



USER MANUAL

SUBMISSION DATE

MAY 23, 2022

FREECELL SECURITY BRACELET
UNIQUE AND HOLISTIC
STANDALONE TRACKING SYSTEM

Contents

1. Introduction.....	3
Sanitization and Re-Use.....	7
Collection.....	7
Inspection.....	7
Cleaning.....	7
Enrollment.....	8
Users Log In.....	8
Dashboard Screen.....	10
Device Screen.....	10
Device Screen.....	11
Device Id.....	11
Serial ID.....	11
Enable.....	11
IMEI.....	11
IMSI.....	11
Target.....	11
Target Screen.....	12
Target Screen Fields.....	12
New Target Screen Fields.....	14
Quick Disabling and Deleting an Exist Target.....	16
Configuring A Target.....	17
Editing Geofencing Zones.....	18
Alert Screen.....	22
Violation Alert Icons.....	22
Top Alert View.....	23
Full Alert View.....	23
Alert Windows.....	23
Map Window in The Alert Section.....	24
Events Screen.....	25
Audit Screen.....	26
User Management Screen.....	27

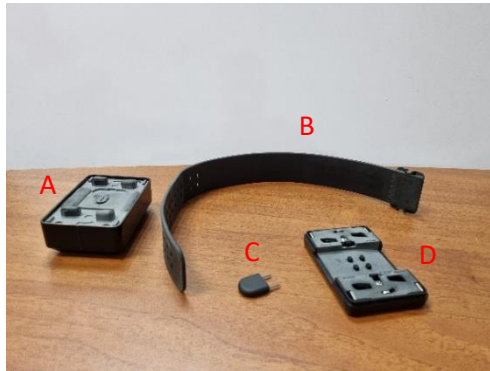
Victim Application	28
Closing the Alarm	29
Proximity Alert.....	31

1. Introduction

This document is intended to be the source reference material for using the version TL01R, with the exception of electronic configuration (including set-up and interaction with the on-line monitoring portal). The emphasis here is upon describing the physical features, charging, correct fitting and removal and the use of the user portal etc.



2. Equipment Description



- A. The rechargeable monitoring device – the main transmitting unit
- B. The strap - to be attached to the ankle of the offender.
- C. The Key to open the device
- D. Top cover - attaches the strap to the main unit

3. Device Fitting and Attaching



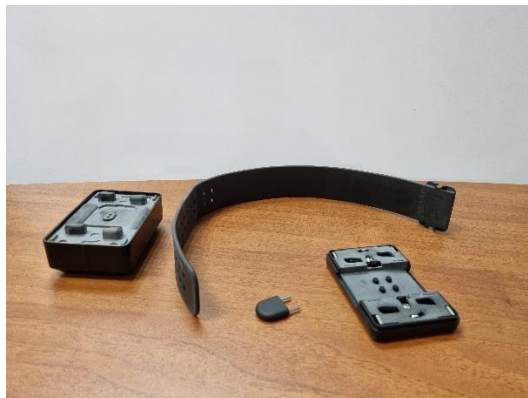
1. Insert the dedicated key into the place designated for it



2. Turn the key in the direction as shown



3. open the case



4. Disassemble the strap from the shell



5. Attach the strap in the direction as indicated on the device



6. Adjust the strap according to the size of the offender's foot



7. Fix the head of the strap according to the layout of the shell so it will be firmly gripped



8. Attach the device to a click sound

9. The device is ready for work

Sanitization and Re-Use

The TL01R monitoring device will be removed by cutting the one-time use strap from the offender leg

Collection

Place the TL01R and strap into a clean plastic bag and return them to the vehicle for inspection and cleaning.

Inspection

The TL01R monitoring device should be inspected for signs of damage, units with damage should be dealt with in accordance with local protocols. Damage includes any significant surface marking which may be indicative of the unit being exposed to high impacts or tampering. Special care should be taken to ensure the following areas are inspected;

- Any seam between plastic casings, damage here may indicate the sealing surfaces of the unit are damaged.
- The inside surfaces of the strap acceptance area. The unit should be returned for testing if there is any sign of wear in this area.

Cleaning

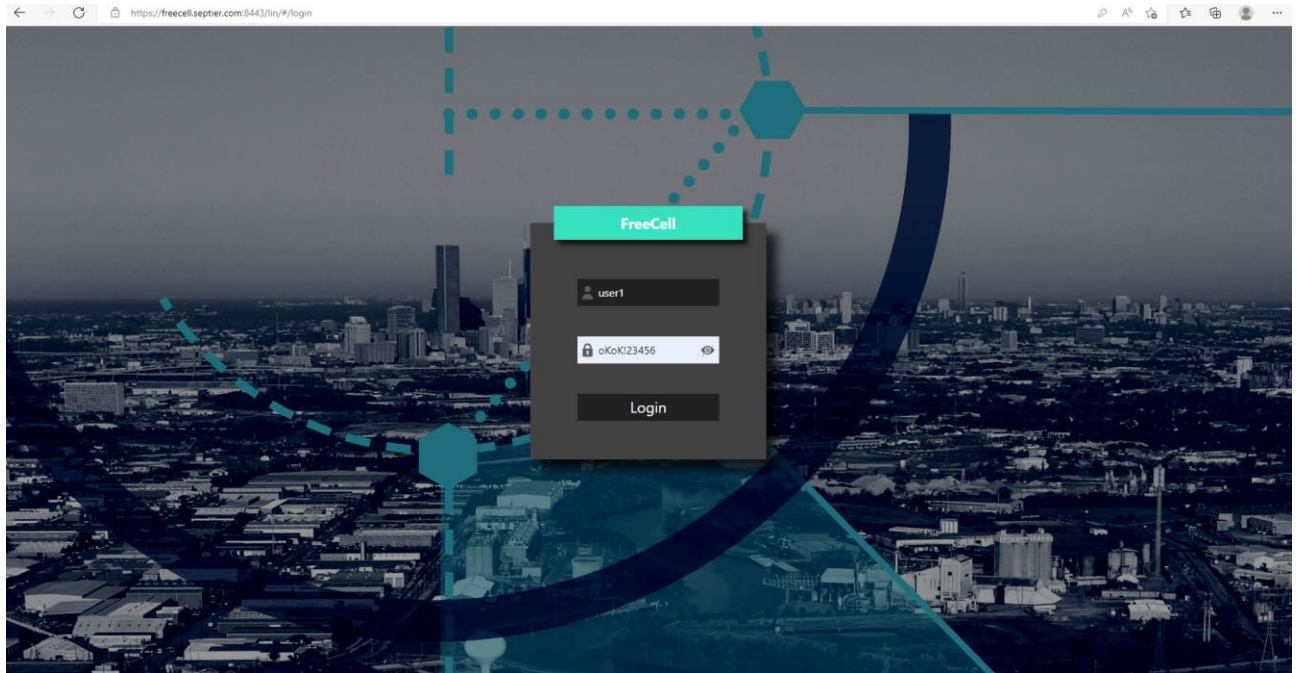
If there is any heavy soiling or biological matter on the unit that is unlikely to be easily removed by a sanitizing wipe, then the unit should be cleaned thoroughly in line with local protocol.

To sanitize a TL01R in the field the following process should be followed;

- Wear gloves.
- Using the removal tool, release the TL01R from the Strap and remove the locking plates.
- Wrap the unit in an approved sanitizing wipe.
- Rub the unit vigorously with the wipe ensuring all surfaces receive a good covering of alcohol.
- Wrap the unit in a new wipe and place in a sealed plastic bag for at least one minute.
- Remove the unit from the bag, dispose of the wipe and allow the unit to dry in a well-ventilated area.

Enrollment

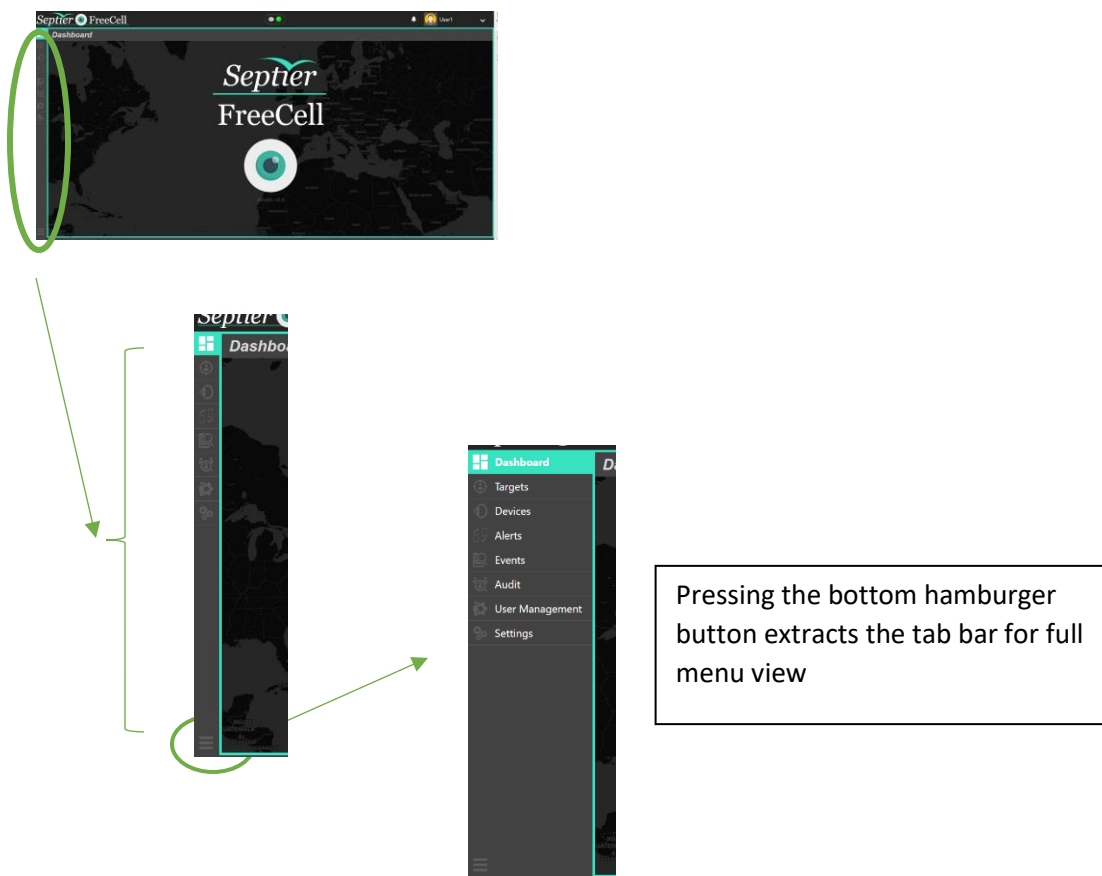
Users Log In



General View

The FreeCell monitoring is an easy intuitive tab control view system

You can switch between the different pages by pressing the tabs at the left side of the screen

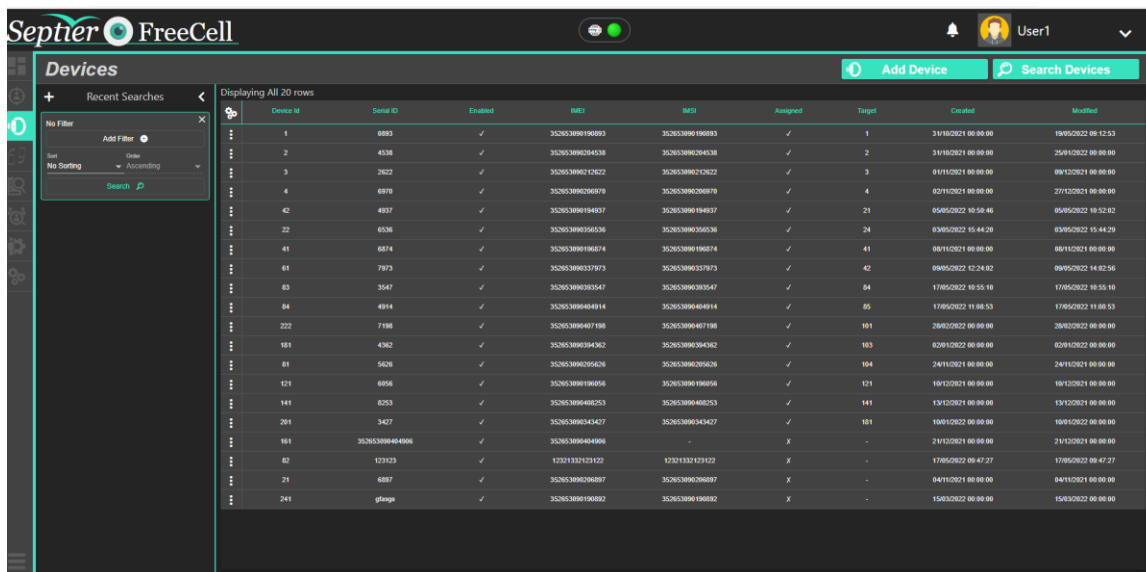


Dashboard Screen

The Dashboard shows the entry screen to the system and the current version



Device Screen



Device ID	Serial ID	Enabled	IMEI	Assigned	Target	Created	Modified
1	0883	✓	352653090190893	✓	1	3/18/2021 00:00:00	18/05/2022 00:12:53
2	4538	✓	352653090204538	✓	2	3/18/2021 00:00:00	25/9/2022 00:00:00
3	2622	✓	352653090212622	✓	3	8/11/2021 00:00:00	09/12/2021 00:00:00
4	6970	✓	352653090206970	✓	4	8/11/2021 00:00:00	27/12/2021 00:00:00
42	4937	✓	352653090194937	✓	21	05/05/2022 10:50:46	05/05/2022 10:52:02
22	6536	✓	352653090356536	✓	24	03/05/2022 15:44:20	03/05/2022 15:44:29
41	6874	✓	352653090196874	✓	41	08/11/2021 00:00:00	08/11/2021 00:00:00
61	7873	✓	352653090337873	✓	42	09/05/2022 12:24:02	09/05/2022 14:02:56
83	3547	✓	352653090303547	✓	84	17/05/2022 10:55:10	17/05/2022 10:55:10
84	4914	✓	352653090404914	✓	85	17/05/2022 11:00:53	17/05/2022 11:00:53
222	7190	✓	352653090407190	✓	101	28/02/2022 00:00:00	28/02/2022 00:00:00
181	4362	✓	352653090304362	✓	103	02/01/2022 00:00:00	02/01/2022 00:00:00
81	5626	✓	352653090205626	✓	104	24/11/2021 00:00:00	24/11/2021 00:00:00
121	6956	✓	352653090196956	✓	121	10/12/2021 00:00:00	10/12/2021 00:00:00
141	8253	✓	352653090408253	✓	141	13/12/2021 00:00:00	13/12/2021 00:00:00
201	3427	✓	352653090343427	✓	181	10/01/2022 00:00:00	10/01/2022 00:00:00
181	352653090404906	✓	352653090404906	-	-	21/12/2021 00:00:00	21/12/2021 00:00:00
82	123123	✓	123211331123123	-	-	17/05/2022 08:47:27	17/05/2022 08:47:27
21	6887	✓	352653090206887	-	-	04/11/2021 00:00:00	04/11/2021 00:00:00
241	glrnga	✓	352653090190882	-	-	15/03/2022 00:00:00	15/03/2022 00:00:00

The Device screen shows all the Security Bracelets available for the organization to work with.

Device Screen

	Device Id	Serial ID	Enabled	IMEI	IMSI	Assigned	Target	Created	Modified
...	1	0893	✓	352653090190893	352653090190893	✓	1	31/10/2021 00:00:00	19/05/2022 09:12:53
...	2	4538	✓	352653090204538	352653090204538	✓	2	31/10/2021 00:00:00	25/01/2022 00:00:00
...	3	2622	✓	352653090212622	352653090212622	✓	3	01/11/2021 00:00:00	09/12/2021 00:00:00
...	4	6970	✓	352653090206970	352653090206970	✓	4	02/11/2021 00:00:00	27/12/2021 00:00:00
...	42	4937	✓	352653090194937	352653090194937	✓	21	05/05/2022 10:50:46	05/05/2022 10:52:02
...	22	6536	✓	352653090356536	352653090356536	✓	24	03/05/2022 15:44:20	03/05/2022 15:44:29
...	41	6874	✓	352653090196874	352653090196874	✓	41	08/11/2021 00:00:00	08/11/2021 00:00:00

Device Id

Will be used for the organization to identify the subject

Serial ID

The identification that is on the device label

Enable

Indicates whether the device is active

IMEI

An International Mobile Equipment Identity, is used to uniquely identify the firmware

IMSI

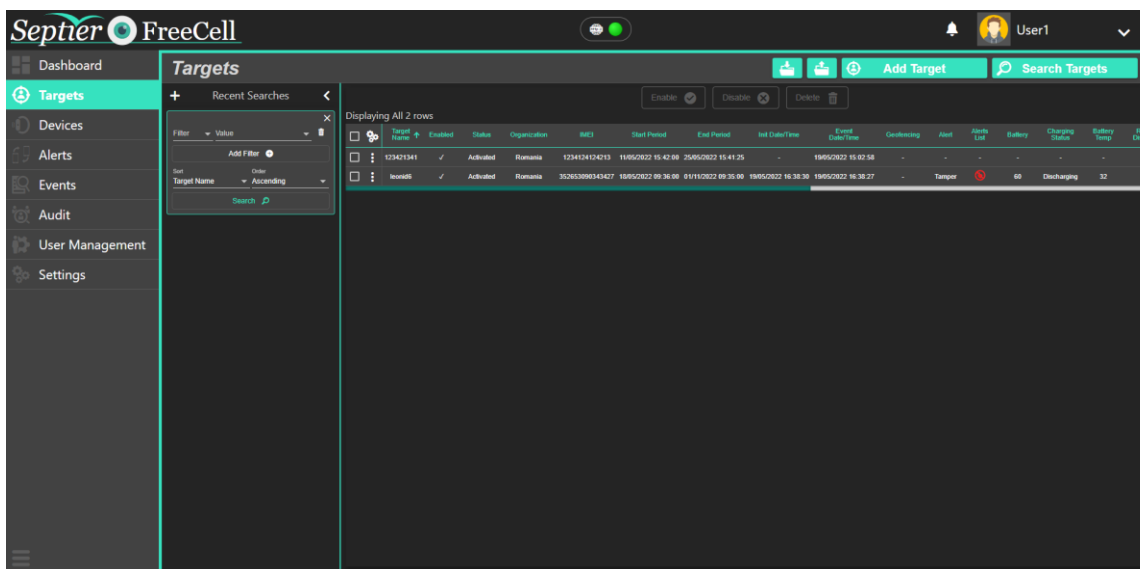
The international mobile subscriber identity – The phone number of the sim that is used in the device

Target

The offender that the device is currently paired to (if any)

Target Screen

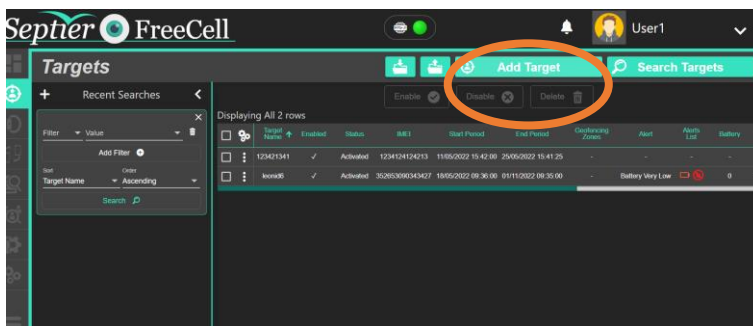
Target screen handles the creation, monitoring and management the subjects that are being monitored, either offenders that use the security bracelet and the victims that use the dedicated phone application.



Target Screen Fields

- Target Name: The Offender/Victim Name as appears at the government files
- Enable: Indicates if the target is activated or disabled. Only enabled targets will be monitored.
- Organization: Indicate the group that is being used.

Adding a New Target



New Target

Target Name *
New Target

☒ Enabled

Target Type
Location

Organization
Romania

Target ID

Address

Target Phone Number

Beacon Mac

Location Parameters

Identifier Type
☒ MSISDN : Value *

☐ Device

Location Interval
Periodic location disabled

Schedule

Until 03/06/2022 12:40:25

Cancel OK

New Target Screen Fields




- Target Name: the name of the offender/victim as you choose (normally the name as appears at the government files)
- Enable: a toggle button for activating and disactivating the device. The target must be enabled in order to monitor its activity.
- Organization: as explained at the device section it Indicates the group that is being used.
- Target Id: the ID number of the subject offender/victim as appears at the government files
- Address: The Address of the subject for monitoring as appears at the government files
- Target phone number: is used for sending SMS notification for important alarms (low battery, and all geo-fencing types), also can be used by the users/police authority to make direct calls to the target (either victim and offender).
- Beacon Mac: the number as appears on the beacon device (a sticker in the back side) so the Septier™ system will pair the security bracelet to the beacon.
for the demo 2 beacon devices will be available.
- MSISDN/Device : for creating a new victim's device in the system choose the MSISDN and insert the phone number of the target (for the demo we will provide 2 phones that have the application already installed – the phone numbers will appear on a sticker in the back)
for creating a new offender, choose the device option and choose for the drop down menu one of the devices that are available (a device that is already in use will be shaded and not clickable).
the device to be chosen would be from the list of devices for the Demo and it will handed by us.
- Location interval: is used for more advanced setting and will not be used for the demo
- Schedule: will allow the user to determine the time intervals for the device to be active. please note that this option is available only when the device is active in general (by toggling the bottom at the top menu as explained in the top of this section). By default, new targets will be active for 2 weeks.
- Mapping Status: indicates that the device is operational activated and monitoring the alerts.










Edit mapping status

After the creation of the new offender device, the user must set the device as operational active










By going into the Edit window (pressing the offender hamburger button))and choosing the Edit Mapping Status











Displaying All 5 rows

Enable  Disable  Delete 

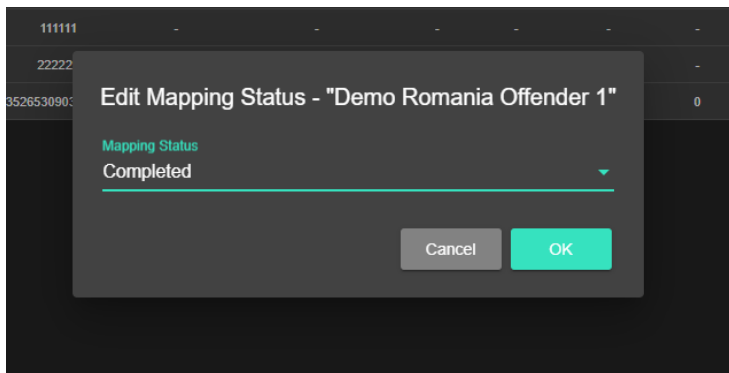
<input type="checkbox"/>		Target Name ↑	Enabled	IMEI	Geofencing Zones	Alert	Alerts List	Battery	Charging Status	Score	Source
<input type="checkbox"/>		Demo Romania Offender 1	✓	352653090356536	2	Geofencing: Leaving home		57	Discharging	100	beacon
<input type="checkbox"/>		Demo Romania Offender 2	✓	352653090337973	1	Geofencing: Leaving home		30	Discharging	70	beacon
<input type="checkbox"/>		Demo Romania Victim 1	✓	111111	-	-	-	-	-	-	gps
<input type="checkbox"/>		Demo Romania Victim 2	✓	222222	-	SOS		-	-	-	gps
<input type="checkbox"/>		leonid6	✓	352653090343427	-	-	-	21	Charging	0	-

Displaying All 5 rows

<input type="checkbox"/>		Target Name ↑	Enabled	IMEI	Geofencing Zones	Alert	Alerts List	Bat
<input type="checkbox"/>		Demo Romania Offender 1	✓	352653090356536	2	Geofencing: Leaving home		5
<input type="checkbox"/>				352653090337973	1	Geofencing: Leaving home		3
<input type="checkbox"/>				111111	-	-	-	-
<input type="checkbox"/>				222222	-	SOS		-
<input type="checkbox"/>				352653090343427	-	-	-	2

-  Target Details
-  Analyze Target
-  Disable Target
-  Edit Target
-  Edit Photo
-  Assign Users
-  Assign Device
-  Edit Mapping Status
-  Edit Geofencing Zones
-  Delete Target

And setting the status as Completed



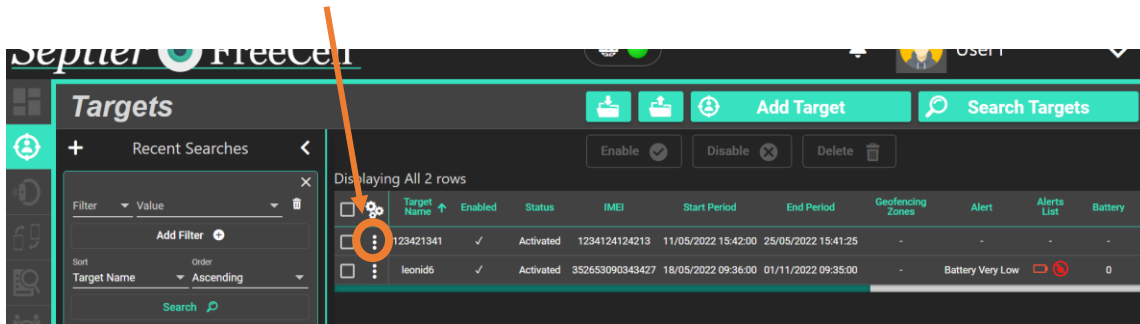
Quick Disabling and Deleting an Exist Target



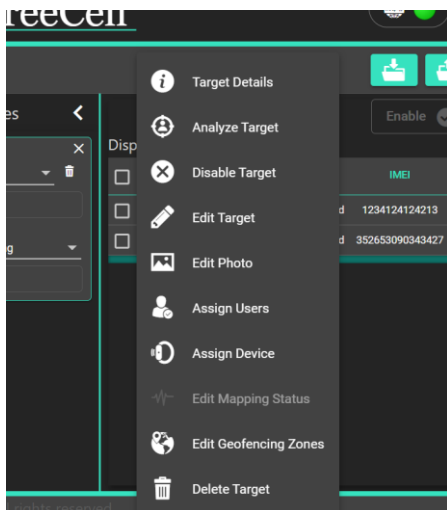
By choosing a target the top option will be available for either enabling/disabling and deleting a target from the system

Configuring A Target

By pressing the target option bottom

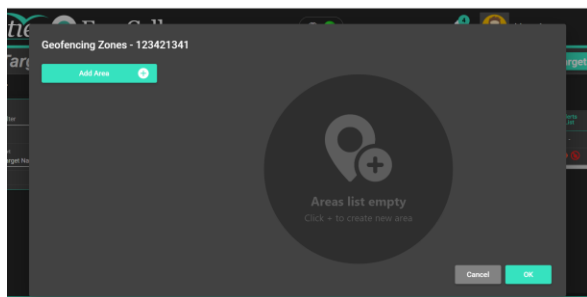


A menu window will be opened

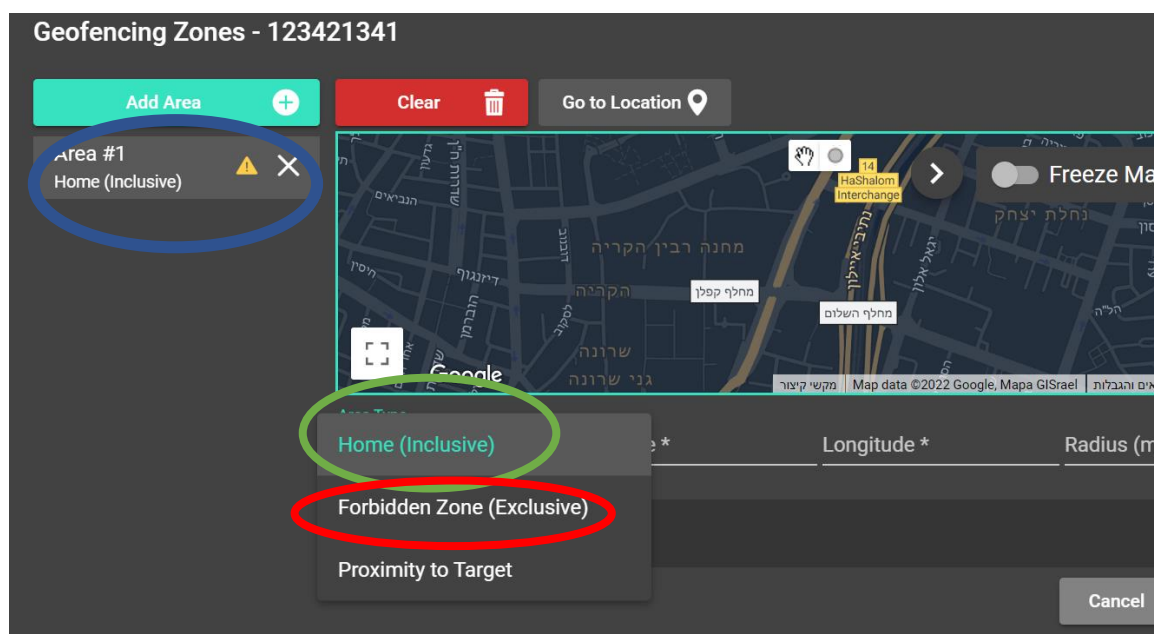


Editing Geofencing Zones

By pressing the option, a new window will pop

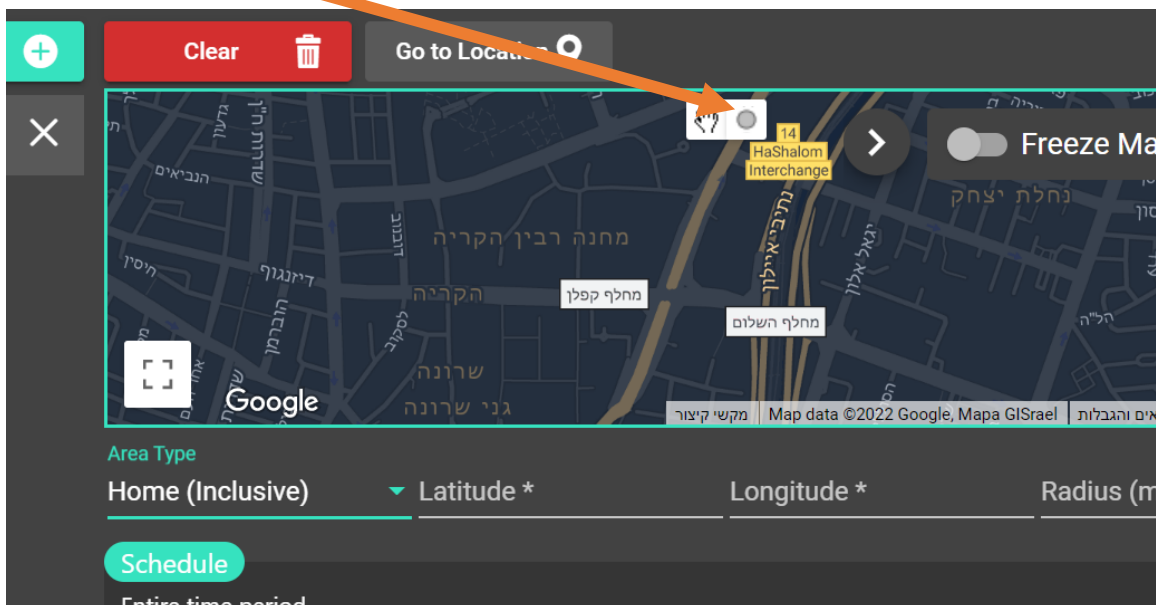


For defining a new geofencing zone, press the Add Area

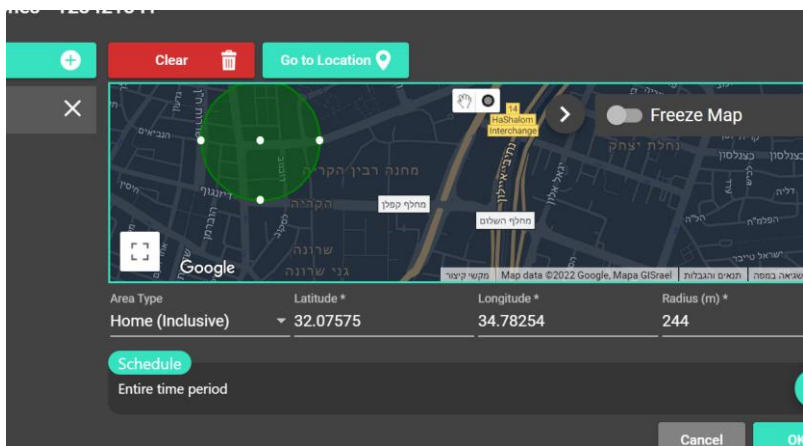


- A new area was added automatically as marked in the blue circle
- For choosing between Inclusive\exclusive\proximity press the left drop down option as marked in the green circle

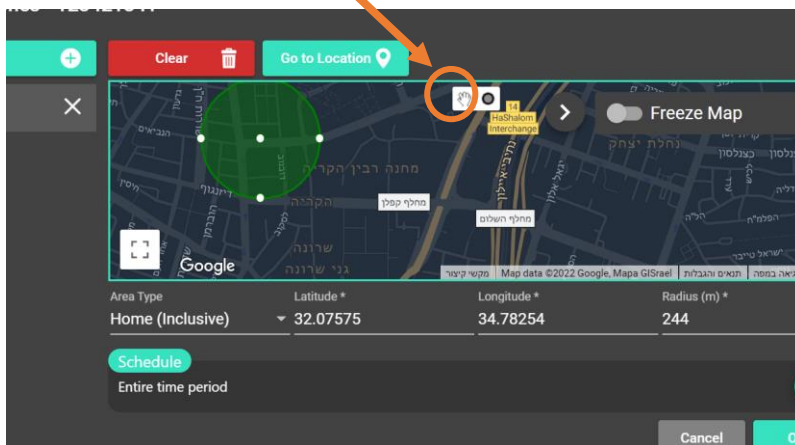
Press the circle option



The Mouse pointer will change to a cross when hovering the map, mark the area you need



By pressing the hand option

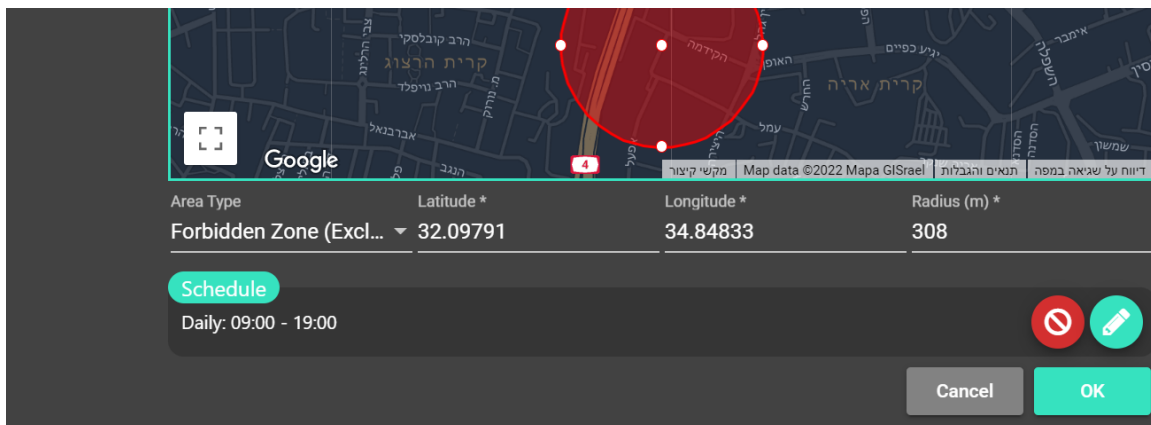


You will be able to move and change the radius of the area needed.

Scheduling the Inclusive / exclusive setting

After setting the inclusive \ exclusive zones the user can set the time intervals for allowing or disallowing the target to move, by pressing the Schedule button and setting the required time.

If no time interval was set by user, the default will be the entire time period.

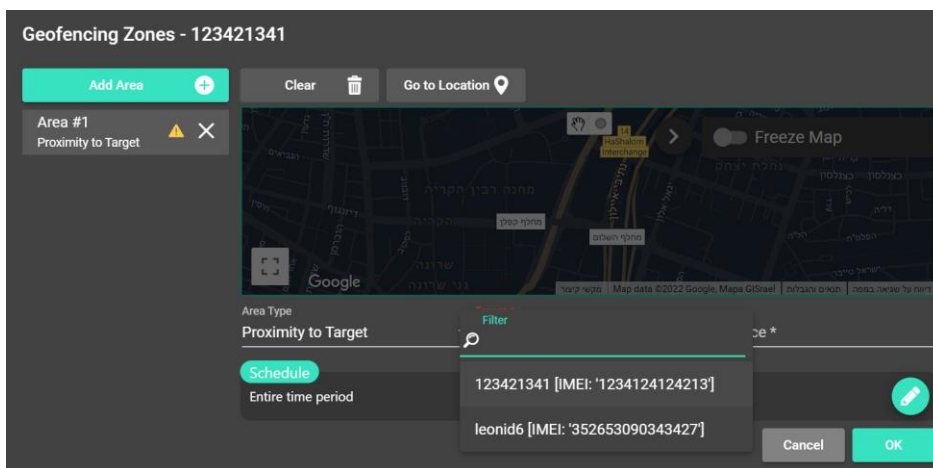


* Note that inclusive area will be marked with green circle and exclusive will be marked with red ones

** The freeze map toggle button will set the view of the map to the chosen place by the user also when switching between other geofencing areas.

Proximity Target

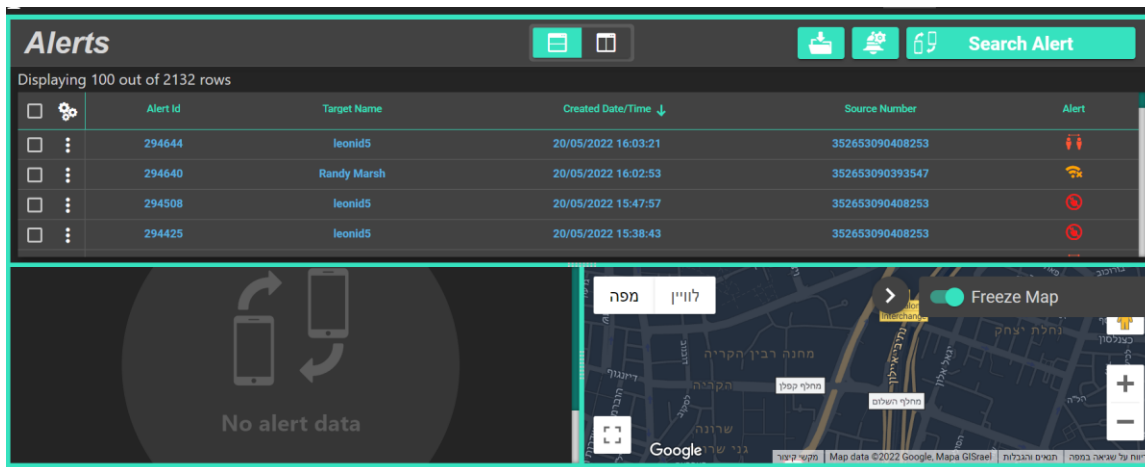
By choosing the proximity option, a drop-down menu of targets will appear and you will be able to choose and search the victim that you want to monitor and alert proximity to.
by pressing "Add Areas" bottom you can add more than one victim for each offender (such as for setting an offender alert to the woman and the family members as well)



The distance for the alert activation is to be set in meters.










Alert Screen

The alert screen will show the alerts caused by violations of the targets as was set by the users



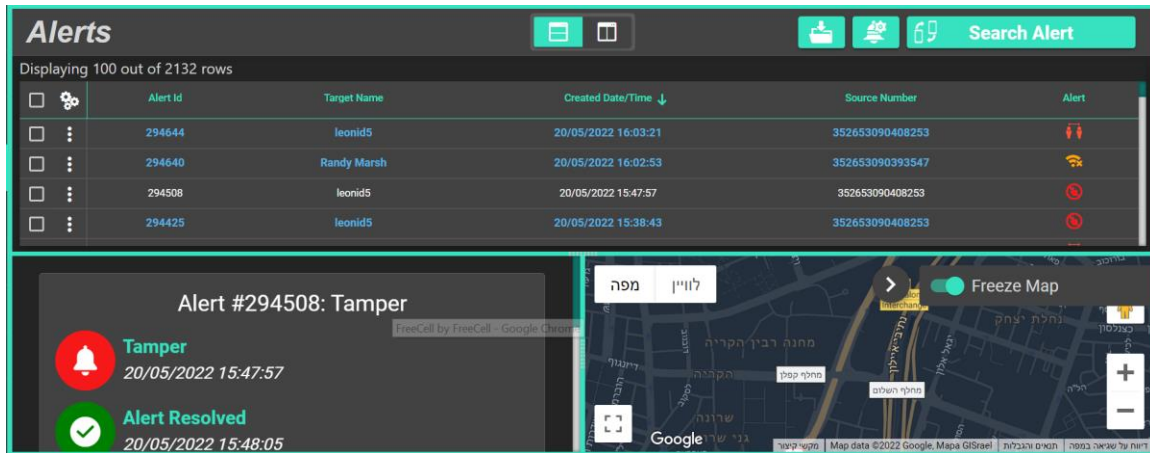
For helping the user quick orientation there are icons for different kind of violations

Violation Alert Icons

-  Device Battery low 20% before empty
-  Device Battery low 5% before empty
-  Tamper
-  proximity
-  Losing communication for 5 minutes
-  Losing communication for 10 minutes
-  Leaving Home
-  Forbidden Zone
-  SOS alert triggered by the victim phone application

Top Alert View

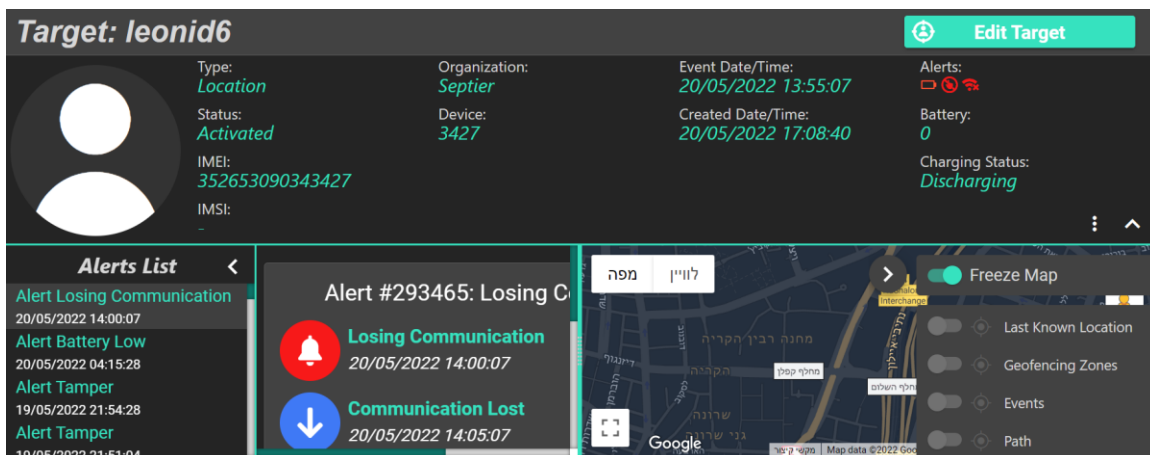
By pressing one click on an alert, a "Top Alert View" will open



- A window with the alert summary of the violation and the alert resolve including text entered by the user.
- A map with the target data will be also shown

Full Alert View

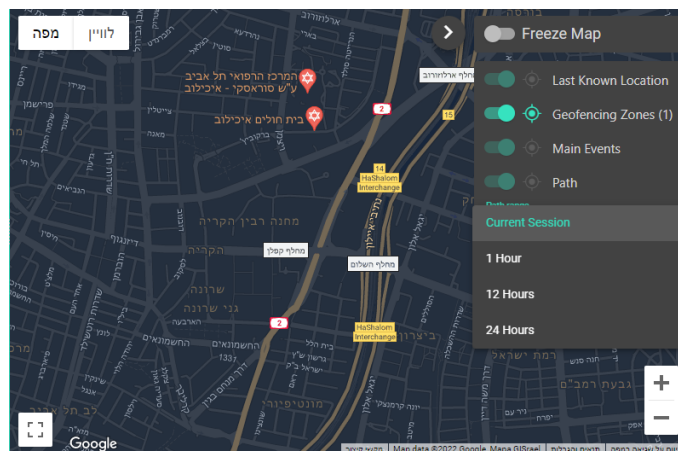
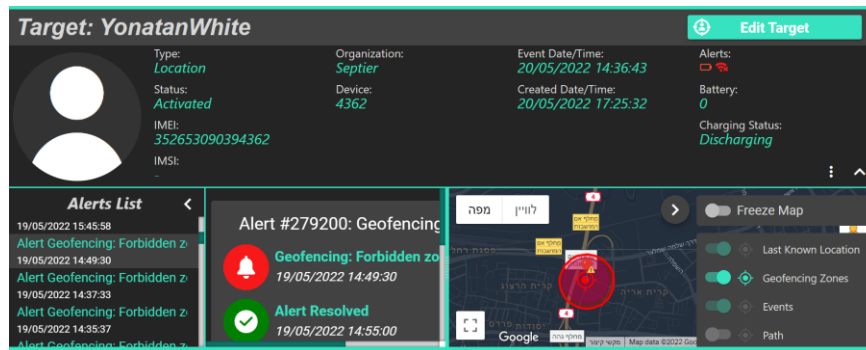
By double clicking an alert a full view windows will be opened



Alert Windows

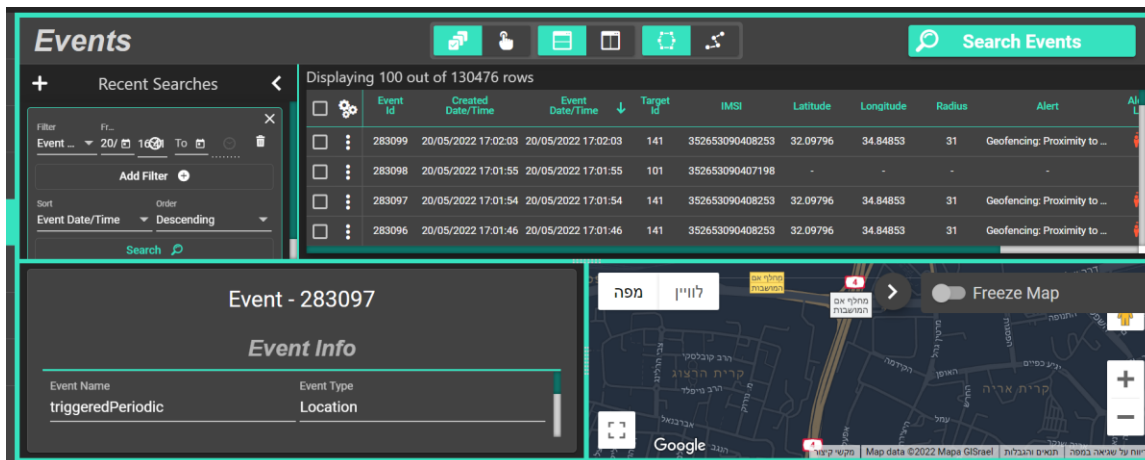
- Top view window will include the summary information of the alert handled
- Alert list window will include a list of all the alerts
- By pressing an alert, the details will be shown in the middle bottom window including the resolve and the text remarks added by the user for the alert

Map Window in The Alert Section



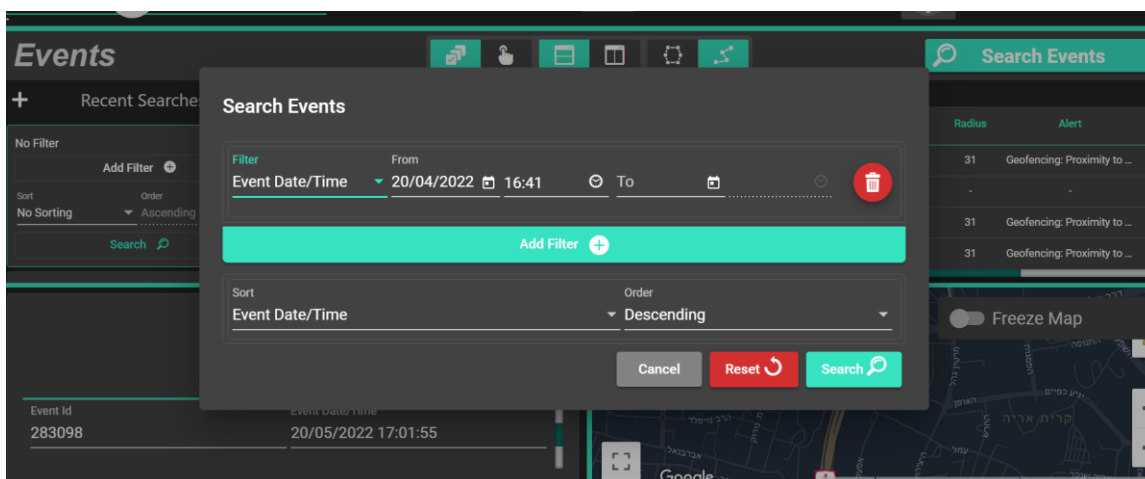
- Last know location – location of the target as was update last by the device
- Geofencing Zones – the settings of the geofencing as where set by the user
- Main Events – main events of the target to be viewed.
- Path – shows the tracked path of the target as where saved by the system, the user can choose between tracked path scopes of 1/12/24 hours to view on the map

Events Screen



Events window will allow the user to watch all the raw data received by the device in an organized way including making searches and filtering information

By pressing the Search Events a new window will pop with more tools for better filtering relevant data

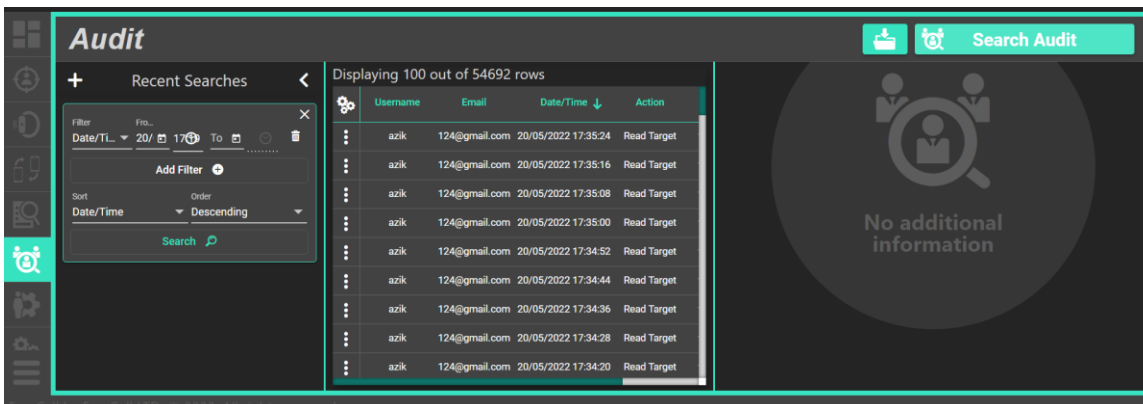


Audit Screen

The audit screen will allow the user to get information about the actions of the different users in the system.

By pressing the Search Audit button, a new window will pop and include more advanced filtering methods and sorting the data

The generated audit can be download as an Excel file by pressing the download button.



Audit

Recent Searches

Filter

From: 20/05/2022 17:00 To: 17:00

Add Filter

Sort: Date/Time Order: Descending

Search

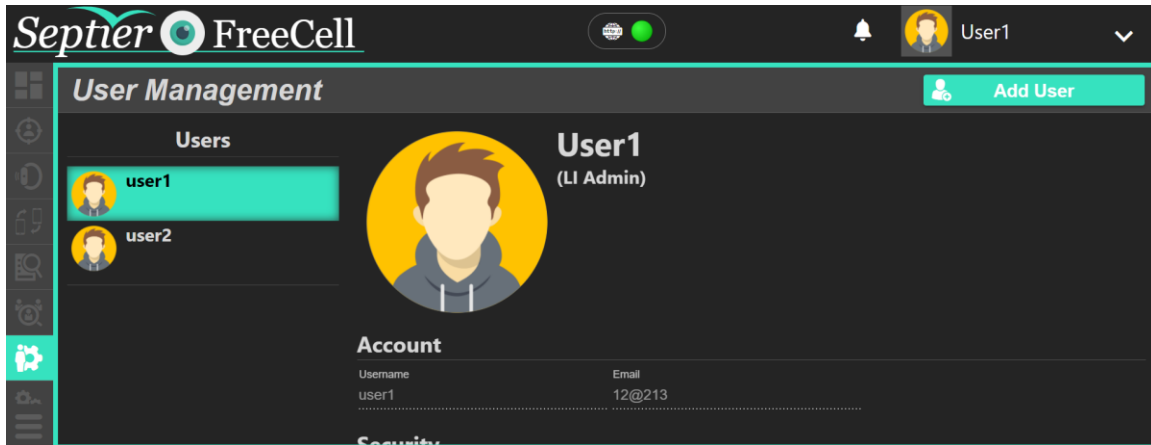
Displaying 100 out of 54692 rows

Username	Email	Date/Time	Action
azik	124@gmail.com	20/05/2022 17:35:24	Read Target
azik	124@gmail.com	20/05/2022 17:35:16	Read Target
azik	124@gmail.com	20/05/2022 17:35:08	Read Target
azik	124@gmail.com	20/05/2022 17:35:00	Read Target
azik	124@gmail.com	20/05/2022 17:34:52	Read Target
azik	124@gmail.com	20/05/2022 17:34:44	Read Target
azik	124@gmail.com	20/05/2022 17:34:36	Read Target
azik	124@gmail.com	20/05/2022 17:34:28	Read Target
azik	124@gmail.com	20/05/2022 17:34:20	Read Target

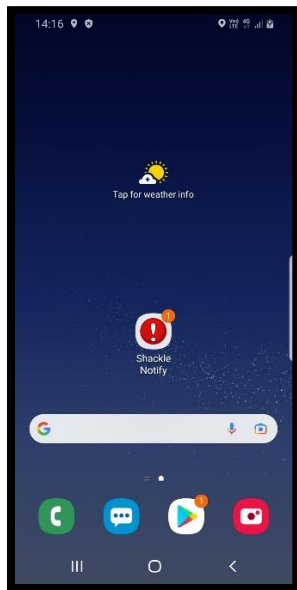
No additional information

User Management Screen

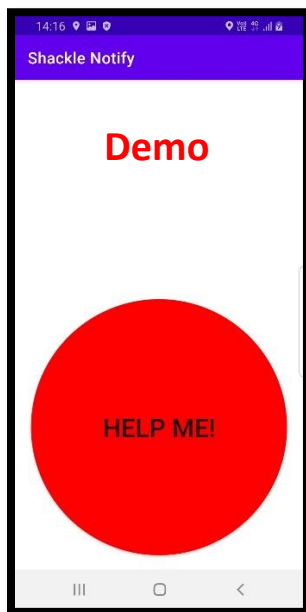
The user management screen allows to create and edit all the different users in the system including setting different kind of users with different permissions



Victim Application



When opening the application, an ongoing cyclical communication between the phone and the server will start for as long and the phone is powered up



when pressing the main button an alert will appear at the monitoring panel.

Displaying All 5 rows

	Target Name	Enabled	RCS	Overhearing Status	Alert	Alerts List	Battery	Charging Status	Screen	Source	Target ID	Address	Target Phone Number	Device Mac
<input type="checkbox"/>	Demo Romania Offender 1	✓	3C76C0860100136	?			68	Charging					977517000015	AC:75:3F:48:79:6F
<input type="checkbox"/>	Demo Romania Offender 2	✓	3C28C0860100137	?			45	Discharging					97262900015	AC:23:3F:48:29:6F
<input type="checkbox"/>	Demo Romania Victim 1	✓	7772777		SOS					GPS				
<input type="checkbox"/>	Demo Romania Victim 2	✓	7772777							GPS				
<input type="checkbox"/>	Victim3	✓	3C76C0860100137								42%			

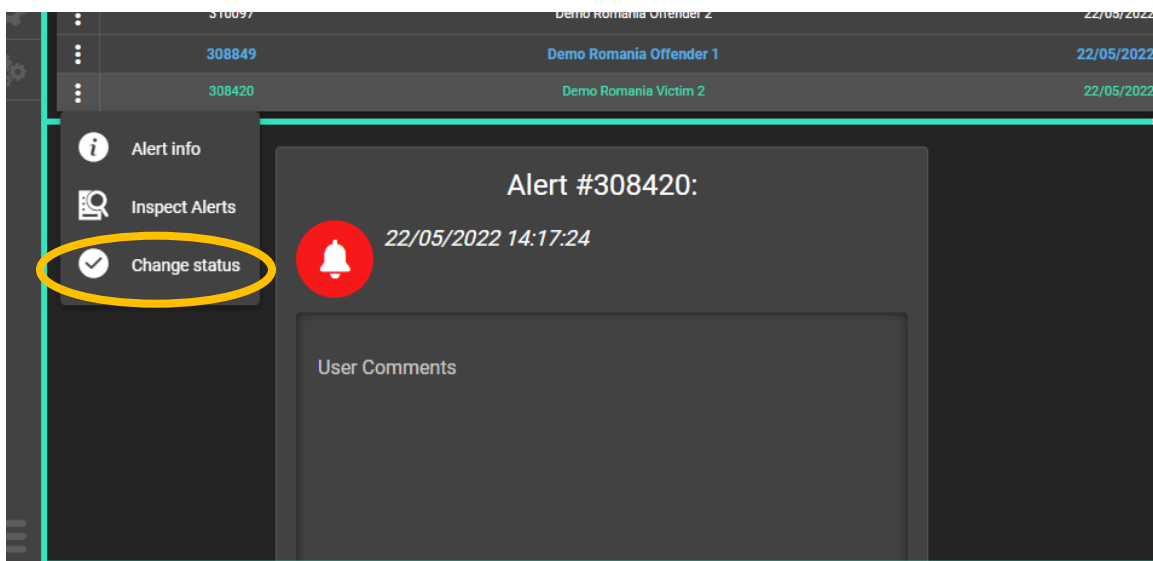


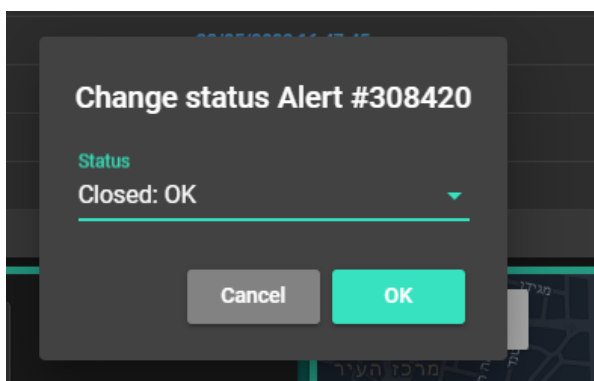
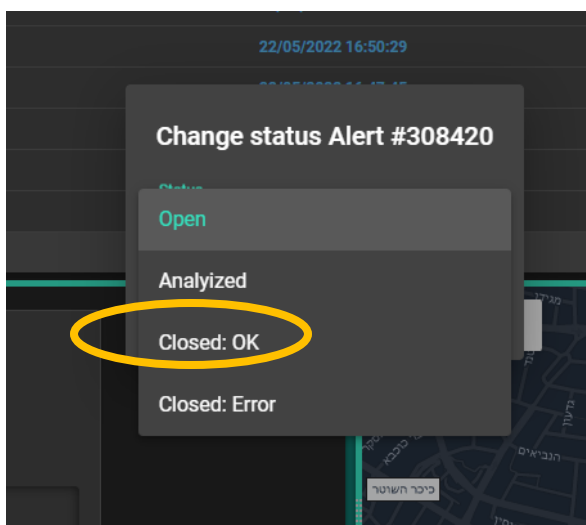
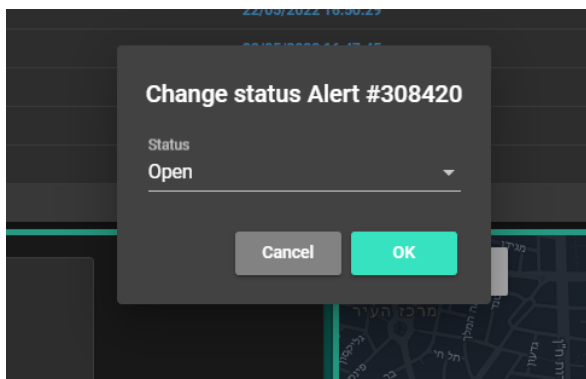
And a notification at the application for sending the SOS will be shown



Closing the Alarm

To set the alarm off, the user will go into the edit window of the alarm by pressing the “hamburger button” and choose the change status






Proximity Alert

The alert will set on when the offender will pass the virtual fence (the distance) as was set by the user.

The alert will include the followings:

- Alarm at the user monitor interface 
- A message that will appear at the victim phone



FCC Warning

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

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Specific Absorption Rate (SAR) information:

This Electronic bracelet meets the government's requirements for exposure to radio waves. The guidelines are based on standards that were developed by independent scientific organizations through periodic and thorough evaluation of scientific studies. The standards include a substantial safety margin designed to assure the safety of all persons regardless of age or health.

FCC RF Exposure Information and Statement

The SAR limit of USA (FCC) is 1.6 W/kg averaged over one gram of tissue. Device types: smart phone (FCC ID: 2A8J9-ADS1M1) has also been tested against this SAR limit. The highest SAR value reported under this standard during product certification for use worn on the body is 0.217W/kg. This device was tested for typical body-worn operations with the back of the handset kept 0mm from the body. To maintain compliance with FCC RF exposure requirements, use accessories that maintain a 0mm separation distance between the user's body and the back of the handset. The use of belt clips, holsters and similar accessories should not contain metallic components in its assembly. The use of accessories that do not satisfy these requirements may not comply with FCC RF exposure requirements, and should be avoided.

Body-worn Operation

This device was tested for typical body-worn operations. To comply with RF exposure requirements, a minimum separation distance of 0mm must be maintained between the user's body and the handset, including the antenna. Third-party belt-clips, holsters, and similar accessories used by this device should not contain any metallic components. Body-worn accessories that do not meet these requirements may not comply with RF exposure requirements and should be avoided. Use only the supplied or an approved antenna.