (SOS) with the smartphone using various manipulations.

➔ **ON/OFF Power button**

The user repeatedly presses the Power button on their smartphone. The rate of pressing the button corresponds to that of switching the screen on and off. The minimum number of presses used to trigger the alert can be configured, by default its value is 4. After the number of presses required, the alert is sent directly. A voice message is broadcast by the smartphone and the vibrator is activated (if the box is checked). The administrator can delete the text of the alarm sending if he wishes this alarm to be silent (for example in case of attack).

➔ **SOS by "Shake"**

The user can trigger an SOS alarm by shaking their smartphone (repeated wrist movements forwards and backwards). This movement causes a pre-alarm unlike the previous one.

➔ **Dedicated SOS button**

On some smartphones, there is a dedicated physical button. This is the case with the RugGear RG310.
**Bluetooth tab**

The user can also trigger a voluntary alarm by pressing a Bluetooth medallion connected to the smartphone. This medallion is offered as an option by NeoSafe.

![SOS and Bluetooth settings](image)

*Illustration 33: LoneWorker settings / Bluetooth tab*

**Location tab**

The geographic location information of the smartphone can be provided by three sources:

- **Device location**
  
  It is mainly about the GPS on board the equipment. In the context of Android smartphones, the operating system can gather information from several sources to improve accuracy. To do this, high precision modes must be activated on the device.

- **Fix address**
  
  The smartphone is used sedentarily, the administrator can directly enter the address of the place. This information will be transmitted to the monitoring station in the event of an alert. This function is only available with the subscription to the SECURITAS Alert Services.
monitoring channel.

➔ eSafeMe Address

The addresses where the smartphone user works are known. The administrator will fill in the list of places on the web interface. The user will report the place of intervention on his smartphone when he arrives there. This function is only available with the subscription to the SECURITAS Alert Services monitoring channel.

When the location by the device is selected, the following functions are available:

➔ Tracking

The smartphone sends its contact details to the server either periodically or based on the distance traveled by the user from the last point. The frequency and/or the distance are configurable.

➔ Where are you?

The system administrator can request the location of the smartphone at any time, via the Where are you? Button on the web interface.

➔ Indoor

The GPS location system works very poorly or not at all under certain conditions, especially in buildings. To overcome this problem, it is possible to locate the smartphone using the wifi hotspots present on the premises. It is not necessary to have a connection to these terminals, only the level of the radio signal is measured. In order to avoid pollution due to external wifi sources, the administrator can fill in a filtering list.

Caution: The use of these location functions requires administrative procedures. We recommend that you contact the relevant services before activating this system.
**Geofencing tab**

This function authorizes the administrator to define geographic areas and to request the generation of events when entering or leaving these areas.

1) Activate / deactivate the function
2) Five zones can be defined. For this, the administrator can directly enter the information in the table by double-clicking on the desired field
3) This button gives access to a graphic tool for the definition of the area selected in the table

Illustration 36: Geofencing zone creation

- Choice of the starting point of the area to create. Drag the mouse while holding the click to define the radius of the area
b) Deleting a zone created  

c) Allows you to zoom in / out the map  

d) Search for a specific address or a specific brand  

e) Modification of an existing zone  

4) At the edge of the area, the GPS can trace locations by being on either side of the circle. In order to avoid repeated entry / exit events, the administrator can enter a margin of uncertainty in relation to the circle. This value is in meters  

5) The texts broadcast in voice by the smartphone, when the events are broadcast, can be personalized in these fields  

**Tags tab**

The principle of Positive Safety is to allocate time to the user. If after this time the user has not come forward, the system triggers an alert. This value can be configured by the administrator. The "Delta Timer" field is the period during which the user is informed (on his smartphone) of the end of the period. This room for maneuver must allow the user time to show up.
1) Whether or not displays the "Security" button on the smartphone screen. The user therefore has the right or not to activate the security system.

2) After an alarm, the smartphone goes into speaker. This function coupled with automatic answer gives the possibility to the user to chat even if he is unable to handle his phone.

3) The sound beacon is an audio assistance to find the smartphone. Following an alert, the smartphone repeatedly emits a sound to guide the rescuers on site.

4) Messages spoken by the smartphone during security activation / deactivation (LWP function).

5) The administrator indicates the status of the security system when the phone starts.

6) Informs the user by voice message and / or the vibrator when connected / disconnected to the mobile data network. Messages are personalized.

7) Allows the smartphone to automatically answer an incoming call following an alert. The activation of this mode can be limited to a given time, adjustable in the "Max duration" field. A value of 0 means that this mode will be deactivated after the first incoming call following the alert, regardless of the time elapsed. The administrator can also limit the auto-hook authorization to a list of specific phone numbers. A number is added to the list by filling in the Number field and then pressing the Add button. Deleting a number from the list is done by selecting it from the list and pressing the Delete button.
Once all the parameters have been entered, the administrator presses the **Save** button to save them on the server. As soon as the smartphone connects to the server, it will recover its configuration. It is possible to force the connection of the smartphone by plugging it into its AC adapter or by pressing the **Test** button. Pressing the **Cancel** button aborts the configuration.

**MDM button**

The MDM (Mobile Device Management) button designates the management in terms of access rights to the device. This section groups together the authorizations for the use of applications embedded on the smartphone, the input and output telephone numbers and then the management of the "user interface / Launcher" screen.

**Main tab**

On the left side, general information on this smartphone is displayed. The frame on the right lists all the other smartphones with the same version number of eSafeMe Pro and on which it is possible to copy the same parameters. Smartphones are selected by checking the smartphone box. The smartphones thus selected will then receive the same parameters.
**Apps tab**

The system allows the administrator to block applications embedded on the smartphone. The user will not be able to launch this software.

- Select the applications to block / allow in the corresponding box
- Press one of the two arrows between the two frames to switch the selected applications

**Other tab**

The administrator can block internet access by checking the disabled Internet option. Please note: this option no longer works on Android ≥ 5.0.0.
**Calls tab**

The phone numbers that the smartphone is allowed to call, or authorized to call the smartphone are listed in the left and right frames.

- Check the "Calls..." box to activate the function
- Enter the telephone numbers to add the list of "Numbers" fields
- Press the **Add** button
- The number appears in the frame below
- To delete a number, the selector in the bottom frame then press the **Delete** button
Launcher tab

This screen is only available with the "Launcher" or "MAM" option. The Launcher is a graphical interface displayed on the smartphone screen. The user will only be able to access the applications available on this screen. Applications are defined by the administrator in this tab.

Illustration 41: MDM settings / Launcher tab

1) Grid size selection
2) Choice of colors. Click on the rectangle to choose a color
3) If full screen is selected, the notification bar at the top of the screen will not be visible
4) The "Notification bar" option indicates whether the user can access this bar. This can be visible but not selectable
5) Representation of the smartphone screen. Select a tile to modify it and associate an application with it. The right screen appears
6) It is possible to create up to three screens, select one to configure it
7) Definition of the PIN code to protect the Secure mode of the phone. The default PIN code is 0000
8) Choice of the background color of the tile being modified. Please note, selecting (Tile color overwrites all independent tile colors.
9) Choice of the image of the tile from a pre-defined list or download of a personalized image
10) Choice of the application launched by the tile. The applications installed on the smartphone appear in a list. It is also possible to select pre-defined actions
11) Indicate the name of the tile and choose the color of the name
12) Press the arrow to move the tile on the screen
13) Delete the selected tile
14) Validation of the tile being created

**MAM tab**

From version 7 of eSafeMe Pro, the system integrates application management (MAM for Mobile Application Management). This tab is used to list the applications under management.

1) Information on the application under management
2) Action requested by the administrator. A color code shows the status of the action: red for an action in progress, green for an action completed
3) Information about automatic application update
4) Information on the request for updates achievable only by wifi
5) Editing application options. The parameters shown in the image on the right appear
6) Changing preferences for the selected application

When all the tabs have been configured, press the **Save** button. Then trigger an event on the smartphone to take the configuration into account.
**Browser tab**

This screen is only visible with the "Browser" or "MAM" option. The Browser is a secure and configurable browser that allows you to control the web access of your fleet of smartphones.

1) Allows you to define the default home page that will open when the application starts
2) Managing site accessibility permissions and downloads
3) Allows the creation of rules
4) Creation of specific rules

*Illustration 43: MDM settings / Browser tab*
Services button

This menu covers the options related to the management of end and end services and Tags. A Tag is a concept that can be compared to a badge reading system. There are many users of this system:

- Monitoring of patrols (security companies)
- Start & End of services (personnel management)
- Positive security (maintaining security in places not covered)
- Precise location of the last place frequented by the user in the event of an alarm

Main tab

On the left side, general information on this smartphone is displayed. The frame on the right lists all the other smartphones with the same eSafeMe Pro version number and on which it is possible to copy the same parameters. Smartphones are selected by checking the smartphone box. The smartphones thus selected will then receive the same parameters.
1) Reading a Tag normally generates an event on the server. In some cases, it may be interesting to request that this event is not recorded in the database (indoor geolocation). Only the last Tag read will be kept.

2) The "Zone entry" and "Zone exit" events can trigger BP1 or BP2 events. Depending on the system settings, this can trigger the start and end of service or the reading of a virtual needle.

3) The generation of a BP1 event by pressing the button on the menu or by cascade of events results in the reading of a geolocated Tag or a virtual Tag. A geotagged Tag is a function based on the definition of a Tag in relation to a GPS location. This system can be part of a round or take & end management. Geolocated Tags are defined by the administrator from the web interface.
Location button

If the smartphone has been configured to respond to this function (LWP / Location), pressing this button asks it to return its geographic position. A Synchro type event is then generated by the smartphone. This event is visible in the Traces and the position on smartphone is accessible by clicking on View on map.
Events

Our system can be likened to an event concentrator. When an event arrives, the server can redirect it to different channels such as: e-mail, push notification, SMS or voice server, remote monitoring, remote monitoring software, web-service, etc.

This page allows you to indicate the redirection channel(s). This can be done for all smartphones or specifically on a given smartphone (common file or specific files).

1) Choose all smartphones or one in particular. It is possible to combine the configuration of the general case and those specific. If events are indicated at the same time for All and for a particular smartphone, it is the configuration of this latter that is taken into account.

2) This button displays a window containing a drop-down list of all the events known to the system. Select an event from the list and confirm with the OK button. This is now displayed in the table (3). This operation has to be started again for each event to be managed.

3) This table displays the events being configured. Select the event line to configure, it will be grayed out.

4) Select the re-routing channel to configure or the GPS setting.

Illustration 45: Events management
➔ **E-mails**

Emails are sent to the email addresses indicated in parallel.

*Caution*: an e-mail is not a secure channel! It should only be used to broadcast information

➔ **PUSH notification**

The server sends notifications to smartphones linked to an eSafeMe Pro license listed in this table. The recipient will see a message displayed on their screen and can press one of the two available buttons. Pressing one of these buttons will generate a Push Acq or Push Nacq event

➔ **SMS**

The server sends SMS to the numbers indicated in parallel.

*Caution*: an SMS is not a secure channel! It should only be used to broadcast information

➔ **Vocal call**

A voice server calls the phone numbers listed in the order displayed. The call cascade stops when one of the parties confirms that the alert has been taken into account by pressing the "*" key on the combined handset. The system accepts up to 5 numbers, if no number takes the alert, an error message is indicated in the web interface (Follow up / Remote monitoring)

➔ **Tracking**

The administrator can ask the system to trigger a tracking of the location of the smartphone following an alert. The available parameters are displayed in the table (5). The period and duration of the follow-up can be modified. The activation of this function for a given event is done in the table (3). Depending on the channel chosen, the system gives the possibility of entering:

- an e-mail address
- a phone number
- a name associated with the telephone number

Press the Modify button, a window opens with the fields to be completed. Confirm with the OK button. The Type selection menu corresponds to a customizable message. The recipients can be taken into account according to the days of the week. The modification or deletion of a recipient is carried out using the Modify or Delete buttons.

5) In order to avoid retyping the same information several times, double clicking on a line in this frame directly inserts the deal in the table (4)

6) The Type button allows you to customize the messages broadcast by the server. A new window appears, it is slightly different depending on the selected channel
Illustration 46: Type modification

a) Choosing a type number from the drop-down list displays the type being edited
b) The Add button allows the creation of other types. Each type is numbered, this number can be selected when creating / changing recipients
c) Personalization of subject for emails
d) Body customization for messages
e) A list of variables is available in this frame, a double-click inserts the chosen variable in the text. The description of these variables can be found in the appendix to this document.
f) Personalization of the texts displayed on the buttons. A maximum of ten characters is allowed.

g) In alarm mode, the smartphone emits a sound in addition to the message display. On the other hand, pressing a button generates an event on the server. It is possible to define the hours of receipt of the notification.

h) Old filtering model: the recipients of the notification can be filtered according to part of their name or the name of the last Tag / tag seen. If the filtered part is identical between the sender and the recipients, the latter will receive the notification.

i) New filtering model: allows you to filter the recipients of notifications based on the name of the smartphone or the name of the last Tag / tag seen. Thus, it is possible to manually define the recipients based on an entry or the name of the sending smartphone.

The modifications are directly taken into account, press Close to return to the previous screen.

7) All data can be exported in Excel, Word, XML, PDF format

Extract

The Extraction database tab allows the sending of all the events generated on a day, a week or a month to defined email addresses.

Illustration 47: Data extraction

The files are sent in XLS format (compatible with the main spreadsheets on the market).
Safety

If a subscription to a remote monitoring channel is available, this page allows you to enter the names and phones of the people to contact in case of emergency.

The remote monitoring procedure is as follows:
When an alarm is received, a doubt is raised by the monitoring station.
This involves calling the LWP to estimate the level of alert and thus provide the most suitable response.
This removal of doubt can be followed by the call of five employees, always with the aim of estimating and solving the problem encountered.
If the Password field is filled in, the remote monitoring service asks the other party to validate its legitimacy.
The remote monitoring officer has the possibility of triggering civil security in the event of a proven disaster (at your expense if false alarm).
Following a doubt raised, a .pdf document summarizing events is available on our servers according to remote monitoring.
Addresses

If a subscription to a remote monitoring channel is available, this page allows you to enter the addresses where users are likely to go, as well as the associated safety instructions. The user tells the system, via the eSafeMe Address application, where he is. In the event of an alarm, the remote monitoring agent receives the information linked to this location.

Illustration 49: Adresses creation
Licenses

This tab shows the licenses associated with the account. The options available with each license are indicated on the check boxes. These can only be modified by NeoSafe.

1) Pressing the Edit button opens the Edit License window to edit the IMEI, smartphone name and phone number (the three fields at the bottom)
2) Viewing the number of licenses assigned to this account
3) License viewing table. Select a line to be able to make changes.

To release the license, simply delete the IMEI. To replace the smartphone with another, fill in the new IMEI. The old smartphone will no longer work with the eSafeMe Pro app. Validate with the OK button to take into account the modifications.

The IMEI number is always a fifteen-digit number found on the smartphone box, under the illustrations:

Illustration 50: Licenses management

Illustration 51: License modification
battery inside the smartphone or in the settings menu from versions 4.x.x of Android. It is also possible to display it on the smartphone by dialing the number *#06#.

Pressing the Import button opens the window to import the necessary information from an Excel file using Drag & Drop. Follow the instructions displayed in the window.

**Beacons**

It is possible to configure all the Bluetooth beacons (Beacons) used for Indoor location.

![Beacons Configuration Window](image)

*Illustration 52: Bluetooth Beacons management*

You can see the information related to the tags, such as the name of the tag, the battery level, etc.

It is possible to modify the information of a tag by clicking on **Modify**.
Tags Forms

This section gathers the following topics:

- Customer creation
- Learning / definition of Tags
- Start & End of service creation
- Patrons creation
- Defining automatic reports
- Forms template creation

Tags

The implementation of rounds, taking & end of service or even the writing of reports / forms is mostly located on the site of end customers. The advantage of grouping these functionalities under this notion is that it is possible to manage them completely independently and adapted to the specific needs of each of the end customers. In addition, they can be authorized to consult data from the sites which concern them, on the web interface or have the reports sent to them by email.
To create a new customer, simply press the **Add** button (1) and enter the name in the field displayed. To rename an existing customer, press the **Modify** button.

A Tag must be assigned to a customer in order to be used in a round or an outlet & end of service. A Tag can be an NFC, virtual (Button 1 on the eSafeMe Pro), geolocated or Wifi tag.

1) New customer creation. Press **Modify** to modify an existing customer
2) The left frame lists the Tags associated with the client
3) The right frame lists Tags known by the system but not associated with a client.
   - Select the desired Tag, possibly change its name in the frame (2) and press the arrow (4) to assign it to the client
4) Depending on the side where the Tag is selected, the arrow displayed goes from right to left or vice versa. Pressing this arrow switches the selected Tag between frames (2) and (3). If a Tag is used in a round or catch & end of service, a message is displayed to indicate this. The Tag must be removed from the round or service before it can be released.
   - The **View Trash** button allows you to view the Tags previously placed in the trash in the right list and, if necessary, replace them with a customer.
5) If the Tag is selected in box (1), the Trash button appears. This button allows you to throw a free tag, it is not deleted from the system. It can be visible again by pressing the button (5).
   - To modify the Tag name : enter the new name and press **Modify**.
6) The Add a geolocated Tag link allows you to create an intangible Tag positioned on the
map. It can be read by different mechanisms:

➔ Association of Button 2 (eSafeMe Pro menu on the smartphone) in search of geolocated Tags

➔ Association for entering or leaving a geographic area in search of geolocated Tags

This system is inviolable because it takes into account the geographic positioning of the person to simulate a Tag reading.

These Tags become usable in the same way as the physical Tags, that is to say in the Patrol or the Start & End of service.

The following page opens to allow positioning of the Tag:

As in all map windows, it is possible to change the zoom value, display a satellite view, etc.
Click on the Tag and move it to the desired location.

The Latitude and Longitude fields are automatically filled. If the coordinates of the location of the Tag are known, it is possible to enter these values and press Enter on the keyboard to position the Tag more quickly. Similarly, it is possible to enter an address to quickly position the Tag at the desired point.

If the Tag selected in one of the two lists is a Geolocalized Tag, an Edit Geolocalized Tag button appears. Pressing this button opens the same page for modifying the coordinates.
Reports

Round or take-out & end-of-service reports can be generated for a specific customer and sent automatically by email.

➔ The upper frame allows you to define the sending of automatic reports for rounds. This report can be sent to as many email addresses as desired. Its periodicity can be daily, weekly or monthly. The KMZ column allows you to receive an additional report for people who use geolocalized Tags. These KMZ files are compatible with Google Earth.

➔ The bottom frame allows you to define the sending of automatic reports for outlets and end of service. This report can be sent to as many email addresses as desired. Its periodicity can be daily, weekly or monthly.

Learning

A physical tag (NFC tag) or Wifi must be read by a smartphone and sent to the server so that it knows it. It is not always easy to recognize a Tag by its number, which is why a learning tool is available to identify and modify on the fly a Tag that has just been read.
Select the customer with whom the Tag should be linked
Select the smartphone to use for learning from the list of smartphones
The table in the center of the screen displays the Tags read
Select the line corresponding to the desired Tag, name it in the bottom frame, then press **Edit** to validate the name. It is also possible to associate it directly with a client
It is possible to do this learning in the field because this page also exists in mobile version
Patrols

This section gives access to the creation, modification or deletion of rounds.

1) Choose the customer with whom the round is associated
2) Choose an existing round by clicking on the corresponding line or press the **Add** button to create a new one. In the latter case, give it a name. To modify or delete an existing round, select the line then press the **Modify** or **Delete** button
3) The Tags in this list make up the round. The order may be important depending on the characteristics of the round (7). This order can be changed using the up and down arrows (5).
   Position 1 being the one at the top.
4) This frame lists all the Tags associated with the chosen client. To assign a Tag to a round, select it in the frame (3), then click on the arrow that appears between the two frames. It is possible to retain several by holding down the Ctrl or Shift key on the keyboard and clicking on the desired line
5) The arrows are used to move a Tag in the round. The icon representing a sheet opens a window in which the administrator can enter instructions associated with the Tag. These instructions will be displayed on the smartphone in the SafeMe Guard app.
6) Pressing this button saves the tag association in the round

7) This framework defines the operation of the round:

- **Random patrol**
  The round can be performed by reading the Tags in any order. It starts automatically on the first Tag read and ends when all the Tags have been read. Tags can be read multiple times.

- **Strict order patrol**
  The round can only be carried out in the order in which the Tags were positioned.

- **First tag then random**
  The most common round in the security world. The round must start with the Start Tag and then continue in random order. It ends when all the Tags have been read at least once.

- **The 1st Tag restart option** interacts with rounds of the Strict Order or 1st Tag type, then random. If this option is checked, reading the 1st Tag a second time will cause the current round to end, with an error and restart a new round.

**Caution:** certain restrictions exist:

- It is impossible to have two rounds with an identical first Tag. Indeed, the system would be unable to know the round to start.
- It is impossible to have identical Tags in several rounds, if these are of Random type. Indeed, the system would be unable to know the round to start.

2) Minimum duration and Maximum duration allow hourly limits to be set on a round.

- Minimum duration causes an error if the complete reading of the round is shorter than the indicated time.
- Maximum duration causes the round to close and a round to be put in error if the round is not finished beyond the allotted time.

Save the characteristics of the round by pressing the Save button on the frame (7)

8) These buttons have the following functions:

- **The Print button** generates a PDF file of the round structure and its characteristics.
- **The Map button** displays a map of the round if it has geolocated Tags.
- **The Schedules button** allows you to indicate a number of rounds to be performed in a time slot. If this number is not respected, a round error event is automatically generated.
- **The button Delete a round**, name, characteristics and description.
Services

This tab allows you to define the Tags for the management of Start & End of service.

The left frame indicates the name of the Tags associated with the chosen customer. Selecting a Tag brings up an arrow allowing it to be moved in the list of Service Tags.

The right frame allows defining the characteristics of the service corresponding to the selected Tag.

Caution, it is possible to define several Tags, it is therefore important to click on the desired Tag before entering the time slots (even if there is only one).

As a reminder, a reading of this Tag generates an event on our Service Start platform. A second reading generates an End of Service event.

You can associate up to two time slots per day. From the moment when ranges are associated, errors in taking & end of service are generated if the reading of these Tags is not done in the ranges indicated. You can allow a margin on the arrival or departure time using the Possible delay and Departure before input fields.

The Max time column allows you to define a time limit to automatically end the service if it has started but is not stopped by a second reading of the Tag.
The No error on timeout check box allows not to create error events, in this case, on our servers.

The Timer and Delta entries allow you to create a timer during a service shift. If these fields are filled, the smartphone which starts taking service on this Tag will automatically receive an alert to be validated within X minutes. Delta represents the time allowed by the system to receive the response. In case of non-response, a timer error event will be generated automatically. This option is very useful to know if a person is still on the job and available, or to generate positive security for people who can enter areas without GSM coverage.

The Save button allows you to save the characteristics of the Tag being edited.

Example of use:

- A person must take duty at 8:00 am. and finish at 6:00 pm
- The person arrives and reads the Service Tag, which causes the service to start on our servers.
- The person leaves in the evening, forgetting to read the Service Tag. The service must be forced to stop so that it can be started again the next day.
- The check box ‘No error on timeout’ allows not to create error events, in this case, on our servers.
Forms

Users can fill out forms and send them to the server using the eSafeMe Forms application. The information template is defined by the administrator.

1) Choice of client to which the form is associated
2) List of existing forms. The buttons give access to the following functions:

- Add a new form
- Change the form name
- Delete the selected form
- Set form options
  - Do not send empty fields: if the user does not fill in certain fields, these will not be sent to the server.
  - Invisible form: this is a form which does not appear in the user’s choice list, but which can be called up in a drop-down list
- Copy a form
- Move a form from one client to another
The check box See invisible forms gives the possibility to display invisible forms (only).

3) This frame shows the fields making up the form. The add, modify and delete functions are located at the bottom of the frame and at the level of each field.

➔ , respectively:
  • Enter edit field mode
  • Delete field
  • Move the field to the top of the form
  • Move the field to the bottom of the form

➔ allows to add respectively:
  • A drop-down list
  • A text field
  • A date / time
  • Check boxes or selectors
  • Photo fields
  • An information field / separators (label) / header / footer
  • A drawing area (signature for example)
  • NFC Tag Reading
  • GPS coordinates

4) When a control is being edited, this frame displays the various associated options. Make the necessary modifications and confirm by pressing OK.

5) When a user fills in and sends a form to the server, it is possible to automatically send it to email addresses. This frame gives the possibility to add or remove them.

A new interface is accessible via the link at the top of the frame (2). Its ergonomics have been redesigned to facilitate creation, in particular with support for Drag & Drop. Viewing forms sent to the server is also available.
Multi-Accounts

For organizational reasons, our customers may ask us to create several accounts. For example, for the management of several agencies. Each of these accounts can be administered locally by the users who are declared there. However, a general administrator may also wish to intervene on these accounts. This is the subject of this section.

**Note:** The creation of accounts and the authorization of access in multi-accounts is only possible by NeoSafe.

Accounts

This tab displays the information in a global way concerning the accounts attached to the multi-account.

1) List of managed accounts. The administrator can activate / deactivate an account via the Active check box. The Connected column indicates if someone is logged into the account.  
2) This button opens the interface for managing the account selected in the table (1) without
having to re-enter an username and password.

3) List of users in the account selected in the table (1). The administrator can activate / deactivate an identifier via the Active check box and, if necessary, disconnect a user via the Connected check box.

**Smartphone**

This tab is only available upon request and agreement from NeoSafe. The objective of this part is to give the administrator the possibility of moving licenses from one account to another.

➔ Select the desired accounts in the left and right frames
➔ Choose the desired licenses and use the arrows in the middle of the two frames to move them.
Real-Time

The operation is the same as the equivalent function in the Traceability section, but on all smartphones in the multi-account.

Illustration 63: Multi-Accounts / Real-Time tab
Statistics

The operation is the same as the equivalent function in the Traceability section, but on all smartphones in the multi-account.

Illustration 64: Multi-Account / Statistics tab
Write us

It is possible to contact NeoSafe directly from the web interface via the Write to us menu.

Illustration 65: Write us messaging

NeoSafe’s response will be available there and a notification will be visible until the new message is read.
Help

Frequently Asked Questions

The Frequently Asked Questions section brings together the most frequently asked questions. A dynamic search field is available. If the subject sought is not available, contact NeoSafe.

Illustration 66: Frequently Asked Questions
Documentations

The technical documentation relating to the NeoSafe web interface and the eSafeMe Pro application are grouped in this menu.

Illustration 67: Technical documentation
Annex

List of variables for "Types" customization

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ADRESSE%</td>
<td>Address returned by Google</td>
</tr>
<tr>
<td>%DATE%</td>
<td>Local phone date</td>
</tr>
<tr>
<td>%DATEGPS%</td>
<td>Phone GPS date</td>
</tr>
<tr>
<td>%DATETAG%</td>
<td>Date of reading of the last Tag</td>
</tr>
<tr>
<td>%EVENEMENT%</td>
<td>Type of event</td>
</tr>
<tr>
<td>%GOOGLE%</td>
<td>Link to Google Map</td>
</tr>
<tr>
<td>%HEURE%</td>
<td>Local phone time</td>
</tr>
<tr>
<td>%HEUREGPS%</td>
<td>Phone GPS time</td>
</tr>
<tr>
<td>%HEURETAG%</td>
<td>Last Tag Reading Time</td>
</tr>
<tr>
<td>%LAT%</td>
<td>Location latitude</td>
</tr>
<tr>
<td>%LNG%</td>
<td>Location longitude</td>
</tr>
<tr>
<td>%NOMKAB%</td>
<td>Name associated with the license</td>
</tr>
<tr>
<td>%NOMTAG%</td>
<td>Name associated with the Tag</td>
</tr>
<tr>
<td>%SNKAB%</td>
<td>License number</td>
</tr>
<tr>
<td>%SNTAG%</td>
<td>Tag identification number</td>
</tr>
<tr>
<td>%TEL%</td>
<td>Phone number associated with the license</td>
</tr>
</tbody>
</table>
Events list

<table>
<thead>
<tr>
<th>Name</th>
<th>Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acq Timer</td>
<td>12</td>
<td>Timer / Positive Security acknowledgment</td>
</tr>
<tr>
<td>Adresse</td>
<td>46</td>
<td>Address sent by eSafeMe Address</td>
</tr>
<tr>
<td>App Timer</td>
<td>57</td>
<td>Starting the Timer with eSafeMe Timer</td>
</tr>
<tr>
<td>Audio</td>
<td>55</td>
<td>Audio metadata</td>
</tr>
<tr>
<td>Bat. Médail</td>
<td>51</td>
<td>Low battery detection on the Medallion</td>
</tr>
<tr>
<td>Bat. OK</td>
<td>16</td>
<td>Phone battery charged</td>
</tr>
<tr>
<td>Batterie</td>
<td>6</td>
<td>Low phone battery detection (~ 20%)</td>
</tr>
<tr>
<td>Bouton 1</td>
<td>4</td>
<td>Press button 1 of eSafeMe Pro</td>
</tr>
<tr>
<td>Bouton 2</td>
<td>5</td>
<td>Press button 2 of eSafeMe Pro</td>
</tr>
<tr>
<td>Bouton 3</td>
<td>29</td>
<td>Press button 3 of eSafeMe Pro</td>
</tr>
<tr>
<td>Bouton 4</td>
<td>70</td>
<td>Press button 4 of eSafeMe Pro</td>
</tr>
<tr>
<td>Bouton 5</td>
<td>71</td>
<td>Press button 5 of eSafeMe Pro</td>
</tr>
<tr>
<td>BT Orange</td>
<td>68</td>
<td>Statistical indicator of operation of a Bluetooth beacon</td>
</tr>
<tr>
<td>BT Rouge</td>
<td>69</td>
<td>Statistical indicator of operation of a Bluetooth beacon</td>
</tr>
<tr>
<td>BT Vert</td>
<td>67</td>
<td>Statistical indicator of operation of a Bluetooth beacon</td>
</tr>
<tr>
<td>Charge.IN</td>
<td>14</td>
<td>Charger connected</td>
</tr>
<tr>
<td>Charge. OUT</td>
<td>15</td>
<td>Charger disconnected</td>
</tr>
<tr>
<td>Chute</td>
<td>2</td>
<td>Fall Detection</td>
</tr>
<tr>
<td>Deb. Ronde</td>
<td>21</td>
<td>Start of Patrol</td>
</tr>
<tr>
<td>Deb. Servi</td>
<td>22</td>
<td>Start of Service</td>
</tr>
<tr>
<td>Deb. Timer</td>
<td>23</td>
<td>Start of Timer / Positive Safety</td>
</tr>
<tr>
<td>Err Nbr Rd</td>
<td>28</td>
<td>Number of rounds error</td>
</tr>
<tr>
<td>Err Ronde</td>
<td>19</td>
<td>Round error</td>
</tr>
<tr>
<td>Err Servi</td>
<td>18</td>
<td>Service Error</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Timer Error / Positive Safety</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Error in instructions sent to remote monitoring</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>End of Patrol</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>End of Service</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>End of Timer / Positive Safety</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>Form sent with eSafeMe Forms</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>GPS is disabled on the smartphone</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>GPS is activated on the smartphone</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>Photo and / or Text sent with eSafeMe Guard</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Immobility Detection</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Server received an unhandled event</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>Entering an INDOOR zone</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>1st start eSafeMe Pro</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>Updating an application on the smartphone</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>ESafeMe Pro app update</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>ESafeMe Pro manual start</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>Start / Stop menu eSafeMe Pro</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Timer / Positive Safety non-acknowledgment</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Critical SMS level</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>Disabling notifications</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Instructions are correctly sent to remote monitoring</td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>Entering an OUTDOOR zone</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>Photo taken with eSafeMe Picture</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Reading a Tag</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>GPS position</td>
<td></td>
</tr>
<tr>
<td>65</td>
<td>A fall pre-alarm has taken place</td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>An immobility pre-alarm has occurred</td>
<td></td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Pro SOS</td>
<td>64 An SOS pre-alarm has taken place</td>
<td></td>
</tr>
<tr>
<td>Push Acq</td>
<td>62 The recipient of a notification has pressed the OK button</td>
<td></td>
</tr>
<tr>
<td>Push Nacq</td>
<td>63 The recipient of a notification has pressed the Cancel button</td>
<td></td>
</tr>
<tr>
<td>Rx. Parm.</td>
<td>41 The smartphone transmits its configuration to the server</td>
<td></td>
</tr>
<tr>
<td>SOS</td>
<td>7 SOS request</td>
<td></td>
</tr>
<tr>
<td>Start</td>
<td>10 Start of LWP mode (security activation)</td>
<td></td>
</tr>
<tr>
<td>Stop</td>
<td>11 LWP mode stop (security deactivation)</td>
<td></td>
</tr>
<tr>
<td>Synchro</td>
<td>30 Synchronization in the smartphone and the server</td>
<td></td>
</tr>
<tr>
<td>Tel Start</td>
<td>52 Phone Start</td>
<td></td>
</tr>
<tr>
<td>Tel Stop</td>
<td>53 Phone Stop</td>
<td></td>
</tr>
<tr>
<td>Test</td>
<td>43 Test requested from the Test button of eSafeMe Pro</td>
<td></td>
</tr>
<tr>
<td>Texte</td>
<td>45 Text sent with eSafeMe Text</td>
<td></td>
</tr>
<tr>
<td>Tx LONE WO</td>
<td>60 Transmission of LoneWorker's settings to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Tx MAM</td>
<td>58 Transmission of MAM parameters to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Tx MDM</td>
<td>49 Transmission of MDM parameters to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Tx MENU</td>
<td>59 Transmission of MENU parameters to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Tx PRO</td>
<td>61 Transmission of PRO parameters to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Tx. param.</td>
<td>42 Transmission of LoneWorker parameters</td>
<td></td>
</tr>
<tr>
<td>TxLauncher</td>
<td>50 Transmission of Launcher parameters to the smartphone</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td>3 Entering or leaving a zone</td>
<td></td>
</tr>
<tr>
<td>Zone IN</td>
<td>36 Entering an area</td>
<td></td>
</tr>
<tr>
<td>Zone OUT</td>
<td>37 Zone exit</td>
<td></td>
</tr>
<tr>
<td>Pdf SECURI</td>
<td>54 Reception of the remote monitoring report</td>
<td></td>
</tr>
</tbody>
</table>
## Illustrations Index

<table>
<thead>
<tr>
<th>Illustration</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Neosafe website</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Client Access</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>Dashboard</td>
<td>7</td>
</tr>
<tr>
<td>4</td>
<td>Header</td>
<td>8</td>
</tr>
<tr>
<td>5</td>
<td>Menus allowing to navigate through the web interface</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>Dashboard display</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>PUSH messages personalization</td>
<td>11</td>
</tr>
<tr>
<td>8</td>
<td>Traces</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>Real Time</td>
<td>16</td>
</tr>
<tr>
<td>10</td>
<td>Smartphone display</td>
<td>17</td>
</tr>
<tr>
<td>11</td>
<td>Remote Monitoring events display</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>Connexions history</td>
<td>18</td>
</tr>
<tr>
<td>13</td>
<td>Patrols display</td>
<td>19</td>
</tr>
<tr>
<td>14</td>
<td>Services display</td>
<td>20</td>
</tr>
<tr>
<td>15</td>
<td>Forms display</td>
<td>21</td>
</tr>
<tr>
<td>16</td>
<td>Statistics / Events</td>
<td>22</td>
</tr>
<tr>
<td>17</td>
<td>Statistics / Usage</td>
<td>23</td>
</tr>
<tr>
<td>18</td>
<td>Statistics / LoneWorker Usage</td>
<td>24</td>
</tr>
<tr>
<td>19</td>
<td>Statistics / Number of uses</td>
<td>25</td>
</tr>
<tr>
<td>20</td>
<td>Beacons display</td>
<td>26</td>
</tr>
<tr>
<td>21</td>
<td>Company informations</td>
<td>27</td>
</tr>
<tr>
<td>22</td>
<td>Users management</td>
<td>28</td>
</tr>
<tr>
<td>23</td>
<td>New User creation - 1</td>
<td>28</td>
</tr>
<tr>
<td>24</td>
<td>New User creation - 2</td>
<td>29</td>
</tr>
<tr>
<td>25</td>
<td>Smartphones settings</td>
<td>31</td>
</tr>
<tr>
<td>26</td>
<td>Menu settings / Main tab</td>
<td>32</td>
</tr>
<tr>
<td>27</td>
<td>Menu settings / Menu tab</td>
<td>33</td>
</tr>
<tr>
<td>28</td>
<td>LoneWorker settings/ Main tab</td>
<td>34</td>
</tr>
<tr>
<td>29</td>
<td>LoneWorker settings/ Pre-alarm tab</td>
<td>35</td>
</tr>
<tr>
<td>30</td>
<td>LoneWorker settings / Fall down tab</td>
<td>36</td>
</tr>
<tr>
<td>31</td>
<td>LoneWorker settings / Immobility tab</td>
<td>37</td>
</tr>
<tr>
<td>32</td>
<td>LoneWorker settings/ SOS tab</td>
<td>38</td>
</tr>
<tr>
<td>33</td>
<td>LoneWorker settings / Bluetooth tab</td>
<td>39</td>
</tr>
<tr>
<td>34</td>
<td>LoneWorker settings / Location tab</td>
<td>39</td>
</tr>
<tr>
<td>35</td>
<td>LoneWorker settings / Geofencing tab</td>
<td>41</td>
</tr>
<tr>
<td>36</td>
<td>Geofencing zone creation</td>
<td>41</td>
</tr>
</tbody>
</table>