

# SECAPP USER GUIDE

## Table of contents

<b>OVERVIEW</b>	<b>2</b>
<b>INSTALLATION</b>	<b>3</b>
DOWNLOADING THE MOBILE APP	3
Download to Android	4
Download to iPhone	7
Download to Windows-Phone	9
USER ID AND PASSWORD	10
Change or reset your password on web browser	10
Change password on Android	12
Change password on iPhone	13
Reset forgotten password	14
MOBILE SETTINGS	15
Settings for iPhone	15
Settings for Android	16
Android version 7 >	19
Settings for Windows phone	20
<b>USER PROFILES</b>	<b>20</b>
<b>BASIC USER FUNCTIONS</b>	<b>21</b>
RECEIVING SECAPP MESSAGES ON MOBILE	21
RECEIVING SECAPP MESSAGES ON WEB BROWSER	24
CHAT	25
REPORTING TASKS RELATED TO THE SECAPP MESSAGE	27
LOCATION TRACKING SETTINGS	29
MAPS AND NAVIGATION	30
SMS-USE	31
<b>MESSAGE SENDER'S FUNCTIONS</b>	<b>32</b>
SENDING A SECAPP MESSAGE	32
Icons and priorities	33
Editing icons	34
Selecting recipients	34
Targeting a message to a location (alarming people to a site)	35
Limiting a message to users based on radius	36
Messaging channels	37
Additional settings	37
Reply automation & Escalation	38
Contents of the Tasks view	41
Adding tasks and categories to the report	43
Monitoring Responses on web browser	44
SENDING A MESSAGE FROM A MOBILE APP	45
Monitoring Responses on mobile app	47
<b>ADMINISTRATOR FUNCTIONS</b>	<b>48</b>
COMPANY SETTINGS AND INFORMATION	48
ADDING AND MANAGING USERS	49
JOINT ORGANIZATIONS	51
ADDING AND MANAGING GROUPS	52
SKILL PROFILES	53
MESSAGE TEMPLATES	53
CREATING A REPORT BASED ON THE INFO FROM TASKS	54
STATISTICS	56

## Overview

Secapp is a disruptive communication and reporting software that connects the industry, public and authority professionals. It is a tool for secure communication and alerting in a world where every device and network can be expected to be hostile and compromised.

Powerful technologies, SSL-secured communication, AES-256 content encryption and active threat analysis makes it possible for us to proudly offer you a messaging system where your messages are truly secure. It is used by over 200 different organizations including hospitals, fire and rescue, cities, schools, oil and production industry and security companies with roughly 20 000 users and 100 000 messages (alerts) sent monthly.

Secapp combines both TETRA (SDS, Call out) and commercial (mobile app, SMS, email, robot calls) communication. This two-way secure platform enables easy-to-use manual and automated messaging, alerting and paging to reach people with the right skills, location and availability. Checklists and reporting enable more in-depth tools to react and recover.

System utilizes location information in giving opportunities delivering messages and alerts to any given area, individual or group via multiple different delivery channels. In addition, the system provides full situational awareness picture via quick reply mechanisms allowing to not only to deliver messages but also to oversee and manage different operations.

Solution has been used for example by Finnish Police, public schools, emergency response personnel and it was also used in the Olympic Games in 2014 to provide privacy, robustness and efficiency both for their daily operations and crisis management. In addition, the solution won the Finnish Chamber of Commerce Cyber Security Track award during spring 2014 where Secapp was evaluated by judges from Airbus Defense and Space, telecom operator Elisa and Nordic wide bank called Nordea.

The team behind Secapp has developed future communication technologies for Nokia and European Space Agency and built business-critical software from finance services to healthcare over a decade. Our team has expertise in high-end scalable mobile and web solutions and years of experience from mission-critical domains. Secapp has received seal of excellence from EU commission, won chamber of commerce Fast Track Cyber and we are among TOP3 Finnish Security Companies by Finnish Security Awards.

By centralizing different communication channels with Secapp, communication becomes a lot less vulnerable for commercial network breakdowns, natural catastrophes, terrorism or limitations set by different environments. Moreover, Secapp is a low threshold deployment solution that can be taken into use even at the same day without any additional devices.

Secapp can be used for example in:

- Healthcare and hospitals
- Fire & Rescue
- Security and property
- Voluntary organizations
- Oil, mining, chemistry and food industry
- Critical infrastructure owners
- Cities and municipalities
- Schools
- Contractors
- Media
- High technology and device vendors
- IT Software and service providers



The control panel enables two-way alerting, work invitations and other communications through delivery channels such as:

1. Web browser
2. Mobile app (Android, iOS, Windows Phone, Windows 10 app)
3. Voice robot calls
4. SMS
5. Email
6. Social media (Facebook, Twitter, LinkedIn)
7. TETRA SDS and call-out protocol

## Installation

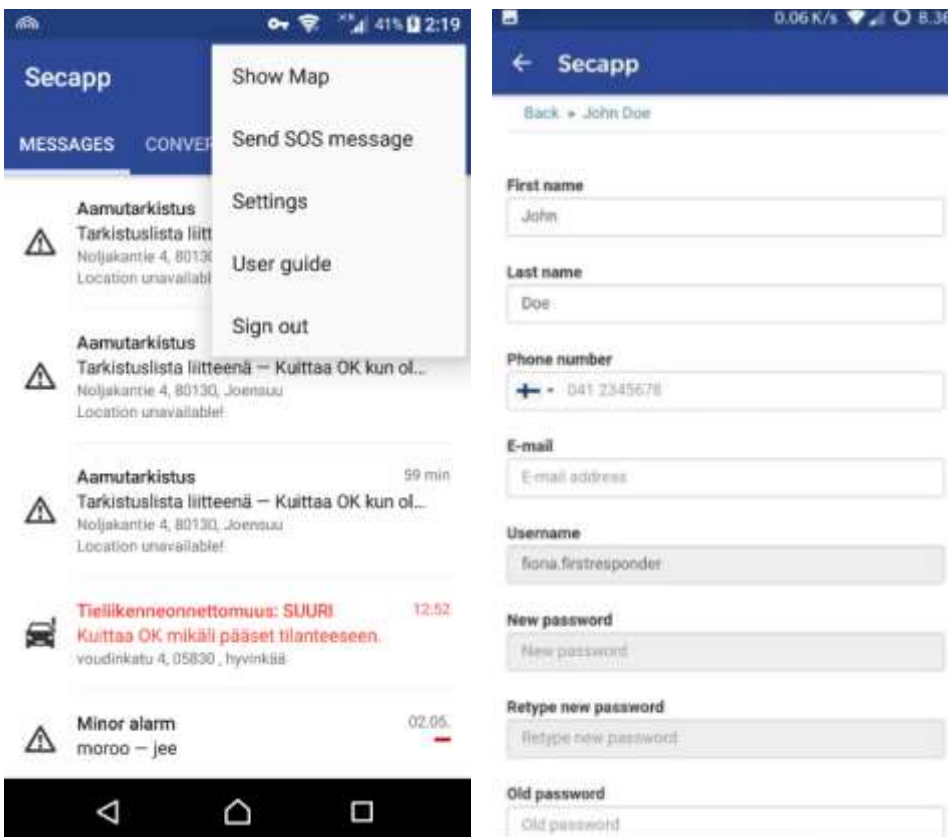
### Downloading the Mobile App

It is recommended to download the Secapp mobile app to get the most out of the system. Secapp works with multiply mobile platforms and you can load the mobile app for Android, iOs and

Windows Phone operating systems. The application can be downloaded from the app store of each app distribution platforms without a charge by searching **Secapp**. You cannot use the system without a user ID and a password. When a user logs in for the first time, he/she will be asked to confirm the application's terms of use.

You can go to your individual settings by clicking the three dots and then **Settings**.

From settings you can edit your own contact details or change your password, number, language and default view. You get to edit your own location settings, skills, notifications, mobile devices and panic buttons as well.

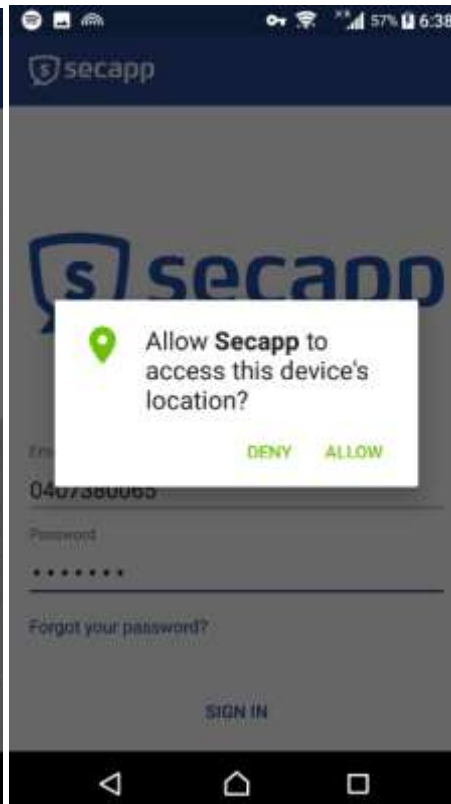
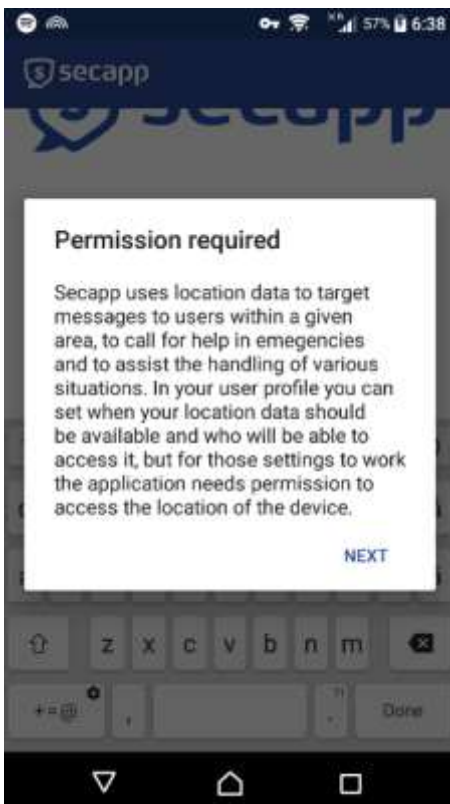


## Download to Android

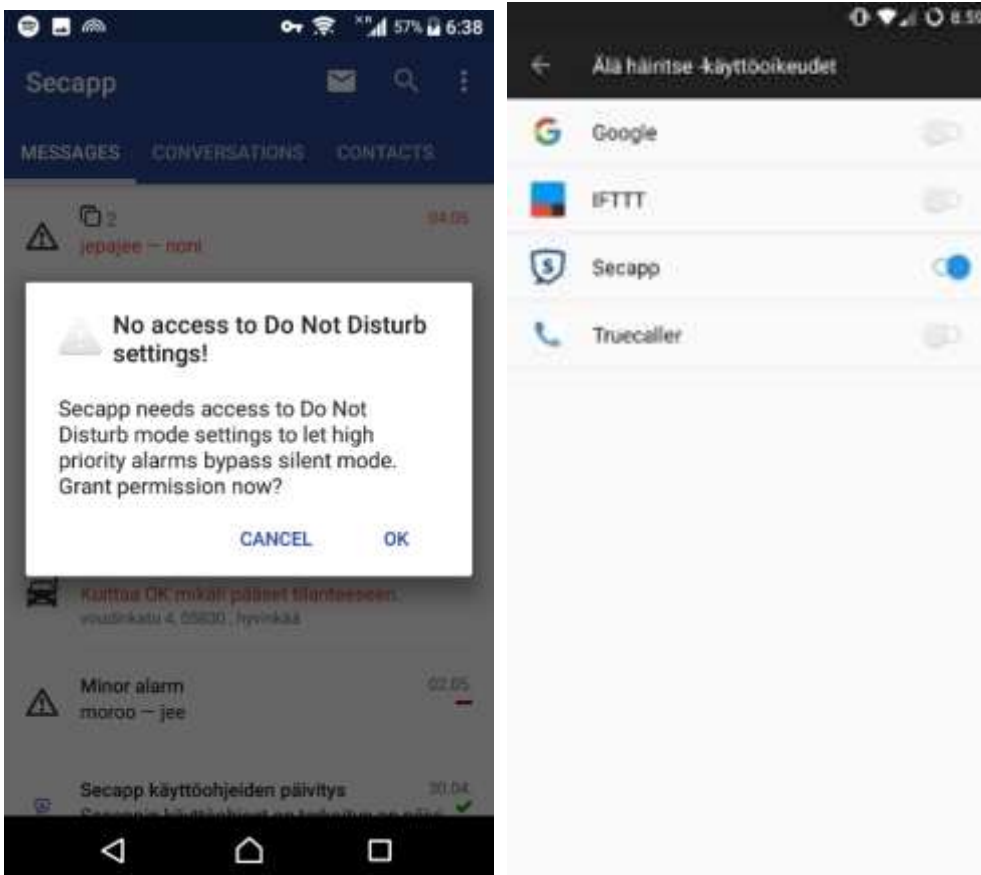
1. Go to Google Play Store to download Secapp mobile app to Android.
2. Search **Secapp** and select it from the listing.
3. Click **INSTALL**. You can find the link to Play Store from Secapp.fi website.
4. Launch the app after installation.
5. Login using the user ID and password. The mobile app will ask permissions to certain settings to work properly. Follow the directions.



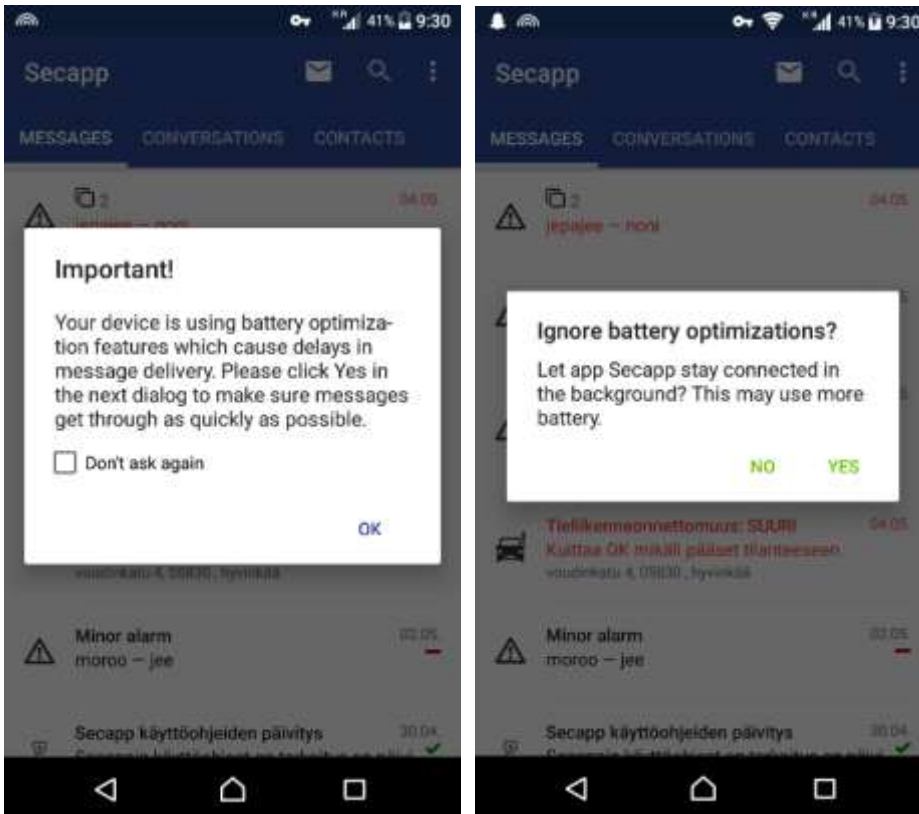
6. Secapp uses location data to target messages to users within a given area, to call for help in emergencies and to assist the handling of various situations. Click **next** and **allow** Secapp to access your device's location. You can change the location settings afterwards by going to app settings found on your phone's settings.



7. Do not disturb settings can be bypassed. Click **Ok** and change the settings for Secapp. Click **Allow**. You can return to the app by clicking the arrow on the upper left.



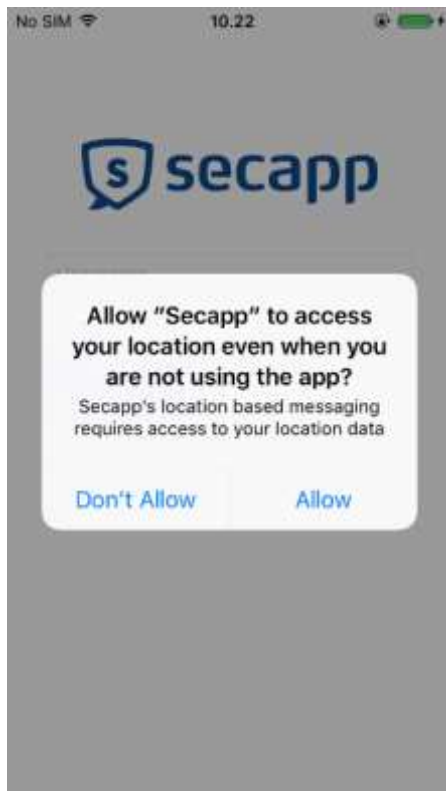
8. Most of mobile devices have automated battery-saving mode. Battery-optimization features will block processes running in the background to save the battery. It is important let Secapp stay connected in the background to get the alarms immediately. Click **Ok** and ignore battery optimizations by clicking **Yes**.



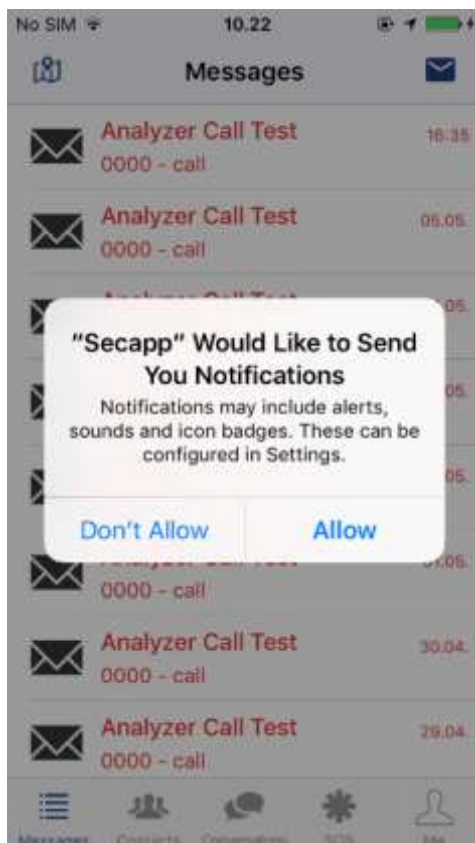
9. Settings for mobile app can be found from the cogwheel or three dots icon above contacts. From settings you can change your alarm sounds and password.
10. Secapp mobile app is now installed for Android. If you have problems with using the app, make sure to check your settings. If Secapp still doesn't work properly, contact your organization's Secapp administrator.

## Download to iPhone

1. Go to Google App Store to download Secapp mobile app to iPhone.
2. Search **Secapp** and select it from the listing.
3. Click **INSTALL**. You can find the link to App Store from Secapp.fi website.
4. Launch the app after installation.
5. Secapp uses location data to target messages to users within a given area, to call for help in emergencies, and to assist the handling of various situations. Click **Always Allow** for Secapp to access your device's location. You can change the location settings afterwards by going to app settings found on your phone's settings.



6. Login using the user ID and password.
7. Secapp would like to send you notifications. Notifications may include alerts and sounds. Click **Allow**.





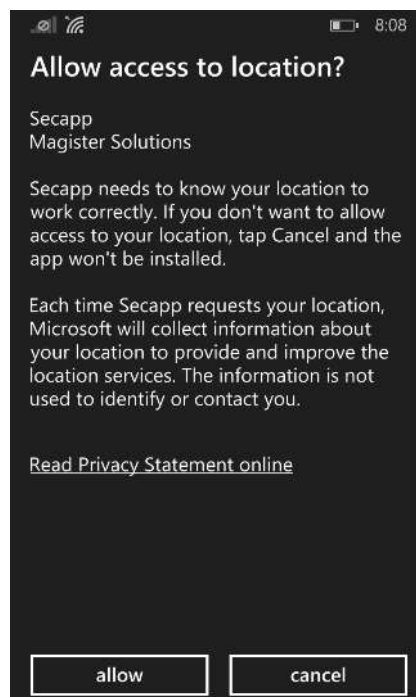
- The application settings can be found from the bottom right in the “Me” icon. From the settings, you can change your password and ringing tones. Open the settings.

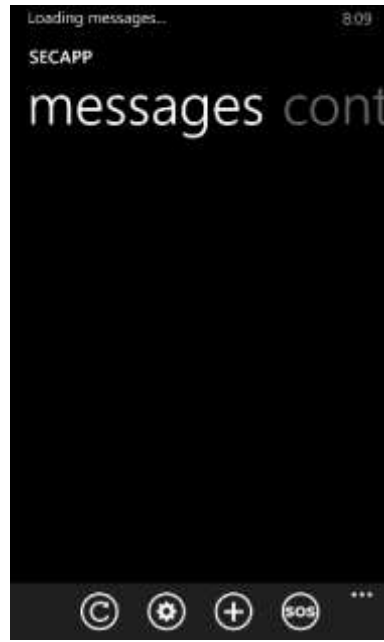
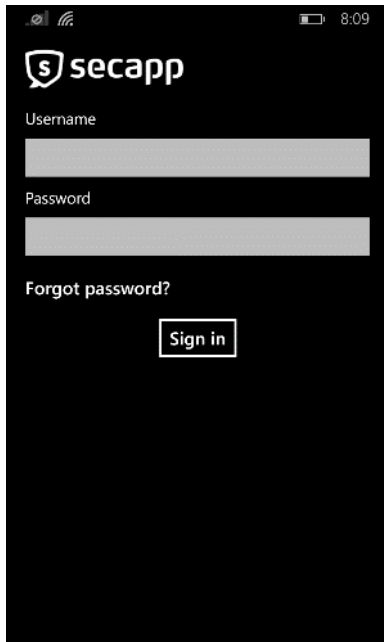


- It is essential that the mobile device alerts even if it's set to silent. Scroll down and turn on "Allow high priority alerts to bypass the phone mute setting". The mute setting is bypassed only in high priority situations when it's important to reach people. Ask more about these situations from your Secapp administrator.
- Secapp mobile app is now installed for iPhone. If you have problems with using the app, make sure to check your settings. If Secapp still doesn't work properly, contact your organization's Secapp administrator.

## Download to Windows-Phone

- Go to Windows Marketplace to download Secapp mobile app to Windows Phone.
- Search **Secapp** and select it from the listing.
- Click **INSTALL**. You can find the link to App Store from Secapp.fi website.
- Launch the app after installation.
- Secapp uses location data to target messages to users within a given area, to call for help in emergencies and to assist the handling of various situations. Click **allow** Secapp to access your device's location. You can change the location settings afterwards by going to app settings found on your phone's settings.





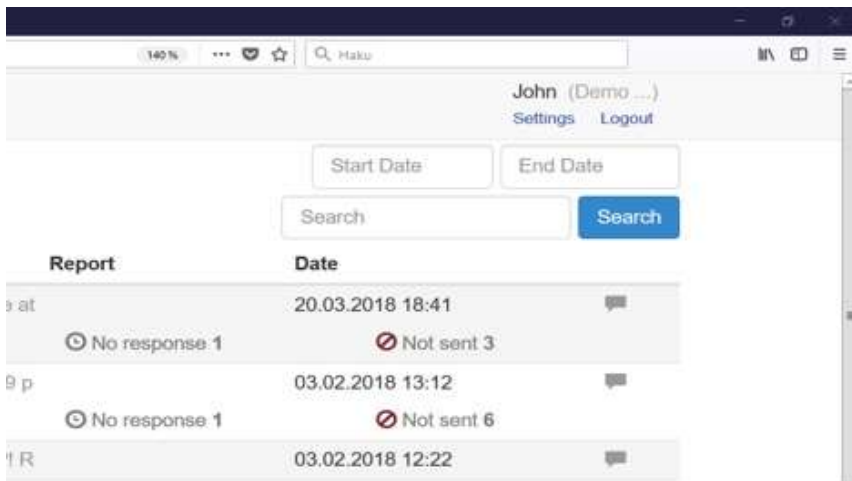
## User ID and password

Using Secapp requires personal user accounts that you can get to your email or SMS from your organization's administrator. User IDs are used when logging in for Secapp's mobile app or web service.

We recommend changing the default password the first time you log in. Passwords can be changed for both in the web browser and the mobile application. The mobile app must be installed before you can change your password through it.

## Change or reset your password on web browser

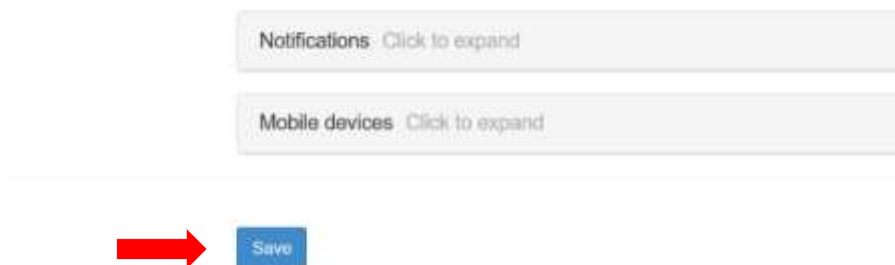
Go to [www.secapp.fi](http://www.secapp.fi) and click **Sign in**. After logging in, click on the top right "Settings" icon below your name.



Enter your new password in "New password" and "Retype new password" fields.

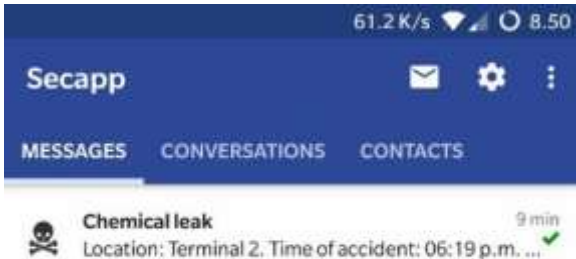
The screenshot shows a user profile form in the "secapp" application. The form includes fields for "First name" (John), "Last name" (Doe), "Phone number" (+ 041 2345678), "E-mail" (E-mail address), "Username" (fiona.firstresponder), "New password", "Retype new password", and "Old password".

Scroll down and click the "Save" button.

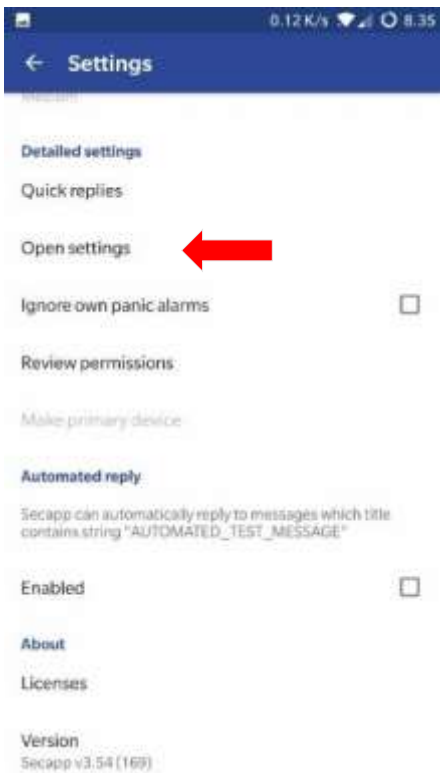


## Change password on Android

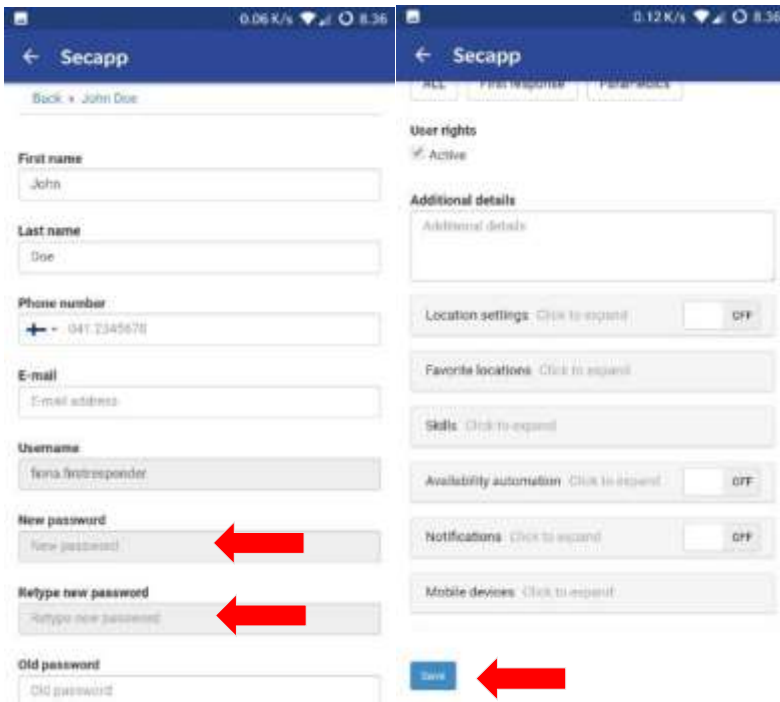
Click the **cogwheel** icon located on top-right of screen and click on **“Settings”**



Scroll the view down and click "Open Settings" line on top of the screen.

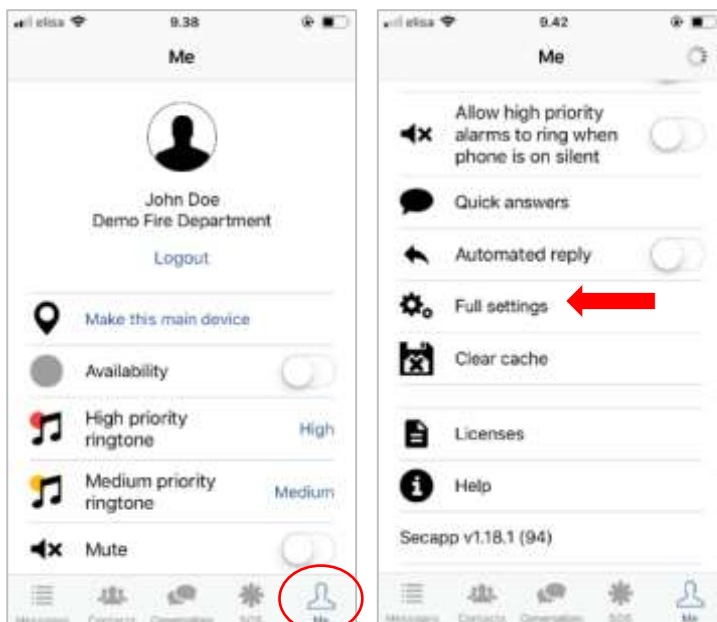


Enter your new password in "New password" and "Retype new password" fields. Scroll down and click **“Save”** button. Return to the main view by clicking an arrow located on top-left. Log in again with an updated password.

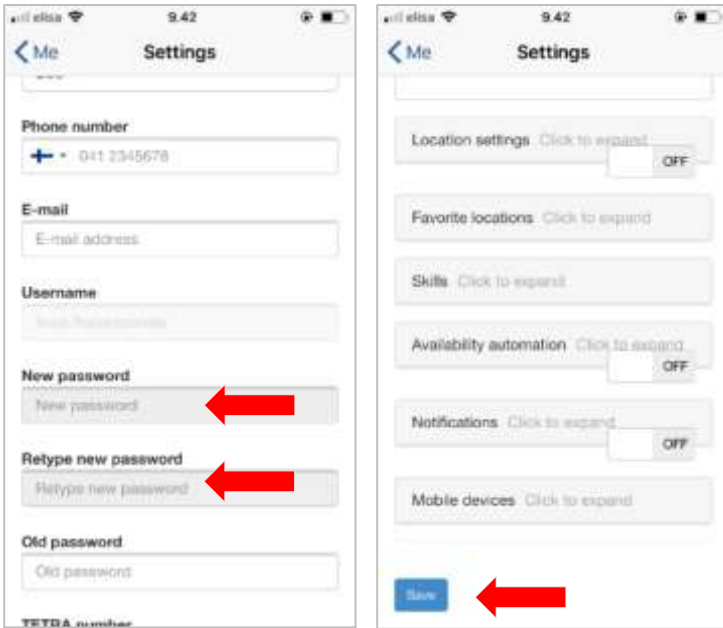


## Change password on iPhone

Open the **Me** icon located in the bottom right. Scroll down to the bottom of the screen and click "Full Settings" line in the middle of the screen.



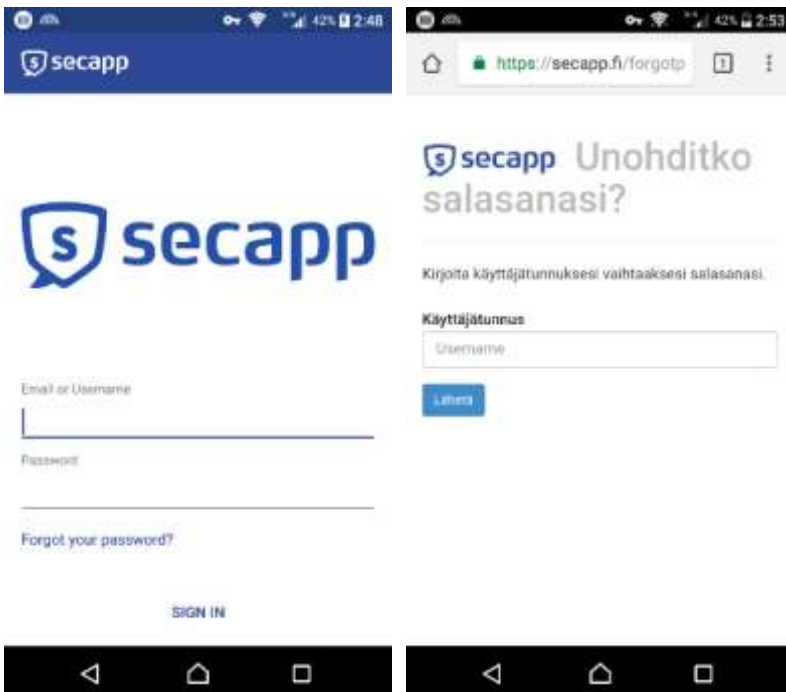
Enter your new password in **New password** and **Retype new password** fields. Scroll down and click **Save**. Return to the main view by clicking an arrow located on top-left. Log in again with an updated password.



## Reset forgotten password

If you've forgotten your Secapp password, open Secapp and click **forgot your password?**

Enter your phone number (User ID) and click send.



We will send you a link to reset your password shortly. If you can't find the reset email, check your spam or trash folders. If you still have issues with logging in, contact your organization's domain administrator.

## Mobile settings

The Secapp mobile application tries to set all the settings right after installation. In some cases, some smartphone setting may remain in the wrong position for Secapp. For example, Huawei phones have very aggressive battery-saving settings.

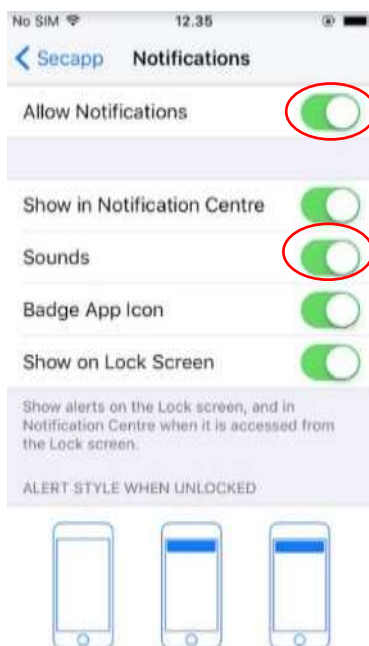
## Settings for iPhone

Make sure the following settings are **ON**:

1. *Settings -> Notifications -> Secapp -> "Allow Notifications" and "Sounds"*.

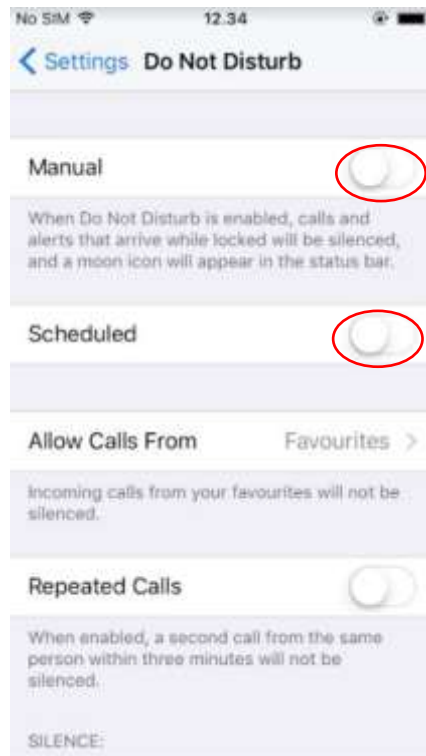
We also recommend keeping all other notification settings on for Secapp.

2. *Settings -> Secapp -> "API Update in Background" and "Mobile Data"*



Make sure the following settings are **OFF**:

1. *Settings -> Battery -> Low power status*
2. *Settings -> Do not Disturb -> Hand / Timed*

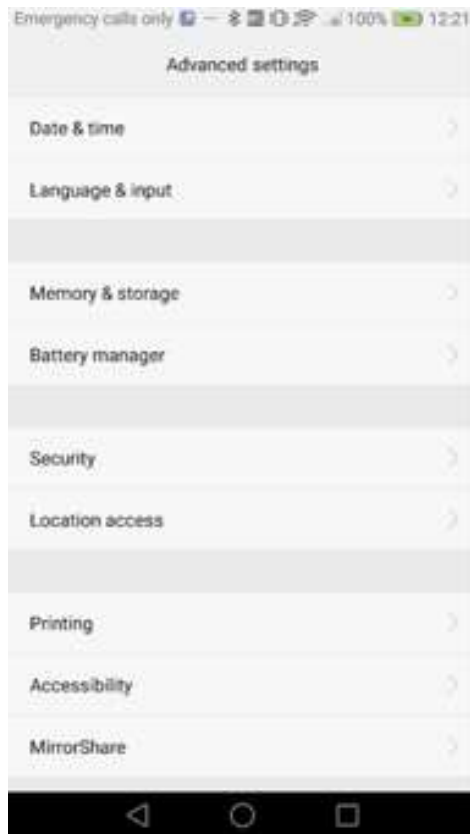


## Settings for Android

1. Set Secapp as a secure application with following steps:

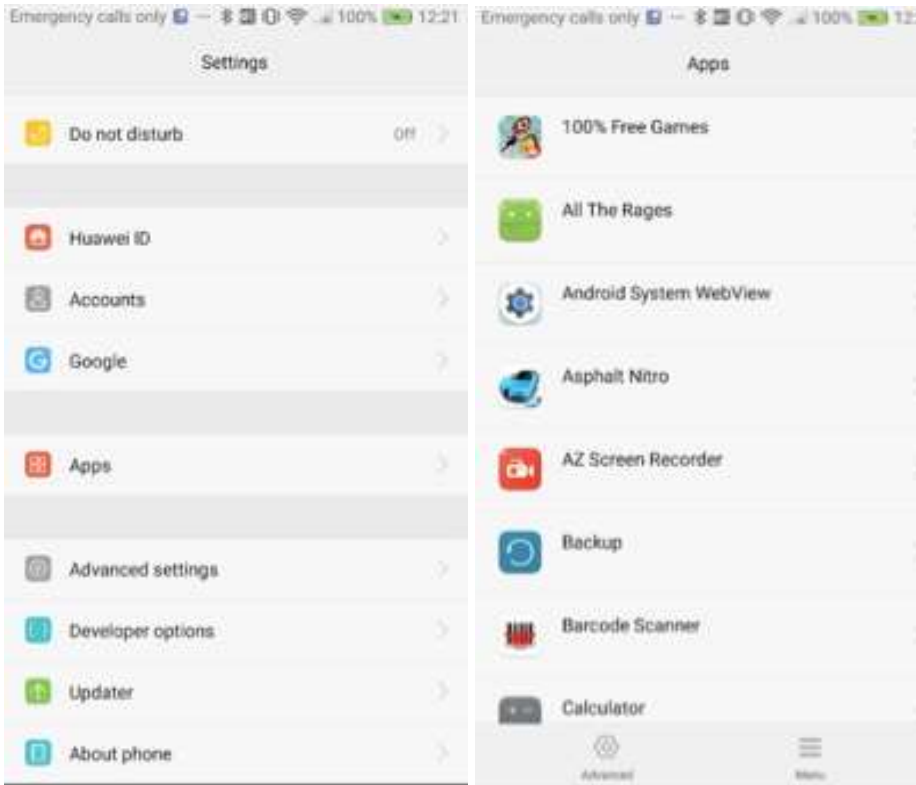
*Settings → advanced settings → battery manager → protected apps → Secapp → protect*





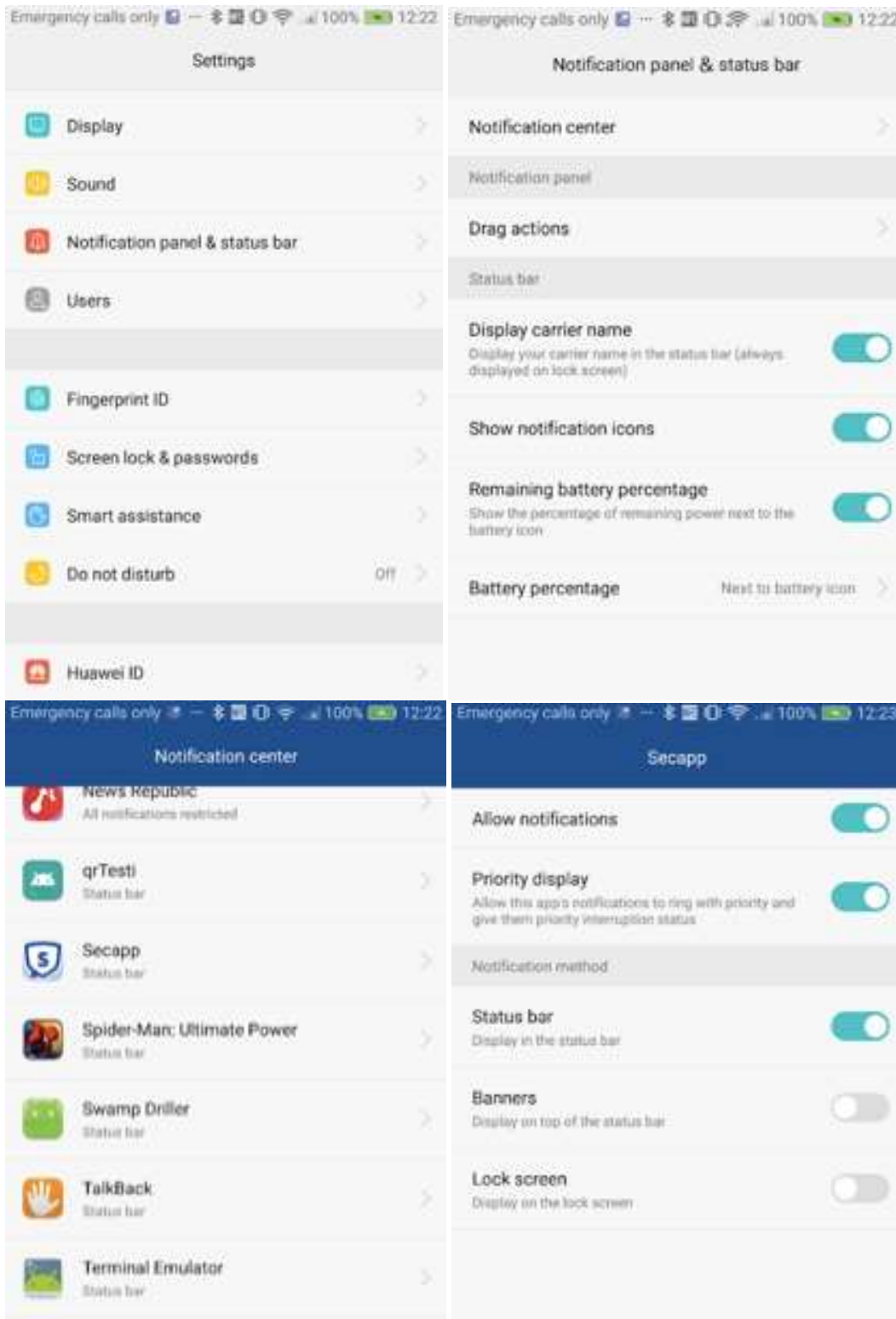
2. Set the battery optimization system to ignore Secapp:

Settings → apps → advanced → ignore battery optimizations → Secapp → ignore



3. Adjust the notification settings:

Settings → notification panel & status bar → notification center → Secapp → click “allow notifications” and “priority display”



Android version 7 >

1. Set the battery optimization system to ignore Secapp:

*Settings -> Apps -> Settings (Small icon at bottom) -> Special access -> Ignore battery optimization -> Find Secapp and set it to "Ignore".*

2. Adjust the notification settings:

*Settings -> Apps -> Secapp -> Notifications -> Enable "Allow notifications" and "Priority display".*

3. Adjust the screen lock settings:

*Settings -> Battery -> Close apps after screen lock -> Set "Don't close" for Secapp.*

## Settings for Windows phone

Make sure the following settings are **OFF**:

1. *Settings -> Battery -> Low power status*

Settings for mobile app can be found from the cogwheel icon. From settings you can change for example your alarm sounds and password.



## User profiles

Secapp user profiles can be divided into three different roles: basic users (message receivers), message senders and administrators. Each role has different entitlements (rights?).

1. Basic users

Basic users can receive and notice (sign?) the messages. They can participate in the conversations under an individual organization. Can edit their own information and activate panic messaging.

2. Message senders

In an organization, a message sender is the person who has the mandate to inform staff or to alert eg. deputies. He/she can send, edit and track messages, and manage the situation.

3. Administrators (main users)

Administrator can control (add, edit and delete) user's contact information, groups, templates and send and receive messages under an individual organization. They can also delete old messages in sight of all the recipients.

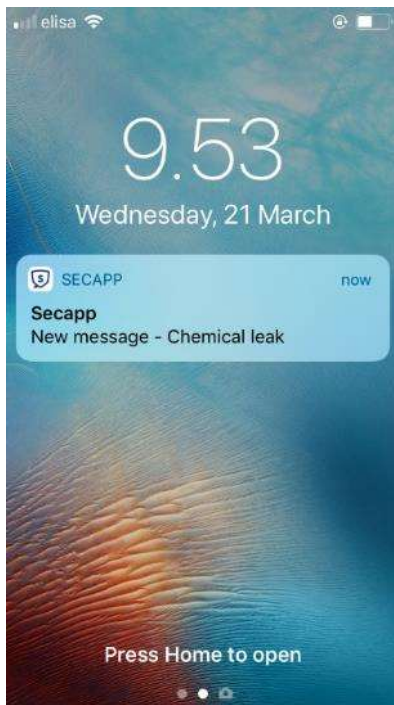
Both administrators and basic users can be added to multiply organizations, allowing them to access more than one organization. Find more about this on [joint organizations](#) chapter.

## Basic User functions

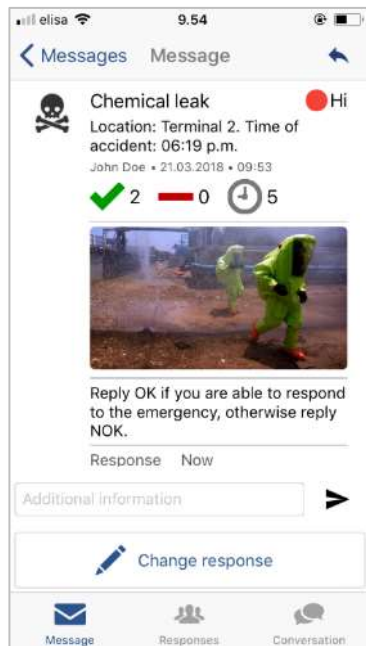
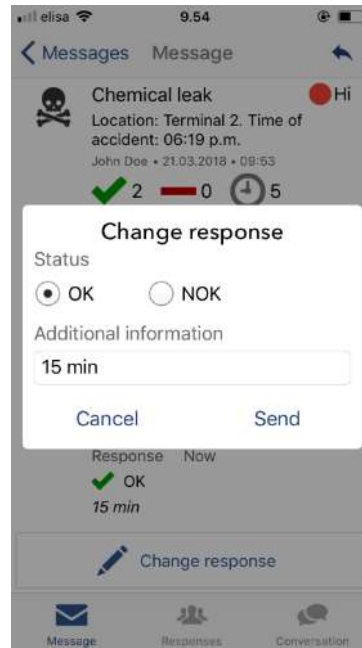
### Receiving Secapp messages on mobile

When the Secapp message arrives, an alarm box appears on the screen. Open the message by clicking the alarm box or "Open". The message includes headline, possible acknowledgments, actual content, and acknowledge buttons:

- **Headline** briefly tells you what the situation is about.
- **Responses** quickly tell how others have reacted to the situation.
- Read carefully the actual contents of the message, as you might be expected to give a certain response.
- On the **Conversation** tab, you can talk with people who received the Secapp message in question and keep track of how the situation is developing.



- With the response buttons (OK / NOK) you can quickly tell how you react to the situation. This information is updated to all those who received the same Secapp message in real time. After replying OK or NOK, you can send additional information. You can also change your response.

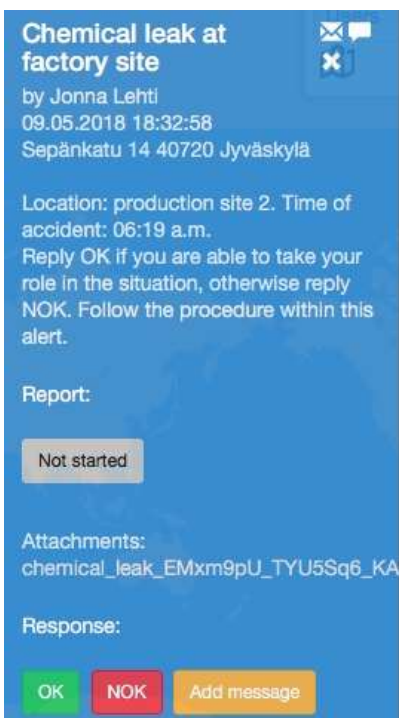


By clicking “Map”, you can also check where the alarm is associated with map.



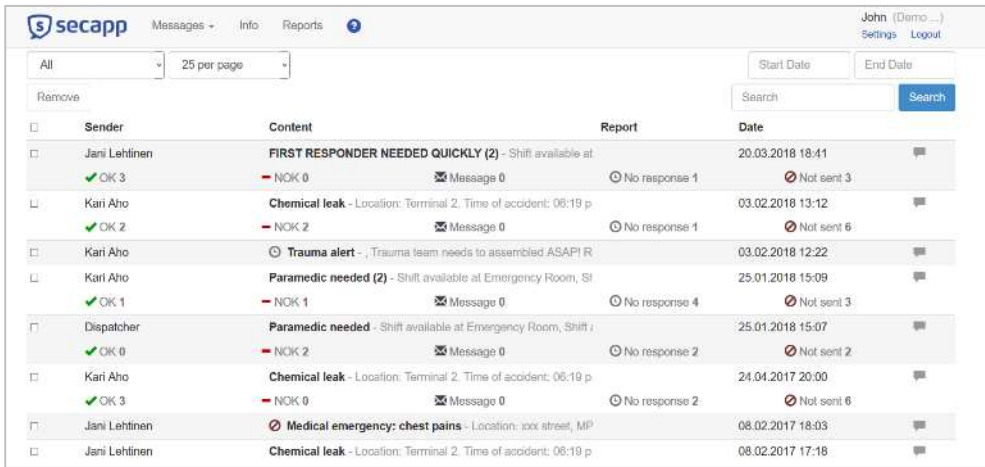
## Receiving Secapp messages on web browser

In addition to the Secapp mobile application, you can also open a message in the web browser. Go to [www.secapp.fi](http://www.secapp.fi) and click Sign in. The web browser works with the same username and password as the mobile application. The web browser is displayed in the Inbox or in the map view.

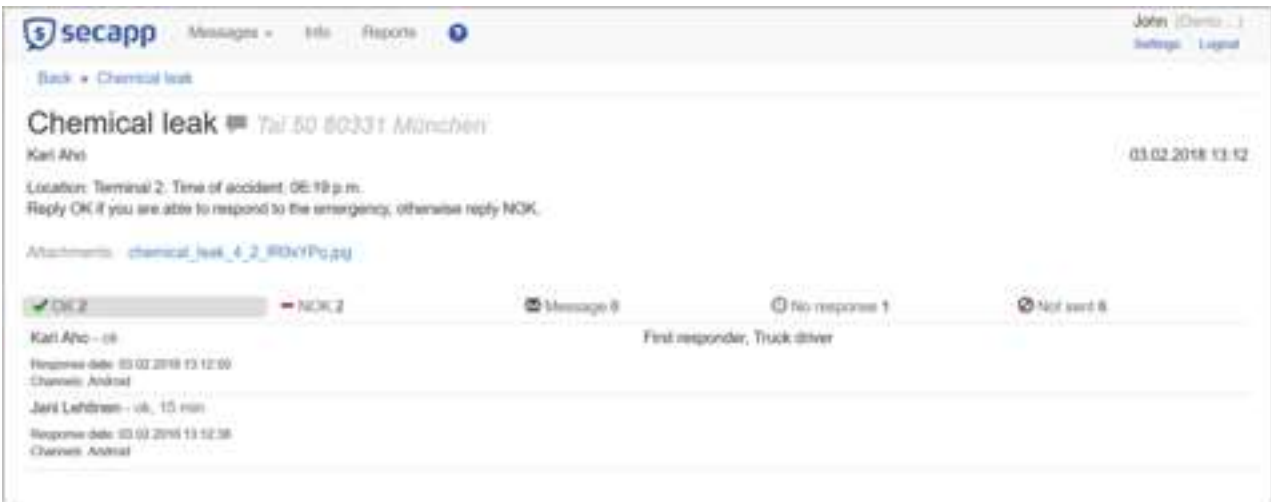




From the Inbox view you can view all the messages that you have received. The latest message is on top of the list. Click on the message to see the content of the message.



	Sender	Content	Report	Date
<input type="checkbox"/>	Jani Lehtinen	<b>FIRST RESPONDER NEEDED QUICKLY (2)</b> - Shift available at		20.03.2018 18:41
	OK 3	NOK 0	Message 0	No response 1
<input type="checkbox"/>	Kari Aho	<b>Chemical leak</b> - Location: Terminal 2. Time of accident: 08:19 p		03.02.2018 13:12
	OK 2	NOK 2	Message 0	No response 1
<input type="checkbox"/>	Kari Aho	<b>Trauma alert</b> - Trauma team needs to assembled ASAP! R		03.02.2018 12:22
<input type="checkbox"/>	Kari Aho	<b>Paramedic needed (2)</b> - Shift available at Emergency Room, SI		25.01.2018 15:09
	OK 1	NOK 1	Message 0	No response 4
<input type="checkbox"/>	Dispatcher	<b>Paramedic needed</b> - Shift available at Emergency Room, Shift		25.01.2018 15:07
	OK 0	NOK 2	Message 0	No response 2
<input type="checkbox"/>	Kari Aho	<b>Chemical leak</b> - Location: Terminal 2. Time of accident: 08:19 p		24.04.2017 20:00
	OK 3	NOK 0	Message 0	No response 2
<input type="checkbox"/>	Jani Lehtinen	<b>Medical emergency: chest pains</b> - Location: xxx street, MP		08.02.2017 18:03
<input type="checkbox"/>	Jani Lehtinen	<b>Chemical leak</b> - Location: Terminal 2. Time of accident: 08:19 p		08.02.2017 17:18



Back • Chemical leak

### Chemical leak

Tal 50 80331 München

Kari Aho 03.02.2018 13:12

Location: Terminal 2. Time of accident: 08:19 p.m.  
Reply OK if you are able to respond to the emergency, otherwise reply NOK.

Attachments: [chemical\\_leak\\_4\\_2\\_08xYFp.ppt](#)

OK 2 NOK 2 Message 0 No response 1 Not sent 6

Kari Aho - ok  
Response date: 03.02.2018 13:12:00  
Channel: Ankkat

Jani Lehtinen - ok, 15 min  
Response date: 03.02.2018 13:12:38  
Channel: Ankkat

First responder, Truck driver

With the response buttons (OK / NOK) you can quickly tell how you react to the situation. This information is updated to all those who received the same Secapp message in real time. After replying OK or NOK, you can send additional information. You can also change your response.

## Chat

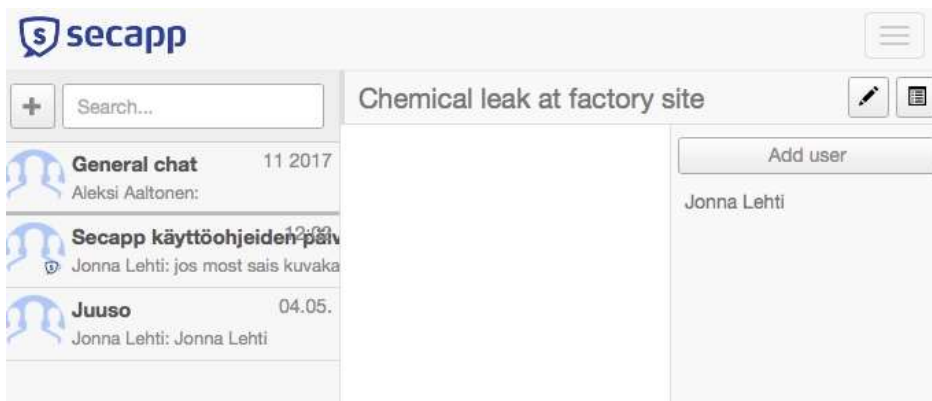
On the chat tab, you can talk with people who received the Secapp message and keep track of how the situation is developing. You can enter text, take or add pictures and files, and add web addresses. You will receive a notification of new messages even if you don't actively follow the conversation view.

Open the chat view on web browser by clicking the speech bubble found on the Secapp message. The browser opens a new tab for the conversation for that alarm.



The conversation view shows all your conversations on the left side, in the middle there is a selected conversation and at the far right you can see the people involved in the conversation.

If you have enough entitlements, you can also add new people to the conversation. New people will get an invitation to join the discussion. They will be also able to see the tasks that may be included in the message. You can add new users above the user list located on the right side of page.



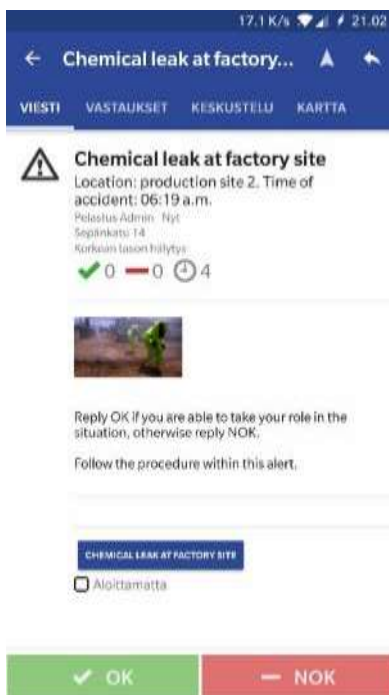
You can delete users from the chats and as well from the alarm messages the same way as adding them.

You can find conversations in the mobile app above / below the message list. The Conversations tab gives you a direct access to the ongoing discussions.



## Reporting tasks related to the Secapp message

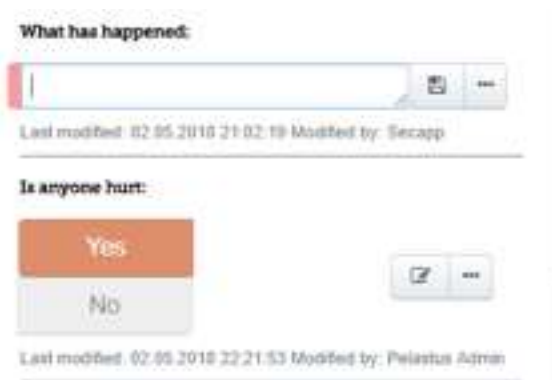
Secapp message can also contain tasks that you can open by clicking a blue button at the bottom of the message. The title of the button is name of the task list. Tasks are divided into categories which help navigating in the task lists. Tasks will open in a new view, from where you can monitor the progress of tasks and, if necessary, change the status of the them by yourself.



The Tasks view can contain individual tasks and categories that are a collection of tasks. You will find the categories at the top of the Tasks view before the individual tasks.

Task status changes automatically if another user changes the status of the task. In addition to the Task view, the change in the status of the task is displayed in a corresponding discussion in the row created by the system.

To change the status of a task, click the pen icon on the right side of the task. You can add text, images or change the status of the task, depending on the type of task. To save a task, click the Save icon on the right side or change the browser's focus elsewhere.

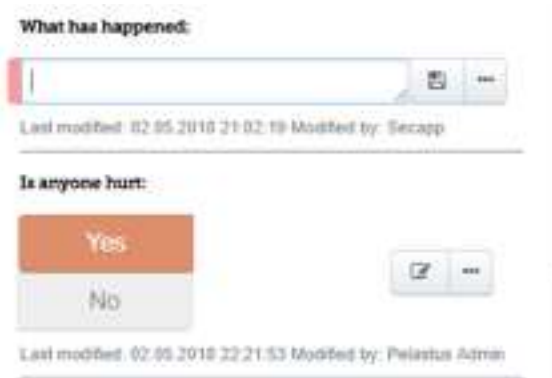


In the web browser, the task view opens next to the chat view on the right side of the browser. You can monitor the progress of tasks and, if necessary, change the status of the tasks. Task status changes automatically if another user changes the status of the task. In addition to the Task view, the change in the status of the task is displayed in a corresponding discussion in the row created by the system.



You can edit tasks or their statuses same way in the web browser: click the pen icon on the right side of the task. You can add text, images or change the status of the task, depending on the type

of task. To save a task, click the Save icon on the right side or change the browser's focus elsewhere.



## Location tracking settings

User location data is a valuable information in creating a situation picture and sending right messages to the right people.

Discuss with your organization's Secapp responsible on how to use location information to make the ground rules clear. Secapp is a flexible system and it allows you to limit geographic information on and off, for example, by day and time.

You can change your own location settings by clicking **Settings** on the top bar and scrolling down to **Location settings**.

Location settings Click to expand  OFF

In addition to your current location, Secapp can also save a history of your past locations.

ON  OFF Allow location history

Specify how long will your location be visible after specific responses.

**Response**

OFF OK

OFF NOK

OFF Message

**Hours**

Always

Below you can specify when will you allow secapp to save your location data.

OFF Enable visibility settings below

**Hours**

Start 23

End 23

**Days**

OFF Mo.

OFF Tu.

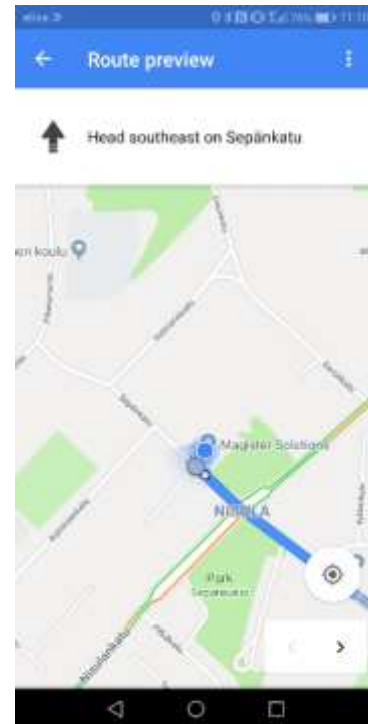
OFF We.

OFF Th.

## Maps and navigation

Secapp lets you get an alert on the map.

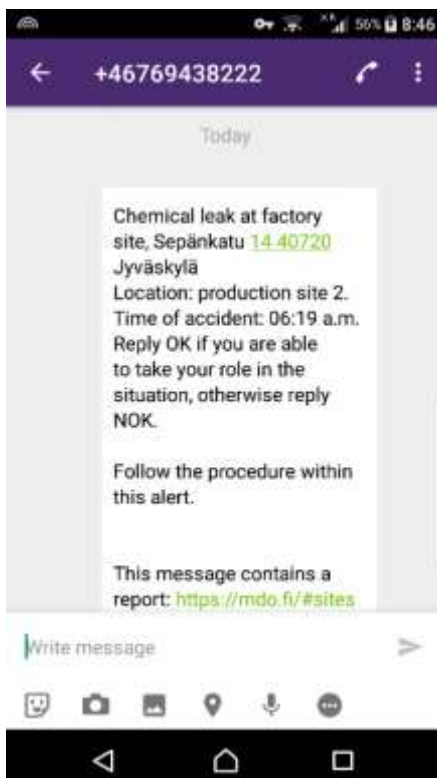
When the message arrives, you can check from the map view where the alarm is located by clicking **Map**.



## SMS-use

If you have an older phone, it is also possible to send and receive SMS-alarms through Secapp.

Follow the directions on the text message and reply OK or NOK. You can also reply without OK/NOK code by typing additional text or typing it after the codes.



**Send a panic message** by typing **SOS**. Send it to the same number where you receive messages.

**Activate dead man's switch** by typing **SWITCH MINUTES** and send it to the same number where you receive messages. You can add additional text after SWITCH MINUTES.

For example: SWITCH 10 checking gas leak in industrial hall 2 alone.

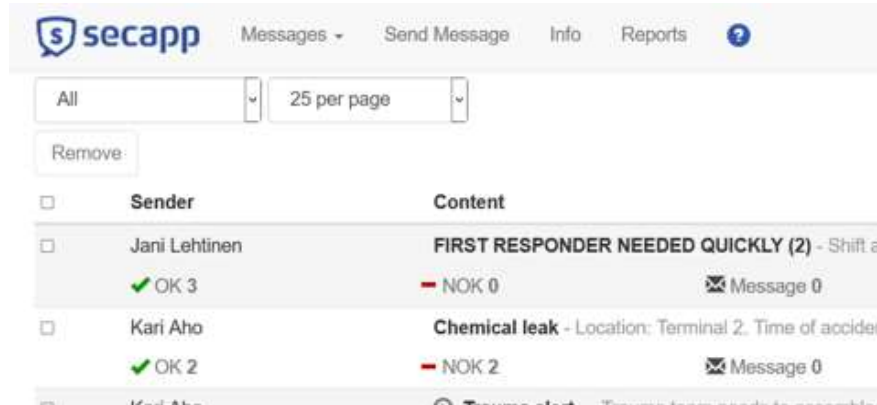
**Stop dead man's switch** by typing **STOP and** send it to the same number where you receive messages.

## Message sender's functions

### Sending a Secapp message

#### Sending a message based on a template

You can send messages both from the mobile app and web browser. Below you can find instructions to sending a message from web browser. If you're entitled to send messages, click "Send message" tab found on top of the page.



After entering to message sending view, choose a message template.

Instructions on editing/adding message templates can be found in the [message template](#) chapter.



The system will automatically fill out fields according to the template.



Message target Click to expand  OFF

Language options: Default

Title: Chemical leak


Description: Location: Terminal 2, Time of accident: 06:19 p.m.

Instructions: Reply OK if you are able to respond to the emergency, otherwise reply NOK.

Scroll down and click **Send**. When the message is successfully sent, "Message sent! View Post" text will appear.

secapp Messages **Send Message** Info Reports John (Demi...)  
Settings Logout

Template: Chemical leak

Icon:  Poisonous

Priority: High

Send to: Users  Groups  Area

Groups: First response -

Additional phone numbers or emails: +00 (00000000) email@gmail.com... (International phone numbers and emails separated by comma)

Message target Click to expand  ON

Language options: Default

Title: Chemical leak

Description: Location: Terminal 2, Time of accident: 06:19 p.m.

Instructions: Reply OK if you are able to respond to the emergency, otherwise reply NOK.

Send to: SMS (-0)  ON Mobile app  ON Email  OFF

TETRA SDS  OFF TETRA Callout  OFF

Additional settings Click to expand

## Icons and priorities

After selecting a message template, you can choose an icon which gives the visual look for the alarm.

Template:

Icon:  Fire

**Priorities** define how messages are transmitted to the recipient's phone, for example when the silent mode is on. You can choose from 3 options:

Low = not easily observed or noticed.

Medium = notifies that the message has arrived.

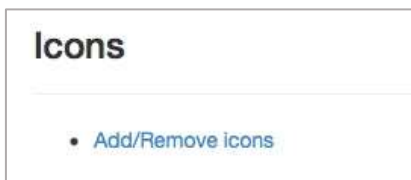
High = raises the attention of the user as well as possible by high volume ringtones and vibration.



A screenshot of a web form element. On the left, the word "Priority" is displayed in a bold, dark font. To its right is a horizontal dropdown menu with a light gray background and a thin border. The word "High" is visible inside the menu, and a small downward-pointing arrow is on the right side of the menu.

### *Editing icons*

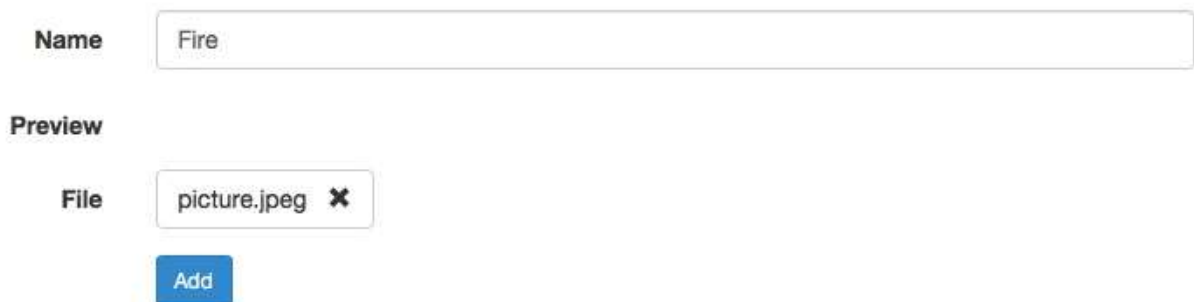
You can edit icons from the **INFO** tab found on the web browser. Click **Add/Remove** icons. The browser opens a new tab.



A screenshot of a web interface section titled "Icons" in a bold, dark font. Below the title is a horizontal line. Underneath the line, there is a single bullet point followed by the text "Add/Remove icons" in a blue, clickable font.

You can delete the icons by selecting the boxes on the left and clicking **Delete**.

Add a new icon by clicking **Add**. Write a name and attach a picture for the icon.



A screenshot of a form for adding a new icon. It consists of three main sections. The first section is labeled "Name" and contains a text input field with the word "Fire" entered. The second section is labeled "Preview" and contains a "File" input field with "picture.jpeg" and a small "X" icon next to it. Below the "File" field is a blue button with the word "Add" written on it.

### *Selecting recipients*

In **Send to** field you can choose to send a message to users, groups or users based on radius (area).

In **Users** field you will be asked to select the users to whom you want to send a message. You can find people by clicking "Search" and typing their name, or you can select all.

In **Group** field you can send a message to an existing group.

In **Area** field you can search for a region's address based on the coordinates. Specify a radius that allows you to restrict recipients, whether they are within the area, leaving the area or entering the area.

In **Additional phone numbers or emails** field you can also add non-established users as recipients. Be sure to include any additional phone number in international format (eg. +358 to beginning)

**Language options** allows you to select alternative languages for the message. The transmitted message is depending on the recipient's default language of choice. For example, if the user's default language is English and the message is created in Finnish and English, Secapp delivers an English message to the recipient.

**Attachments** allows you to attach other documents such as pictures or videos to your post.

### *Targeting a message to a location (alarming people to a site)*

In **Area** section, you can find a location of a region based on the coordinates or address. Define a radius that limits the recipients whether they are inside, leaving the area, or entering the area. Secapp lets you get a situational picture on the map base, as well as alert users to or near the scene.

#### **Send ALERT to user when user enters a certain area/scene:**

1. Send message
2. Send to area
3. Define area by adding address, coordinates or select from a map
4. Condition users entering radius
5. Set start and end dates
6. Add message content and send

How the dispatcher can know who has entered a certain area?

Users are added to the message recipients when they enter the area, so from inbox or map. Alternatively, if dispatcher wants separate notification from each user, when sending message adjust "send to" parameter which is by default set to area. If you change it to area and users, for instance, you can select users that also get alerted separately when someone enters the area

#### **Send ALERT to user when user leaves a certain area:**

Works similarly as entering area, just change condition to users leaving area

How the dispatcher can know who has left the area?

Again, they are added to message recipients or separate notification if wanted.

How the start time and end time values are used for geolocation alerts?

Those times define how long geofencing is enabled.

**Send alert to supervisor automatically if the prime intended worker does not respond within a certain time:**

Additional settings -> message automation and escalation -> Type escalate message -> Reply count 0 and set desired time and to whom message will be sent.

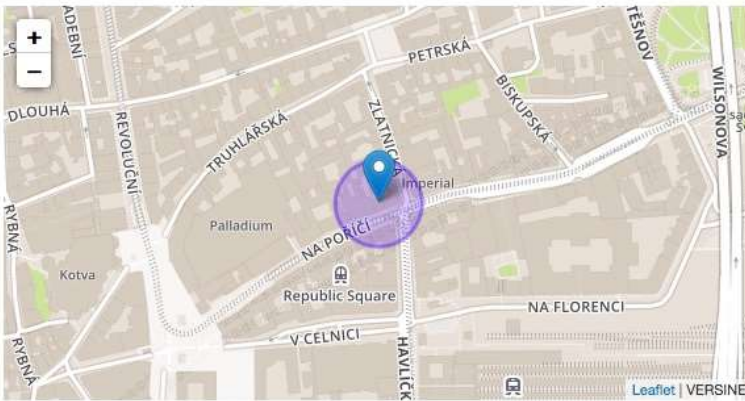
### Limiting a message to users based on radius

Additionally, you can make the area restriction message to individual users or groups.

For example, select "Send" to the person to whom the message goes (For example Mike the Manager). Select the person to whom the notice concerns (Fred the Firefighter). In this case, Mike receives notice when Fred arrives / leaves the area.

**Area** Search by address

Lat  Lon  Radius (m)



Condition

Start Date  End Date

Send to

Limit to

Select group(s)

## Messaging channels

In the “**Send to**” section you can select the channels that you want to use with sending your message. Note that the Robot Call only supports Finnish or English. The audio file must be selected to transmit audio files.

The image shows a 'Send to' settings interface with the following elements:

- SMS (~0)**: A toggle switch set to **ON**.
- Mobile app**: A toggle switch set to **ON**.
- Email**: A toggle switch set to **ON**.
- Robot call**: A toggle switch set to **OFF**.
- Audio call**: A toggle switch set to **OFF**.
- TETRA SDS**: A toggle switch set to **OFF**.
- TETRA callout**: A toggle switch set to **OFF**.
- TETRA callout priority**: A dropdown menu currently showing the value **1**.

A message to **mobile app** or **SMS** is sent as an alternative to users. In other words, if a user has a mobile application active, a message is sent only to a mobile app. If the user does not have a mobile application at all or it's not active, the message will be delivered as a text message if the user's phone number is listed in the user information.

**Robotic calls** are always delivered to all recipients who have a telephone number listed in the user information.

An **email** message is always delivered to all recipients who have the e-mail address listed in the user information.

**TETRA** messages are always delivered to all recipients who have the TETRA number listed in the user information. Note that the TETRA communication channel must be activated separately for your organization. If you do not see it in the communication channel, please contact Secapp's support or sales representative.

## *Additional settings*

From additional settings you can set a timed message to be sent and target messages by receiver's skills or availability. You can also automate your communications according to recipient responses to alarms.

Additional settings Click to expand

Timed Click to expand OFF

Display responses to everyone OFF

Encrypt Click to expand OFF

Availability Click to expand OFF

Skills Click to expand OFF

Reply automation & Escalation Click to expand OFF

Forward replies Click to expand OFF

Report Click to expand OFF

### *Reply automation & Escalation*

Secapp can be used to automate messaging in a variety of ways in situations where further communication is desired based on recipient responses.

For example, a follow-up instruction can be sent based on different answers (OK/NOK).

Click **Send message** or **Templates** -> **Additional settings** -> **Reply automation & Escalation**. Select action 1 where you give instructions to recipients based on their responses.

Report Click to expand ON

Template

Preserve existing values ON

**Send message immediately to replier:** You can type a message that the recipient sees immediately after their response (OK/NOK). You can send the automated message separately to the users who have replied OK or NOK.

**Send a conditional message to repliers:** select OK/NOK and the desired number of responses when eg. OK responses have been obtained. Then define what you want to say to your OK responders before the condition is met. Click “add message” and send to users who have replied OK. Click “Add”.

Reply automation & Escalation [Click to expand](#) ON

Action 1 +

**Type**  
Send a conditional message to repliers

**Reply type**  
OK

**Reply count**  
3  
Equals

**Before condition is met:** Messages  
Add message

**When condition is met:** Messages  
Add message

**Deadline (Minutes)**  
ON  
10

**Escalate message:** when the recipient responds to the message, you can send a new message to the user, group or users in certain location.  
For example, alerting one employee to work. Select 1 reply count and deadline (minutes). If replies do not arrive at a certain time, you can extend the recipients by clicking “Add message” and selecting the users. A new message can be sent to the user, resend the original message, or expand the original message.

Reply automation & Escalation Click to expand  ON

Action 1 +

Type: Escalate message

Reply type: OK

Reply count: 3 Equals

Send to	Title
Users	

Deadline (Minutes):  ON 10

You can add multiply actions by clicking +.

**Forward replies** if you want to get for yourself or for all message recipients information about what recipients have replied to the message you send. You can choose through which channels (email, SMS, mobile) this information is delivered.

Forward replies Click to expand  ON

**Forwarding replies to everyone** will generate a large amount of additional messages being sent. You might want to disable the **SMS** message channel if you are sending the message to a large number of recipients.

Reply type: OK

Forward to: Sender

Send to:  OFF SMS  ON Mobile  ON Email

**Timed:** Sending a message can be automated to timing dependent and automating repetitions. Options are once, daily, weekly, monthly, and yearly. Selecting the repetition frequency will open the possibility to specify when the message is to be sent.



Additional settings [Click to expand](#)

Timed [Click to expand](#)  ON

Repeat

Date/Time

Repeat	Date/Time	
Daily	10/05/2018 18:00	<input type="button" value="Remove"/>

**Display responses to everyone:** users responses will be visible to all message recipients if this feature is turned on. When turned off, only responses of the recipients are imported into control panel.

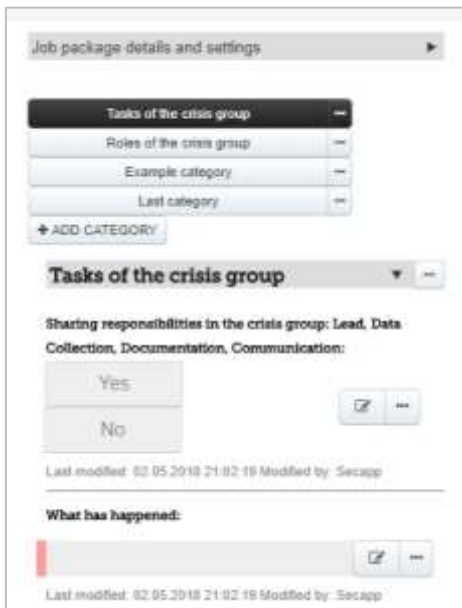
**Encrypt:** communication can be protected with a password. Add the desired password. The recipient must have the correct password in order to read the message.

**Availability:** The message can be targeted according to how the user has determined their own presence; either to those who are present or to those who have defined themselves as absent.

**Skills:** the messages can be targeted to the right people according to the desired skills. The message can be targeted according to the skill profiles so that the desired recipient has one or all of the selected competences. It may be useful for the organization to know, for example, those with a security guard card and / or first aid competence.

## Contents of the Tasks view

The Tasks view can include individual tasks and categories that are a collection of tasks. You will find the categories at the top of the Tasks view above individual tasks.



You can add tasks and to-do lists as an attachment to the message from the **Additional settings** section under **Report** tab.



Secapp supports fourteen different types of tasks that help to describe the situation as easily and comprehensively as possible. The most commonly used task types with descriptions:

**Clear text:** The user can write a text for the job.

**YES/NO choices:** the user selects the Yes or No according to what the description of the task asked.

**Image:** The user can add a picture from a computer or phone.

**Video:** The user can add a video from a computer or phone.

**Attachment:** The user can add any file from a computer or phone

**Numeric value:** The user can only enter a numeric value for the job.

**Date:** The task includes a date selector and, if required, the time can be entered as well.

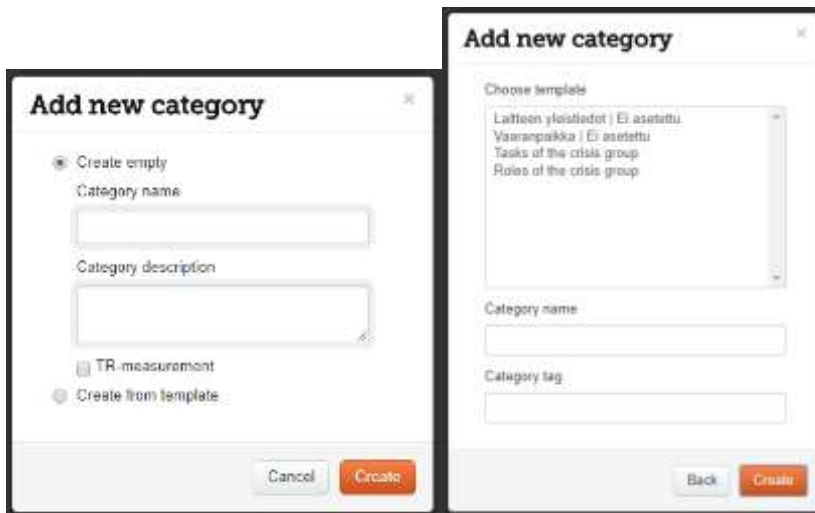
**Selection list:** There are several answer options for the task, one or more of which are selected. Defining the selection lists can be found from reports tab.

**Dynamic Selection List:** The task has multiple response options where you select one. This option opens a previously defined sub-category under a task that may include more than one task. Defining the selection lists can be found from reports tab.

**Signature:** The user enters a signature for the job. Works best with touch screens, such as a phone or tablet.

### *Adding tasks and categories to the report*

You can also add new tasks to your task list. To add a task, click the three points at the top right of the to-do list and select Insert and Add task below it.



In “Add new task” view, you are asked to first define the task and task filling instructions. After that, select the type of task (result) to display a preview of the selected task type. Finally, you can choose the optionality of the task and whether it is a material or not. Click "Add". The task is created last in the task list. You can edit the task information (e.g., order) by clicking three-point icon.

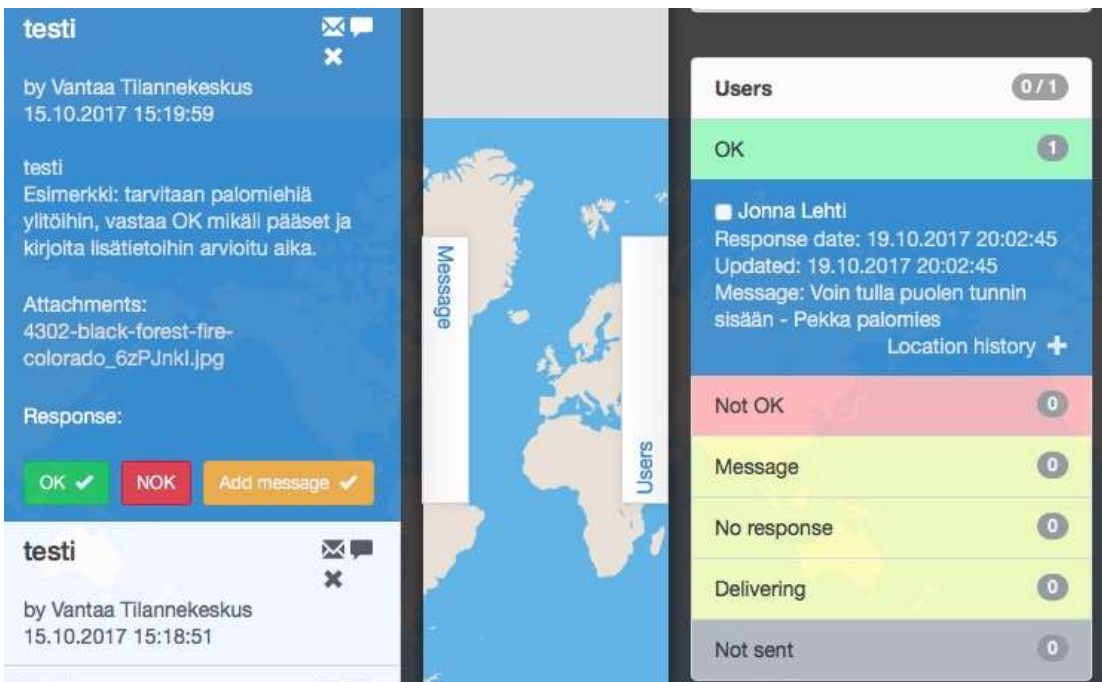
Categories contain tasks and there are two types: **top-level categories** and **sub-categories** in the task list. The categories allow you to split a task list into logical entities and create a navigation. You can add a top-level category above the task list, below the categories with the "Add category" button. You can create either a blank category then add tasks, or create a category from a category template. Category templates are like building blocks to quickly create versatile task lists.



You can add a subcategory from the same place as an individual task: click the three points at the top right of the task list and select "Add" and "Add Subcategory".

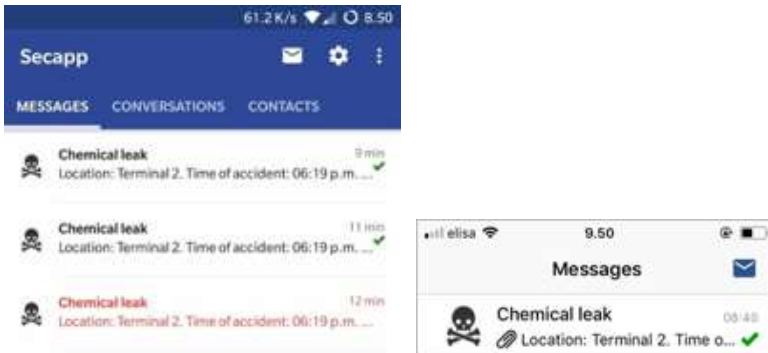
### Monitoring Responses on web browser

You can track the recipient's responses of messages from the right side of the web browser. You can quickly see how responders have responded, as well as if the message is on the way or the transmission fails. This situation is updated as recipients acknowledge your message. Click on a single user to see exact response times, and as well additional messages from him/her. You can view the location history of a user if he/she has allowed the use of the location in their settings.

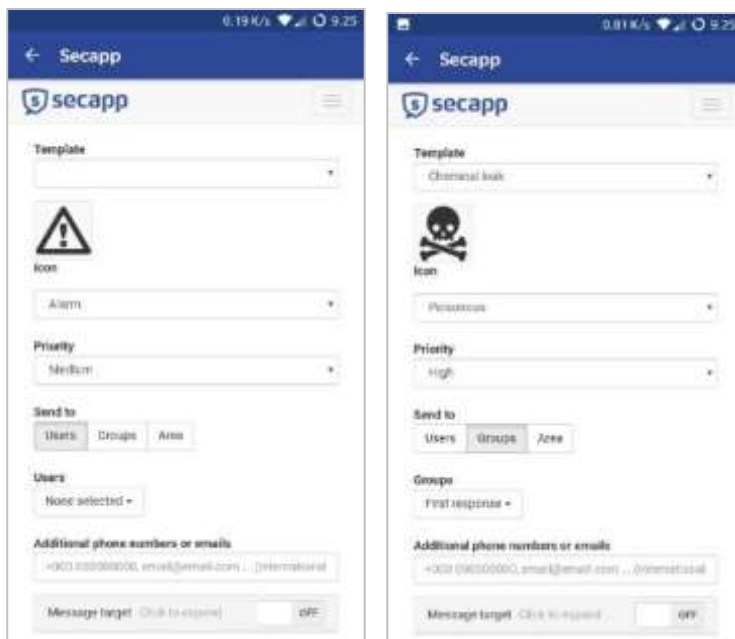


## Sending a message from a mobile app

You can easily send a Secapp message via the mobile application Messages view. If you have the privileges to send Secapp messages, the envelope icon will be displayed at the top right of the Messages view.



Click the envelope to access the message view. Select the template you want to use from the drop-down list in the top menu. The system automatically fills out the fields for sending a message.



Scroll down to the title field. Make sure the title and description fields and the instructions are correct.

From **additional settings** you can set a timed message to be sent and target messages by receiver's skills or availability. You can also automate your communications according to recipient responses to alarms.

**Timed:** Sending a message can be automated to timing dependent and automating repetitions. Options are once, daily, weekly, monthly, and yearly. Selecting the repetition frequency will open the possibility to specify when the message is to be sent.

**Reply automation & Escalation:** You can build an automatic message by the type of responses. For example, a follow-up instruction can be sent based of different answers OK / NOK.

*Send message immediately to replier:* You can type a message that the recipient sees immediately after their response (OK/NOK).

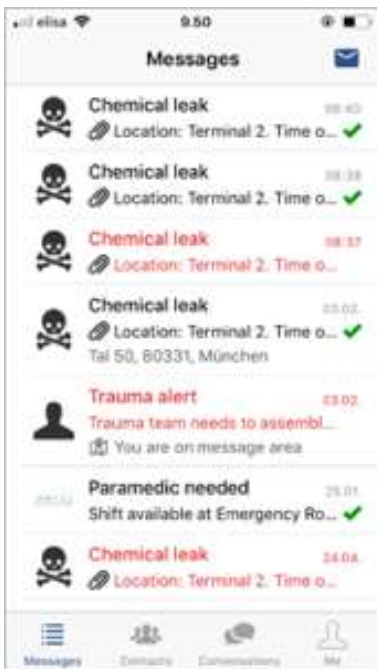
*Send a conditional message to repliers:* select OK/NOK and the desired number of responses when eg. OK responses have been obtained. Then define what you want to say to your OK responders before the condition is met. Click “add message” and send to users who have replied OK. Click “Add”.

*Escalate message:* when the message recipient responds, you can forward a new message to a user, group, or users in certain region.

Scroll down and click “Send”. When the message is successfully sent, "Message sent! View Post" text will appear. Click the arrow on the top left to return to the messaging view.



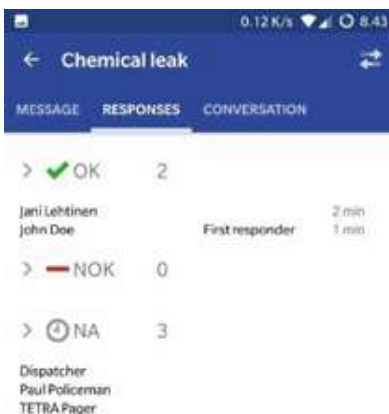
In the “Message” view you will see all the Secapp messages you have received, and you can open an individual message by clicking it. Next to the message list, you can see Contacts and Conversations tabs. The Conversations tab allows you to access the ongoing conversations directly, and the Contacts tab will show you the most important contact information, where you can start a private conversation.



## Monitoring Responses on mobile app

Click a Secapp message to enter the responses view. The responses tab shows how other people in the message have reacted to the situation. You can see the response of the person (OK / NOK) or if he/she has not yet reacted (clock icon and NA).

If the user has written additional information on their response it will be shown after his/her name. You can also see the user's skills if they're listed on their information.



## Administrator functions

### Company settings and information

In order to edit the basic information of your organization, click **INFO** in the top bar. Fill out the basic information fields and click **Save**.

**Registration:** User registration settings can be changed in the drop-down menu. The user can register themselves to the system here under defined conditions.

*Pending activation* means that the user registers themselves and the administrator must approve the registration before user can access to the system.

*Only staff* means that only staff members can register new users.

*Free* means that anyone can freely register to a company's or organization's service.

**List company publicly in registration** defines whether the company is listed on the [www.secapp.fi](http://www.secapp.fi) registration page. By leaving this box blank, a business cannot be found in a public listing.

**Location update interval:** you can select how often the user's location information is sent to the system. Choose the value that matches your organization's needs. Note that the shorter interval means more accurate positioning, but at the same time the phone's higher power consumption.

**SMS warning limit:** the use of text messages is charged separately. In order to avoid unexpected costs, you can set an alarm limit for the number of sent text messages. The system warns you when you are sending a large number of text messages. There are no extra costs for the use of other messaging channels.

**Show mobile map to:** define how your organization can utilize the map view on mobile.

**Editing user skills:** can be limited so that no one can edit them, only staff-level users can edit, or anyone can edit user's skills.

**Editing panic button templates:** can be limited so that no one can edit them, only staff-level users can edit, or anyone can edit panic button templates.

**Enable userlist group property filter:** can be turned on/off and to select the default groups for which the filtering can be done.

**Enable panic buttons:** activate for use on smartphones if required by the organization and users. For example, on for security and off for event marketing.

**Allow SOS messages:** in older phones is the same as a panic button on smartphones. By sending SOS as a text message, the location and the request for help are forwarded.



**Enable dead man's switches:** selected for use in, for example, personal security in situations where user operates alone and is at risk of being unable to alert itself. The user determines himself a time by which the alarm will be canceled.

## Adding and managing users

You can add users on web browser by clicking "Users" and "Add". Fill in the basic information (name, phone number, email).

**Username:** You may use user's device phone number as their username.

**Password:** define a password for the user.

**Retype password:** type password again to confirm the password.

The system can automatically send the username and password to the new user by e-mail or SMS.

**Send password to user:** Click the button to YES-position and choose to send the password by e-mail or as a text message.

The image shows a web form for adding a user. The fields are as follows:

- First name:** Input field with placeholder text "First name".
- Last name:** Input field with placeholder text "Last name".
- Phone number:** Input field with a country code dropdown set to "+41" and a placeholder "041 2345678".
- E-mail:** Input field with placeholder text "E-mail address".
- Username:** A greyed-out field with the text "User phone number is used as a default username".
- Password:** A greyed-out field with the text "Password will be autogenerated".
- Retype password:** A greyed-out field with the text "Retype password".
- Send password to user:** A section containing a radio button labeled "NO", the text "Send password to user", and a dropdown menu currently set to "Email".

At the bottom of the form, there is an "Advanced settings" bar with a "Click to expand" link. Below this bar are two buttons: a blue "Add user" button and a white "Add user and send message" button.

**Advanced settings:** bar opens a selection of settings that you can customize as needed for adding users or edit their information later.

**Language:** Language Selection to determine the user's default language. The setting also changes the interface language: Finnish / English. The default language also has an effect on sending the messages.

**Default view:** specifies whether to open a map or inbox-view as a main view after logging in.

**Availability:** select the basic setting of whether to display the user as an offline or not. This is an important setting because messages can be targeted according to user's presence information.

**Active:** is a basic user level. This user can only receive and respond to messages. The user can also be set to inactive so that the profile remains in storage, but the user cannot log in to the service, for example, during the leave of absence, and no messages are sent to him before the status is changed back to active.

**Staff:** opens a full management view for your organization. User can manage user data, group information, templates, and organizational settings. The staff-level domains will also be able to send messages.

**Can send messages:** can be given to the basic user, allowing the user to send messages but not manage the organization's information.

**Additional details:** you can enter additional information about that user.

**Location settings:** The ON / OFF switch determines whether a user's location is allowed to be used to make a location-based situation picture and messages.

If the location is **allowed**, the menu also allows you to make the following choices for the visibility of the user's location:

- **Allow location history:** select to show the location history or just the last known location of a user.
- **Specify how long will your location be visible after specific responses:** How many hours the user's location will be displayed after he or she responds to the message either OK, NOK or with an open message.
- **Visibility settings:** you can specify when (time / days) allow Secapp to save user location information and who has the right to view them. Visibility can be determined by the accuracy of a single user or group level.

**Favorite locations:** You can specify fixed locations that you want to receive regionally targeted messages. For example, you can specify the home or workplace to your favorite locations, so you can get messages targeted on the area, even if you aren't at the area at that moment. Radius determines how wide area you receive messages from.

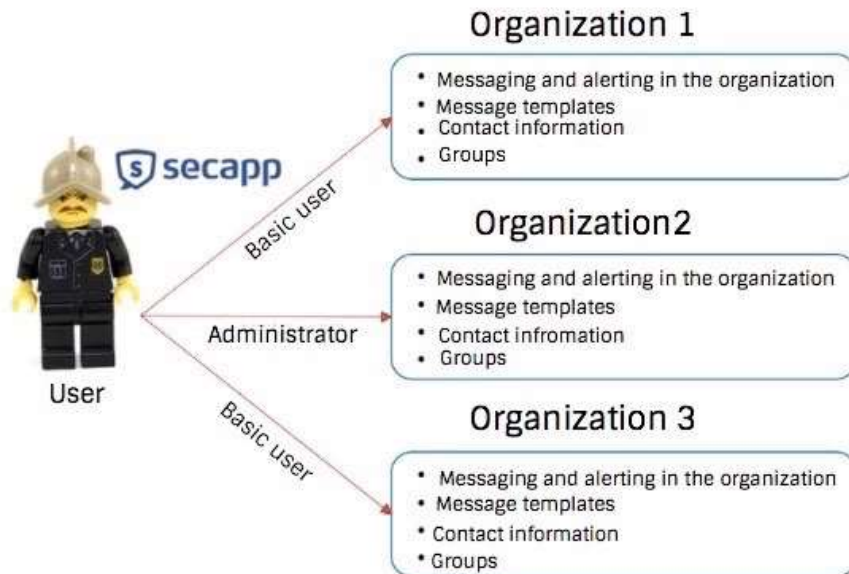
**Skills:** you can add skills to users that are relevant to the organization. In the future, the messages can be targeted according to the desired skills profiles. Organizational skill profiles are created from the "INFO" tab. The period of validity can be added if there is a temporary qualification and/or authorization for example for a temporary security guard.

From the "INFO" page you can also define who has the right to edit the skills information.

## Joint organizations

Both basic users and the administrators can be added to a joint organization by the responsible administrator.

A single Secapp user can belong to more than one organization and have different roles, for example, act as an administrator in one, and as a basic user in another.



People and groups can be added and created without restriction in the context of permissions.

New users can be created in the following ways to the organization:

1. Administrators add all the users, which means that free registration is not allowed.
2. Users can self-register their information in to the system under the company/organization, but administrators must accept the users.
3. Allowing completely free registration under the company/organization (ie. the administrator does not need to approve the users separately).

The system also supports the import (and updating) of user data as a mass either by a separate file or directly from another system.

You can edit the user information from the “**Users**” tab and then selecting the user.

**Companies** Demo Pelastus ✕ Demo Fire Department ✕ +

**Groups** Crisis Team ✕ +

**User rights**  Active  Staff

**Additional rights**  Can send messages

**Additional details**

## Adding and managing groups

The use of groups will bring efficiency in your organization's communications.

To create groups, click **GROUPS** and **Add group** from the top bar. Enter the name of the desired group and click **Add**.

[Back](#) » [Add Group](#)

**Name**

**Id**

**Type**

### Users and groups that belong to the group

Users (?) Groups (0)

25 per page

**Name**

To add users to a group, select **GROUPS** -> **GROUPS** -> Wanted Group-> **Add Users**.

Select users and click **add** to insert user to the selected group. The user can be removed from the selected group by selecting the user and clicking **delete**.

Always remember to click **save** the button to save the changes after adding or deleting users.

## Skill profiles

With skill profiles, you will be able to target messages to the right people. It may be useful for the organization to know, for example, those with a security guard card and / or first aid competence.

In the top bar, click **INFO** followed by **Skills** -> **Add/Remove skills** -> **Add**. Add the required number of different skills by completing the Name of the Skill (eg. First Aid) and Description (eg. EA1 / EA2) -> Click **Add** to save.



## Message templates

Message templates create efficiency and speed in communication when sending similar messages repeatedly, or if you need to quickly get directions to recipients.

In the top bar, click **TEMPLATES** and **Add**.

**Priorities** define how messages are transmitted to the recipient's phone, for example when the silent mode is on. You can choose from 3 options:

Low = not easily observed or noticed.

Medium = notifies that the message has arrived.

High = raises the attention of the user as well as possible by high volume ringtones and vibration.

In **Send to** field you can choose to send a message to users, groups or users based on radius (area).

In **Users** field you will be asked to select the users to whom you want to send a message. You can find people by clicking "Search" and typing their name, or you can select all.

In **Group** field you can send a message to an existing group.

In **Area** field you can search for a location of a region based on the coordinates or address. Specify a radius that allows you to restrict recipients, whether they are within the area, leaving the area or entering the area.

In **Additional phone numbers or emails** field you can also add non-established users as recipients. Be sure to include any additional phone number in international format (eg +358 to beginning)

**Language options** allows you to select alternative languages for the message. The transmitted message is depending on by the recipient's default language of choice. For example, if the user's default language is English and the message is created in Finnish and English, Secapp delivers an English message to the recipient.

**Attachments** allows you to attach other documents such as pictures or videos to your post.

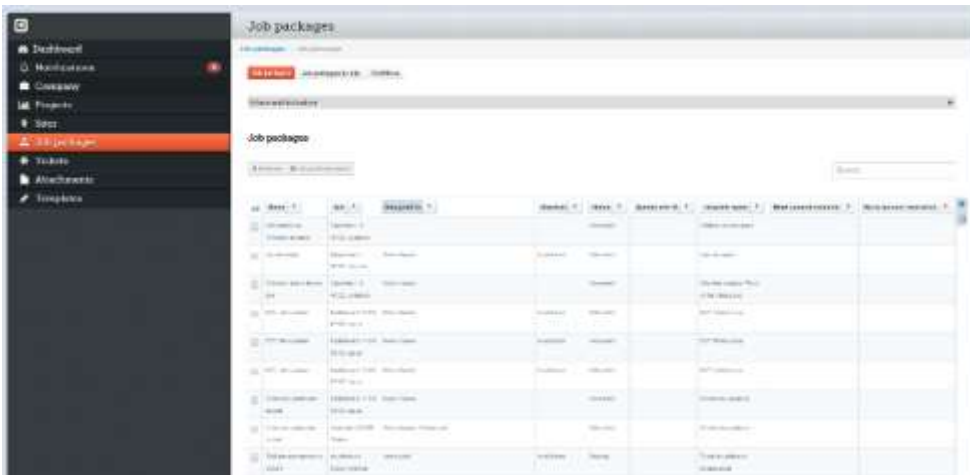


The screenshot displays the configuration options for creating a message in Secapp. At the top is an "Add template" button. Below it is a car icon labeled "icon". A dropdown menu shows "Traffic" selected. The "Priority" dropdown menu shows "Medium" selected. Under "Send to", there are three tabs: "Users", "Groups", and "Area". The "Groups" tab is active, showing a dropdown menu with "(Demo Fire Department) Paramedics" selected. Below this is a text field for "Additional phone numbers or emails" containing "+000 000000000, email@email.com ... (international phone numbers and emails separ". A "Message target" section has a "Click to expand" link and a toggle switch set to "OFF". The "Language options" section shows "Default" selected with a plus sign button. At the bottom, the "Title" field contains "Car accident".

## Creating a report based on the info from tasks

It is possible to create versatile reports based on data input from tasks with Secapp. Open Reporting View by clicking "**Reports**" in the top menu. Depending on your browser settings, Secapp may request permission to open reports in another window.

The Reports view opens in the Job Packages view.



At the far right there is a search box to find the right task list.  
 After finding the right task list, open the task list by clicking its row in the search results. Below you can see a list of tasks filled in a task list, select "**Document generation**" in the menu.



Find the right task list from the list by either manually scrolling or using the browser search function: Ctrl + F and enter the same search term you previously used. After you have found the correct task list, click "**Generate Document**". The browser opens a window that defines the contents of the document being created. You can formulate the appearance, categories, and tasks of the document. The document is created when you click "**Save PDF**" on the bottom of the window. You can also save document templates that will help you build a specifically structured documents in the future.

### Generate document

**Document information:**

Title

Address

Location

Author

Date

Comments

Security classification

Images per row

Select all

- Tasks of the crisis group
  - Sharing responsibilities in the crisis group: Lead, Data Collector,
  - Documentation, Communication
  - What has happened
  - Is anyone hurt
  - How rescue has progressed (are people in or out?)
  - Where are the people gathered?
  - Has the rescue service been alerted?
  - Is the rescue of the plant site?
  - Are people left in production facilities? Check number of the people
  - What happens next
  - What is the next scenario?
  - Messages during the first hour
  - Possible photos of the situation
- Roles of the crisis group
  - Leads the operation
  - Keeps track of the course of events and actions
  - Creates internal communication material
  - Prepares the authority communication material
  - Organizes press conferences / interviews
  - Maintains communication with internal stakeholders

Cancel Save as a template Save PDF

## Statistics

The **Stats** tab lets you quickly see information divided by phone model, users, and sent messages. The data is presented by the numbers in the table. The statistics facilitates the monitoring of the situation of the organization, as well as the use and development of the system.

### Date range

Start	10/5/2018
End	10/5/2018
Get	

### General statistics

SMS	Android	Windows Phone	iOS	Email
0	0	0	0	0

Voice	Voice price	Voice duration
0	0	0:00:00

Messages	Area / Location	Timed	Encrypted
0	0	0	0

### Users

Admin	Staff	Normal	Inactive	Total
1	12	4	1	18

Android Devices	WP Devices	iOS Devices
?	?	?

### Groups

29
----