



WEB-monitoring system

v.1.5

Administrator Guide

monitor.fidtrace.com

Disclaimers

Copyright © 2011 Marton Networks LLC

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate, but are presented without express or implied warranty. Users must take full responsibility for the applications of any products specified in this document.

Marton Networks disclaims all warranties with regard to this software, including all implied warranties of merchantability and fitness. In no event shall Marton Networks and its contributors be liable for any special, indirect, or consequential damages or any damages whatsoever resulting from loss of use, data, or profits, whether in an action of Contract, negligence, or other tortious action, arising out of or in connection with the use or performance of this software.

The information in this document is proprietary to Marton Networks LLC.

Trademarks

FidTrace is trademark of Marton Networks. All other trademarks are the property of their respective owners. Mention of third-party products is for information purposes only and constitutes neither an endorsement nor a recommendation. Marton Networks assumes no responsibility with regard to the performance or use of these products.

Statement of Conditions

Marton Networks is constantly improving internal design, functionality and reliability, and therefore reserves the rights to make changes to the products described in this document without notice. Marton Networks does not assume any liability that may occur due to the use or application of the product and services described herein.

Table of Content

Introduction	4
A Tree	6
User settings and Authentication	8
Managing OrgUnits	10
Managing Objects	13
Sensors & Events	14
Managing Devices	15
Managing Sensors	18
Sensor Events	20
Logical & Continuous Sensors	21
Setting Virtual Sensors	22
Adding & Checking Devices & Sensors	23
Management of Report Templates.....	24
Transactions	26
Appendix 1 - Object & Hardware Events.....	27
Appendix 2 - Data Field list in Statistical reports	29

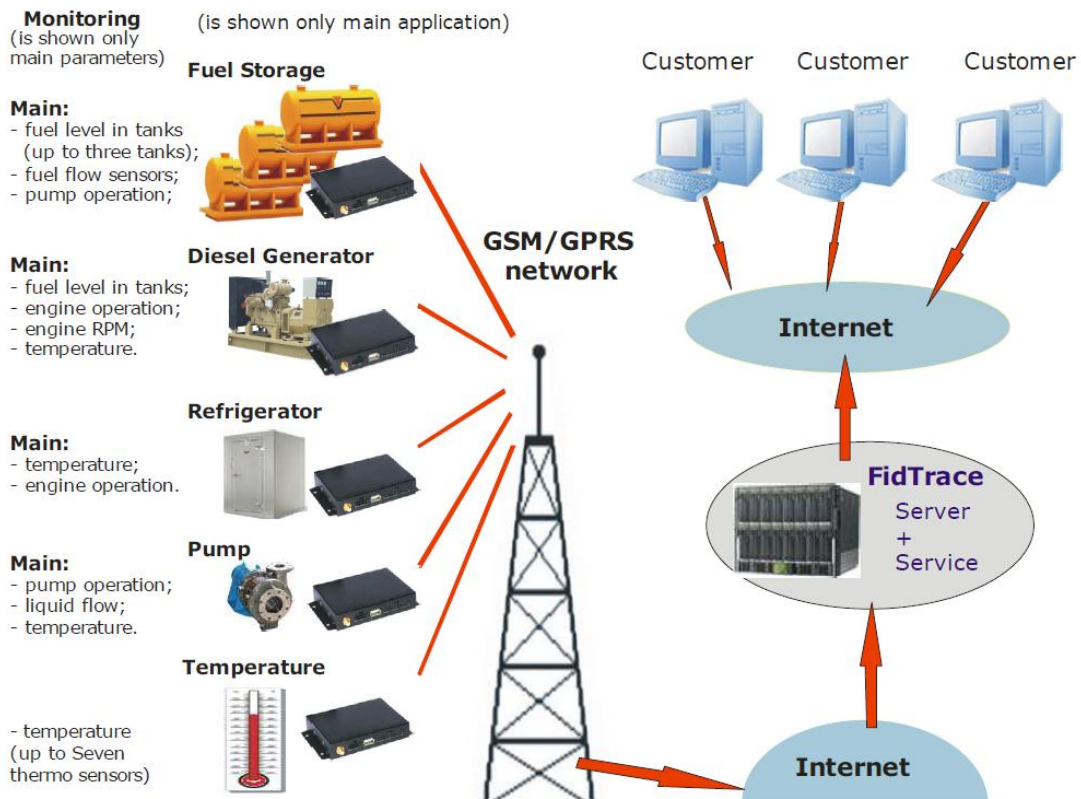
Introduction

FidTrace is server-based software for collecting and monitoring data related to objects and sensors. Devices with sensors and mobile connection to the Internet send data to the server that collects and monitors received data, generate alerts and reports.

This document is a short version of FidTrace administrator guide, to help users to understand FidTrace settings and customization features, how to connect GuardMagic devices to FidTrace server and configure objects.

Another document – FidTrace User Guide describes how to use FidTrace for monitoring. It is highly recommended to read the User Guide prior to the Administrator guide, and to investigate user (Demo) login in monitor.fidtrace.com prior performing administrative actions.

GuardMagic Hardware manual has important information related to connection of sensors and device communication with FidTrace. We assume that the sensors are already connected to the device, calibrated if necessary and the devices were tested in stand-alone mode of operation.



The original concept of the FidTrace monitoring system allows user to define custom features of objects monitored via **Sensors** and object-associated **Events** that provide all object features monitoring in most user-friendly form.

FidTrace statistical reports provide highly consolidated data. Only if necessary the user may “drill-down” the reports and get more detailed data from the inside of the report.

Recommended WorkStation (desktop or laptop) requirements

Pentium P4 Dual, Core2Duo or i3-i7 CPU

At least 2 Gb RAM

At least 3 Gb free hard disk space

At least 128 Mb graphics card

At least 1280x1024 resolution, 15- or 19-inch display

Any standard Internet browser – IE, Firefox (preferred), Chrome, Opera, Safari.

A Tree

Only authorized operators may access information stored in FidTrace, using a standard web-browser. Following roles are defined by default with different access rights – **User, Manager & Administrator**.

The tree in left part of FidTrace screen is a hierarchical structure that shows all objects, sensors, devices and users that the operator has been granted access to (and has rights to change). The checkboxes to the left of each object allow users to monitor only selected sensors and objects.

The screenshot displays the FidTrace Monitor web interface. On the left is a hierarchical tree structure with expandable nodes and checkboxes. The main area shows a 'Statistics Rep.' for the period 30.04.11 00:00 - 03.05.11 23:59. It includes a table with columns for Sensor, Event type, and dates (April, May, May Total). Below this is an 'Alerts' section with a table listing events with columns for DateTime, Path, Object, Device, Sensor, Event/Alert, S/E, and Severity.

Sensor	Event type	April	May	May Total
Abnormal down		2	1	3
Abnormal up		1	2	3
Critical down		2	1	3
Critical up		1	2	3
Down		1	4	5
Level high		1	1	2
Level low		1	1	2
Level very high		1	2	3
Level very low		1	1	2
Up		1	3	4
Diesel Temper. Average 08:42:00 05:40:48 01:37:00 04:31:09				
Diesel Temper. Count 8 20 8 28				
Diesel Temper. Max 33:12:00 59:56:00 11:56:00 59:56:00				
Diesel Temper. Min 00:04:00 00:04:00 00:04:00 00:04:00				
Down		2	1	3
Level high		2	1	3
Level low		1	1	2
Level very high		2	1	3
Level very low		1	1	2
Up		1	1	2

DateTime [dd/mm/yy]	Path	Object	Device	Sensor	Event/Alert	S/E	Severity
01.07.11 20:19:00	Demo/Demo Region 1/Demo-Area	Object 1	1193046	Main Door	Close	Start	Warning
01.07.11 18:19:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	8000001	U95-2	Level very high	End	Alarm
01.07.11 18:19:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	8000001	Diesel	Level very high	End	Alarm
01.07.11 17:31:00	Demo/Demo Region 1/Demo-Area	Object 1	1193046	Diesel	Abnormal down	End	Warning

A Manager may create and manage object trees with any count of levels and objects according to the administrative or/and geographical structure of his Enterprise. He is also administrating other users and administrators of this enterprise that will be able to monitor data and to receive alerts. All operators (users and managers) are shown as icons on the same tree; these icons are placed above the objects in the tree branch. Icon placement shows the scope of each account. The difference between **Administrator** and **Manager** roles is that the Administrator may have no rights to view data due to confidentiality reasons.

Users are allowed only to view information related to the Enterprise he/she is employed in. It is: real-time data, reports, alerts. Access rights are given by Managers.

In FidTrace monitor tree each operator is displayed as an icon, and he/she has access only to the branches below his/her icon.

Additional account of **DemoUser** was created for FidTrace demonstration purposes. DemoUsers have limited access to some settings; changes in configuration are not saved after they log out.


Administration of FidTrace features is allowed/granted in “Settings mode” (the first bookmark in main frame), ordinary users have no access to this bookmark.

After the Administrator obtains the name & password to enter fidpark.com/monitor and enters for the first time, the tree may have only one operator icon with no other objects at all.

“**Settings**” bookmark can be accessed only by Administrators and allows configuration of all items in the tree. Devices icons are hidden when working in monitor and report mode. Administrators also have access to “Transactions” bookmark where all System events (SystemEventLogs) are listed, like add/edit users, objects, devices etc., also all logins/logouts.

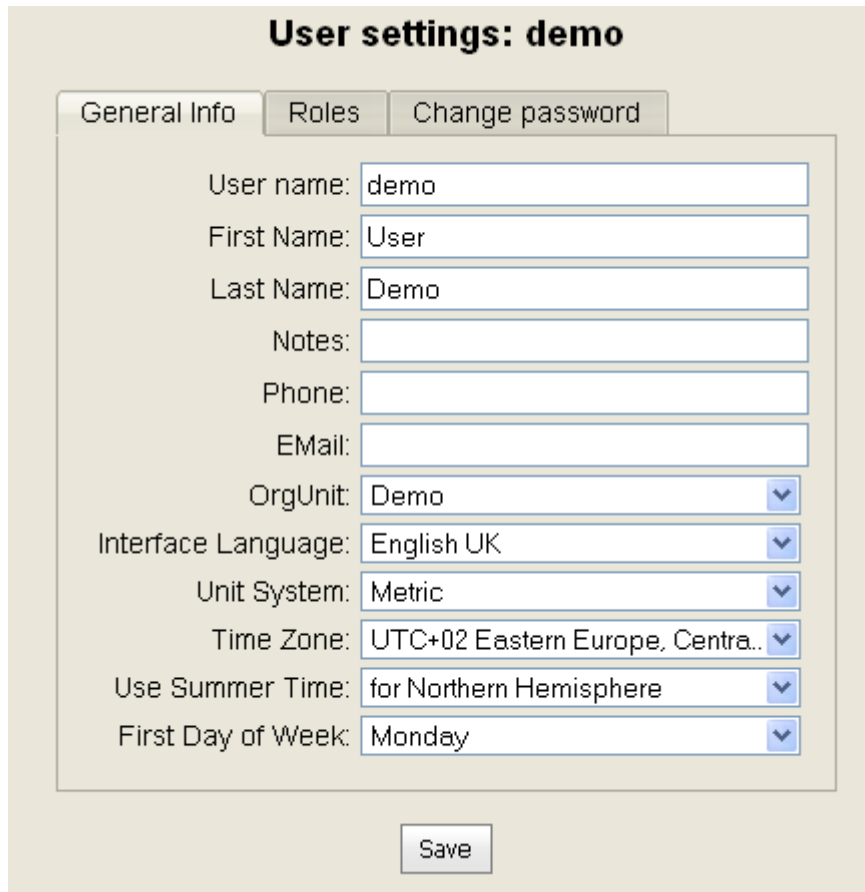
The screenshot displays the FidTrace web interface. At the top, there are navigation tabs: Settings, Map monitoring, Table monitoring, Chart Rep., Statistics Rep., and Transactions. The current time is 17:11:52 UTC+02 DST. Below the tabs is a map of the United Kingdom with a red pin on Ipswich. Below the map is an 'Alerts' section showing a table of system events.

Date/Time	Path	Object	Device	Sensor	Event/Alert
06.05.11 12:52:00	Demo/Demo Region 1/Demo-Area	Object 1	1193046	Diesel	Need refueling
06.05.11 12:32:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	8000001	Main Door	Close
06.05.11 12:28:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	8000001	Main Door	Open
06.05.11 12:24:00	Demo/Demo Region 1/Demo-Area	Object 1	1193046	Main Door	Close

For more comfortable monitoring, Administrators and Users may add, edit and delete one or more **Templates** of selected Objects with the help of set of checkboxes. All Template icons  are placed below the Object tree.

User settings and Authentication

It is necessary to check settings of the system (related to account), this may be done by clicking on the User/Administrator icon and “Settings” bookmark.



User settings: demo

General Info Roles Change password

User name: demo

First Name: User

Last Name: Demo

Notes:

Phone:

E-Mail:

OrgUnit: Demo

Interface Language: English UK

Unit System: Metric

Time Zone: UTC+02 Eastern Europe, Centra..

Use Summer Time: for Northern Hemisphere

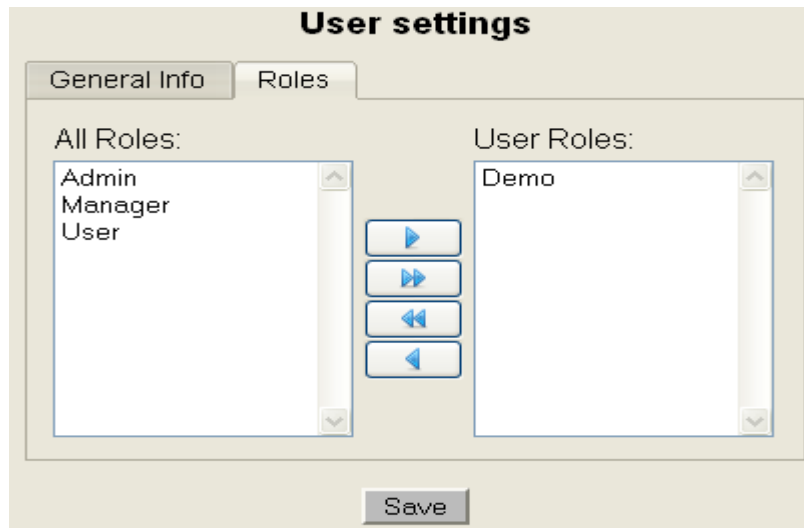
First Day of Week: Monday

Save

You will see a form that should be filled with following data:

- Login/User Name (view only)
- User data (First and Last name, phone, notes)
- e-mail address, will be used to send alerts
- OrgUnit – the highest scope level (tree branch) for this User/Administrator
- Interface language
- Metric/Imperial Unit System
- UTC Time zone (you should see proper time on FidTrace screen),
- Summer Time correction – Yes/No
- First day of the week (usually – Monday or Sunday)

FidTrace has a set of User Permissions for tight control of virtually any operation. The permissions are grouped into Roles, each user is granted one or several roles (User, Manager and Administrator). As an Administrator you should never remove this role, otherwise you may lose control and may need to contact your dealer in order to recover your rights.



After clicking "Save", the settings will be recorded.

You may create other users/administrators:

- via 👤 icon above the tree area,
- via submenu "Add user" displayed by right-click mouse button, pointing at any tree item.

Note 1: Users/their icons may be created on any tree level that will limit the access by sub-tree objects to the right of the icon. In order to grant user access to all objects the icon must be placed in the root.

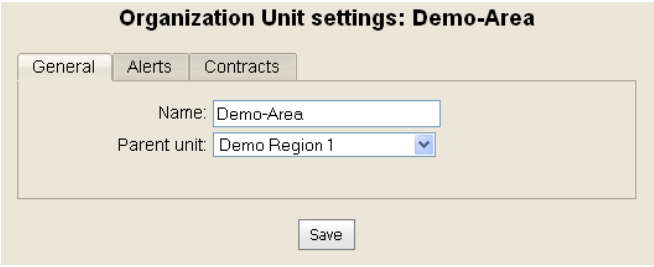
Note 2: The icons for users 👤 and for administrators 👤 are slightly different.

Managing OrgUnits

FidTrace allows creating an object tree structure that may be similar to Enterprise administrative or territorial structure. Anyway, it is up to the Administrator, how to arrange the objects and how many tree levels (orgunits) will be used. For example, tree may be divided by branches, cities, regions etc. Moreover, the tree structure may be updated later, and this will not affect reports.

In order to add a new Object 🚗 or an OrgUnit 🏠, it is necessary to click the right mouse button in Settings mode on its parent OrgUnit and select “Add Unit” command. In case there is no parent OrgUnit, the icon “Add Unit” 🏠 on top of the tree may be used.

You will see the Organization Unit Setting form (General bookmark) in main window with the parent OrgUnit in second line (“empty” for root item). Red stars indicate the fields that need to be entered correctly. The screen with the new object icon will refresh automatically in few seconds after “Save” command for this item. We recommend choosing the names of OrgUnits self-descriptive and not too long, this will simplify interpretation of reports.



The screenshot shows a web form titled "Organization Unit settings: Demo-Area". It has three tabs: "General", "Alerts", and "Contracts". The "General" tab is active. Inside the form, there are two input fields: "Name:" with the value "Demo-Area" and "Parent unit:" with a dropdown menu showing "Demo Region 1". A "Save" button is located at the bottom center of the form.

Two more bookmarks are used to define an OrgUnit -- Alerts and Contracts.

“**Alerts**” bookmark provides list of users that will receive an e-mail when appropriate Object & Hardware Alerts start & end. For the list of Alerts see Appendix.

Organization Unit settings: Demo

General Alerts **Contracts**

Mail sender:

Apply alert settings to all child units:

All users:

Mail recipients:

- **Mail sender** is an e-mail address that will be shown as outgoing/reply address. This address should be included in Safe Senders list by all e-mail recipients. For example, in case of Outlook client this should be done in Tools => Options => Preferences => Junk E-mail).
- Mail recipient names are selected from “All users” defined list for the Enterprise. The form shows just user names, because their e-mails (if exist) are taken from user Settings. It is allowed to add users without access to data – just as recipients of Alert e-mails.
- **Apply alert setting to all child units** – flag to extend these settings to all child Orgunits.

The “**Contracts**” bookmark allows the Enterprise Manager to view, how many and what type of the Devices are configured in the whole Enterprise tree. The Administrator of parent object (e.g. area distributor) sets the quotas (max. amount & types/models of Devices) according to the service Contract with this Enterprise.

Devices are grouped in 3 groups depending on the amount of sensors attached to the each device – Small, Middle, Large.

Organization Unit settings: Demo Region 1

General Alerts **Contracts**





Contract: Max device count:
 Small: Middle: Large:

Type ▲	Cost level	Used	Max count	Reserved	Available
VB5	Middle	1	1	0	0
== Total ==	= Total =	1	1	0	0
== Total ==	Small	0	1	0	0
== Total ==	Middle	1	1	0	0
== Total ==	Large	0	0	0	0

The Administrator may see the quotas (max. amount of Devices, their types/models) for the Enterprise (subtree) in “Max count” column, and the amount of really connected devices – in “Used” column. It is allowed to attach less powerful devices instead of more powerful devices. If the Manager is trying to install more devices or more powerful devices than it is allowed according the Contract, FidTrace will generate an error message. If “Max count” is zero, there is no quota at all for this device.

The “Contract” field may contain the service contract number just for reference purpose, “Max. device count” may be set separately for small, medium and large GuardMagic devices.

To edit OrgUnit settings just select the Object from the tree in Settings mode, change the Object Settings fields and press “Save”. All information related to this OrgUnit will be preserved because the database identifies OrgUnit Index rather than OrgUnit Names. You may move the OrgUnit (with all branches below) to another parent unit, change the name or list of recipients.



Deletion of existing OrgUnits has two stages. After you click the right mouse button and select “Delete Unit” command, this OrgUnit and all OrgUnits and Objects below will be just marked for deletion – the icons will change (from  to  and from  to , their names will be strikethrough. No new data will be accepted from all objects below this OrgUnit, but the existing data and reports will be still available.

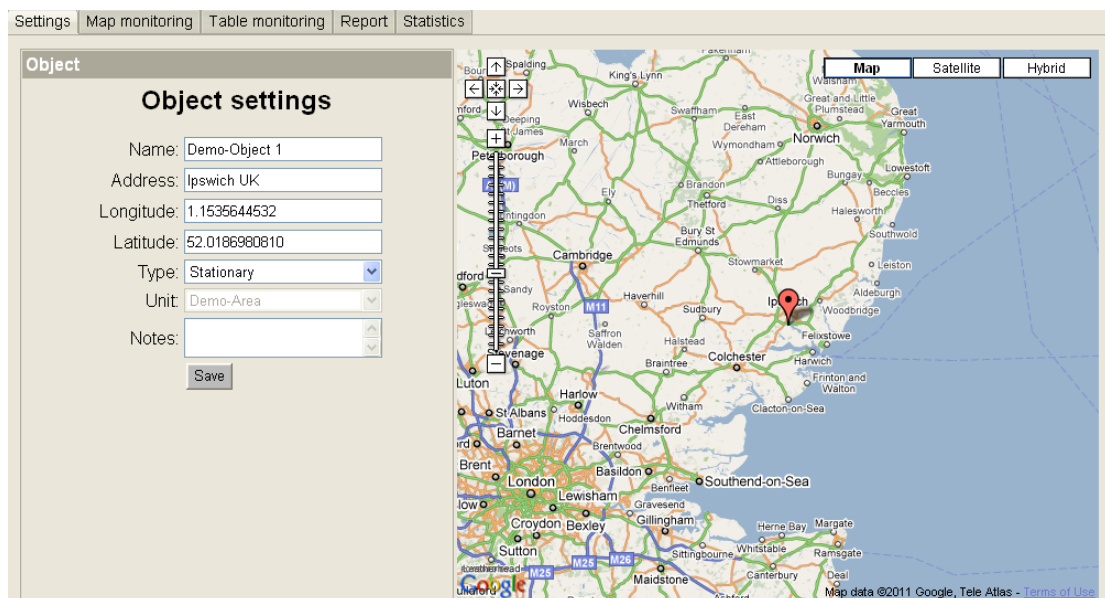
Later you may select “Delete permanently” clicking the right mouse button on the “Deleted” OrgUnit icon. All data records, devices, sensors, users, history related to all Objects below this OrgUnit will be removed from the system, therefore this operation should be done with caution.

You may also perform “Undelete” command on this OrgUnit as well as for each OrgUnit and Object below that were also marked for deletion.

Managing Objects

An Object is basic FidTrace element that is being monitored - e.g. car, fuel tank, diesel-generator, workshop etc. Properties of different objects are defined via settings (name, type etc.) and monitored as data via appropriate sensors attached to each object. The position (geographical coordinates) for stationary objects is also related to settings. The objects normally are incorporated into a geographically distributed administrative structure (legal entity) named Enterprise with or without OrgUnits. Any tree branch in FidTrace should end with an Object / Device / Sensors chain.

In order to add a new Object  it is necessary to click the right mouse button in Settings mode on its parent OrgUnit and select “Add Object” command . In case there is no parent OrgUnit, the icon “Add Object” on top of the tree may be used.



The Object is defined by the following data fields:

- Name, Address, Notes – optional text fields;
- Longitude, Latitude – geographical coordinates of the stationary object to show it's icon on the map with selected objects being monitored. It is possible just to click on the object position in the map shown below object setting fields in order to get this info.
- Type (stationary) – reserved for future use.
- Unit – shows the parent OrgUnit of the object. Changing this field will cause object movement to appropriate OrgUnit branch of the tree.

It is recommended to assign Object names that are short & self-descriptive; this will simplify interpretation of reports.

After the Object was created we may attach one or more Devices with Sensors to this Object.

Editing and deleting Objects is similar to these operations with Orgunits (see above).

Sensors & Events

Sensors (fuel amount, temperature, power, door etc.) are connected to a **Device** that is communicating with data server via GSM channel. All sensors are grouped into four classes according to the measuring specifics:

- continuous (temperature, pressure, liquid level, voltage),
- logical (tamper, switch, state etc),
- UID (employee with ID card), option
- Geo (GPS-position), option

Continuous Sensors produce continuous values (like fuel amount, temperature, speed etc.). **Logical Sensors** have True/False state (ignition on/off, door open/close etc.).

Values of **Virtual Sensors** are converted from “real” continuous sensors via superposition of few sensors e.g. smoothed fuel level, few sensors average, power dissipation. Virtual sensors allow easy defining of additional object features and events to be monitored, faster report generation.

Calibration table of a Continuous Sensor is a table for converting sensor output data to physical value, e.g. fuel level sensor value to % of full tank. Some continuous sensors need such conversion. “Smart” linear sensors (e.g. some temperature sensors) don’t need calibration, but for scaling their calibration table should have two number-value pairs (min & max values) for linear conversion to physical values. Like (0, 20°) and (511, 130°) for temperature sensors. For more detailed information about GuardMagic sensor calibration see Hardware user manual.

Object Events are defined as information, related either directly to logical sensors (tamper, switch, door open, UID access to premises etc.), or when continuous sensor value (rate of change of the value) crosses some predefined thresholds (critical level or temperature, fuel drain etc.). These **events** may be set in Event settings.

Hardware Events are defined as logical events related to the **Device** hardware and communication between the Object and monitoring server – like “Sensor failure”, “Communication problem”, “MainPowerAlarm” etc. FidTrace monitoring uses similar user interfaces for both Object and Hardware events that makes the diagnostics procedures simple and user-friendly.

A couple of **Events** may be associated with each of the continuous sensors – “Low 1”, “Low 2” “High 1”, “High 2” for the value itself or “Down 1”, “Down 2”, “Up1”, “Up2” for the speed/rate of value change. The appropriate nicknames should be selected for each Event depending of the nature of sensor and object, for example - “critically down” for “Down 2”, if the fuel consumption becomes abnormal, “refueling” for “Up 2”, or “Overheat” for “High 2” of temperature sensor. Choosing “Off” option under the “Event Settings” suppresses this event.

The thresholds should not be too small, otherwise wrong events will be generated due to noise, waves, dissipation. The resulting changes of temperature, fuel level etc., are anyway – with or without events, registered in statistical reports as “Change”, i.e. difference between start and end date/time.

Several events related to one continuous sensor may occur simultaneously (overlap) – e.g. “High 1” and “High 2”, or “Down 1” and “Down 2”.

The Events for logical sensors are just nicknames of their states – e.g. “Alarm” for “Door open”, or “In operation” for “Ignition on”.

Full list of predefined Object and Hardware related Events see in Appendix 1.

Event severity – grouping of all events in severity levels, depending on actions to be taken. Notification, Warning and Alarm groups are defined by default. For each Event Manager may set Severity level and a set of actions to be done – send e-mail or SMS, on-screen message etc. All events are recorded in a journal/database.

Note: It is strongly advised to define only the events that are necessary for the reports and for Object control, to set the appropriate thresholds for the selected events, and to choose the appropriate severity level/actions. Generating of extra events is unreasonable as it slows down the monitoring and makes the reports clumsy.

For a fuel station these events may be defined as “Down 1”=“Consumption” (Information), “Down 2”=“Fuel Leak” (Alarm), “Up 1”=“Refueling” (Warning), “Low 1”=“Need refueling” (Warning), “Low 2”=“Critically low Alarm” (Alarm), “Up 2”= “Over fueling” (Alarm) .

The following notification of each sensor is used in FidTrace:

Enterprise/OrgUnit Level-1/OrgUnit Level-2/.../Object/Sensor. In Demo version this will look like, e.g. Demo/Demo Region 1/Demo-Area/Object 1/Diesel.

Managing Devices


Device is a piece (box) of hardware with connected sensors that periodically transmits data to monitoring server via communication channels. Each device


has a unique Factory Number (Manufacturer ID) that is linked to an Object, where device is installed. All Devices are divided into Large, Middle & Small according to the amount of available sensor ports. The object data remain intact if a Device is moved to another object.

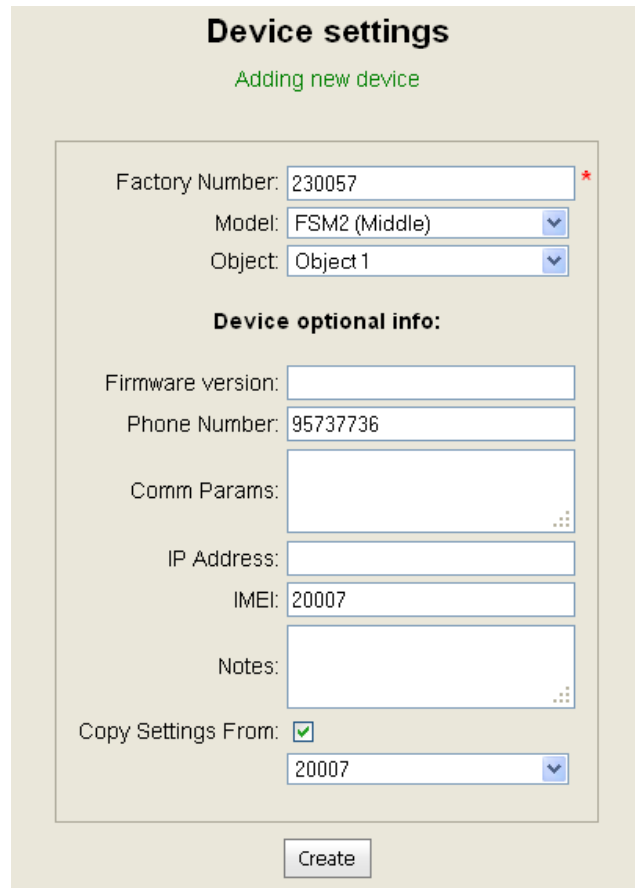


FSM2 Device

According to the FidTrace concept one or more Devices may be associated with the Object (or Sensors on this Object are connected to this Device). If one Device is serving to more than one Object, you may create a “virtual” or “logical” object.

Note: The Device icon  is visible only in the tree in Settings mode, in other bookmarks these icons are hidden and Sensors are shown just as Object features.

Devices are created similarly to OrgUnits and Objects, using right mouse key or the “Add Device” icon . The device initial settings form contains following data fields:



Device settings
Adding new device

Factory Number: *

Model: ▼

Object: ▼

Device optional info:

Firmware version:

Phone Number:

Comm Params:

IP Address:

IMEI:

Notes:

Copy Settings From: ▼

- **Factory number** – unique device ID that is used to mark all data packets from this Device (see Hardware manual)
- IMEI, IP address, Phone number, Firmware version, Communication Parameters – optional info for support information purposes, see Hardware manual
- (GuardMagic) **device model name**, select from list
- Object - the parent Object of this device
- If the flag “Copy settings from” is set, the Administrator may select the Factory Number of one of already configured devices, which will be copied. Copying includes model and all sensors with their calibration tables & event definitions.

Note 1: Only unique decimal device number should be written in the device “Factory Number” field (it can be found on the device circuit board). Any device nicknames or side descriptions may be written in the “Notes” field.

Note 2: The Device icon & its factory number are visible in the tree in “Settings” mode only. Users are observing only Objects and their Sensors.

Clicking on the “Create” button will link new device with the Object in the tree and Device settings form in main frame will slightly change:

Device settings: 230057

Device created

Factory Number:

Model: ▼

Object: ▼

Device optional info:

Firmware version:

Phone Number:

Comm Params:

IP Address:

IMEI:

Notes:


It is possible to delete the Device at this point (more precisely – to mark for deletion) or to change the settings of the Device and associated Sensors.

Note: It is very important to check and modify all Device and Sensor settings (including calibration) after copying a Device.

An existing device may be deleted just like an Object (see above), updated or moved to another Object (for example, in case of replacing faulty Device). This may be done by clicking on the device in settings mode (OrgUnits, Objects, Devices – you can rearrange structure of your organization in this way), then in the “Object” field choosing respective parental OrgUnit or Object and pressing “Update” button.

In order to move an OrgUnit, Object, Device to another branch of the tree one can just change the Parent field in Settings and press “Update” button.

Managing Sensors

A “real” or Virtual Sensor may be added to the Device similarly to the cases with an Object, Device or OrgUnit, using right mouse button or the icon “Add sensor”  .

Sensor settings
Adding new sensor

General Info

Name: *

Device:

Type:

Connector:

Notes:

Create

The initial form is shown above, after successful creation the form gets two more bookmarks – Calibration & Event settings:

Sensor settings: Diesel

General Info Calibration Event Settings

Name:

Device:

Type:

Connector:

Period of running AVG:

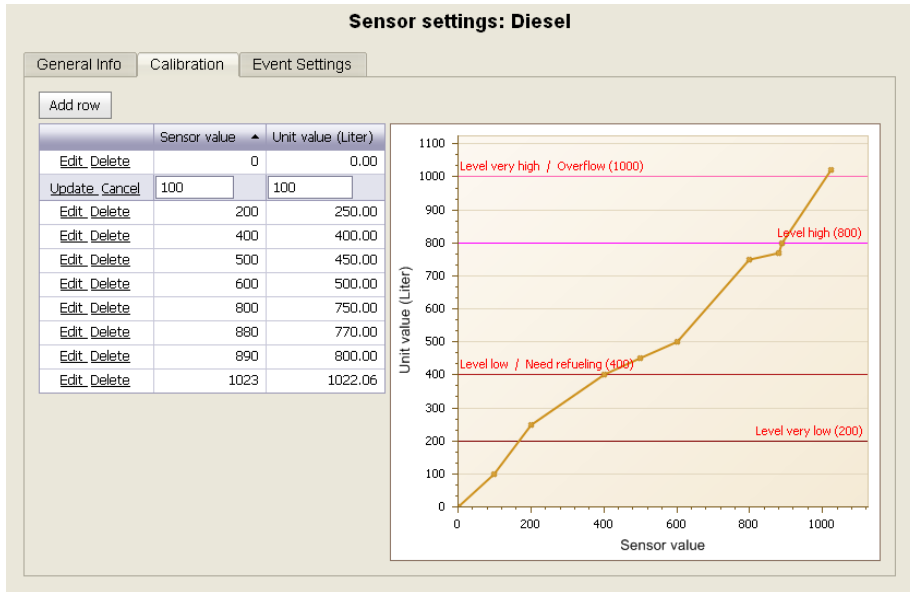
Notes:

Save

The **Sensor** general information is defined by the following data fields:

- Name – will be used to identify this sensor in monitoring, reports and alerts
- Device – parent device
- Type – selection of more specific nature of the sensor that allows using proper measurement units, naming states of logic sensors etc. (see Appendix 2)
- Connector – physical implementation/connection of this sensor to the Device (socket type and number)
- Period of running AVG - number of sequential values (usually 1-5) for running average filtration (1 – no filtration), used to get smoothed data related to fluctuating fuel level, temperature, power etc.
- Notes – any text/comment in free form.

The bookmark “Calibration” is shown only for non-logical sensors and only after the sensor is created and saved.



Sensor calibration table contains pairs “sensor value – real amount”. In any case this table must contain two such pairs for minimal and maximal values (e.g. for empty and full tank). In case of only two pairs, this table allows to recalculate physical data – e.g. temperature sensors with data in range of 0 to 1023 and the temperature from 10° C to 90° C.

The logical sensor named “Internal door” has type = “door”, therefore the states may be named as “open” and “closed” instead of True/False. Detailed description for setting and adjusting sensors is given in appropriate Hardware Manuals.

For more detailed information on sensor calibration see Hardware Manual.

Sensor Events

Sensor settings: Diesel

General Info Calibration Event Settings

Event	Value, Liter	Severity, Action	Event Nickname
Level very high	999.99	Alarm, Alert	Overflow
Level high	800.01	Information, Alert	= Event
Level low	400.00	Warning, Alert	Need refueling
Level very low	199.98	Warning, Alert + e-mail	= Event

Event	Value, Liter/s	Severity, Action	Event Nickname
Up 2	0.08	Alarm, Alert	= Event
Up 1		Off	= Event
Down 1		Off	= Event
Down 2	-0.04	Information, Alert	= Event

Save

Any event is defined by its name, nickname and severity level (e.g. Alarm, Warning and Notification) and is generated, when sensor data or data change rate is crossing the defined threshold/value for an event.

Events are displayed in the Alerts & Events frame, and Fidtrace server may also take some actions according to the “Action” field of Sensor Settings/Event Settings. The alert may be sent as an e-mail or/and SMS to one or more e-mail addresses of users listed in Organization Units/Alerts.

All Hardware alerts are generated in case of a malfunction within the device or sensor itself (so called Internal events/Alarms), have no nicknames, and are sent to the predefined e-mails by default.

Logical & Continuous Sensors

For the **logical** sensors the events may be tied to one or both states, e.g. “Door open” (Alarm) and “Door closed” (Notification). It is not mandatory to link an event to a logical sensor – quite often it is enough to use it in a statistical report related to this logical sensor. For example, we may wish to know how many times per selected period of time (day, week, month) a door (window, gate, etc.) was open, for how long, average, minimal and maximal opening times.

There are two predefined threshold groups for any **continuous** sensor that may or may not be used in any combination:

Static level:

- critically low
- low
- high
- Critically high

Level rate of change:

- Up 2
- Up 1
- Down 1
- Down 2

An Administrator may assign any event nickname and severity to any of these events, e.g.:

- “Overfueling” to Warning for Critically high,
- “Empty Tank” to Alarm for Critically Low,
- “Theft” to Alarm for Down 2.

Example 1. The set of **fuel level** events (100 liter fuel tank) may be defined as:

- 90 liters – Critically high (alarm)
- 80 liters – high (warning)

- 10 liters – low (warning)
- 5 liters – critically low (alarm)

Example 2. The set of **fuel level change** events (-10 liter/sec to 10 liter/sec) may be defined as:

- + 5 liter/sec – Up 2 - refueling (notification)
- - 2 liter/sec – Down 1 - consumption (warning)
- - 10 liter/sec – Down 2 - Leakage (alarm)

Setting Virtual Sensors

Virtual sensors allow defining additional object features and events to be monitored, faster report generation. The values of **Virtual Sensors** are converted from “real” continuous sensors via superposition of few sensors, e.g. smoothed fuel level, few sensors average or power dissipation. The default type of calculated virtual sensors in current FidTrace version is only:

- **Moving average** – Average value of several sensors of the same type, may be used to get data related to large object with several sensors installed e.g. temperature in large premises.

The screen form for adding Virtual sensors allows combining a Virtual sensor from “real” sensors attached to the parent device. In the “Type” field user may select how to process “real” sensors.

Virtual sensor settings
Information updated

General Info | Calibration | Event Settings

Name: Flow Average
 Device: 1193046
 Type: Average many sensors
 Step: 3
 Notes:

All Sensors: Diesel, Diesel Temper., U95, U95 Temp.
 Selected Sensors: RPM & flow 1, RPM & flow 2

Save

After the Virtual sensor is created, you may set Events like for “real” sensors in additional bookmark.

Note 1: The “real” sensors that are source of virtual ones may be still used in reports and alerts.

Note 2: Calibration is not needed for Virtual Sensor settings because the source is already calibrated if necessary.

Adding & Checking Devices & Sensors

There are two stages of connecting a Device to FidTrace server :

- Connecting the Device (see “Managing Devices”)
- Connecting the Sensors (see “Managing Sensors”)

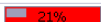

After a Device with one or more Sensors is configured in FidTrace it is possible to look for alerts (like “Device disconnected” or “Sensor not active”) in Alert window, but there is also a simpler way – to use “Table monitoring” of appropriate sensors that of course should be ticked in the tree.

For connecting the device to the FidTrace server via Internet, user must enter the appropriate server IP and Port addresses:

Server IP: 159.148.12.206

Port number: 3999

The font color of sensor data indicates the status of Device – if the Device is currently connected, the color is black and otherwise the color is red.


Date/Time [dd/mm/yy]	Path	Object	Sensor	Value	Units	%
30.09.11 10:43:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	Diesel motor state	off		
30.09.11 10:43:00	Demo/Demo Region 2/Demo-Subregion 2	Object 2	Diesel	1017.00	Liter	 21%
30.09.11 07:31:00	Demo/Demo Region 1/Demo-Area	Object 1	Diesel Temper.	200.70	°C	 69%

The Date/Time column indicates Date & Time of last message arrived from this sensor. In case this field is empty it means that information from this sensor never arrived.



This allows users to do a simple check of communication Sensors - Device as well as Device – Server.

Please note that most fuel sensors don’t work without a calibration table, but for communication checking purposes this table may have just two lines – (0,0) and e.g. (1023, 100). The calibration values may be entered on a later stage using either local GM software or FidTrace monitor.

Management of Report Templates

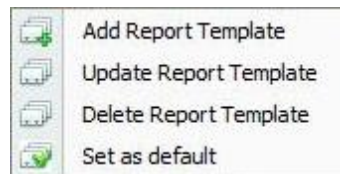
The users may save the frequently used report templates under appropriate names (like Favorites in Windows). These templates will be available as icons  below the Object tree that will carry all current settings - selected sensors/objects, time interval, fields and settings, event category (object/hardware) and date/time interval. A specific name should be assigned to each template that will allow easily identify report in the future.

New report templates may be created in following ways:

- Right clicking in the organization tree and choosing “Add Report Template” (corresponding icon )
- Using  icon on top of the organization tree

New template will carry all report settings that are visible on screen or were used last time. In order to create a slightly different new report template you may just create a report with an existing template, change the report settings and create a new template that will inherit current settings.





Right-clicking on an existing Report Template icon  will open a menu:



As seen in the picture above, menu allows user to add new, delete or update current template. Report template with the “set as default” flag enabled will be used for the first report after user logs in. Next reports will be based on the previously saved templates.

Note 1: For chart reports the templates carry only report header, sensors/objects and time interval.

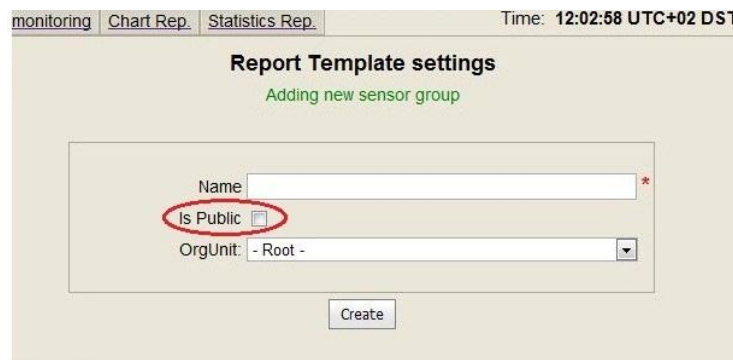
Note 2: If “Previous” or “Last” days/weeks etc. time interval was set, then real interval is calculated according to current day/time.

Note3: Templates without any selected sensors are colored red , public templates are colored blue , and personal templates - gray . And template that is set as default will be shown with ticked icon, i.e. .

When clicking on the template icon all preselected sensors will be shown and used for observation. To edit/change the sensor group it is necessary just to “Save” Report Template settings after modifying the checkboxes.

The user may set his Report Template as public, i.e. accessible by all users in

the branch (OrgUnit) by selecting “Is Public” checkbox. This feature is particularly useful when creating template(s) that will be used by other users as well.



The “OrgUnit” field allows to change the parent and make the public template available to bigger or smaller user group (according their access rights and placement in the tree).


As the template icons are arranged flat rather than in the tree, it is necessary sometimes to see the “owner” of the template (who was the last person updating the template), and what is the parent OrgUnit the template belongs to. This information is shown when the mouse points to the template icon.

The “**Reports**” bookmark has some Options:

- First & Last Events restricted by **Date/Time Interval** or the **Event itself**. For example, if the selected Date/Time interval is inside an event (the event starts before, and ends after the interval), then for the first option Event is restricted by the Interval, for the second one – by the Event itself, so it may be longer than the Interval.
- Report Title – text that may be appended to the default title or may replace it.
- Show/Hide subtotals

Note 1: Administrators and managers have access to all templates (created by users or managers that are beneath them in object tree) that were made Public.

Note 2: Only User who created public template or user from the higher position in the hierarchy tree can delete such public template.

Note 3: If a user has no access to some or all objects/sensors in the public template created by another administrator or user, then the template will not include these items. If the user has no access to all sensors, the template will be shown in red color .

Transactions

The Transactions mode provides Administrators with a journal of all user interactions with FidTrace system and is a powerful tool to locate and solve problems.

Date Time	User name	Table	ID	Name	Type	Notes
19.04.11 14:37:56	User Demo	User	30	demo	User logout	::1
19.04.11 14:37:46	User Demo	User	30	demo	User login	159.148.12.225
19.04.11 14:37:45	User Demo	User	30	demo	User logout	159.148.12.225
19.04.11 14:37:41	User Demo	User	30	demo	Wrong password	159.148.12.225
19.04.11 11:02:01	User Demo	Sensor	29	U95 Ignition	Edit sensor	"U95 Motor"=>"U95 Ignition"
19.04.11 10:25:43	User Demo	User	30	demo	User login	159.148.12.225
18.04.11 18:39:34	Global Admin	User	6	GlobalAdmin	User logout	::1
18.04.11 18:39:24	Global Admin	Object	28	Object 1	Edit object	"Demo-Object 1"=>"Object 1"
18.04.11 16:34:21	User Demo	User	30	demo	User logout	159.148.12.225
18.04.11 16:34:11	User Demo	User	30	demo	User login	::1
18.04.11 16:05:37	Global Admin	User	6	GlobalAdmin	User login	159.148.12.225
18.04.11 11:11:16	User Demo	User	30	demo	User logout	::1
18.04.11 11:11:06	User Demo	User	30	demo	User login	192.168.1.109
18.04.11 11:05:17	User Demo	User	30	demo	User logout	192.168.1.109
18.04.11 11:05:07	User Demo	User	30	demo	User login	127.0.0.1
18.04.11 10:57:12	User Demo	User	30	demo	User logout	127.0.0.1
18.04.11 10:57:02	User Demo	User	30	demo	User login	127.0.0.1
18.04.11 10:57:01	User Demo	User	30	demo	User logout	127.0.0.1
18.04.11 10:56:58	User Demo	User	30	demo	Wrong	127.0.0.1

- Table – one of the following values - Devices, Sensor, Report Templates, Objects, Users
- ID – record number in this table
- Type = transaction
- Notes – detailed information related to this transaction.

The table is divided into pages. One may click to column header and a small triangle on the right of this header will show **sorting** sequence (clicking again will invert sorting sequence). The blank fields below column headers allow filtering data. Advanced filtering with many filtering options may be done, when clicking on key icons of selected columns. The line below the table will indicate full filtering script.

Appendix 1 - Object & Hardware Events

Event name	Default level	Notes
Main object events		
Level very high	Alarm	
Level high	Warning	
Level low	Warning	
Level very low	Alarm	
CriticalUp	Alarm	
AbnormalUp	Warning	
AbnormalDown	Warning	
CriticalDown	Alarm	
Up		
Down		
On	Information	
Off	Information	
Hardware events		
Main power on	Data collect information	
Device disconnected	Data collect information	
Sensor is not calibrated	Data receive alarm	
Parameter ID of virtual sensor not exist	Data receive alarm	
Not enabled or not configured	Data receive alarm	
Error state	Data receive alarm	
Time stamp of device not valid	Data receive alarm	
Device connection timeout error	Data receive alarm	
Hardware diagnostics		
Wrong packet control value	Alarm	For internal use (hidden)
Wrong device protocol type	Alarm	
Wrong device type	Alarm	For intern use error (hidden)
Unrecognized device factory number	Alarm	
Wrong packet length	Alarm	
Accept client failure	Alarm	
Receive_socket_exception	Alarm	
Send socket exception	Alarm	

Unrecognized device number	Alarm	
Wrong type of packet	Alarm	
Wrong type of record	Alarm	
Error in table server options of db	Alarm	
Sensor table dont have required record in db	Alarm	
Wrong or unrecognized device IP	Alarm	
Unrecognized connector	Alarm	
Global Exception	Alarm	
Threshold ID of virtual sensor not exist	Alarm	
Send&Receive information	Information	

Appendix 2 - Data Field list in Statistical reports

The Data Field list has 14 available data types and aggregations:

Group	Short name	Description
Event Day/Time	Dif T (Min)	Minimum value of event durations
	Dif T (Max)	Maximum value of event durations (for example – maximum duration of all “Critically down” events aka fuel thefts)
	Dif T (Avg)	Average of event durations (for example – average duration of refueling or “Abnormal up” events)
	Dif T (Count)	Total count of events (for example – count of “Abnormal up” events aka refueling)
Event-related Sensor Values	Min S (Min)	Minimum value of sensor minimum value for aggregated events (for example – minimum fuel level value for all “Critically low” events)
	Min S (Avg)	Average value of sensor minimum values for aggregated events (for example – average of minimum fuel level values for all “Critically low” events)
	Max S (Max)	Maximum value of sensor maximum value for aggregated events (for example – maximum fuel level value for all “Critically high” events)
	Max S (Avg)	Average value of sensor maximum value for aggregated events (for example – average of maximum fuel level values for all “Critically high” events)
	Dif S (Min)	Minimum value of sensor value difference on End & Start for aggregated events
	Dif S (Max)	Maximum value of sensor value difference
	Dif S (Avg)	Average value of sensor value difference
	Avg S (Avg)	Average value of sensor average value for aggregated events
Change speed	Avg V (Avg)	Average value of rate of change of the sensor value during each of chosen event (for example – average fuel consumption in l/sec during events “Abnormal down”)

- Custom program name & Custom Logo – these two options are set by default in FidTrace. In some special cases this may be changed to Distributor’s Name & Logo.